Android

CovPass-App: Kann man einen Screenshot erlauben?

Lukas Böhl, 16.08.2021 - 07:12 Uhr

Sowohl in der CovPass- als auch in der Corona-Warn-App lassen sich mit Android-Geräten keine Screenshots der Impfzertifikate machen. Warum das so ist und ob man Bildschirmaufnahmen trotzdem erlauben kann, erfahren Sie hier.

Während das iPhone Screenshots in den Apps für den digitalen Impfpass ohne Weiteres zulässt, ist diese Funktion auf Android-Geräten gesperrt. Grundsätzlich ist die Sperre auch sinnvoll, denn so wollen die Entwickler verhindern, dass man die QR-Codes beliebig oft verschickt und Dritte diese als ihre eigenen ausgeben können. Das Fälschen eines Impfdokumentes wird als Urkundenfälschung geahndet und kann hohe Strafe nach sich ziehen, wie wir bereits an anderer Stelle berichtet haben. Man sollte seine QR-Codes daher niemals teilen.

Nichtsdestotrotz kann es praktisch sein, den QR-Code nicht nur in den entsprechenden Apps zu speichern. Denn einige Nutzer haben in den Bewertungen der Appstores von verschwundenen Impfzertifikaten nach einem Update der App selbst oder des Betriebssystems berichtet. Damit so etwas nicht während der Reise passiert, kann es Sinn machen, die QR-Codes zusätzlich als Bild auf dem Smartphone zu hinterlegen. Auf den Geräten von Apple lässt sich dazu ganz einfach ein Screenshot machen. Aber gibt es auch für Android-Geräte einen Weg, um Screenshots in der CovPass-App zu erlauben?

Alternative zum Screenshot

Grundsätzlich gibt es einige Möglichkeiten, um bei Android-Geräten einen Screenshot trotz der voreingestellten Sperre zu machen. Allerdings sind diese für Laien kaum umsetzbar oder nur mit teils fragwürdigen Apps zu bewerkstelligen. Im Normalfall sind sie den Aufwand und das Risiko einer Kompromittierung des Handys nicht wert. Aber es gibt auch eine Alternative zum Screenshot: Fotografieren Sie die gedruckten QR-Codes einfach ab. Da auch diese als Nachweis akzeptiert werden, können Sie diese abfotografieren und auf dem Handy speichern. So kommen Sie um den Screenshot herum. Oder Sie führen einfach eine Kopie der Ausdrucke im Reisegepäck mit sich.

Auch interessant: Unterschied zwischen CovPass- und CovPassCheck

Smartphone App

Karte statt App

Digitaler Impfpass als Scheckkarte

Lukas Böhl, 20.08.2021 - 10:11 Uhr

Der digitale Impfpass ist auch als Scheckkarte zu haben. Aber was taugt diese Lösung und wird sie überall anerkannt? Wir klären auf.

Es gibt mittlerweile einige Anbieter, die den digitalen Impfpass als praktischen Ausdruck im Scheckkartenformat anbieten. Insbesondere das Start-up Immunkarte hat von sich reden gemacht und mit Apotheken in ganz Deutschland ein flächendeckendes Netzwerk aufgebaut, über die der kartenförmige Impfpass bezogen werden kann.

Wird der Impfpass im Scheckkartenformat anerkannt?

Theoretisch sollte es keine Probleme bei der Anerkennung des Impfpasses im Scheckkartenformat geben. Schließlich handelt es sich dabei nur um einen Ausdruck des QR-Codes, der in den Apps dargestellt wird. Außerdem ist es auch erlaubt, die gedruckten QR-Codes aus der Apotheke mit sich zu führen und diese als Impfnachweis vorzuzeigen. Es spielt so gesehen keine Rolle, in welcher Form der QR-Code vorliegt. Allerdings kontrollieren immer noch viele Einrichtungen nur auf Sicht und nicht mit der offiziellen Prüf-App. In einem solchen Fall könnte es eventuell zu Missverständnissen kommen.

Was kostet der Scheckkartenimpfpass?

Anders als der digitale Impfpass werden die Kosten bei den Scheckkarten nicht aus der öffentlichen Hand finanziert. Hierbei handelt es ich um ein privatwirtschaftliches Angebot. Beim Start-up Immunkarte kostet der Impfpass 9,90 € und kann in teilnehmenden Apotheken in ganz Deutschland erworben werden. Ob sich dieser Kostenaufwand für etwas lohnt, das es auch völlig kostenlos gibt, sollte jeder für sich selbst entscheiden.

Auch interessant: Welcher Impfpass gilt im Ausland?

Wie sieht es mit dem Datenschutz aus?

Laut Angaben von Immunkarte werden Vorname, Nachname, Adresse, gegebenenfalls die E-Mail-Adresse und eine verschlüsselte Version des QR-Codes gespeichert. Der digitale Impfpass speichert zwar insgesamt mehr Informationen, die bleiben aber auf dem lokalen Speicher des Smartphones. Darüber hinaus wurden die Corona-Warn-App und die CovPass-App vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüft und für sicher befunden. Rein aus Datenschutzgründen macht der Umstieg auf die Scheckkarte also keinen Sinn. Wer hier wirklich Bedenken wegen der Datensicherheit auf dem Smartphone hat, kann eine Kopie der gedruckten QR-Codes aus den Apotheken und Impfzentren mit sich führen.

Lesen Sie jetzt weiter: Kann man einen Screenshot in der CovPass-App machen?

Coronavirus – ein Erreger fordert uns heraus
Hier geht es zu unserem Themendossier >>

Aktuelle Meldungen, wissenswerte Hintergründe und nützliche Tipps – in unserem Dossier bündeln wir alle Artikel zu Corona.

Corona-Schutzimpfung 15:27 · 19. August 2021

COVID-19-Impfstoffe – eine logistische Herausforderung

Nicht nur die COVID-19-Impfstoffherstellung und –zulassung sind eine

Herausforderung, auch die Logistik ist komplex. Welche Schritte der Impfstoff durchläuft, bis er im Impfzentrum zum Einsatz kommt, erklären wir Ihnen hier.

Die Logistik hinter dem COVID-19-Impfstoff. Bild: Shutterstock / MagioreStock

Eine größere Impfkampagne als die gegen das Coronavirus gab es in Deutschland noch nie: Im Wissen, dass Impfstoffe die wirksamste Möglichkeit sind, die Pandemie einzudämmen und sich vor COVID-19 zu schützen, haben alle an der Impfstoffentwicklung beteiligten Expertinnen und Experten die Zusammenarbeit enger und die Prozesse effizienter gestaltet – ohne dabei Abstriche bei der Sorgfalt zu machen. Dies führte zu deutlichen Optimierungen der Verfahrensabläufe und einem Zeitgewinn bei der Entwicklung.

Neben der Impfstoffentwicklung und –zulassung sind die Herstellung und auch die Logistik, insbesondere die Lagerung und der Transport der Impfstoffe, eine Herausforderung: Es gilt, die zugelassenen Impfstoffe in millionenfacher Menge herzustellen, abzufüllen und zu verpacken, die Verteilung zu organisieren und die

Impfstoffdosen dann auf die Reise bis zum Ort der Verwendung zu schicken. Welche Schritte eine Impfstoffdosis bis zur Verimpfung im Impfzentrum durchläuft, erfahren Sie hier:

1. Die Produktion: Wie und wo werden COVID-19-Impfstoffe hergestellt?

Bislang sind vier COVID-19-Impfstoffe in der EU zugelassen: Die mRNA-basierten Impfstoffe von BioNTech/Pfizer und Moderna sowie die vektorbasierten Impfstoffe von AstraZeneca und Johnson & Johnson.

Die EU-Kommission verhandelt für alle in der EU zugelassenen Impfstoffe zentral mit den Herstellern Lieferverträge für alle Mitgliedstaaten. Von BioNTech/Pfizer wurde der Bundesregierung eine Lieferung von bis zu 120 Millionen Impfdosen für dieses Jahr angekündigt. Mit Moderna ist 2021 die Auslieferung von mindestens 78 Millionen Impfdosen vereinbart. AstraZeneca hat Deutschland eine Lieferung von bis zu 56 Millionen und Johnson & Johnson von rund 37 Millionen Impfdosen angekündigt. Weltweit sind mehrere Milliarden Impfdosen nötig, um das Ziel der Herdenimmunität gegen COVID-19 zu erreichen.

Für diese immensen Mengen bedarf es einer großindustriellen Produktion. Dabei sind alle pharmazeutischen Hersteller bestrebt, ihre Produktionskapazitäten durch Kooperationen bzw. Auftragsherstellung noch auszuweiten.

So produziert das Mainzer Unternehmen BioNTech etwa in Kooperation mit dem Pharmakonzern Pfizer an mehreren Standorten. Seit Anfang Februar 2021 nutzt das Unternehmen zusätzlich eine neue Produktionsstätte in Marburg, um der hohen weltweiten Nachfrage nachkommen zu können. Dort werden im ersten Halbjahr 2021 bereits 250 Millionen Dosen des Impfstoffs hergestellt. Weitere 500 Millionen Impfdosen sind bis zum Jahresende 2021 geplant.

Zudem gibt es Kooperationen mit weiteren Pharmaunternehmen, die einen Teil der BioNTech/Pfizer-Impfstoffproduktion übernehmen. So wird beispielsweise der französische Konzern Sanofi sein Werk in Frankfurt für die Abfüllung des BioNTech-Impfstoffes nutzen.

Die Hersteller der anderen bisher in der EU zugelassenen Impfstoffe binden ebenfalls externe Partner ein: Der US-Produzent Moderna produziert beispielsweise mit dem Schweizer Pharmaunternehmen Lonza in Visp. Das britisch-schwedische Pharmaunternehmen AstraZeneca lässt unter anderem Chargen seines Impfstoffes bei der deutschen Firma IDT Biologika in dessen Werk in Dessau abfüllen, die für die Kapazitätserweiterung einen dreistelligen Millionenbetrag aufwenden wird.

Die Herausforderungen in diesem Schritt:
Da sich die Impfstoffe aus verschiedenen Komponenten und Inhaltsstoffen zusammensetzen, sind die Pharmaunternehmen bei der Herstellung auf Zulieferungen angewiesen. Sie beziehen die Wirk- und Hilfsstoffe von Dienstleistern weltweit. Dafür mussten sie in kürzester Zeit ein Netzwerk mit hoch spezialisierten Zulieferern aufbauen. Durch den rapiden Anstieg des Bedarfs der einzelnen Bestandteile der COVID-19-Impfstoffe könnte es immer wieder zu Lieferengpässen kommen.

Zudem ist die Herstellung ein komplexer Prozess, für den nicht jede beliebige Produktionsstätte geeignet ist und die Errichtung neuer Werke oder der Umbau schon bestehender ist zeitintensiv.

Hinzu kommt: bei den mRNA-Impfstoffen, wie zum Beispiel jenen von BioNTech/Pfizer und Moderna, handelt sich um neuartige Impfstofftypen. Das bedeutet, dass auch die fachliche Expertise der Angestellten in den Werken und die Anforderungen an die Produktionsstätten aufgebaut werden müssen. Auch solche Prozesse benötigen Zeit.

Zudem ist auch die Einhaltung von Qualitätsstandards für jede einzelne Impfstoffcharge erforderlich – alle Produktionsstätten müssen zu jeder Zeit die erforderlichen Kriterien und Maßstäbe einhalten, damit jede Person, die geimpft wird, den gleichen hochwertigen Schutz erhält.

2. Die Verpackung: Was gilt es bei der Verpackung der COVID-19-Impfstoffe zu beachten?

Nach der Produktion werden die Impfstoffe in Durchstechflaschen steril abgefüllt und verpackt – auch das geschieht in Anlagen, die von den Behörden zertifiziert wurden.

Die Herausforderungen in diesem Schritt:
Auch das für die Durchstechflaschen benötigte Glas muss in der erforderlichen Menge bezogen werden. Hier wird spezielles Glas benötigt, das für unterschiedliche Kühltemperaturen geeignet ist und bei dem es zu keiner chemischen Reaktion mit dem Inhalt kommt. Die Pharmaunternehmen nutzen dafür Borosilikatglas (Typ-I Glas), das die hohen Ansprüche erfüllt.

Ist der Impfstoff in die einzelnen Glasfläschchen abgefüllt, werden sie verschlossen und in spezielle Kartons, die die erforderlichen Lagertemperaturen den Anforderungen entsprechend konstant halten können, verpackt. Diese werden dann für den Transport auf Paletten bereitgestellt.

3. Die Auslieferung: Wohin gehen die fertigen COVID-19-Impfstoffe?

Nach der Herstellung des Impfstoffs, die Abfüllung und Verpackung der Impfstoffe einschließt, werden diese an zentrale Stellen in den EU-Mitgliedstaaten geliefert.

In Deutschland werden die Impfstoffdosen von der zentralen Stelle dann weiter an die Bundesländer transportiert. Die verfügbaren Mengen an Impfstoffdosen werden dabei gemäß dem Bevölkerungsanteil an die Bundesländer verteilt. Diese haben dafür spezielle Anlieferungsstellen eingerichtet. Ausgenommen ist dabei der Impfstoff von BioNTech/Pfizer, den das Unternehmen direkt an die von den Bundesländern benannten Stellen liefert. Die Bundesländer sind bezüglich der Impfungen in den Impfzentren zuständig für die sachgerechte und sichere Lagerung und Verteilung von COVID-19 Impfstoffen vor Ort sowie die Beschaffung von Impfzubehör, beispielsweise Spritzen und Kanülen.

Von den benannten Stellen der Bundesländer aus werden die Impfstoffe dann an die Impfzentren geliefert.

Bezüglich der Impfungen in den Arztpraxen und durch Betriebsärztinnen und Betriebsärzte
besteht ein anderer Lieferweg. An diese impfenden Stellen werden die Impfstoffdosen einschließlich Zubehör von der zentralen Stelle an den pharmazeutischen Großhandel und von dort über die Apotheken geliefert.

Die Herausforderungen in diesem Schritt:
Aufgrund der Produkteigenschaften und Anforderungen an Lagerung und Transport der verschiedenen Impfstoffe sind gegebenenfalls unterschiedliche Logistikkonzepte erforderlich.

So müssen die Impfstoffe bei unterschiedlichen Kühltemperaturen gelagert und transportiert werden. Comirnaty® von BioNTech/Pfizer ist bei -90 Grad Celsius bis -60 Grad Celsius sechs Monate haltbar. Spikevax® (COVID-19 Vaccine Moderna) ist sieben Monate bei -25 Grad Celsius bis -15 Grad Celsius haltbar.

Nach dem Auftauen muss es schnell gehen: Der ungeöffnete Impfstoff von BioNTech/Pfizer ist nach dem Herausnehmen aus dem Gefrierschrank vor der Verwendung 1 Monat bei 2 Grad Celsius bis 8 Grad Celsius und bis zu zwei Stunden bei Temperaturen bis 30 Grad Celsius haltbar. Der ungeöffnete Impfstoff von Moderna kann 30 Tage bei 2 Grad Celsius bis 8 Grad Celsius gelagert werden.

Der Impfstoff von AstraZeneca ist logistisch etwas leichter handhabbar: Da er nicht tiefgefroren werden darf, kann er bei 2 Grad Celsius bis 8 Grad Celsius sechs Monate lang gelagert und direkt verimpft werden.

Auch der Vektor-Impfstoff von Johnson & Johnson ist einfacher in der Handhabung: Der ungeöffnete Impfstoff ist bis zu drei Monate bei 2 bis 8 Grad Celsius, also der Temperatur eines Kühlschrankes, haltbar. Bei -25 Grad Celsius bis -15 Grad Celsius ist der Impfstoff bis zu zwei Jahren haltbar.

Diese Kühlkette muss auch beim Transport der Durchstechflaschen zu den Impfzentren oder den Apotheken, die die Betriebe und Arztpraxen beliefern, weiterhin sichergestellt sein. Um die Temperatur zu jedem Zeitpunkt kontrollieren

> zu können, installieren die Hersteller oder Logistikdienstleister an den Verpackungen Sensoren, die die Temperatur kontinuierlich messen. Die pharmazeutischen Unternehmen untersuchen auch nach Zulassung die Stabilität ihrer Impfstoffe weiter und prüfen ebenfalls, ob gegebenenfalls einfachere Transport-und Lagerungsbedingungen ermöglicht werden können.

4. Die Corona-Schutzimpfung: Wo wird geimpft?

Von den Anlieferstellen der Länder werden die Impfstoffe in die Impfzentren gebracht. Es gibt darüber hinaus mobile Impfteams, die beispielsweise stationäre Pflegeeinrichtungen aufsuchen. Mehr zur Impfung im Impfzentrum haben wir in diesem Artikel zusammengefasst.

Die Belieferung der Arztpraxen und Betriebsärztinnen und Betriebsärzte erfolgt hingegen über den pharmazeutischen Großhandel und die Apotheken. Informationen zur Corona-Schutzimpfung in Betrieben finden Sie hier. Wie die Impfung gegen COVID-19 in Arztpraxen abläuft, lesen Sie hier.

Karte Liste

Fragen und Antworten zum digitalen Impfnachweis

Was ist der digitale Impfnachweis?

Der digitale Impfnachweis ist eine zusätzliche Möglichkeit, um Corona-Impfungen zu dokumentieren. Geimpfte können damit Informationen wie Impfzeitpunkt und Impfstoff bequem auf ihren Smartphones – entweder in der CovPass-App oder in der Corona-Warn-App – digital verwalten.

Wo finden Bürgerinnen und Bürger Informationen zur CovPass-App und dem

Impfzertifikat?

Informationen zum digitalen Impfnachweis und zu den Apps hat das RKI (Robert Koch-Institut) hier zusammengestellt: https://digitaler-impfnachweis-app.de/ (https://digitaler-impfnachweis-app.de/).

Fragen und Antworten findet man hier: https://digitaler-impfnachweis-app.de/faq/ (https://digitaler-impfnachweis-app.de/faq/).

Warum machen wir das?

Zu Beginn des Jahres wurde durch den Europäischen Rat beschlossen, einen interoperablen und standardisierten Impfnachweis auf den Weg zu bringen. Das digitale COVID (Coronavirus Disease)-Zertifikat der EU (Europäische Union) soll den freien Personenverkehr innerhalb der EU (Europäische Union) erleichtern. Mit dem CovPass hat Deutschland diese europäische Entscheidung umgesetzt. Das digitale COVID (Coronavirus Disease)-Zertifikat der EU (Europäische Union) (typo3/#_msocom_1)bildet den Rechtsrahmen für die Lösungen der Mitgliedsstaaten.

Wie funktioniert der digitale Impfnachweis?

Der digitale Impfnachweis wird in der Arztpraxis, in einem Impfzentrum oder in einer Apotheke generiert. Nach Eingabe oder Übernahme der Daten wird ein 2D-Barcode (QR-Code) erstellt, den die Nutzer auf einem Papierausdruck mitbekommen und später mit der CovPass-App oder der Corona-Warn-App einscannen und nutzen können. Die App speichert die Impfbescheinigung nur lokal auf dem Smartphone.

Wo bekommt man den digitalen Impfnachweis?

Bürgerinnen und Bürger können in den bekannten Appstores die CovPass-App herunterladen, um die Impfzertifikate (QR-Codes) einzuscannen. Ihr Impfzertifikat erhalten Bürgerinnen und Bürger nach ihrer Impfung beim Arzt oder im Impfzentrum. Alternativ kann man sich das digitale Zertifikat auch nachträglich in der Apotheke ausstellen lassen. Die App zeigt den vollständigen Impfschutz 14 Tage nach der letzten benötigten Impfung an. Wer möchte, kann den digitalen Impfnachweis auch in der Corona-Warn-App nutzen, die ebenfalls die Möglichkeit des Einscannens und Verwaltens der digitalen Impfzertifikate (QR-Codes) bietet. Bürgerinnen und Bürger sollten die ausgehändigten QR-Codes aufbewahren, um sie bei Bedarf erneut einscannen zu können (z.B. (zum Beispiel) bei einem Handywechsel).

Müssen sich Personen, die das Zertifikat "Impfung 2 von 2" digital erhalten haben,

das erste Zertifikat nachträglich besorgen?

Personen, die bereits vollständig geimpft sind, benötigen lediglich das Zertifikat „Impfung 2 von 2“ um ihren Impfschutz nachweisen zu können.

Ab wann steht der digitale Impfnachweis zur Verfügung?

Die Impfzertifikate werden als QR-Code von nun an schrittweise von den Impfzentren, Ärzten und Apotheken ausgestellt.

Wie wird der Nachweis einer Impfung geprüft?

Das Impfzertifikat (QR-Code) wird z.B. (zum Beispiel) über die CovPass-App oder die Corona-Warn-App (CWA) digital oder alternativ durch den beim Impfen erhaltenen Ausdruck des QR-Codes genutzt. Für Dienstleister, die den Impfstatus überprüfen möchten, gibt es eine Prüf-App ("CovPassCheck-App"). Damit kann der Impfstatus ähnlich wie ein Barcode eines Flug- oder Bahntickets gescannt werden. Bei einer Überprüfung von dem QR-Code werden in der CovPassCheck-App nur der Status des Zertifikats, Vorname(n), Nachname und das Geburtsdatum angezeigt. Alternativ bleibt auch ein Nachweis mit dem analogen Impfpass möglich.

Wie soll ein Missbrauch verhindert werden?

Der digitale Impfnachweis darf nur von autorisierten Personen in Impfzentren, Arztpraxen, Apotheken und Krankenhäusern ausgestellt werden. Bei der Überprüfung von digitalen Impfnachweisen ist ergänzend ein Lichtbildausweis vorzulegen. Der digitale Impfnachweis ist kryptographisch vor Veränderungen geschützt.

Was ist mit Personen, die bereits geimpft sind. Bekommen die auch einen digitalen Impfnachweis?

Ja. Für bereits vollständig Geimpfte, die sich in einem Impfzentrum haben impfen lassen, werden die QR-Codes in der überwiegenden Zahl der Bundesländer per Post nachversandt oder durch Online-Portale zur Verfügung gestellt. Ergänzend können auch Apothekerinnen und Apotheker sowie Ärztinnen und Ärzte nachträglich Impfnachweise ausstellen.

Wie wird dabei sichergestellt, dass die Informationen aus dem gelben Impfheft echt und nicht gefälscht sind?

Bei der Prüfung der analogen Impfpässe ist besondere Aufmerksamkeit geboten. Das gilt sowohl

dann, wenn der analoge Impfpass genutzt wird, um z. B. (zum Beispiel) Geschäfte zu betreten. Und es gilt auch dann, wenn die Informationen von dem analogen in einen digitalen Impfpass übertragen werden. Die Fälschung von Impfpässen ist strafbewehrt. Das gilt für analoge wie für digitale Impfdokumente.

Bekommen Ärzte und Apotheker eine Vergütung für die Ausstellung der Impfnachweise?

Ja, Ärztinnen und Ärzte sowie Apothekerinnen und Apotheker erhalten eine Vergütung, die in der Corona-Impfverordnung geregelt ist.

Kann man auch im digitalen Impfnachweis speichern, dass man bereits infiziert war oder negativ getestet wurde?

Auch negative Tests oder eine durchgemachte Corona-Infektion können sich in der CovPass-App und auch CWA als Testzertifikat bzw (beziehungsweise). Genesenenzertifikat hinterlegen lassen.

Anspruch auf ein Genesenenzertifikat haben alle Personen, die eine Infektion mit dem Coronavirus SARS-CoV-2 (Severe Acute Respiratory Syndrome Coronavirus 2) durchgemacht haben. Voraussetzung ist der Nachweis eines positiven PCR (polymerase chain reaction)-Test-Ergebnisses. Der PCR (polymerase chain reaction)-Test darf maximal sechs Monate alt sein und muss mindestens 28 Tage zurückliegen. Liegt der Test nicht mehr vor, kann man sich die Nachweise neu ausstellen lassen. Das Genesenenzertifikat kann durch die Person, die einen Test durchführen oder überwachen darf, ausgestellt werden.

Wie kommen genesene Personen an ein Zertifikat für die App, wenn die Covid-Erkrankung länger als ein halbes Jahr zurückliegt?

Der in der Verordnung genannte Zeitraum von maximal 180 Tagen und mindestens 28 Tagen bezieht sich nur auf die Ausstellung eines Genesenennachweises. Das heißt, eine Person, die die Erkrankung durchgemacht hat, kann nur innerhalb dieses Zeitraums einen solchen Nachweis ausgestellt bekommen. Nach Ablauf dieser Frist und bevor eine Impfung stattgefunden hat, gilt die Person als nicht vollständig geimpft und eben auch nicht als genesen.

Davon unabhängig gilt eine Person als vollständig geimpft, wenn sie entweder zwei Impfungen erhalten hat oder genesen ist und eine Impfung erhalten hat. Der Nachweis der Genesung wird mit einem positiven PCR (polymerase chain reaction)-Test belegt.

Es kann also auch jemand nur einmal geimpft werden und als vollständig geimpft gelten, der die Krankheit durchgemacht hat ohne einen Genesenennachweis erhalten zu haben, z.B. (zum

Beispiel) weil die Erkrankung länger als 180 Tage zurücklag.

Wo können Genesene ein Impfzertifikat erhalten?

Sowohl Genesenenzertifikate als auch Genesenenimpfzertifikate können zurzeit in Arztpraxen bereits ausgestellt werden, die das Webportal von IBM nutzen. Bei der Integration in das IT (Informationstechnologie)-System der Arztpraxis oder des Impfzentrums hängt die Umsetzung von den Zeitplänen des individuellen Anbieters ab. Für die Genesenenzertifikate haben dies auch bereits einige IT (Informationstechnologie)-System Hersteller für die Arztpraxen technisch umgesetzt und zur Verfügung gestellt.

Genesenenimpfzertifikate sind zudem in der Apotheke erhältlich. Genesenenimpfzertifikate bescheinigen eine Impfung. Genesene erhalten dabei abweichend nur eine Impfdosis. Dieses Impfschema (1 von 1 Impfungen) wird im Zertifikat vermerkt.

Wo werden Daten beim digitalen Impfnachweis gespeichert?

Alle digitalen Impfnachweise werden nur temporär im Impfprotokollierungssystem erstellt und anschließend gelöscht. Dauerhaft gespeichert werden sie nur dezentral auf den Smartphones der Nutzer.

Ist ein zentrales Impfregister geplant?

Nein, jeder kann selbst entscheiden, ob und wann er diese Daten löscht.

Wie werden die digitalen Impfnachweise von Kindern gespeichert?

Bei Bedarf können auch die Nachweise von Angehörigen verwaltet werden.

Wer hat den digitalen Impfnachweis entwickelt?

Der digitale Impfnachweis ist ein Projekt im Auftrag des Bundesministeriums für Gesundheit. Die Anwendung wurde von den Unternehmen UBIRCH, IBM Deutschland, govdigital und Bechtle entwickelt. Das Robert Koch-Institut ist als Herausgeber verantwortlich für die Ausgestaltung der Anwendung sowie für die sorgfältige Prüfung der Anforderungen an Datenschutz und Datensicherheit.

Warum wurde kein EU (Europäische Union)-weites Projekt für ein Zertifikat ausgeschrieben?

Eine gemeinsame EU (Europäische Union)-Ausschreibung hätte zu viel Zeit benötigt und wäre

aufgrund der unterschiedlichen Impfinformationssysteme in den Mitgliedstaaten auch schwierig umzusetzen gewesen. Beim EU (Europäische Union)-Ansatz geht es um die Regelung eines Anerkennungsrahmens. Bei der Umsetzung des Digitalen Impfnachweises in Deutschland wurden und werden die EU (Europäische Union)-Vorgaben von vornherein berücksichtigt.

Kann man mit dem digitalen Impfnachweis innerhalb Europas problemlos reisen?

Mit dem CovPass setzt Deutschland das europäische Zertifikat in Deutschland um. Deutschland ist auch bereits an den sogenannten europäischen Gateway-Server angeschlossen. Damit können die Zertifikate EU (Europäische Union)-weit sowie in Island, Liechtenstein, Norwegen und der Schweiz genutzt werden.

Kann man mit dem digitalen Impfnachweis international problemlos reisen?

Zur Anerkennung von Impfungen auf internationaler Ebene (außerhalb der EU (Europäische Union)) laufen derzeit noch die Gespräche.

Ist der gelbe analoge Impfausweis jetzt noch gültig?

Ja. Der digitale Impfnachweis ist lediglich ein freiwilliges und ergänzendes Angebot. Wenn Geimpfte keinen digitalen Impfnachweis besitzen oder diesen verloren haben, ist der Impfnachweis über das bekannte „gelbe Heft“ weiterhin möglich und gültig.

5. August 2021

EDUCATION

What is Proof of Authority Consensus? Staking Your Identity on The Blockchain

BY BRIAN CURRAN - JULY 5, 2018

As the cryptocurrency space continues to evolve at an accelerated pace, experimentation and implementation of a variety of consensus models is inevitable.

Proof of Authority (PoA) consensus is not necessarily a new consensus mechanism (has been around since March 2017), but has been implemented in some interesting platforms as a compromise between consensus models targeting complete decentralization and more efficient, centralized models.

How Does Proof of Authority Consensus Work?

Contents [Show]

First, PoA was proposed by a group of developers in March 2017 (the term was coined by Gavin Wood) as a blockchain based on the Ethereum protocol. It was developed primarily as a solution to the problem of spam attacks on Ethereum's Ropsten test network. The new network was named Kovan and is a primary test network available to all Ethereum users today.

PoA consensus is essentially an optimized Proof of Stake model that leverages identity as the form of stake rather than actually staking tokens. The identity is staked by a group of *validators* (authorities) that are pre-approved to validate transactions and blocks within the respective network. The group of validators is usually supposed to remain fairly small (~25 or less) in order to ensure efficiency and manageable security of the network.

Read about Proof of Stake

The main characteristics of a PoA network are a low requirement of computational power, no requirement of communication between nodes to reach consensus, and continuity of the network is independent of the number of the available genuine nodes since they are pre-approved and verifiably trustable through cross verification in the public domain.

PoA is designed to be less computationally intensive than PoW models that require expending electricity to solve algorithms. Further, PoA removes a primary concern within the PoS model that although stakes between two parties may be equal, their value to each party may vary significantly depending upon their holdings. For instance, Alice may have 1,000 XYZ tokens staked and Bob may also have 1,000 XYZ tokens staked, however, Alice has $10 million outside of her stake and Bob only has $10,000 outside of his. Therefore, Bob is much more likely to invested in the success of the XYZ network than Alice since his stake represents a substantially larger portion of his overall finances.

There are 3 basic requirements to become a validator which have important implications on the incentive structure driving their actions towards honest behavior.

1. Their identities need to be formally identified on-chain with the ability to cross-reference these identities through reliable data available in the public domain (such as a public notary database).
2. Eligibility to becoming a validator must be difficult to obtain in order to ensure the long-term prospective position of the validator is one of clear incentive, both financially and reputationally, to remain an honest validator.
3. There must be complete uniformity in the process for establishing validators.

as part of the network in the long-term and reputation as the disincentive to act dishonestly. Any validator who acts maliciously can easily be removed from the validation process and replaced. The end result for that validator would be a public hit to their reputation as well as a loss of future financial earnings. The use of reputation through identity is of especially particular relevance to contemporary times. As Warren Buffet put it:

> **"It takes 20 years to build a reputation and 5 minutes to ruin it. If you think about that, you'll do things differently."**

In the current climate of social media in the age of the Internet, we have seen repeatedly how easy it is for people to completely lose their reputation through public condemnation based on something as miniscule as a poorly thought out comment or remark (whether deserved or not). The increasing awareness of the fragility of reputation in the public domain should serve as a potent incentive for validators to act honestly within the system.

Read about Nakamoto Consensus

Concurrently, the use case of PoA is largely seen as most effective for permissioned (private) blockchains. For instance, a network of verifiable banks that each acts as their own validator. A majority is needed to confirm the state of the blockchain and they retain improved efficiency in transaction verification and consensus without having to discard a substantial amount of influence, privacy, or power in the process.

Current Implementations of PoA Consensus

As mentioned earlier, PoA consensus is used in Ethereum's Kovan testnet. It is also used by a number of fairly well-known platforms and as of this point, seems to be the most plausible consensus mechanism for institutions looking to implement private blockchain networks.

Proof of Authority Network (POA Network) is quite obviously a platform founded on the principle of implementing PoA consensus in their blockchain. POA Network is a public platform for smart contracts that exists as an Ethereum sidechain with their nodes consisting of independent validators. They use the public notary database as the mechanism for validator eligibility as it is readily available in the public domain for anyone to verify and can be easily cross-referenced with their on-chain verification. Essentially, validators go through formal identity verification by using 2 steps. A client side POA Network Dapp as well as through the public notary system.

In case you are unfamiliar with the notary system, it is difficult to obtain a notary license and requires an extensive, formal background check by the government. This process satisfies the primary requirements seen above for becoming a validator.

ing process which creates an impossible hurdle for the forging of identities in one process or the other since verifications are required. With substantial recent buzz surrounding the potential of side chains, POA Network represents an interesting implementation of PoA consensus in a public network.

Another implementation of PoA consensus in a different space is with the VeChainThor blockchain network. Their network focuses on being an enterprise-grade public blockchain for the transparent flow of information and tracking, primarily in the supply chain and logistics realm. VeChain selects the validator nodes through their own proprietary verification process and elucidates the significant advantages afforded to them by using PoA consensus in their network as being the efficiency with which it confirms transactions and the state of the blockchain.

Read our Guide to Vechain

If Vechain relied on PoS or PoW for their consensus model, scalability solutions that are still being overcome by cryptocurrencies like Bitcoin and PoS platforms would need to be researched, optimized, and implemented properly, which would cause substantial delay in the launch of their platform. Allowing companies that are already participating in the supply chain industry to become validators within their network also aligns their self-interests into a collective that helps create network security often seen as easier to achieve in private and permissioned blockchain networks.

Some other implementations of optimized versions of PoA consensus include Hyperledger and Ripple. Hyperledger Fabric's consensus is predicated on Practical Byzantine Fault Tolerance but employs PoA consensus as part of its open-source umbrella framework for consortium blockchains. Ripple uses an iterative form of PoA consensus and more in-depth information on their consensus process can be found here.

Advantages and Concerns With PoA Consensus

While PoA consensus is being implemented in some public blockchains, they still lack the true decentralization that Bitcoin and Ethereum, among others aspire to be. Not that PoA consensus platforms actually claim to be fully decentralized, but rather a compromise between decentralization and the efficiency afforded by centralization.

On one hand, some concerns with the PoA model are that it is more or less just a slightly more distributed, yet still efficient version of a centralized system. With a heavy emphasis in the cryptocurrency community on the idealistic nature of decentralized systems, private blockchains, or even some public blockchains, claiming to provide a better model for data integrity are seen with a healthy dose of skepticism. Further, imagine a PoA consensus network of banks that exists as a private blockchain network. Censorship and blacklisting of transactions or certain vendors using their

(banks), therefore the idea of utilizing blockchain as an immutable form of a ledger really becomes obsolete at this point.

Another concern stems from an issue that may seem a bit bizarre but actually has happened before and under the right circumstances, can definitely happen again. It is the fact that some people simply do not care about their reputation. Or similarly, the payoff of ruining their reputation in the form of the result they achieve, whether that result is a direct derivative of their actions within the network or a financial incentive garnered from a third party to act dishonestly, is simply more than the cost. This is the inherent problem with a model of validators that is limited in number, they are subjected to outside influence from third parties, especially if those third parties have a significant interest in seeing the network fail.

The advantages of a PoA consensus network are fairly obvious. Increased efficiency in transaction times and overall network consensus. These models using PoA consensus are also much more effective with decentralized applications and are easily scalable compared to decentralized networks. Further, innovations in relevant technology may help to further secure such networks where validators are independent of one another and susceptible to third party intervention. For instance, Intel's SGX secure enclave computing technology has been floated as a method of helping to secure the validator software running on their node from outside interference.

Conclusion

From a consensus model designed to overcome some of the inherent problems with the Ropsten test network to a formal validation method of public blockchains focusing on smart contracts, sidechains, and the immense industry of global supply chain tracking, Proof of Authority consensus is an important development in the further advancement of testing and implementing different consensus mechanisms.

missioned blockchains, or as a crucial sidechain to a public and decentralized network, is yet to be seen.

Important Note: There have been reports of scammers approaching companies via Telegram, LinkedIn and Other Social platforms purporting to represent Blockonomi and offer advertising offers. We will never approach anyone directly. Please always make contact with us via our contact page here.

Brian Curran

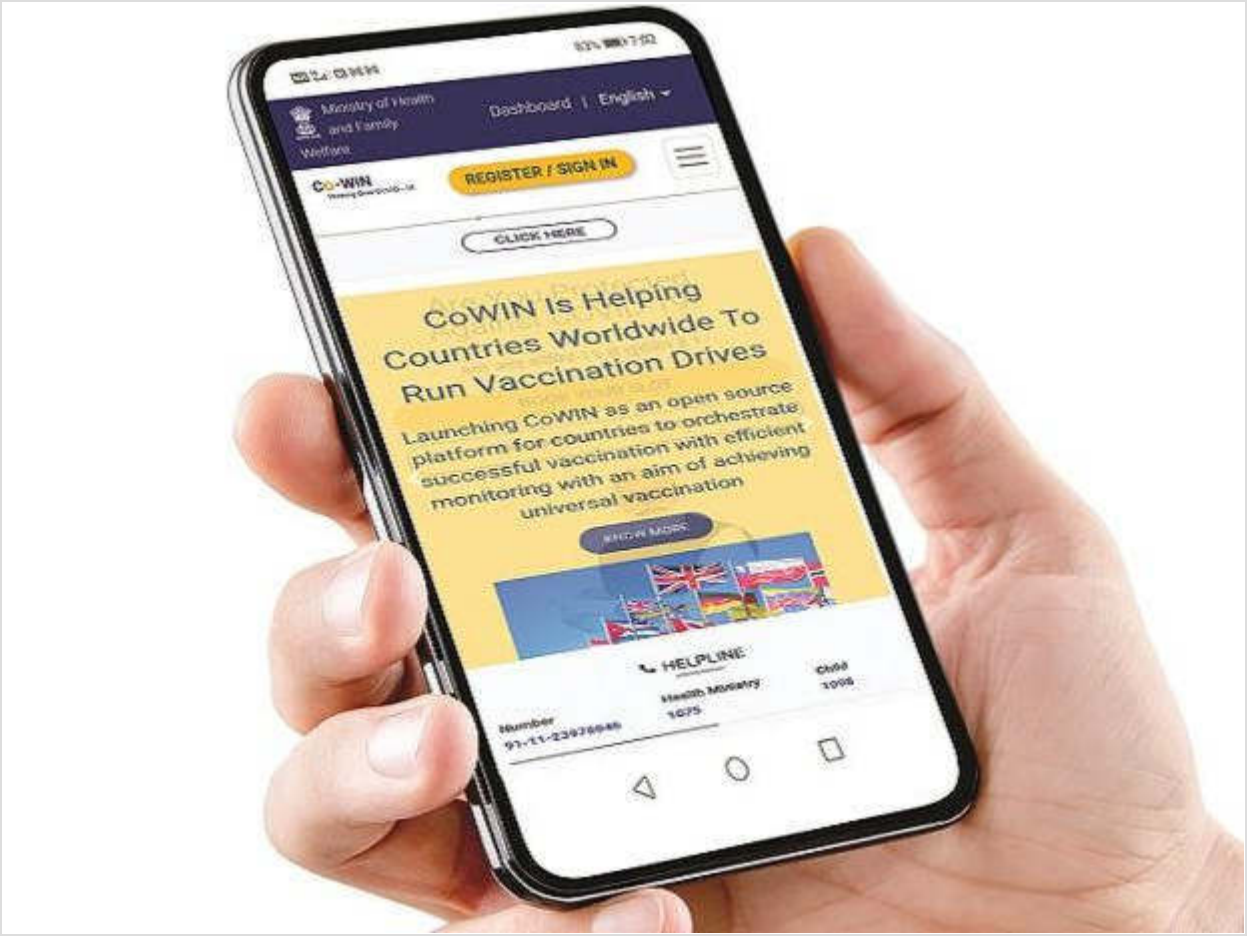
Get Inspired By The Best Altcoin of 2021 - Student Coin (STC)

Business Standard

CoWIN goes global: India makes tech open source, 142 nations show interest

This is perhaps the first time any nation is making a software platform developed by its public sector initiative open for the world

Sohini Das | Mumbai July 05, 2021 Last Updated at 18:34 IST



India is making its digital platform for Covid19

India has administered over 350 million doses of vaccine through this platform so far

vaccination drive, CoWIN, open source for all countries to access, adapt and use. This is perhaps the first time that any country is making a software platform developed by its public sector open for the world.

Speaking at the CoWin Global Conclave on Monday, Prime Minister Narendra Modi said, “Soon, CoWIN will be available to any and all countries.” The software can be customised to any country according to local requirements.

India has administered over 350 million doses of vaccine through this platform so far.

Highlighting the importance of technology in fight against the pandemic, Modi said India had made its Covid tracking and tracing app Aarogya Setu open source as soon as it was technically feasible. He pointed out that with nearly 200 million users, the Aarogya Setu app was a readily available package for developers, and had been tested in the real world for speed scale. “This pandemic has made many people realize the fundamental truth of this philosophy…. That's why CoWin is being prepared to be made open source.”

The conclave was attended by representatives of 142 countries including Afghanistan, Bangladesh, Bhutan, Maldives, Guyana, Antigua & Barbuda, St. Kitts & Nevis and Zambia amongst others. These countries are keen to adopt CoWin for digitizing their Covid19 vaccination drive.

ALSO READ: **Covid LIVE: Domestic carriers allowed to operate at 65% passenger capacity**

Union Health Minister Harsh Vardhan said, “In my humble opinion, Co-WIN is the crown jewel of our Digital India initiative. This platform shall go down in history for facilitating inoculation of a large percentage of the world’s population with ease, while simultaneously ensuring complete transparency.”

According to National Health Authority CEO R S Sharma, CoWIN is one of the fastest growing tech platforms in the world. Sharma was appointed to head CoWIN earlier this year.

CoWin is an extension of the electronic vaccine intelligence network eVIN that is used to collect real-time data on the vaccination programmes. CoWIN is a cloud-based IT solution for planning, implementing, monitoring, and also evaluating Covid19 vaccination in India. This platform not only tracks vaccinations on a real-time basis, but also the wastage of doses.

“Given how precious each dose of the vaccines is, governments are also concerned about making sure that each dose is tracked and wastage is minimized. All of this is not possible without an end-to-end digital approach,” Modi added. People do not need to carry around fragile pieces of paper to prove anything, the PM said.

Sharma said CoWIN recorded over 200 million registrations in four months, and 300 million registrations in just five months.

“The journey began with providing a digitally verifiable identity to all Indians through Aadhaar,” Sharma, who was earlier mission director of the Unique Identification Authority of India (UIDAI), said.

Under the Digital India initiative, the country has been focusing on increasing the reach of technology. One such initiative is Unified Payments Interface (UPI) launched in 2016. The interoperable payments system has registered more than 2.7 billion monthly digital transactions worth over $67 billion. On a monthly basis, it accounts for more transactions than debit and credit cards at POS terminals combined. Nandan Nilekani, architect of Aadhaar and non-executive chairman Infosys, earlier this year at a RedSeer event said that NPCI was rolling out a complete open source-based UPI for international markets.

By making the Co-WIN platform available to the world, India is also taking a stand that will be unique to the world, according to experts. Pramod Varma, chief architect of Aadhaar and India Stack, said, "With CoWIN, India has created a unique model that addresses diversity, is interoperable and hence the ecosystem is friendly that allows for innovation."

IEEE Open Journal of Engineering in Medicine and Biology

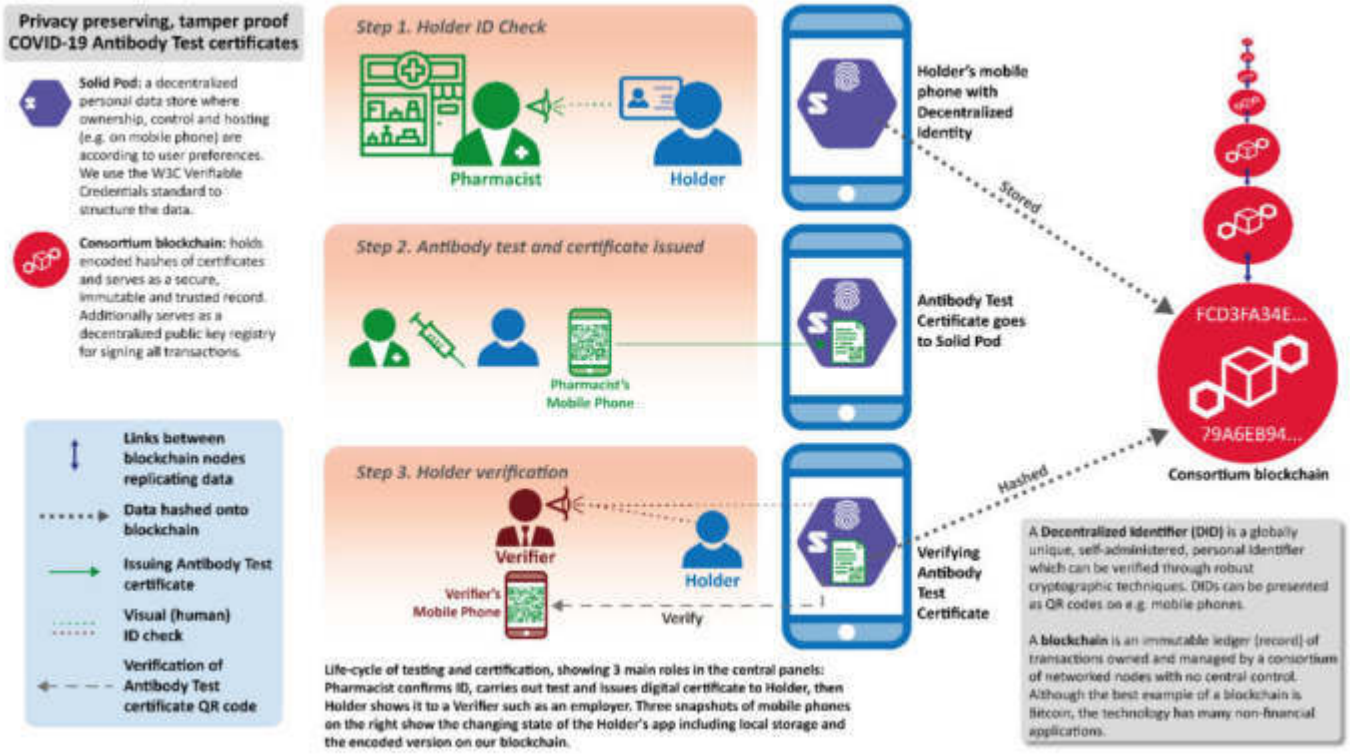
Technology

COVID-19 Antibody Test / Vaccination Certification
There's an app for that

Marc Eisenstadt, Manoharan Ramachandran, Niaz Chowdhury, Allan Third, John Domingue*

Visual Summary / Graphical Abstract + Legend

(Rotated/enlarged image overleaf, followed by full paper and Supplementary Materials)

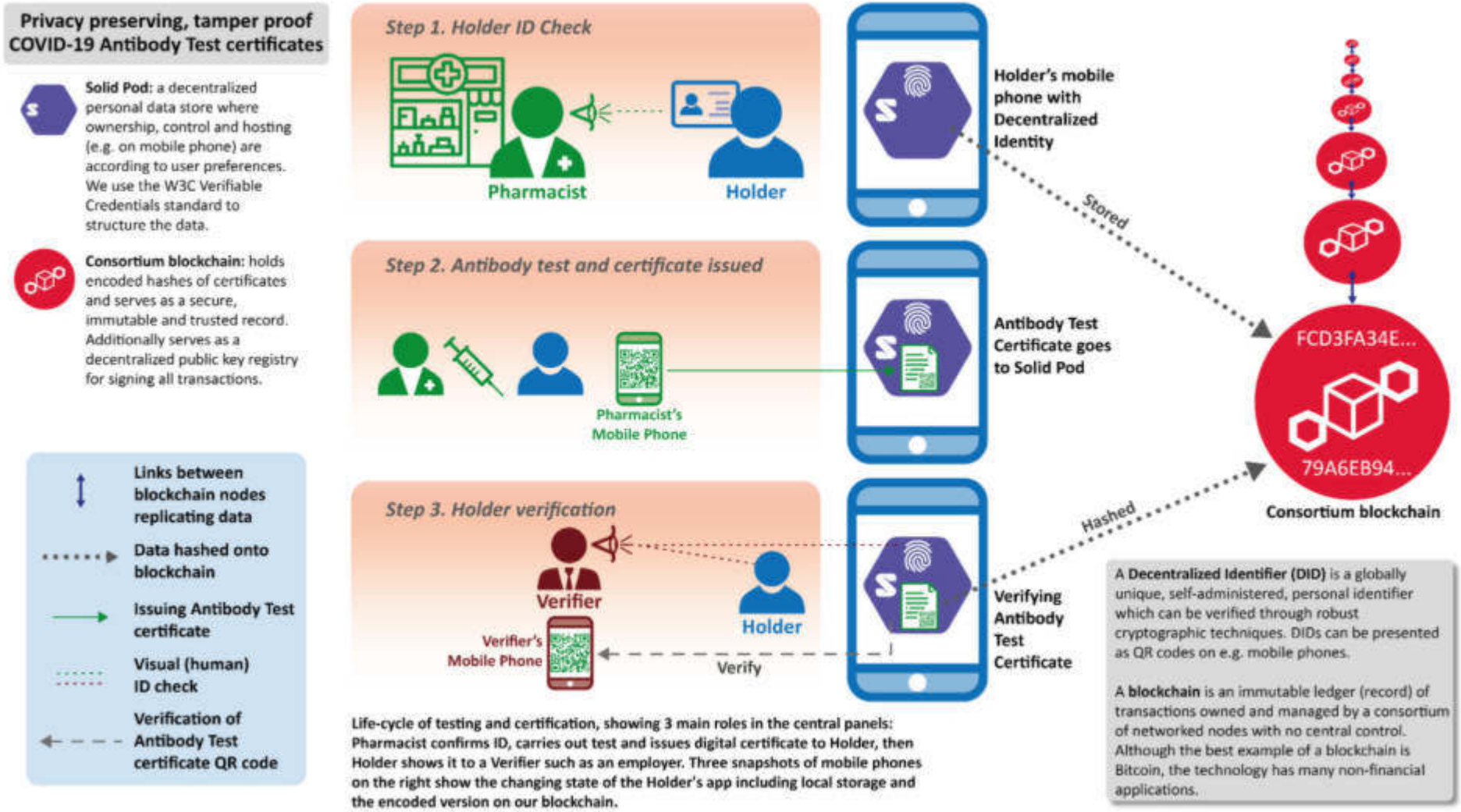


This work addresses the issues involved in providing robust certification for COVID-19 immunity (assuming the biological premise of 'immunity' is ultimately confirmed). Methods: We developed a prototype mobile phone app and scalable distributed server architecture that facilitates instant verification of tamper-proof test results. Personally identifiable information is only stored at the user's discretion, and the app allows the end-user selectively to present only the specific test result with no other personal information revealed. Behind the scenes it relies upon (a) the 2019 World Wide Web Consortium standard called 'Verifiable Credentials', (b) Tim Berners-Lee's decentralized personal data platform 'Solid', and (c) a consortium Ethereum-based blockchain. Results: Our architecture enables verifiability and privacy in a manner derived from public/private key pairs and digital signatures, generalized to avoid restrictive ownership of sensitive digital keys and/or data. Benchmark performance tests show it to scale linearly in the worst case, as significant processing is done locally on each app. For the test certificate Holder, Issuer (e.g. doctor, pharmacy) and Verifier (e.g. employer), it is 'just another app' which takes only minutes to use. Conclusions: The app and distributed server architecture offer a prototype proof of concept that is readily scalable, widely applicable to personal health records and beyond, and in effect 'waiting in the wings' for the biological issues, plus key ethical issues raised in the discussion section, to be resolved.

***Full Paper Citation:**
M. Eisenstadt, M. Ramachandran, N. Chowdhury, A. Third and J. Domingue, "COVID-19 Antibody Test/Vaccination Certification: There's an App for That," in *IEEE Open Journal of Engineering in Medicine and Biology*, vol. 1, pp. 148-155, 2020, doi: 10.1109/OJEMB.2020.2999214.

COVID-19 Antibody Test / Vaccination Certification: There's an app for that

Marc Eisenstadt, Manoharan Ramachandran, Niaz Chowdhury, Allan Third, John Domingue*



Life-cycle of testing and certification, showing 3 main roles in the central panels: Pharmacist confirms ID, carries out test and issues digital certificate to Holder, then Holder shows it to a Verifier such as an employer. Three snapshots of mobile phones on the right show the changing state of the Holder's app including local storage and the encoded version on our blockchain.

***Full Paper Citation:** M. Eisenstadt, M. Ramachandran, N. Chowdhury, A. Third and J. Domingue, "COVID-19 Antibody Test/Vaccination Certification: There's an App for That," in *IEEE Open Journal of Engineering in Medicine and Biology*, vol. 1, pp. 148-155, 2020, doi: 10.1109/OJEMB.2020.2999214.

COVID-19 Antibody Test/Vaccination Certification: There's an App for That

Marc Eisenstadt, Manoharan Ramachandran, Niaz Chowdhury, Allan Third, and John Domingue

Abstract*—*Goal: **As the Coronavirus Pandemic of 2019/2020 unfolds, a COVID-19 'Immunity Passport' has been mooted as a way to enable individuals to return back to work. While the quality of antibody testing, the availability of vaccines, and the likelihood of even attaining COVID-19 immunity continue to be researched, we address the issues involved in providing tamper-proof and privacy-preserving certification for test results and vaccinations.** ***Methods:*** **We developed a prototype mobile phone app and requisite decentralized server architecture that facilitates instant verification of tamper-proof test results. Personally identifiable information is only stored at the user's discretion, and the app allows the end-user selectively to present only the specific test result with no other personal information revealed. The architecture, designed for scalability, relies upon (a) the 2019 World Wide Web Consortium standard called 'Verifiable Credentials', (b) Tim Berners-Lee's decentralized personal data platform 'Solid', and (c) a Consortium Ethereum-based blockchain.** ***Result*****s: Our mobile phone app and decentralized server architecture enable the mixture of verifiability and privacy in a manner derived from public/private key pairs and digital signatures, generalized to avoid restrictive ownership of sensitive digital keys and/or data. Benchmark performance tests show it to scale linearly in the worst case, as significant processing is done locally on each app. For the test certificate Holder, Issuer (e.g. healthcare staff, pharmacy) and Verifier (e.g. employer), it is 'just another app' which takes only minutes to use.** ***Conclusions:*** **The app and decentralized server architecture offer a prototype proof of concept that is readily scalable, applicable generically, and in effect 'waiting in the wings' for the biological issues, plus key ethical issues raised in the discussion section, to be resolved.**

***Index Terms*—Blockchain, COVID-19, coronavirus, decentralized, immunity certification.**

***Impact Statement*—As soon as COVID-19 antibody testing, vaccines, and likelihood of immunity surpass quality thresholds, our tamper-proof and privacy-preserving certification can be rapidly deployed. Our approach is applicable to any certification scenario.**

Manuscript received April 20, 2020; revised May 22, 2020 and May 28, 2020; accepted May 28, 2020. Date of publication June 1, 2020; date of current version June 26, 2020. This work was supported by the UK Government Office for Students' Institute of Coding and two projects funded under the European Union's Horizon 2020 research and innovation programme: QualiChain (grant agreement number 822404) and DEL4ALL (871573). *(Corresponding author: John Domingue.)*

The authors are with the Knowledge Media Institute, The Open University, Milton, Keynes MK7 6AA, U.K. (e-mail: marc.eisenstadt@open.ac.uk; manoharan.ramachandran@open.ac.uk; niaz.chowdhury@open.ac.uk; allan.third@open.ac.uk; john.domingue@open.ac.uk).

This article has supplementary downloadable material available at https://ieeexplore.ieee.org, provided by the authors.

Digital Object Identifier 10.1109/OJEMB.2020.2999214

I. Introduction

THE Coronavirus/COVID-19 pandemic of 2019/2020 is still taking its terrible toll as we write this [1]. Tests for the presence of antibodies *could* offer a way for people who can prove COVID-19 immunity to go back to work [2], [3]. There are, however, challenges concerning the biological premise of 'immunity': the strength and longevity of COVID-19 immunity after infection are matters of current debate and research, as are the sensitivity and robustness of the relevant tests [4], [5] and the race to develop a viable vaccine [6], [7].

Given the scale of the pandemic and financial fallout, it is plausible that 'COVID-19 antibody test / vaccination certification' (henceforth 'CAT/VC'), if shown to be robust, will be in great demand. Bearing in mind the legal and ethical implications of such certification, raised in [8], [9] and our Discussion, we feel that for either the current pandemic or a pandemic of the future, the concept of certification has a place, *particularly when the recipient is employed in healthcare or other key sectors.*

But what form should certification take? A signed or stamped letter is the centuries-old default, and straightforward to roll out at scale, as long as there is some point-of-test proof of identity. Our approach is based on the view that for such a sensitive and likely high-value certificate, a paper version is too vulnerable to alteration or forgery (an exception arises in environments that are 'lower tech' for socio-economic reasons and we later describe a printed certificate to address this case). A digital certificate makes the most sense, provided that it can be: (i) Privacy-preserving (because as proud as the holder might be of new-found 'immunity', personal data can be re-purposed in unpredictable ways [10]), (ii) un-forgeable, (iii) easy to administer, (iv) easily verifiable while still preserving privacy, (v) scalable to millions of users, and (vi) cost-effective.

All of this effort would be wasted without public acceptance, which is increasingly challenging in an era of suspicion about data-collecting apps [11]. Toward this end, we argue not only for the decentralized approach underlying our design and implementation below, but also for its benefits in allowing individuals who have been tested to change their minds and quit the scheme, knowing that even cryptographically encoded data will be 'orphaned' (no data pointing to it), rendering it meaningless. Also,

in the Supplementary Materials, we emphasize the importance of having strong oversight by an ethics watchdog to ensure best endeavours to avoid unleashing a Pandora's Box of undesirable side-effects.

How best to undertake such a challenge? Modern smartphone apps and several key technologies such as public key cryptosystems and immutable blockchain records offer some tantalizing prospects for the path we envisage, if they can satisfy the above criteria. Below, we look at the methods by which this can be achieved, assuming a scenario involving testing by a known authority (e.g. a healthcare practitioner or pharmacist), as opposed to self-testing at home. This main paper assumes an 'On-Site Test for Antibodies + Issuance of Digital Certificate Including Photo ID' in order to explain our approach, and in the Supplementary Materials we describe variations for (a) 'Issuing Digital Certificate Without Photo ID', (b) 'Issuing Paper Certificate', (c) 'Off-Site Testing Via External Lab', and (d) 'Vaccination + Certification'

II. Methods

We focus on the design and implementation of a prototype mobile phone app and requisite decentralized server architecture, intended to facilitate verification of tamper-proof test results. Our design involves a novel hybrid architecture based on (a) the 2019 World Wide Web Consortium standard called 'Verifiable Credentials', (b) Tim Berners-Lee's decentralized personal data platform 'Solid', and (c) a Consortium Ethereum-based blockchain. We work through (d) a plausible use case scenario, then (e) describe the key 'onboarding' and certification steps in detail; and (f) provide benchmark tests to anticipate scaling performance.

A. 'Verifiable Credentials' For Digital Certification

Verifiable Credentials [12] is a W3C standard that builds upon Public Key Infrastructure (PKI), the public/private key pairs that facilitate digital signatures in widespread use today. The W3C extensions standardize the definitions of document formats to make them machine-readable and communicable, and to generalize PKI, which tends to be costly and highly centralized. The generalization involves a decentralized registry for cryptographic keys, typically residing in a blockchain — this allows every public key to have its own unique address, known as a Decentralized Identifier (DID). The key roles and transactions, adapted for our specific use case, are illustrated in Fig. 1.

The 'Issuer', in our case a trusted pharmacy or the UK National Health Service (NHS), can issue credentials such as blood test results and vaccination certificates. 'Holders' (typically citizen end-users) can store them in their own preferred way, for example in digital wallets that are part of a mobile phone app. 'Verifiers', such as employers, or establishments seeking proof of some attribute, can ask the Holder to present such proof concerning these credentials. Verifiers also check digital signatures against what is known as a 'verifiable (decentralized) data registry': this is the blockchain where the DIDs mentioned above reside.

Fig. 1. Main roles and workflow in W3C Verifiable Credentials [12], adapted for our COVID-19 Antibody Testing use case.

B. 'Solid': Decentralized Personal Data

We pointed out in [13] that the over-centralization of data, particularly its consolidation into 'silos' by brand-name IT services and social network providers, is of increasing concern. Decentralization is an ideal starting point for storing sensitive data, including medical, financial, and other personal data — but only if security and privacy are significantly better than what can be offered by traditional centralized systems.

We identified a promising approach to widespread deployment, known as Solid, initiated by Sir Tim Berners-Lee [14], [15]. Solid aims to decentralize the Web by transferring control of data from a central authority to users, thereby allowing users to retain complete ownership of their data, which they store in what are called 'Solid Pods' — analogous to a personal web server that is hosted either locally on a mobile phone, or hosted with a cloud provider of the individual's choice, or both. The key distinction from centralized approaches is that even in the provider-hosted case, the provider's access to the data is limited by the user's preferences.

In [16] we proposed an approach combining Solid Pods and distributed ledgers, of the type familiar to the blockchain community, to facilitate the complete decentralization of data. The key ingredients of this combination are illustrated in Fig. 2, which also provides an overview of the main test/certify/verify life cycle. Our methods give users total control over their data while maintaining the integrity of the stored information through blockchain-based verification.

As in Fig. 1, the 'Holder' is the primary individual who is self-motivated to obtain the certificate of COVID-19 antibody test results in order to be admitted to a workplace or other location. Holders own, manage, and control their own Solid Pods (shown as hexagons in the Holder's mobile phone in Fig. 2 at A, E, and F), which contain their personal data. In Fig. 2, our Holder's Solid Pod contains a elements of a physical ID such as a driving license ('thumbprint' icon at A) and the Holder's signed and countersigned certificate of COVID-19 antibody test results — represented in Fig. 2 as a document in which is embedded a special QR code (F). The Holder is free to store the Solid Pod data on his/her mobile phone, on a personal favorite cloud provider, or both (we only show the mobile phone version for simplicity). At any time, Holders can move or delete data, as it remains under

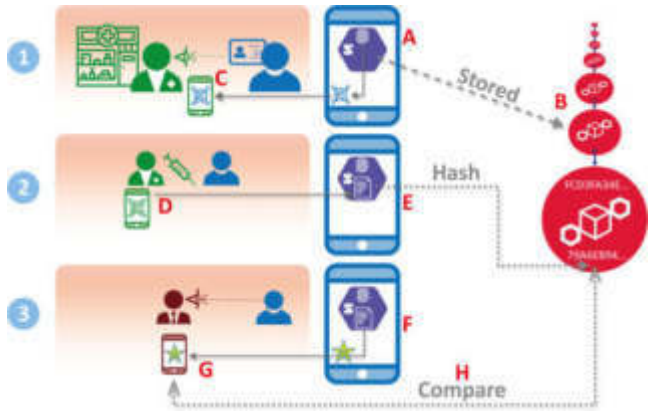


Fig. 2. Steps in testing, certification, and verification, showing a Solid Pod (hexagon) hosted on the Holder's mobile phone (labels A, E, F), with minimal hash storage for verification. The circles at B depict replicated blockchain nodes on multiple servers, receding into the distance.

their ownership. One-way encoded 'hashes' of the data (only a few bytes in size) are held, as shown by the dashed arrows in Fig. 2 (E and H), on a blockchain to support independent verification.

C. Consortium Blockchain

In our design, we use a 'Consortium blockchain', shown in Fig. 2(B) as circles (depicting multiple replicated blockchain nodes receding into the distance): this is not a fully public blockchain like Ethereum or Bitcoin, but rather a blockchain shared specifically by a *Consortium* of known providers who have signed up to the Ethics Guidelines we describe in the Discussion Section. The Open University-led Consortium blockchain is a private Ethereum network known as OpenEthereum (formerly Parity Ethereum) [17], [18] which uses a 'Proof of Authority' consensus mechanism [19] wherein several nodes can be in the mutually-agreed privileged position of being allowed to confirm transactions. As we go to press, our Consortium blockchain comprises nodes run by The Open University, BT, Condatis, Inrupt, and the Chiba Institute of Technology near Tokyo, with expansion planned as our prototype implementation is scaled up via other large-company partnerships now under discussion. This approach contrasts with that of Bitcoin and other early blockchains which use the slow and ecologically unfriendly Proof of Work, wherein massive computing power enables nodes to have a better chance of confirming transactions. The Consortium approach gives us the kind of distributed scalability that increases security, but without the widespread public availability that may serve as a disincentive for individuals to participate.

D. Use Case Scenario

In our scenario, the Issuer (Pharmacy) needs to authenticate that the Holder is who they say they are, and thus requests that the Holder display (a) a physical ID, such as a Driving License or a Passport, and (b) a QR code which is scanned by the Issuer using the Issuer's mobile phone app, both of which are shown in Fig. 2 (C). At this point the Issuer taps to accept the ID, and the Holder's photo is 'burned' into the upcoming steps so that at the final step of verification there will be no need to display the same physical ID. The next steps are as follows:

2) The blood test is performed, and the certificate with results is issued as soon as the results are available (off-site lab tests are dealt with in the Supplementary Materials). The Issuer (first scanning a printed QR code if preferred) generates a digitally-signed test result as a new QR code (labelled D in Fig. 2) for transmission to the Holder, thereby providing a Verifiable Credential which is digitally signed by both the Issuer and the Holder, and stored on the Holder's Solid Pod (Fig. 2, D and E). At label E we also see that a hash of the Verifiable Credential is stored on the Consortium blockchain to facilitate verification at step 3.
3) The Holder can now present a provably valid certificate to the Verifier. To avoid someone else impersonating the Holder, the Holder's ID photo was already 'burned' into the digital certificate at Step 1, so the Holder needs to present only the QR code (F and G in Fig. 2)

At H in Fig. 2 we see that the Verifier's app automatically verifies both digital signatures and the certificate against the hash stored on the Consortium blockchain, and confirms acceptance of the COVID-19 Antibody Test Certificate. The certificate stores quantitative test results, such as antibody type (e.g. 'IgG') and level, so it is up to the Verifier's own contextually guided procedures to decide whether to admit the Holder, for example, to work.

E. Primary design (Onboarding and Certification)

Below we separately describe the details for (i) 'Onboarding' for Issuers, Holders and Verifiers, and (ii) how Certification works behind the scenes. The companion step of (iii) Verification is conceptually similar, and thus provided separately in the Supplementary Materials, as are the more straightforward descriptions of the server and mobile app functional architectures.

1) Onboarding: There are three entities involved in the operations: Issuers, Holders and Verifiers. The onboarding process lets all of them install and configure the app. The configuration process for each of them is distinct and requires specific documentation.

Issuers: The onboarding of a potential Issuer (Fig. 3) begins with the person downloading and installing the app. The app then instructs the Issuer to complete an in-app form. Because the Issuer has the ability to test, validate and issue certificates to individuals, the app employs *two factor authentication* for all potential Issuers. We anticipate using the API provided by the General Pharmaceutical Council, or an equivalent, to cross-check the registration and the branch information of the likely Issuer (this is simulated in our prototype — discussions about API access are underway), followed by email verification. The former requires the person to input appropriate information into the form, while the latter asks the potential Issuer to provide a valid official email address at the company's registered domain name. The app sends a special link to that Issuer's email address to complete the registration. Data provided by the potential Issuers resides on each Issuer's Solid Pod.

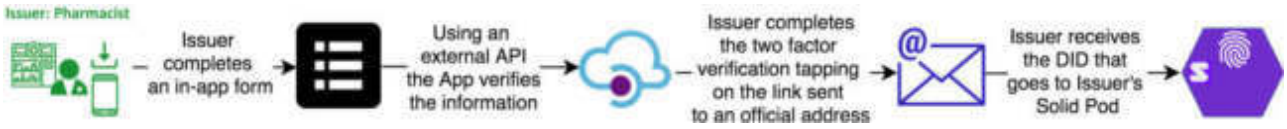


Fig. 3. Issuer onboarding timeline details.

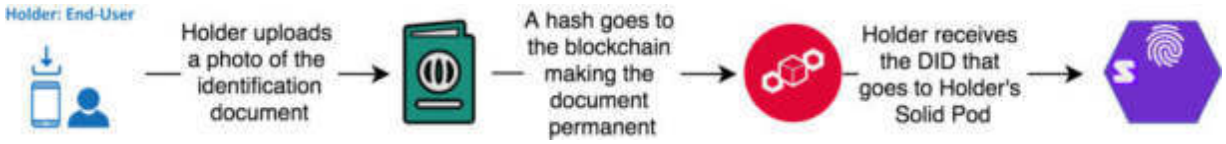


Fig. 4. Holder onboarding timeline details.

Fig. 5. Verifier onboarding timeline details.

Holders: The process of onboarding a Holder (Fig. 4) involves adding an identification document such as a driving license or passport. The document number is used to generate the Decentralized ID (DID) that acts as the anchor for the Holder. A potential Holder first downloads and installs the app followed by adding a photo of the identification document. This document resides in the Holder's Solid Pod. This photo document is deemed permanent (but remains on their personal Solid Pod) and once submitted, cannot be changed again. The app then provides the Holder with the DID, leaving the owner of the account ready for testing and certification.

Verifiers: Of the three main roles, the process of onboarding Verifiers is the most straightforward. Anyone willing to act as a Verifier can download the app and start verifying. There is no need to create an account for verifying a Holder's certificate. As the Verifier submits no data, the steps of the Verifier onboarding timeline (Fig. 5) do not involve Solid Pods.

2) Certification: The certification process requires a Holder to visit an Issuer with the exact document used for identification at the time of onboarding. At this point the Issuer matches this document with the copy stored in the Holder's Solid Pod, viewing it on the app and tapping to accept the ID. The Holder's photo is 'burned' into the upcoming steps so that at the final step of verification, there will be no need to display the same physical ID. In Fig. 6, we see the 'behind the scenes' view of certification, including the Holder's Solid Pod with the ID.

The app is designed to work in a completely decentralized environment. Its functionalities run across the Issuer's, Holder's, and Verifier's phones as well as on the hosting servers, but does not have access to any data from a central database. Every time the app needs to execute an operation, it reads the data from a particular user's Solid Pod (and only with the user's permission). In Fig. 6, at (A) we see that the app reads the allowed identity details from the Holder's Solid Pod, and at (B) compares their hash with the corresponding hash on the blockchain and confirms this on the Issuer's phone display.

Once the identity is confirmed, via physical document checks and Verifiable Credentials demonstrating ownership of the relevant DIDs, the Issuer conducts the antibody test and initiates the process of generating a certificate at (C). A certificate is a set of data in W3C RDF (Resource Description Framework) format [20] containing the test results and a Verifiable Credential for the just-tested Holder. While the hash of the certificate goes onto the blockchain at (D), the original document resides in the Solid Pod (E). It is notable that neither the blockchain nor a third-party centralized server stores the personal data of the Holder.

The Holder has the option of keeping a copy of the certificate in a cloud server of his or her choice. In the event of losing the phone, the Holder can retrieve the data from the cloud and restore the certificate in the regenerated local Solid Pod of the replacement phone. This certificate is visible on the Holder's app in the form of a QR code, giving an easy-to-scan option for Verifiers.

3) Verification: The innards of Verification are conceptually similar to what we have just shown for Certification and are thus provided separately in the Supplementary Materials.

F. Benchmark Testing

To anticipate scalability, we benchmarked three operations (Issuing, Verifying, and Uploading) against a baseline ping that simply echoed a response following a request.

For both Issuing and Verifying we used two variants, to assess the difference between generating hashes (a) locally within the mobile phone app and (b) externally on a server before adding to the blockchain. The Uploading times are purely the times for uploading a certificate to a Solid Pod stored in the cloud, in case that is the Holder's preference.

III. Results

A. COVID-19 Antibody Test Certification: App Characteristics

Our 'COVID-19 antibody test certification' (CAT/VC) app builds upon the Verifiable Credentials and Solid frameworks

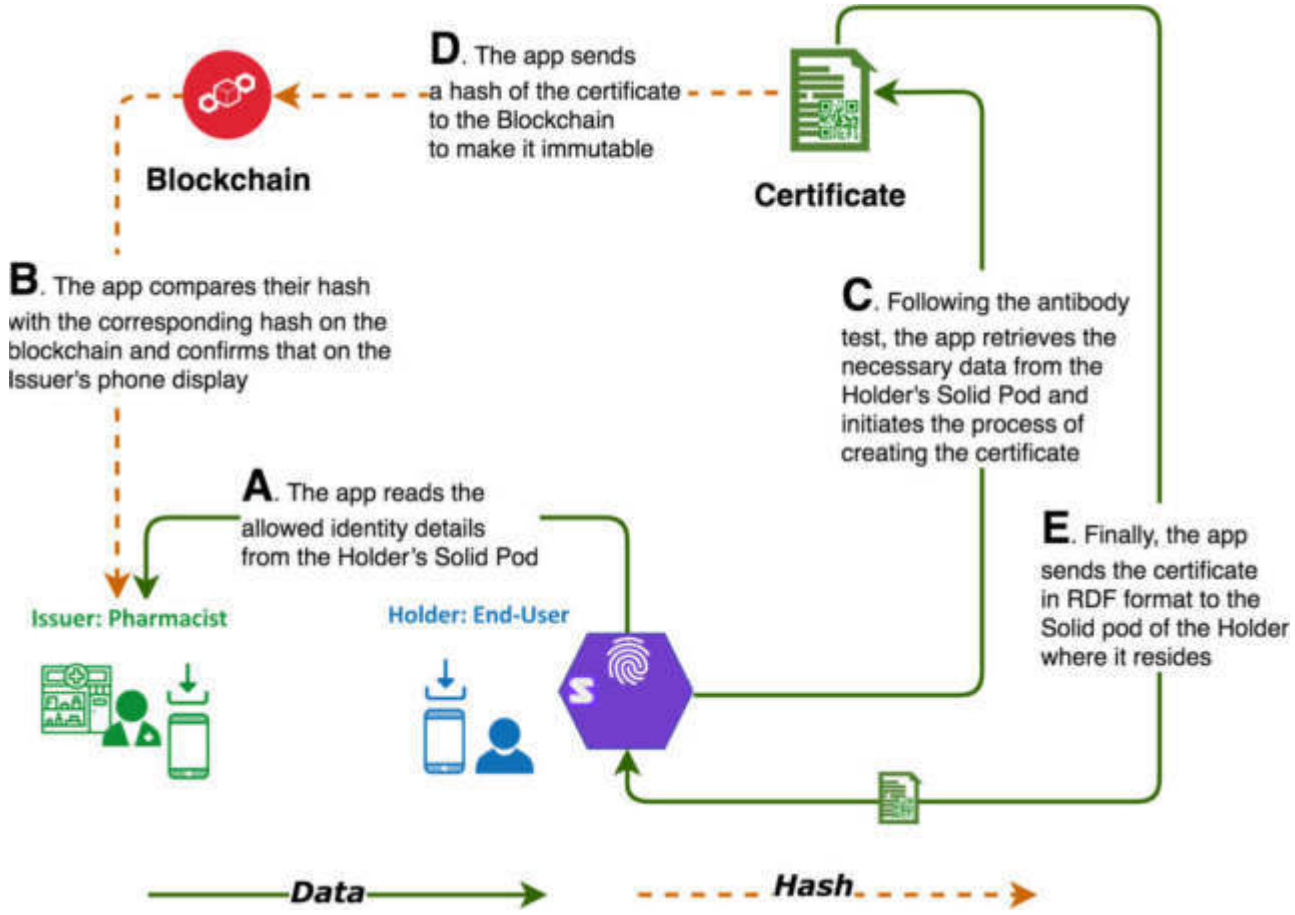


Fig. 6. Certification: main dataflows.

described in Section II, plus our own expertise developed over the past 5 years in the area of blockchain-based certification [21], [22]. The result combines the following characteristics:

- Wholly resident on the end-user's smartphone, yet usable as a paper-only certificate in appropriate socio-economic contexts, as described in the Supplementary Materials.
- One-tap scan, display, and verification of antibody test results, which are owned by the user.
- The app only reveals verifiable CAT/VC results without revealing any personally sensitive information, at the discretion of the user.
- The details of Verifiable Credentials, Solid Pods, and Ethereum blockchain are hidden: from the user's point of view, it is 'just another app'.

B. Performance Benchmarking Results

Fig. 7 shows the time to completion in seconds (Y axis) of all six operations where we sent between 1 and 100 simultaneous requests (X axis): the fastest (baseline) ping is the lowest line. Uploading is the second least expensive operation, while Verifying and Issuing are the two most expensive operations of our app. The relative difference in time between operations involving locally generated hash (LH) and server-generated hash (SH) is modest for Issuing (6.9% difference between 'Issuing SH' and 'Issuing LH'), but more twice that for Verifying (17.1% difference between 'Verifying SH and 'Verifying LH'). This behavior is understandable, as Issuing requires writing on the blockchain through transactions (i.e. the method that allows adding an entry to the distributed ledger) while Verifying involves only a look up at a particular ledger entry.

Linear growth for all operations indicates that our architecture is capable of handling scale-up without surprise: there is simply no inter-node or inter-app communication or interaction overhead, so by improving the configuration of the common infrastructures in the architecture, such as any Solid cloud server, blockchain node, or any other intermediate element, the architecture can serve more parallel requests, i.e. reduce the response time. Implications and additional results are discussed below and in the Supplementary Materials.

IV. Discussion

A. Deployment, Integration, and Scale

Our focus is on trusted certification, and for this reason we remain committed to deployments involving nationally approved locations such as pharmacies or UK National Health Service surgeries rather than home testing (off-site lab tests are described in the Supplementary Materials). With our approach, deploying

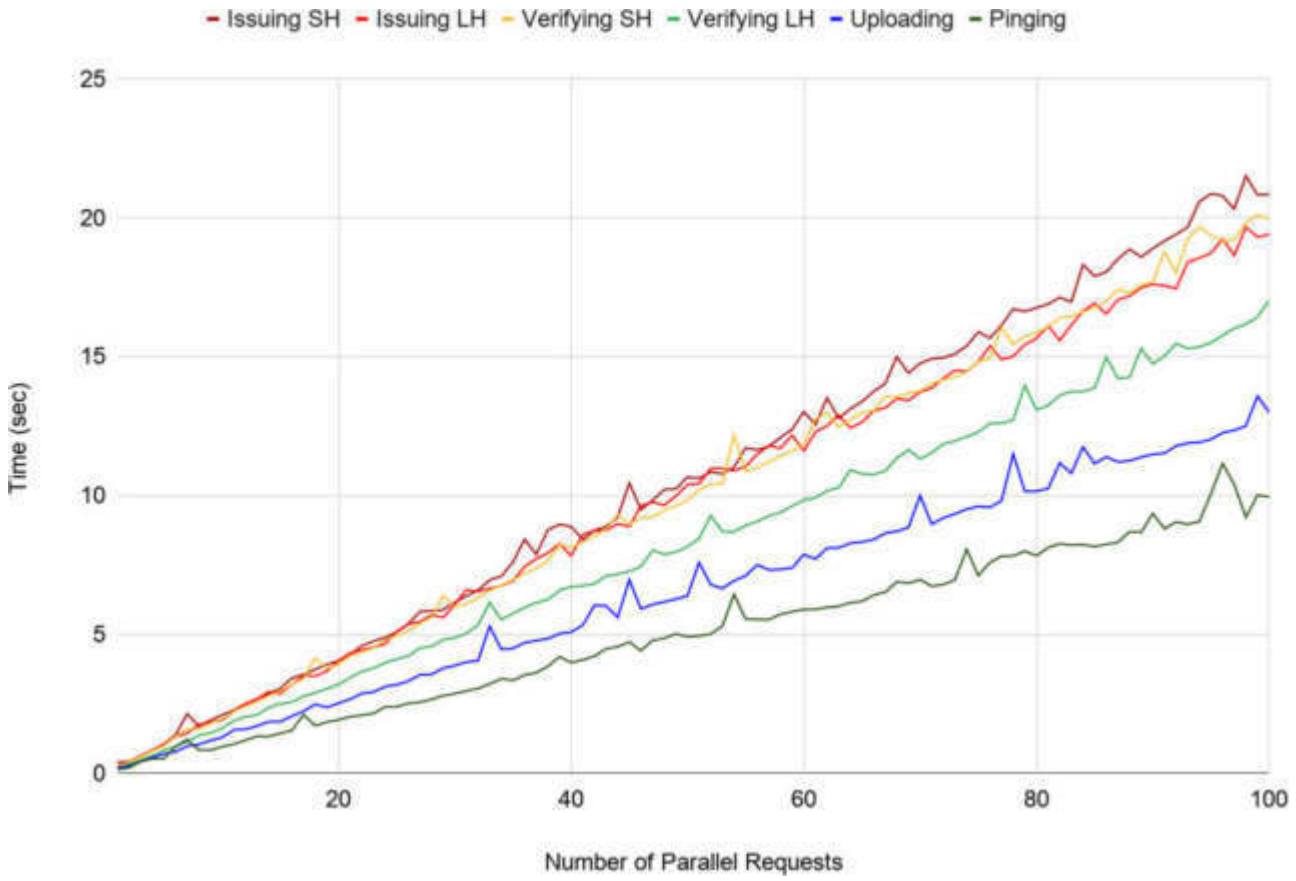


Fig. 7. Time to issue up to 100 parallel requests for 'Issuing' (SH=Server Hash and LH=Local Hash), 'Verifying' (SH=Server Hash and LH=Local Hash) and Uploading of Solid Pod data vs baseline standard 'Ping'.

the decentralized servers requires another dozen or so Consortium members in addition to the five already engaged, plus about two days of training, which can be handled in parallel for all Consortium members via webinars, as we already do in our current work with blockchain-based educational certification [23]. The mobile phone app itself requires just a download and less than 30 minutes of training for Issuers, and even less for Verifiers and Holders—we anticipate developing a video tutorial for all scenarios. More significantly is the 'buy-in' i.e. acceptance by certified pharmacies and, in the UK, the National Health Service, and integration with existing work practice, ethics guideline approval, and agreement about what, if any, data needs to be stored centrally (no central storage is required at all by our approach). For a full-scale rollout, it would be necessary to further stress-test our prototype along the lines we have already started as described in the preceding Sections.

The technology itself is inherently scalable as our Results section shows: transactions on the Consortium blockchain typically take under 5 *seconds* to be confirmed after entry by the Issuer, after which other steps such as verification are subjectively instantaneous. This scales well, as the architecture is inherently distributed across servers (blockchain nodes) and mobile phone apps. Moreover, we have shown worst case results, covering the case when (a) all Solid servers are hosted on the same machine, (b) all blockchain transactions are being sent to the same specific node, and (c) all users are acting simultaneously. In the best case scenario, all simultaneous users would connect to their own Solid servers, and any simultaneous blockchain transactions would each involve different blockchain nodes, so performance overhead would be constant for each additional user. Realistically, i.e. in between these cases, there would be ample numbers of Solid servers, many dozens to hundreds of blockchain nodes, and natural spacing between transactions, and thus performance overhead for each additional user would be minimal.

Collaborative possibilities for rollout and integration are promising, as new initiatives in this niche are rapidly emerging [24].

B. Beyond Antibody Test Certification

Our scenario highlights antibody testing, but the technology is identical for vaccination certification, as we describe in the Supplementary Materials — this may prove even more popular once vaccines have been suitably tested and approved [6], [7]. The app and decentralized server architecture are readily scalable and applicable generically. For example,

- People could demonstrate that they are eligible to use different methods of transport or to visit public places such as libraries, theaters, or holiday destinations.

- Utility/building/repair staff seeking access to a place of residence, even in 'normal' healthy times, could 'prove their roles'.
- More generally, the entire area of 'Decentralized Verifiable Personal Health Records', as described in [25], particularly if augmented by the W3C Verifiable Credentials standard [12], can benefit from the approach described herein.

C. Ethics

New technologies bring new challenges for society. Commentators have argued (e.g. in [8], [9], [26]), that certification of the type we have envisaged, even when totally private and tamper-proof, would entail multiple risks, notably: (a) disenfranchising the poor and others who do not have access to the technology or the tests, or have access but 'fail' the test, and (b) becoming a stepping-stone for future governments to deploy the same concept either to enable or to enforce discrimination based on immunity and other arbitrary conditions. To avoid this technology becoming 'weaponized' for discriminatory purposes, we advocate several measures including optional rather than mandatory use, adherence with UK NHS Information Governance guidelines [27], [28] and oversight by an Ethics Committee. This issue is analyzed in detail in the Supplementary Materials.

V. Conclusion

The perceived need for a COVID-19 Antibody Test / Vaccination Certificate, if shown to be biologically robust and to conform to proposed ethical guidelines, has motivated us to develop a mobile phone app based around Verifiable Credentials, distributed storage of cryptographic public/key pairs, and the decentralized verification of data with confidentiality. This has enabled us to provide a facility that is 'just another app' from the viewpoint of the end-user, healthcare professionals, employers and other relevant authorities — thereby providing a tamper-proof record owned entirely by the end-user, and allowing the end-user selectively to reveal solely the proof of test results without surrendering other personal information (e.g. age, address, blood type, other discovered antibodies or immune deficiencies or other inadvertent revelations in the data set, for which certificate Holders may have no idea how this information might be used by someone else in the future), and requiring only mobile phone app downloads from everyone in the loop. This app and its secure digital certificate thus become a powerful adjunct/enhancement to traditional paper-based certification from the NHS or Pharmaceutical testing authorities — and without the need for the costly installation of special 'e-ticket reader' hardware: the same mobile phone app is sufficient for the task at hand, regardless of which of the three roles is involved. Many other uses of secure and private certification via mobile phone app and decentralized servers are additionally made possible, and our infrastructure can be embedded into any other app or web portal through APIs.

Acknowledgment

The authors would like to thank Ben Hawkridge, Pasquale Iero, Michelle Bachler, Kevin Quick, and Harriett Cornish of KMi, plus Open University Professor of Biology David Male for timely advice about immunology, Dr. Elias Ekonomou of Condatis for raising the prospect of Verifiable Personal Health Records, and external readers Mia Eisenstadt and Zaid Hassan for their input regarding ethical considerations.

References

[1] "Coronavirus COVID-19 global cases by the center for systems science and engineering (CSSE) at Johns Hopkins University," 2020. [Online]. Available: https://gisanddata.maps.arcgis.com/apps/opsdashboard [Accessed: Apr. 2, 2020].

[2] The Guardian, "'Immunity passports' could speed up return to work after Covid-19," Mar. 30, 2020. [Online]. Available: https://www.theguardian.com/world/2020/mar/30/immunity-passports-could-speed-up-return-to-work-after-covid-19 [Accessed: Apr. 2, 2020].

[3] The Guardian, "No 10 seeks to end coronavirus lockdown with 'immunity passports'," Apr. 2, 2020. [Online]. Available: https://www.theguardian.com/politics/2020/apr/02/no-10-seeks-to-end-covid-19-lockdown-with-immunity-passports [Accessed: Apr. 3, 2020].

[4] S. Malapaty, "Will antibody tests for the coronavirus really change everything?" *Nature* (News) Apr. 18, 2020. [Online]. Available: https://www.nature.com/articles/d41586-020-01115-z [Accessed: Apr. 19, 2020].

[5] D. Male, J. Golding, and M. Bootman, "How does the human body fight a viral infection?" Open University, OpenLearn Course Module, Milton Keynes, UK, 2020. [Online]. Available: https://www.open.edu/openlearn/science-maths-technology/biology/how-does-the-human-body-fight-viral-infection [Accessed: Apr. 7, 2020].

[6] T. Thanh Le *et al.*, "COVID-19 vaccine development landscape," *Nat Rev Drug Discov*, vol. 19, no. 5, pp. 305–306, Mar. 2020, doi: 10.1038/d41573-020-00073-5. [Online]. Available: https://www.nature.com/articles/d41573-020-00073-5

[7] N. Lurie, M. Saville, R. Hatchett, and J. Halton, "Developing Covid-19 vaccines at pandemic speed," *N. Engl. J. Med.*, vol. 382, no. 21, pp. 1969–1973, May 2020, doi: 10.1056/NEJMp2005630.

[8] Ada Lovelace Institute, "Exit through the app store?" Apr. 20, 2020. [Online]. Available: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf [Accessed: May 5, 2020].

[9] "The dangers of blockchain-enabled 'Immunity Passports' for COVID-19," May 18, 2020. [Online]. Available: https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290. [Accessed: May 21, 2020].

[10] C. Cadwalladr, "The Cambridge Analytica files," *Guardian*, 2018. [Online]. Available: https://www.theguardian.com/news/series/cambridge-analytica-files. [Accessed: Apr. 20, 2020].

[11] Business Insider, "Experts call on UK to not use contact tracing app for surveillance," Apr. 29, 2020. [Online]. Available: https://www.businessinsider.com/cybersecurity-experts-uk-government-contact-tracing-surveillance-2020-4?r=US&IR=T. [Accessed: Apr. 30, 2020].

[12] W3C.org, "Verifiable credentials data model 1.0," W3C.org, Nov. 19, 2019. [Online]. Available: https://www.w3.org/TR/vc-data-model/ [Accessed: Apr. 7, 2020].

[13] J. Domingue, A. Third, and M. Ramachandran, "The fair trade framework for assessing decentralized data solutions," in *Proc. Companion World Wide Web Conf.*, pp. 866–882, 2019. [Online]. Available: http://oro.open.ac.uk/60149/ [Accessed: Apr. 14, 2020].

[14] A. V. Sambra *et al.*, "Solid: A platform for decentralized social applications based on linked data," Technical Report, MIT CSAIL & Qatar Computing Research Institute, 2016. [Online]. Available: https://pdfs.semanticscholar.org/5ac9/3548fd0628f7ff8ff65b5878d04c79c513c4.pdf [Accessed: Apr. 15, 2020].

[15] "Solid MIT," 2017. [Online]. Available: https://solid.mit.edu/ [Accessed: Apr. 10, 2020].

[16] M. Ramachandran, N. Chowdhury, A. Third, J. Domingue, K. Quick, and M. Bachler, "Towards complete decentralized verification of data with confidentiality: Different ways to connect solid pods and blockchain," in *Proc. Companion Web Conf. (WWW '20 Companion)*, Apr. 20-24, 2020, pp. 645–649. [Online]. Available: https://doi.org/10.1145/3366424.3385759 and http://oro.open.ac.uk/69607/1/DecentWeb-FinalCamReady.pdf [Accessed: Apr. 13, 2020].

[17] openethereum/openethereum, "Fast and feature-rich multi-network Ethereum client," Apr. 6, 2020. [Online]. Available: https://github.com/openethereum/openethereum [Accessed: Apr. 14, 2020].

[18] "Transitioning parity ethereum to openethereum DAO," Dec. 16, 2019. [Online]. Available: https://www.parity.io/parity-ethereum-openethereum-dao/ [Accessed: Apr. 14, 2020].

[19] "What is proof of authority consensus? (PoA) staking your identity," Jul. 5, 2018. [Online]. Available: https://blockonomi.com/proof-of-authority/ [Accessed: Apr. 14, 2020].

[20] "RDF — semantic web standards," Mar. 15, 2014. [Online]. Available: https://www.w3.org/RDF [Accessed: Apr. 13, 2020].

[21] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *Proc. 11th Eur. Conf. Technol. Enhanced Learning*, Sep. 2016, pp. 490–496, [Online]. Available: https://doi.org/10.1007/978-3-319-45153-4_48 [Accessed: Apr. 14, 2020].

[22] A. Mikroyannidis, A. Third, J. Domingue, M. Bachler, and K. Quick, "Blockchain applications in lifelong learning and the role of the semantic blockchain," in *Blockchain Technology Applications in Education*. R. C. Sharma, H. Yildirim, and G. Kurubacak, Eds. Pennsylvania, United States: IGI Global, pp. 16–41, Nov. 2019.

[23] A. Mikroyannidis, J. Domingue, M. Bachler, and K. Quick, "A learner-centred approach for lifelong learning powered by the blockchain," in *Proc. EdMedia: World Conf. Educational Media Technol.*, 25-Jun. 29, 2018, pp. 76–81. [Online]. Available: http://oro.open.ac.uk/55989/ [Accessed: Apr. 14, 2020].

[24] Coindesk. "COVID-19 'immunity passport' unites 60 firms on self-sovereign ID project," Apr. 13, 2020. [Online]. Available: https://www.coindesk.com/covid-19-immunity-passport-unites-60-firms-on-self-sovereign-id-project [Accessed: Apr. 19, 2020].

[25] S. Wang, D. Zhang, and Y. Zhang, "Blockchain-based personal health records sharing scheme with data integrity verifiable," *IEEE Access*, vol. 7, pp. 102887–102901, Jul. 2019.

[26] The Guardian | Editorial, "The Guardian view on immunity passports: an idea whose time has not come," [Online]. Available: https://www.theguardian.com/commentisfree/2020/apr/03/the-guardian-view-on-immunity-passports-an-idea-whose-time-has-not-come [Accessed: Apr. 3, 2020].

[27] "NHS information governance," 2015. [Online]. Available: https://www.england.nhs.uk/ig/about/ [Accessed: Apr. 9, 2020].

[28] "About the NHS IG Toolkit," 2015. [Online]. Available: https://www.igt.hscic.gov.uk/resources/About%20the%20IG%20Toolkit.pdf [Accessed: Apr. 9, 2020].

Supplementary Materials

COVID-19 Antibody Test / Vaccination Certification
There's an app for that

Marc Eisenstadt, Manoharan Ramachandran, Niaz Chowdhury, Allan Third, John Domingue*

I. Introduction

In this supplementary materials section we provide the following extras: Introduction — more about the premise of immunity; Methods — (a) how we achieve robust privacy, (b) more details about how Verification works and the functional architecture and mobile phone app infrastructure, (c) scenario variations for (i) Issuing a Digital Certificate Without Photo ID, (ii) Issuing a Paper Certificate, (iii) Off-Site Testing Via an External Lab, and (iv) Vaccination + Certification; Results — additional aspects of system performance; Discussion — further observations about rollout and ethical issues.

The premise of immunity: Throughout most of the COVID-19 pandemic, the World Health Organisation (WHO) has advocated a 'test-isolate-trace' approach [1]. In parallel, there has been a worldwide cooperative effort to develop a vaccine [2] and to develop numerous serological tests for the presence of antibodies [3]. If immunity is strongly implied by the outcomes of these latter tests, then individuals could be allowed to get back to work, particularly in healthcare and other key areas [4], [5]. The WHO initially warned that the very premise of COVID-19 immunity was itself uncertain [6]. Yet the fast pace of research is already showing promising signs that early testing was flawed, the presence of antibodies in recovered individuals has been confirmed, and re-infection now seems increasingly unlikely [7], [8]. True, some immunologists have argued that COVID-19 immunity could be very weak, because 'reinfection is an issue with the four seasonal coronaviruses that cause about 10% to 30% of common colds' [9]. But others in that same discussion argue that immunity could be valid for 'a year or two', a view shared by Male, who with Golding and Bootman has written a clear exposition on the life-cycle of infection, antibody detection, and likely immunity to COVID-19 [10]. A related challenge is the *quality* of the testing: test *sensitivity* (% positive detection for the right antibodies, so high sensitivity means few false positives) and *specificity* (% negatives correctly detected, so high specificity means few false negatives) are undergoing great scrutiny even as we write this [11], and are naturally a matter of concern, because they must be sufficiently high to make the approach worthwhile. In the meantime, our research aims to find an approach to achieve highly robust certification, so that it is ready to deploy as-and-when the ongoing biological research satisfies the necessary quality criteria.

II. Methods

A. The design of robust privacy

Several important guidelines concerning privacy were set out by the Sovrin Foundation, a nonprofit organisation with over 70 corporate partners including IBM, Cisco and others, which has the aim of 'driving greater interoperability and a new trust model for securely sharing private information' [12]. We adopt a variation of the three principles set out in the Sovrin.org White Paper [13], modifying their item 2 as shown below.

1) Pairwise-unique DIDs and public keys

As Sovrin.org explains, *'Imagine that when you open a new account with an online merchant, instead of giving them a credit card number or phone number, you gave them a DID created just for them. They could still use this DID to contact you about your order, or to charge you a monthly subscription, but not for anything else. If* […] *your DID were compromised in any way, you would just cancel it and give them a new one—without affecting any other relationship.* [consequently…] *a pairwise-pseudonymous DID is not worth stealing.'* [13]

2) Minimum and Encoded Data Storage / User's Choice

According to [13], *no* private data should be stored on the ledger, even in hashed form, to make it future-attack-proof. Sovrin accepts, as do we, the need for pseudonymous identifiers (DIDs), pseudonymous public keys, and agent addresses (e.g. the mobile phone app endpoints) to be stored in a decentralized ledger, but in addition we offer the user a *choice* regarding whether and where to host personal information (mobile phone, favorite cloud provider, or both), plus the barest minimum for verification purposes, namely *hashes* (irreversible encodings) of private data. This has the following benefits:

- Serves as a user-storage 'vault' for later recovery in case of loss.
- This 'vault' (i.e. the Solid Pod) can reside on the user's phone, or on a favorite cloud provider, or both — it is always the user's choice.
- To facilitate later independent verification, it uses a blockchain with distributed nodes run by a Consortium of trusted providers so that there is neither a single point of failure nor a single 'owner' even of the hash of the certificate.

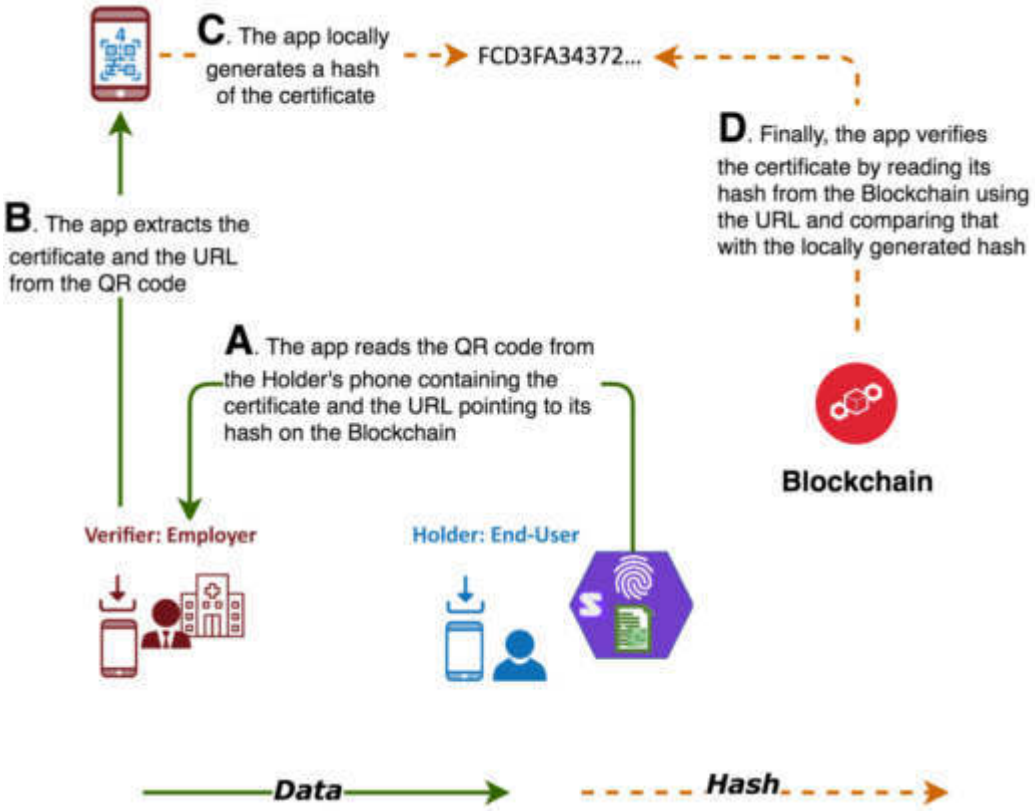


Fig. S1. Verification: main dataflows.

- Even so, it only stores a hash on the Consortium blockchain — a non-reversible but provably correct encoding of the certificate rather than the certificate itself.

This is a powerful privacy-preserving and tamper-proof approach that we call Minimum and Encoded Data Storage / User's Choice. Verborgh [14] has a deeper discussion of the nature and importance of these types of emerging paradigm shifts.

3) Selective disclosure

It is essential that users (certificate Holders) should only have to reveal just the portions of their own personally-held private data that are relevant to specific transactions (e.g. proving that you are 18 years of age or older, in order to make certain purchases or access certain locations, but without revealing your actual age or date of birth). This is made possible by the technology known as *cryptographic zero knowledge proofs* [15–17], so named because they provide, to the Verifier who wishes to know, proof of something specific (such as 'Age ≥ 18'), but with the Verifier having no knowledge of any other details, in this case actual age or date of birth. The 'secret sauce' of zero knowledge proofs, as illustrated in [16], [17], is that a mathematical function works through a proof of some fact (such as age being greater than or equal to X, or the existence of a certain credential), in such a way that the actual steps involved in executing the proof only reach a positive outcome if the fact is true (for example, the positive outcome may require a certain number of steps to execute): so the proof is valid, but still only indirect (e.g. counting the steps executed) without touching the raw data [15], [16].

B. Verification and implementation details

This section describes the operations that underpin the functioning of *verification,* as well as the overall implementation infrastructure and mobile phone app.

1) Verification

The process of verifying a certificate is an on-demand action. A Verifier cannot validate a certificate unless requested. It requires a Holder to go to a Verifier for this purpose. A Verifier can be an employer or other individual or organisation to whom the Holder wants or needs to present the certificate. Fig. S1 shows the main data flows involved in Verification.

In Fig. S1, we see that once requested, at (A), the app reads the QR code from the Holder's phone. This QR code (which is generated from the data that itself is stored in the Solid Pod) has two components: the certificate and a URL pointing to the hash on the blockchain. At (B), the app extracts these components and at (C) locally generates a temporary hash of the certificate. Finally (D), the app fetches the hash stored on the blockchain and compares it with the local hash. The

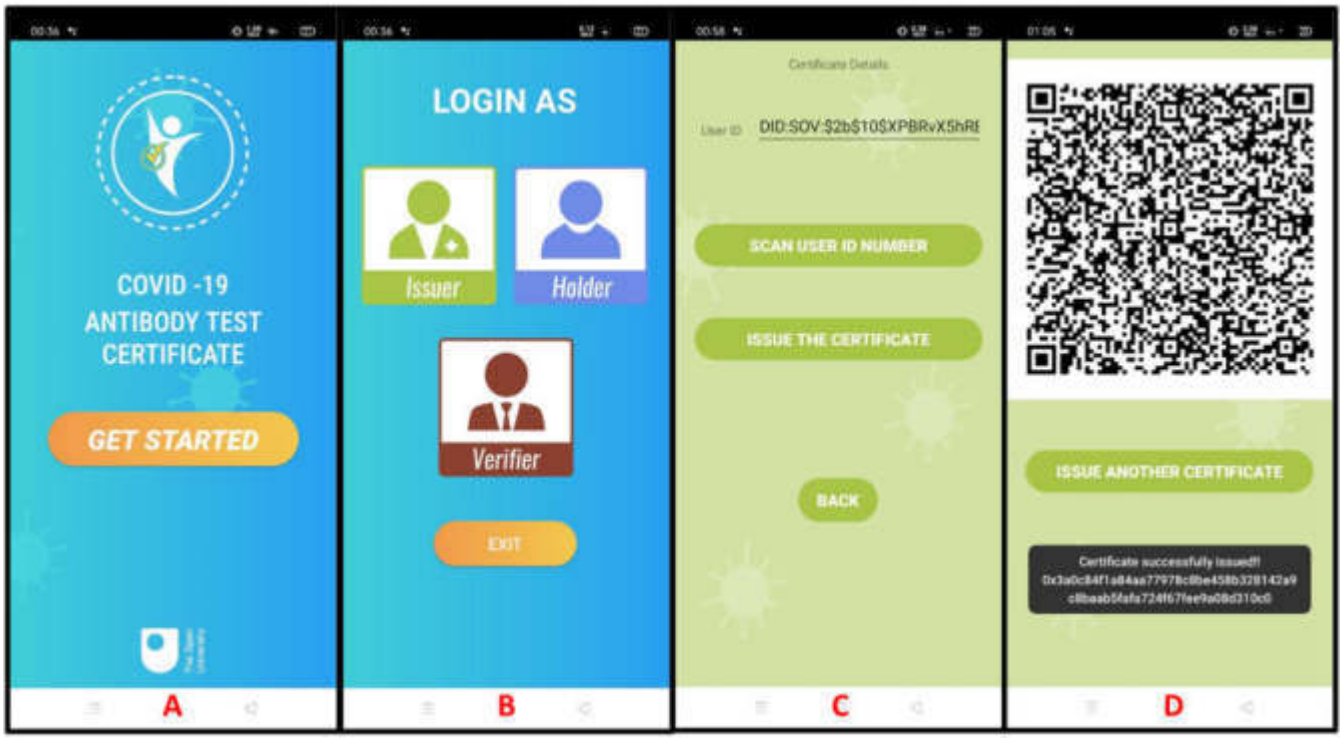


Fig. S2. Representative screen shots of the running mobile app showing (A) home screen, (B) multiple routes for login for the three main roles, just about to tap on 'Issuer', (C) about to issue the certificate having already scanned the user's ID number, displayed at the top, (D) certificate QR code, ready to be scanned by the Holder's mobile phone app.

matching of the hashes indicates the validity and the authenticity of the certificate stored in the Solid Pod of the Holder. At the same time, the physical identity of the Holder can be confirmed by the Verifier via the Holder's photo ID which will already have been 'burned' into the mobile phone app certificate. The digital identity of the Holder can be confirmed by verifying the Verifiable Credential (embedded in the certificate) based on the relevant Holder DID.

2) The functional infrastructure

The components of our implementation communicate with each other via current Web standards — Hypertext Transfer Protocol Secure (HTTPS), RDF (primarily in the JSON-LD format), Verifiable Credentials, and Decentralized Identifiers — and via blockchain protocols (specifically, Ethereum protocols). The volumes of data and computational requirements are typically small and can be handled by a mobile device (full blockchain nodes are an exception, due to the potential size of the full chain data).

The main software functions required by the implementation are as follows:

Generate QR codes: Implemented using standard libraries to generate QR codes for identity and immunity certificates.

Generate hashes: Using standard libraries, certificates are transformed into a canonical RDF format before hashing, in order to ensure robust reproducibility of hashes, for verification.

Communicate with Blockchain: The Parity library is used to communicate with our Consortium blockchain. A light client library can handle read/write interactions with the blockchain without requiring a phone to maintain a full copy of the blockchain.

Communicate with Solid Pods: Communication with Solid takes place using the Solid REST API [18], to read and write personal data regarding the Holder to and from their Solid Pod with user permission.

Manage Issuer and Holder Credentials: Issuer and Holder credentials are stored in public/private key wallets containing DIDs. The authorization for an Issuer to create certificates can be represented as a Verifiable Credential issued by the relevant regulatory authority to the Issuer, which any participating party can verify. Currently we use Streetcred ID [19] to generate DIDs for the Issuers, Holders and Certificates.

Generate Verifiable Credentials: Certificates are created at issue time, and their contents asserted as the Claim elements in Verifiable Credentials to be stored in the Holder's Solid Pod, with metadata describing the relevant blockchain records forming the Proof. This provides a sharable data structure which permits anyone to check its authenticity.

3) The mobile phone app

Fig. S2 shows representative screen shots of the mobile phone app, which provides all the necessary UI elements for the Issuer, Holder and Verifier to perform their actions. At the time of writing, the main functionalities of the mobile phone app include the ability to scan and generate QR codes and generate hashes for text and images. For the QR code scan and generate functions to work, the mobile phone app is packed with necessary libraries to support QR code functions and only works on smartphones with built-in camera functionality. The mobile phone app also contains the hashing libraries. As the mobile phone app needs to communicate with a server, an active internet connection is necessary for HTTPS server calls.

For speed of implementation for the current prototype, a Node.js Express server does all the heavy lifting for the app, with the functionalities explained above. This is a temporary solution, however, given the urgency of the current situation.

C. Scenario variations

Throughout the paper we have focused on a scenario involving 'On-Site Test for Antibodies + Issuance of Digital Certificate Including Photo ID', but there are some key variations easily incorporated into our design, namely (i) 'Issuing Digital Certificate Without Photo ID', (ii) 'Issuing Paper Certificate', (iii) 'Off-Site Testing Via External Lab', and (iv) 'Vaccination + Certification', described in turn below.

1) Variation 1: Issuing Digital Certificate Without Photo ID

In our scenario in the main paper, Fig. 2, the Issuer (Pharmacy) needs to authenticate that the Holder is who they say they are, and thus requests that the Holder display both a physical ID, such as a Driving License or a Passport and also a QR code which is scanned by the Issuer using the Issuer's mobile phone app. At this point there is in fact a choice: the Issuer can either (a) tap to accept the ID, in which case the Holder's photo will be 'burned' into the upcoming steps so that at the final step of verification, there will be no need to display the same physical ID, or (b) leave the Holder to display the physical ID once again at verification time.

If path (b) is chosen, there are other implications. At Verification time, to avoid someone else impersonating the Holder, the Holder must present not only the certificate, but also some proof of identity. In this variation, the Verifier can confirm the identity of the Holder by visually inspecting a physical ID card, and separately scanning the Holder's presented QR code (without ID incorporated) to verify just the certificate.

2) Variation 2: Issuing Paper Certificate

At step 2 of our main scenario, the test certificate can in fact be provided purely on paper, which has a dual purpose for the Holder: (a) a fallback in case of mobile phone failure; (b) a 'tech-agnostic' option which enables us to provide certification in a more appropriate manner for cases of socio-economic deprivation. This alternative means that some of the advantage of digital certification will be missing, but the use of printed QR codes which include the image of the Holder are still a useful advance over plain paper certificates. It also provides an alternative for individuals with little access to technology, but for whom a paper-based QR code printout can serve as a 'good enough' and 'effectively tamper-proof' certificate.

3) Variation 3: Off-Site Testing Via External Lab

It is likely that in many cases, particularly where large volume or high-quality serology testing is required, the Holder's blood sample has to be sent to a separate lab for processing. In this variation, the Pharmacist can issue a certificate that is flagged as being in a 'pending' state. The lab technician will also have a login to the app, via an additional button on the login screen, and see the list of pending certificates waiting for processing and approval. Once the lab technician has the results for a blood sample, the technician has to scan the QR code attached to the sample (this incorporates the Holder's digital ID, but with no personal information exposed to the lab technician) and then tap a button to issue the certified results to the relevant Holder. At this point, the Holder receives a notification with details of the certified result.

Note that the steps in this variation are just like the steps in 'supply chain provenance' gaining increasing traction in the blockchain 'farm-to-fork' world, typified by the IBM Food Trust [20]. Such efforts are also gaining ground in the area of vaccine supply chain provenance [21]. At each step of the chain, each participant adds the information pertinent to their niche, and digitally signs, while cross-checking automatically for authenticity of provenance at earlier steps in the supply chain. For blood samples, both the issuer and lab technician would add serial numbers and details for the blood sample and containers, syringes as necessary, and respective registration numbers / IDs for their roles as pharmacist and lab technician. At Verifier stage, and even for the lab test manufacturer, similar procedures would be deployed so that the integrity of the whole testing life cycle was ensured.

4) Variation 4: Vaccination + Certification

Although the most forward-looking variation (because vaccine research, development, approval, and deployment may take the longest [2]), it fits very smoothly into our existing scenario life cycles. Essentially, the Issuer as described throughout the main section of the paper becomes the person administering the vaccination jab (as opposed to taking a blood sample), and certifying that this has happened in the same manner described for the antibody test certificate. The approach to 'supply chain provenance' discussed in the preceding paragraph also applies to this variation, because the Issuer will have to include details of the vaccination source and batch within the certificate.

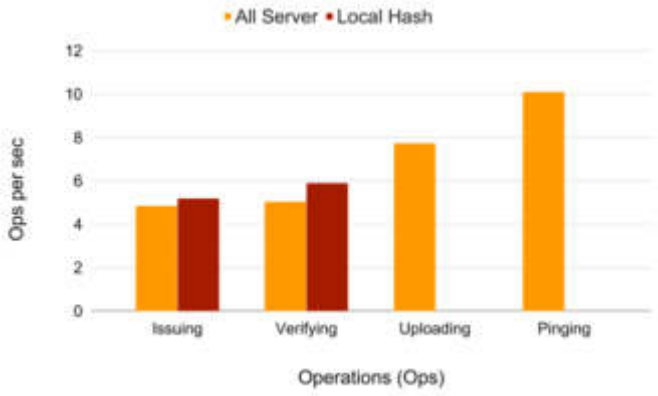


Fig. S3. Operations per second for Issuing (Server vs Local hashing), Verifying' (Server vs Local hashing), Uploading and (baseline) 'Pinging'.

III. Results

Fig. S3 shows the number of operations per second (Ops/sec) for Issuing, Verifying, Uploading, and Pinging, calculated from the slope of the 1-100 parallel operations timing described in the main paper. It demonstrates that while the current configuration is constant, our architecture can serve about five certificate issuances per second. For verifications, although we experimented with both local and server variants, in practice the hash will be generated locally (within the mobile phone app), giving us the ability to verify about six certificates per second with the existing infrastructure.

This observation shows us that the operations of Issuing and Verifying are twice as expensive as the simplest server ping. Except for some common infrastructure, the architecture is decentralized, i.e. one issuer issues (or verifier verifies) one certificate using one smartphone at a time even if we have hundreds of thousands of parallel requests. Even some commonly held infrastructure can be more distributed, such as the Solid pods. In this experiment, we used just one Solid cloud server for all requests, but in practice, users will have their Solid pod hosted on multiple servers or their own mobile phone. Therefore, if only those common and fixed infrastructures are scaled up, or load-balancing is applied to divert requests over multiple machines, performance time will significantly improve, with a concomitant speedup of Issuing and Verification not requiring architectural re-design.

IV. Discussion

A. More about rollout

The architecture presented in the main paper and Supplementary Material above is all built on standard library modules, and therefore joining a Consortium blockchain to help roll this out at scale is relatively straightforward, subject to suitable testing and deployment. The key hurdles are primarily Issuer credentials and the critical mass of the Consortium blockchain. In the case of Issuer credentials, we mentioned in section II.E.1 about Onboarding that we use two factor authentication for Issuers, and an API provided by the General Pharmaceutical Council to cross-check registration — this of course is subject to approval, and relevant discussions are already underway. As for the Consortium blockchain, a strong Consortium of industrial and academic partners needs to be established, after which addition of new members is just a matter of approval by the existing Consortium and the distribution of training and instruction materials. Alternatively, 'parallel' consortia can be created by cloning our approach. Given related ongoing work [22] that we mentioned in the main paper, we are optimistic that critical mass can be achieved.

B. Ethical considerations

It should be clear from the previous sections that the concepts underlying Verifiable Credentials and the Decentralized Verification of Data with Confidentiality are diametrically opposed to any kind of central data storage or 'Big Brother'-style snooping and data collection, and indeed provide excellent and agreed standards for avoiding such snooping and data collection. To be clear, in the approach we advocate in this paper,

> *Personally identifiable information is stored entirely under the Holder's control (on a mobile phone, on the Holder's cloud provider of choice, or both), and additionally for later verification purposes in minimal (a few bytes) encoded form (hash) on a Consortium blockchain. Moreover, the app allows the user selectively to present only the specific test result, with no other personal information revealed.*

How is it possible that no personal information is stored in a database? What about the certificate itself? That's the beauty of Verifiable Credentials, Zero Knowledge Proofs and our approach of Minimum and Encoded Data Storage / User's Choice: taken together, this combined approach offers cryptographically signed, verifiable, un-tamperable proof that the certificate being shown was really granted by a known testing authority to the person in question, even without showing the name, address, phone number or even UK NHS number of the person holding it.

Everything in this app is decentralized. Anyone wishing to abandon involvement in this kind of certification can just delete the Verifiable Credentials stored on their Solid Pods. There will be no records whatsoever, as if they had never been on the system. Deleting data on the Solid Pods will also turn the hashes on the blockchain into 'orphans' (no data pointing to the hash), i.e. the hashes will become meaningless: it is not possible to recover the original data from a hash.

This almost-too-good-to-be-true approach does raise a fresh concern, raised briefly in the main paper: the same techniques we are advocating seem to open up what we call the *'Private Verifiable Credentials Paradox'*: your digital mobile phone app certificate is so much more private and tamper-proof than the old paper or database versions that it *could* (deliberately or accidentally), be weaponized *for discrimination against your fellow citizens*. In other words, a potential problem, according

to critics, is not that the architecture is too weak, but that it is too strong.

Clearly, the more powerful methods of today and tomorrow have the potential to open up a Pandora's Box of Bad Use, if not by the modern democracies in which we may have grown up, then by *some* authority in another time or place - as the world has witnessed all too tragically in the past. We started this project with the noble aim of facilitating a way to get people back to work and heading towards recovery from the devastating impact of the Coronavirus Pandemic of 2019/2020. If COVID-19 antibodies can indeed be shown reliably to confer immunity, and the overwhelming support for the 'test-test-test' mantra of the World Health Organization continues to hold, then people *are* going to get tested, in overwhelming numbers, and certificates *are* going to be issued in one form or another.

But we are not adopting a 'give-up-and-accept-our-fate-in-the-hands-of-bad-actors' approach. Yes, a secure digital certificate could hypothetically be weaponized to a greater degree than a paper one, but the actual degree could be something of a mind-set illusion. *Any* certification method has such potential, and therefore, rather than casting the technology in terms of 'good vs evil' we think our approach is best considered as something that involves a trade-off between (a) the advantages of getting people back to work using good privacy-preserving fraud-prevention methods and (b) the disadvantages of discriminatory (mis)use of such methods. Our approach to this trade-off is strongly to nudge things towards (a), and therefore we propose the following concrete steps to achieve this:

- App usage should be strictly opt-in/optional: a paper certificate must always be allowed by default, just as with, say, train or airline tickets. This helps introduce the concept and technology in a gentle manner: people will ultimately decide what they prefer for themselves.
- Implementations must comply with UK NHS Information Governance (IG) guidelines [23], [24]. Compliance should in principle be straightforward, because (a) in our approach, personally identifiable information is stored entirely under the Holder's control, and additionally for later verification purposes in minimal hash-encoded form on a Consortium blockchain, and (b) the app allows the user selectively to present only the specific test result, with no other personal information revealed. Even so, the UK NHS IG documents provide a strong guiding framework for ensuring continuing compliance, particularly with respect to relevant EU GDPR requirements such as 'Right to erasure' and 'Right to data portability': our architecture by its very design avoids database storage of personally identifiable information, but oversight of possible misuse/abuse of this and related technologies needs to be maintained, as the next three bullet points suggest.
- COVID-19 Antibody Test Certificates should only be applied to workers in healthcare and other comparable key sectors, as defined by the appropriate UK Parliamentary process (for example, the list of key exceptions to mandatory business closure during the current pandemic was specified by the UK Ministry of Housing, Communities, and Local Government), with input from an Ethics Committee mentioned next.
- An Ethics Committee, comparable in scope and composition to the UK NHS Research Ethics Committees, should have oversight of actual deployment of the approach advocated herein.
- The approach should be reviewed on a 3-monthly basis.

In a timely and thoughtful analysis of the ethical complexities surrounding COVID-19 antibody test certificates, Persad and Emanuel [25] argue convincingly for the label 'immunity-based licenses' (rather than 'immunity passports') as a way to focus on the positive benefits granted to those who have been infected with COVID-19, without necessarily worsening the lives of those who have not been infected.

Ethical standards are challenging to uphold, but uphold them we must: we see a strong emphasis on ethics as the best way to negotiate a path towards a 'pandemic end game' in a manner acceptable to the widest possible audience.

V. Conclusions

Will such an app be suitable as part of a 'pandemic exit strategy' for helping get people back to work in key sectors? There are many issues to be addressed first, including the rigorous scrutiny and approval of antibody tests, likelihood and longevity of immunity, agreement concerning ethical oversight, and acceptance by the public. Our approach is intended to ensure that the procedures for creating tamper-proof, verifiable, privacy-preserving certificates are 'ready to go' while waiting for antibody/immunity tests to achieve the required state of robustness and acceptance. We believe that, just as with train e-tickets, end-users will 'vote with their feet' and deploy the app in large numbers once its benefits have been demonstrated. To take a stance against what we call the 'Pandora's Box of Bad Use', we proposed ethical guidelines at the end of the Discussion, which we believe are essential for the principled development and deployment of the prototype described in this paper.

References

[1] BBC News, "WHO head: 'Our key message is: test, test, test.'" [Online]. Available: https://www.bbc.co.uk/news/av/world-51916707/who-head-our-key-message-is-test-test-test [Accessed: Apr. 2, 2020].

[2] T. Thanh Le et al., "COVID-19 vaccine development landscape," *Nat Rev Drug Discov*. https://www.nature.com/articles/d41573-020-00073-5.

[3] A. Pethick, "Developing antibody tests for SARS-CoV-2," *Lancet*, vol. 395 (10230), pp. 1101–1102, Apr. 4, 2020. DOI: 10.1016/S0140-6736(20)30788-1

[4] BBC News, "'Immunity passports' could speed up return to work after Covid-19." [Online]. Available: https://www.theguardian.com/world/2020/mar/30/immunity-passports-

could-speed-up-return-to-work-after-covid-19 [Accessed: Apr. 2, 2020].
[5] The Guardian, "No 10 seeks to end coronavirus lockdown with 'immunity passports.'" [Online]. Available: https://www.theguardian.com/politics/2020/apr/02/no-10-seeks-to-end-covid-19-lockdown-with-immunity-passports [Accessed: Apr. 3, 2020].
[6] CNBC, "WHO officials say it's unclear whether recovered coronavirus patients are immune to second infection." [Online.] https://www.cnbc.com/2020/04/13/who-officials-say-its-unclear-whether-recovered-coronavirus-patients-are-immune-to-second-infection.html [Accessed: Apr. 13, 2020].
[7] The New York Times, "After Recovery From the Coronavirus, Most People Carry Antibodies." [Online]. Available: https://www.nytimes.com/2020/05/07/health/coronavirus-antibody-prevalence.html. [Accessed: May 11, 2020].
[8] A. Wajnberg, M. Mansour, E. Leven *et al.* "Humoral immune response and prolonged PCR positivity in a cohort of 1343 SARS-CoV 2 patients in the New York City region." *medRxiv*. May 2020:2020.04.30.20085613. doi:10.1101/2020.04.30.20085613
[9] NPR Radio/Web. If You Get Coronavirus And Recover, Do You Develop Immunity? [Online]. Available: https://www.npr.org/sections/goatsandsoda/2020/03/20/819038431/do-you-get-immunity-after-recovering-from-a-case-of-coronavirus. [Accessed: Apr. 14, 2020] .
[10] D. Male, J. Golding, and M. Bootman, "How Does The Human Body Fight A Viral Infection?" Open University, OpenLearn Course Module, Milton Keynes, UK, 2020. [Online]. Available: https://www.open.edu/openlearn/science-maths-technology/biology/how-does-the-human-body-fight-viral-infection [Accessed: Apr. 7, 2020].
[11] "Global Progress on COVID-19 Serology-Based Testing." Johns Hopkins Bloombert School of Public Health, Center for Health Security." [Online]. Available: https://www.centerforhealthsecurity.org/resources/COVID-19/serology/Serology-based-tests-for-COVID-19.html. [Accessed: May 11, 2020].
[12] "About Sovrin.org." [Online]. Available: https://sovrin.org/ [Accessed: Apr. 14, 2020]
[13] Sovrin.org, "A Protocol and Token for Self-Sovereign Identity and Decentralized Trust." [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf [Accessed: Apr. 14, 2020].
[14] R. Verborgh, "Paradigm shifts for the decentralized Web Online." [Online]. Available: https://ruben.verborgh.org/blog/2017/12/20/paradigm-shifts-for-the-decentralized-web/. [Accessed: Apr. 14, 2020].
[15] "Zero-knowledge proof." [Online]. Available: https://en.wikipedia.org/wiki/Zero-knowledge_proof [Accessed: Apr. 14, 2020].
[16] A. S. Delight, "Zero Knowledge Proof of Age Using Hash Chains." [Online]. Available: https://www.stratumn.com/thinking/zero-knowledge-proof-of-age-using-hash-chains/ [Accessed: Apr. 14, 2020].
[17] S. Angel and M. Walfish, "Verifiable Auctions for Online Ad Exchanges," *ACM SIGCOMM*, vol. 13. [Online]. Available: https://cs.nyu.edu/~mwalfish/papers/vex-sigcomm13.pdf [Accessed: Apr. 14, 2020].
[18] "Solid HTTPS REST API Spec." [Online]. Available: https://github.com/solid/solid-spec/blob/master/api-rest.md [Accessed: Apr. 14, 2020].
[19] "Getting Started with Streetcred ID." [Online]. Available: https://docs.streetcred.id/docs/getting-started [Accessed: Apr. 14, 2020].
[20] "IBM Food Trust - United Kingdom | IBM." [Online]. Available: https://www.ibm.com/uk-en/blockchain/solutions/food-trust. [Accessed: 13-May-2020].
[21] B. Yong, J. Shen, X. Liu, F. Li, H. Chen, and Q. Zhou, "An intelligent blockchain-based system for safe vaccine supply and supervision," Int. J. Inf. Manage., vol. 52, p. 102024, Jun. 2020. doi:10.1016/j.ijinfomgt.2019.10.009
[22] Coindesk. "COVID-19 'Immunity Passport' Unites 60 Firms on Self-Sovereign ID Project." [Online]. Available: https://www.coindesk.com/covid-19-immunity-passport-unites-60-firms-on-self-sovereign-id-project [Accessed: Apr. 19, 2020].
[23] "NHS Information Governance." [Online]. Available: https://www.england.nhs.uk/ig/about/ [Accessed: Apr. 9, 2020].
[24] "About the NHS IG Toolkit." [Online]. Available: https://www.igt.hscic.gov.uk/resources/About%20the%20IG%20Toolkit.pdf [Accessed: Apr. 9, 2020].
[25] G. Persad and E. Emanuel, "The Ethics of COVID-19 Immunity-Based Licenses ('Immunity Passports')." *JAMA.* May 6, 2020. [Online]. Available: https://dx.doi.org/10.1001/jama.2020.8102 [Accessed: May 20, 2020].

An official EU website

How do you know?

European Commission

EU Digital COVID Certificate

The EU Digital COVID Certificate Regulation entered into application on 01 July 2021. EU citizens and residents will now be able to have their Digital COVID Certificates issued and verified across the EU.

Learn how to get the certificate from your national health authority by selecting your country on the interactive map below.

What is the EU Digital COVID Certificate?

An EU Digital COVID Certificate is a digital proof that a person has either

- been vaccinated against COVID-19
- received a negative test result or
- recovered from COVID-19

Key features of the certificate

- Digital and/or paper format
- with QR code
- free of charge
- in national language and English
- safe and secure
- valid in all EU countries

How can citizens get the certificate?

National authorities are in charge of issuing the certificate. It could, for example, be issued by test centres or health authorities, or directly via an eHealth portal. Information on how to get the certificate should be provided by the national health authorities.

The digital version can be stored on a mobile device. Citizens can also request a paper version. Both will have a QR code that contains essential information, as well as a digital signature to make sure the certificate is authentic.

Member States have agreed on a common design that can be used for the electronic and paper versions to facilitate the recognition.

Select your country on the interactive map below to learn how to get the certificate from your national health authority.

In technical testing phase to connect	Technically ready to connect	Effectively connected

An official EU website How do you know?

Ukraine

In technical testing phase to connect:	Done
Technically ready to connect:	Done
Effectively connected:	Yes

Vatican City

In technical testing phase to connect:	Done
Technically ready to connect:	Done
Effectively connected:	Yes

How will it help free movement?

The EU Digital COVID Certificate will be accepted in all EU Member States. It will help to ensure that restrictions currently in place can be lifted in a coordinated manner.

When travelling, the EU Digital COVID Certificate holder should in principle be exempted from free movement restrictions: Member States should refrain from imposing additional travel restrictions on the holders of an EU Digital COVID Certificate, unless they are necessary and proportionate to safeguard public health.

In such a case – for instance as a reaction to new variants of concern – that Member State would have to notify the Commission and all other Member States and justify this decision.

How will the certificate work?

How do you know?

The EU Digital COVID Certificate contains a QR code with a digital signature to protect it against falsification.

When the certificate is checked, the QR code is scanned and the signature verified.

Each issuing body (e.g. a hospital, a test centre, a health authority) has its own digital signature key. All of these are stored in a secure database in each country.

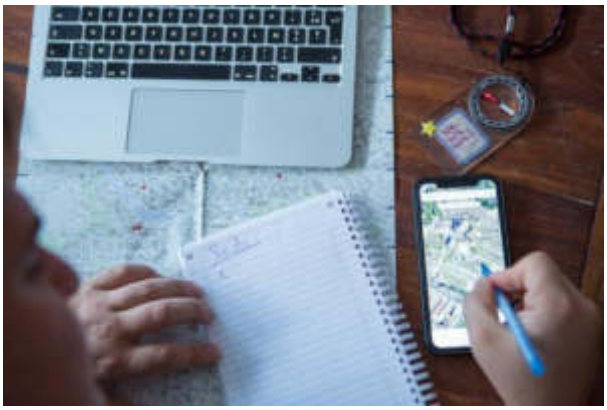
The European Commission has built a gateway through which all certificate signatures can be verified across the EU. The personal data of the certificate holder does not pass through the gateway, as this is not necessary to verify the digital signature. The European Commission also helped Member States to develop national software and apps to issue, store and verify certificates and supported them in the necessary tests to on-board the gateway.

Will citizens who are not yet vaccinated be able to travel to another EU country?

Yes. The EU Digital COVID Certificate should facilitate free movement inside the EU. It will not be a pre-condition to free movement, which is a fundamental right in the EU.

The EU Digital COVID Certificate will also prove the results of testing, which is often required under applicable public health restrictions. The certificate is an opportunity for Member States to adjust the existing restrictions on public health grounds.

An official EU website



How do you know?

The recommendation on coordinating free movement restrictions in the EU was amended mid-June with a view to the holiday season, further clarifying exemptions for fully vaccinated and recovered persons, efforts to ensure family unity (exempting children traveling with their parents from quarantine, if parents are exempted) and the updated colour-coding of the ECDC map.

Does it matter which vaccine citizens received?

Vaccination certificates will be issued to a vaccinated person for any COVID-19 vaccine.

When it comes to waiving free movement restrictions, Member States will have to accept vaccination certificates for vaccines which received EU marketing authorisation. Member States may decide to extend this also to EU travellers that received another vaccine.

Fully vaccinated persons with the EU Digital COVID Certificate should be exempted from travel-related testing or quarantine 14 days after having received the last dose of a COVID-19 vaccine approved for the entire EU. The same is true for recovered persons with the certificate.

What about tests?

Persons with a negative test in the EU Digital COVID Certificate format should be exempted from possible quarantine requirements, except when they come from areas heavily affected by the virus. The Member States agreed on a standard validity period for tests: 72 hours for PCR tests and, where accepted by a Member State, 48 hours for rapid antigen tests.

What data does the certificate include? Is the data safe?

The EU Digital COVID Certificate contains necessary key information such as name, date of birth, date of issuance, relevant information about vaccine/ test/recovery and a unique identifier. This data remains on the certificate and is not stored or retained when a certificate is verified in another Member State.

The certificates will only include a limited set of information that is necessary. This cannot be retained by visited countries. For verification purposes, only the validity and authenticity of the certificate is checked by verifying who issued and signed it. All health data remains with the Member State that issued an EU Digital COVID Certificate.

Questions and answers about the EU Digital COVID Certificate

Questions and answers on the latest update regarding the coordination of COVID-related measures restricting free movement in the EU

Re-open EU: up-to-date information on travel and health measures

Find up-to-date information on travel and health measures in European countries, including on quarantine and testing requirements for travellers, to help you exercise your right to free movement. The information is updated frequently and available in 24 languages. This should help you plan your travel in Europe, while staying safe and healthy.

Visit Re-open EU

Timeline

27 January 2021

Guidelines laying out interoperability requirements of digital vaccination certificates were adopted, building on discussion held between the Commission and Member

States in the eHealth Network since November 2020.

17 March 2021

The Commission proposed a legislative text establishing a common framework for an EU certificate.

14 April 2021

The Council adopted its mandate to start negotiations with the European Parliament on the proposal.

22 April 2021

Member States' representatives in the eHealth Network agreed on guidelines describing the main technical specifications for the implementation of the system. This was a crucial step for the establishment of the necessary infrastructure at EU level.

7 May 2021

The Commission started the pilot test of the EU interoperability infrastructure (EU Gateway) that will facilitate the authentication of the EU Certificates.

20 May 2021

The European Parliament and the Council agreed on the EU Digital COVID Certificate.

1 June 2021

EU Gateway (interconnection of national systems) goes live.

1 - 30 June 2021

Warm-up phase: Member States can launch the certificate on a voluntary basis provided they are ready to issue and verify certificates, and have the necessary legal base in place.

mid-June 2021

Revised Council Recommendation on travel within the EU.

1 July 2021

The EU Digital COVID Certificate enters into application throughout the EU.

1 July - 12 August 2021

Phase-in period: If a Member State is not yet ready to issue the new certificate to its citizens, other formats can still be used and should be accepted in other Member States.

Documents

Commission Implementing Decision (EU) on the equivalence of COVID-19 certificates issued by North Macedonia

19 August 2021

English

Url link - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D1381

Available languages (23)

Commission Implementing Decision (EU) on the equivalence of COVID-19 certificates issued by Ukraine

19 August 2021

English

Url link - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D1380

Available languages (23)

Commission Implementing Decision (EU) on the equivalence of COVID-19 certificates issued by Turkey

19 August 2021

English

Url link - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D1382

Available languages (23)

Digitales COVID-Zertifikat der EU: EU-Gateway startet in sieben Ländern einen Monat früher als geplant

Brüssel, 1. Juni 2021

Heute ist ein weiterer wichtiger Meilenstein des digitalen COVID-Zertifikats der EU erreicht, denn das technische System auf der EU-Ebene, mit dem die Zertifikate sicher und unter Wahrung des Datenschutzes geprüft werden können, geht online. Das EU-Zertifikat wurde von der Kommission vorgeschlagen, damit wir im Sommer wieder gefahrlos reisen können. Es ist kostenlos, sicher und für alle zugänglich. Bei dem Zertifikat, das in elektronischer Form und auf Papier ausgestellt werden kann, handelt es sich um einen Nachweis, dass die Inhaberinnen und Inhaber gegen das Coronavirus geimpft sind, negativ getestet wurden oder von COVID-19 genesen sind.

Nachdem das Europäische Parlament und der Rat am 20. Mai eine politische Einigung über die Verordnung mit den Einzelheiten für das Zertifikat erzielt haben, geht das technische Herzstück des EU-Systems heute online. Über dieses in nur zwei Monaten errichtete EU-Gateway können die im QR-Code der Zertifikate enthaltenen Sicherheitsfunktionen geprüft werden. So können sich Bürger und Behörden vergewissern, dass die Zertifikate echt sind. Dabei werden keine personenbezogenen Daten weitergegeben oder gespeichert. Mit der heutigen Inbetriebnahme des Gateways sind die Vorarbeiten auf EU-Ebene nun abgeschlossen.

Seit dem 10. Mai haben bereits 22 Länder das Gateway erfolgreich getestet. Die Verordnung gilt zwar erst ab dem 1. Juli, aber alle Mitgliedstaaten, die die technischen Tests absolviert haben und Zertifikate ausstellen und prüfen können, können das System nun auf freiwilliger Basis nutzen. Sieben Mitgliedstaaten – **Bulgarien, Dänemark, Deutschland, Griechenland, Kroatien, Polen** und **Tschechien** – haben beschlossen, sich schon heute an das Gateway anzuschließen und damit zu beginnen, EU-Zertifikate auszugeben, andere wiederum wollen das digitale COVID-Zertifikat der EU erst dann einführen, wenn alle Funktionen auf der nationalen Ebene geschaffen wurden. Daher werden in den kommenden Tagen und Wochen mehr Länder hinzukommen. Über den aktuellen Stand informiert eine eigens eingerichtete Website.

Nächste Schritte

Die politische Einigung vom 20. Mai muss nun vom Europäischen Parlament und vom Rat noch förmlich angenommen werden. Die Verordnung tritt am 1. Juli in Kraft, wobei den Mitgliedstaaten, die noch mehr Zeit brauchen, bis sie Zertifikate ausstellen können, eine Übergangsfrist von sechs Wochen eingeräumt wird. Parallel dazu wird die Kommission die Mitgliedstaaten weiterhin technisch und finanziell dabei unterstützen, sich an das Gateway anzuschließen.

Stellungnahmen aus dem Kommissionskollegium

Der für den Binnenmarkt zuständige EU-Kommissar Thierry **Breton** erklärte: *„Die heutige Inbetriebnahme des Gateways ist ein wichtiger Schritt, der es den Mitgliedstaaten ermöglicht, mit der Nutzung des Gateways und der Ausstellung von digitalen COVID-Zertifikaten der EU zu beginnen. Sieben Mitgliedstaaten sind ein guter Anfang. Ich appelliere an die anderen, sich möglichst bald anzuschließen. Wenn die Vorbereitungen rechtzeitig abgeschlossen werden, kann das System ab dem 1. Juli, ab dem die vorgeschlagene Verordnung gilt, uneingeschränkt in Betrieb gehen, und die EU wird bis zum Sommer wieder offen sein.*"

Stella **Kyriakides**, EU-Kommissarin für Gesundheit und Lebensmittelsicherheit, fügte hinzu: *„Das digitale COVID-Zertifikat der EU zeugt von dem Mehrwert elektronischer Gesundheitsdienste für unsere Bürgerinnen und Bürger. Die Mitgliedstaaten sollten unbedingt in den kommenden Wochen ihre nationalen Systeme zur Ausstellung, Speicherung und Prüfung von Zertifikaten fertigstellen, damit das System rechtzeitig zur Ferienzeit funktionsfähig ist. Die EU-Bürgerinnen und -Bürger freuen sich darauf, wieder zu reisen, und möchten dies in aller Sicherheit tun können. Das EU-Zertifikat trägt entscheidend dazu bei.*"

Didier **Reynders**, Kommissar für Justiz, erklärte hierzu: *„Mit dem digitalen COVID-Zertifikat der EU können die europäischen Bürgerinnen und Bürger wieder frei und sicher reisen. Es zeugt von Europas*

technologischer Spitzenposition unter voller Wahrung unserer Werte und Grundsätze – Datenschutz, Inklusion und Verhältnismäßigkeit. Es ist wichtig, dass alle Mitgliedstaaten die nächsten Wochen nutzen, um die Vorbereitungen abzuschließen, damit das System ab dem 1. Juli voll funktionsfähig ist."

Hintergrund

Am 17. März 2021 legte die Europäische Kommission einen Vorschlag für ein COVID-Zertifikat der EU vor, damit EU-Bürgerinnen und -Bürger ihr Recht auf Freizügigkeit in der EU während der Pandemie auf sichere Weise ausüben können. Am 20. Mai erzielten das Europäische Parlament und der Rat eine vorläufige Einigung über den Vorschlag.

Parallel zum Gesetzgebungsverfahren hat die Kommission mit Vertretern der Mitgliedstaaten im eHealth-Netz, zu dem sich für elektronische Gesundheitsdienste zuständige nationale Behörden freiwillig zusammengeschlossen haben, intensiv an der technischen Umsetzung gearbeitet. Am 21. April wurden Leitlinien mit technischen Spezifikationen angenommen, die auf im Januar verabschiedeten und im März aktualisierten Leitlinien aufbauen. Am selben Tag wurde auch der im März gebilligte Entwurf eines Vertrauensrahmens vorgelegt. Außerdem wurde mit den Mitgliedstaaten ein Gestaltungsmuster entwickelt, damit die in Papierform ausgestellten COVID-Zertifikate der EU leichter erkennbar sind.

Das EU-Gateway wurden von T-Systems und SAP entwickelt und ist im Rechenzentrum der Kommission in Luxemburg angesiedelt. Über das Gateway können die digitalen Signaturen in den QR-Codes der Zertifikate geprüft werden, ohne dass personenbezogene Daten weitergegeben oder gespeichert werden. Die erforderlichen Signaturschlüssel sind auf Servern auf nationaler Ebene hinterlegt. Über das Gateway können nationale Apps und Systeme in der ganzen EU zu Prüfzwecken auf diese Schlüssel zugreifen.

Die Kommission hat auch Referenzsoftware und Apps für die Ausstellung, Speicherung und Prüfung der Zertifikate entwickelt, um die Einführung in den Mitgliedstaaten zu erleichtern. Die Referenzsoftware und Apps wurden auf GitHub veröffentlicht und werden von 12 Mitgliedstaaten genutzt.

Die neuesten von den Mitgliedstaaten übermittelten Informationen über die Maßnahmen im Zusammenhang mit dem Coronavirus sowie Reisebeschränkungen sind über die Plattform „Re-open EU" abrufbar.

Weitere Informationen

Vorschläge für ein digitales grünes Zertifikat zur Erleichterung der Freizügigkeit in der EU

Vorschlag für ein digitales grünes Zertifikat für Drittstaatsangehörige, die sich rechtmäßig in einem Mitgliedstaat aufhalten oder dort wohnen

Vorschlag der Kommission zur Änderung der Empfehlung des Rates vom 13. Oktober 2020 für eine koordinierte Vorgehensweise bei der Beschränkung der Freizügigkeit aufgrund der COVID-19-Pandemie

Fragen und Antworten (aktualisiert)

Factsheet

Website

Neues Videomaterial

Video über das digitale COVID-Zertifikat der EU

Re-open EU

IP/21/2721

Kontakt für die Medien:

Christian WIGAND (+32 2 296 22 53)
Johannes BAHRKE (+32 2 295 86 15)
Katarzyna KOLANKO (+ 32 2 296 34 44)
Charles MANOURY (+32 2 291 33 91)

Kontakt für die Öffentlichkeit: Europe Direct – telefonisch unter 00 800 67 89 10 11 oder per E-Mail

Related media


Urban mobility - Tram

What is CoWIN and what you need to register on the app for Covid vaccine shot

The CoWIN app is not yet public, but has utilities for every level of user — from civil servants to public health system managers, vaccinators, and potential beneficiaries.

ABANTIKA GHOSH

5 January, 2021 8:00 am IST

A health worker getting the vaccine during a dry run in Delhi | Representational Photo: Manisha Mondal | ThePrint

New Delhi: As India prepares to roll out what Prime Minister Narendra Modi has called the world's largest Covid-19 vaccination programme, the Covid Vaccine Intelligence Network (CoWIN) system is emerging as its backbone.

The initial target is to vaccinate 30 crore people, for which the first four target groups have already been identified and defined. For these groups, the vaccination process will start when they receive a message on their mobile phones — first about their inclusion in the list of priority beneficiaries, and subsequently, about the date and time of vaccination.

However, there will also soon be an option on the app, as and when it goes public, to self-register, along with the relevant identification and other documents. That is the eventual plan.

ThePrint brings you insight into this app and the registration process.

Also read: Strict follow-up, informed consent from recipients — conditions set for cleared Covid vaccines

---

About CoWIN

For several years now under its universal immunisation programme, India has been using a vaccine intelligence system called eVIN (electronic vaccine intelligence network), which provides real-time feedback of vaccine stocks, power outages, temperature fluctuations etc. CoWIN is essentially an extension of eVIN. It is a cloud-based IT solution for planning, implementation, monitoring, and evaluation of Covid-19 vaccination in India.

It has utilities for every level of user — from civil servants in national and state capitals to public health system managers, vaccinators and, at a later stage, potential beneficiaries.

According to the operational guidelines for Covid-19 vaccination prepared by the Ministry of Health: "The system allows for creation of users (admins, supervisors, vaccinators), registration of beneficiaries (bulk upload and individual registration), facilities/planning unit and session sites followed by planning and scheduling sessions and implementation of vaccination process."

The guidelines add: "CoWIN system on a real time basis will track not only the beneficiaries but also the vaccines, at national,

state and district level. This will allow the system to monitor the utilisation, wastage, coverage of Covid-19 vaccination at national, state, district and sub-district level."

Every detail, from the sites where vaccinations are carried out to the number of beneficiaries and even the batch number, doses per vial and schedule of the vaccine, will be uploaded on the digital platform.

Initial registration only through districts

Once the complete list of healthcare workers and frontline workers is received — these are the first two priority groups for vaccination — their registration will be done through bulk upload of data by district authorities. Each facility that is a hospital or a clinic will also add the details of individuals working with them. The software will check for errors or duplications, and then allow upload of only the verified entries.

Vaccinators will then create session sites with the relevant details and the number of beneficiaries that will get the vaccines. This will generate SMSes that beneficiaries will get, informing them of the time and place. Once vaccination is done, the vaccinators will again upload that information. If a beneficiary fails to turn up, they can be slotted for a later date.

Self-registration will come later

The option of self-registration will be available only at a later date, once the initial groups have been completed. People willing to get vaccinated can register themselves by uploading any one of 12 identification documents. These are:

– Aadhaar card

– Driving licence

– Health insurance smart card issued under the scheme of Ministry of Labour

– MGNREGA job card

– Official identity card issued to MPs/MLAs/MLCs

– PAN card

– Passbook issued by bank/post office

– Passport

– Pension document

– Service identity card issued to employees by central/state govt/PSUs/public limited companies

– Smart card issued by Registrar General of India under National Population Register

– Voter ID card

A person will have three authentication options to choose from — biometric, OTP-based and authentication using date of birth etc. If the last is successful, a green tick will appear against the entry.

"Self-registration module will be made available in the later phases of implementation," say the operational guidelines.

Also read: Everything you need to know about Covaxin, India's controversial Covid vaccine candidate

---

Pakistan and China are preparing for a Taliban govt they don't trust. So should India

Pakistan's interest in an influential role for the Haqqani group in a Taliban government is on account of its anti-Indian agenda. We must be prepared.

ThePrint

IVRS - 1921

Aarogya Setu

General

What is Aarogya Setu?

2. Why should I use Aarogya Setu?

3. How do I get started with Aarogya Setu?

4. Is Aarogya Setu available for feature phones and landlines

5. What are the key features of Aarogya Setu?

The key features of Aarogya Setu include:

- Automatic contact tracing using Bluetooth
- Self-Assessment test based on ICMR guidelines
- Risk Status of User
- Updates, advisory and best practices related to COVID-19
- Geo-location based COVID-19 statistics
- Nationwide COVID-19 statistics
- Emergency COVID-19 Helpline contacts
- List of ICMR approved Labs with COVID-19 testing facilities
- e-Pass integration
- Support for 12 Languages

6. How does contact tracing work on Aarogya Setu?

7. How does the self-assessment test on the Aarogya Setu app work?

8. How does Aarogya Setu calculate my risk of infection?

9. What do the various colours of the Home screen on Aarogya Setu app signify?

10. How does Aarogya Setu know if someone has turned COVID-19 positive?

11. If my neighbour tests positive for COVID-19, will the fact that my app has connected with his on Bluetooth mean that I am marked as positive for COVID-19 even if I have remained indoors and never

IVRS - 1921

Aarogya Setu

13. Is Aarogya Setu available in multiple languages?

14. Where can I read the Terms of Service and Privacy Policy of Aarogya Setu?

15. How do I share feedback and suggestions for Aarogya Setu?

16. The App is showing "You are Safe" on my mobile, but it is showing "Low risk of infection" on my parent's phone. We are staying in the same house and we have not gone out of our house during the last 2 weeks. How's this possible that it shows different risk levels for different members of the family?

17. I'm not COVID-19 positive, but the App is showing that I'm COVID-19 positive. My mobile number was used by my relative during his COVID-19 Sample testing, He has tested positive for COVID-19. What should I do if the App is showing a wrong COVID-19 status.

Privacy

Technical

Troubleshooting

Content owned, updated and maintained by the MyGov, MeitY. Aarogya Setu Platform is designed, developed and hosted by National Informatics Centre, Ministry of Electronics & Information Technology, Government of India.

Last Updated:July 17, 2020 at 10:37 am - wwwaarogyasetu-w5r97

September 8, 2021 | 2:39 pm

COVID-19 Vaccines

On August 23, the FDA announced the full approval of the Pfizer-BioNTech vaccine for the prevention of COVID-19 disease in individuals age 16 and older. Read more.

DETAILS >

GOVERNOR
KATHY HOCHUL

MARCH 26, 2021 | Albany, NY

Governor Cuomo Announces Launch of Excelsior Pass to Help Fast-Track Reopening of Businesses and Entertainment Venues Statewide

CORONAVIRUS (/KI /CORONAVIRUS) HEALTH (/KI /HEALTH) PUBLIC SAFETY (/KI /PUBLIC-SAFETY) TECHNOLOGY (/KEYWORDS /TECHNOLOGY)

Digital Pass Offers Free, Voluntary Way to Share COVID-19 Vaccination or Negative COVID-19 Test Status in Accordance with New York State Guidelines

Proven, Secure Technology Developed in Partnership with IBM Following Successful Pilot

As Part of Initial Launch, Excelsior Pass Can Be Used by Participating New Yorkers at Theaters,

Major Stadiums and Arenas, Weddings Receptions, Catered Events & Other Events in Accordance with New York State Guidelines

Madison Square Garden and Times Union Center to Implement Excelsior Pass; Additional Locations Will Begin Utilizing this Platform as Program Expands

Interested New Yorkers Can Opt In to Use Excelsior Pass and Learn More Here; Interested Businesses Can Opt In and Learn More Here

Images of Excelsior Pass are Available Here

Initiative First Announced in Governor's 2021 State of the State Address

Governor Andrew M. Cuomo today announced the launch of Excelsior Pass — a free, voluntary platform developed in partnership with IBM, which utilizes proven, secure technology to confirm an individual's recent negative PCR or antigen test result or proof of vaccination to help fast-track the reopening of businesses and event venues in accordance with New York State Department of Health guidelines. Similar to a mobile airline boarding pass, individuals will be able to either print out their pass or store it on their smartphones using the Excelsior Pass Wallet app. Each Pass will have a secure QR code, which participating businesses and venues can scan using a companion app to verify proof of COVID-19 negative test results or proof of vaccination. An individual's data is kept secure and confidential at all times.

As part of this initial launch, participating New Yorkers may choose to use Excelsior Pass to verify their COVID-19 vaccination or negative test results as needed to gain entry to major stadiums and arenas, wedding receptions, or catered and other events above the social gathering limit. Interested New Yorkers can opt in to use Excelsior Pass and learn more here (https://covid19vaccine.health.ny.gov/excelsior-pass); interested businesses can opt in and learn more here (https://forward.ny.gov/excelsior-pass-business). Major venues have already announced they will begin utilizing this technology in the coming weeks, including Madison Square Garden in New York City beginning next week and the Times Union Center in Albany. Beginning April 2, Excelsior Pass will expand to smaller arts, entertainment and event venues.

"New Yorkers have proven they can follow public health guidance to beat back COVID, and the innovative Excelsior Pass is another tool in our new toolbox to fight the virus while allowing more sectors of the economy to reopen safely and keeping personal information secure," **Governor Cuomo said.** "The question of 'public health or the economy' has always been a false choice — the answer must be both. As more New Yorkers get vaccinated each day and as key public health metrics continue to regularly reach their lowest rates in months, the first-in-the-nation Excelsior Pass heralds the next step in our thoughtful, science-based reopening."

New York State is the first state in the U.S. to formally launch this potentially transformational technology. Prior to its launch, two successful pilot demonstrations were held in recent weeks, along with a beta test where thousands of New Yorkers participated in a limited roll out of the technology to provide feedback on user interface and results.

Interested New Yorkers can download the Excelsior Pass Wallet app for Android here (https://protect2.fireeye.com/v1/url?k=f11cd584-ae87ecbb-f11e2cb1-000babda0031-5d1d456539e94d58&q=1&e=352517a6-a42c-4201-bc48-c4a39dfb5929&u=https%3A%2F%2Fplay.google.com%2Fstore%2Fapps%2Fdetails%3Fid%3Dgov.ny.its.healthpassport.wallet) and for iOS here (https://apps.apple.com/us/app/nys-excelsior-pass-wallet/id1552933587). Interested businesses can download the Excelsior Pass Scanner app for Android here (https://protect2.fireeye.com/v1/url?k=ce65f844-91fec17b-ce670171-000babda0031-ff1d40351b693292&q=1&e=352517a6-a42c-4201-bc48-c4a39dfb5929&u=https%3A%2F%2Fplay.google.com%2Fstore%2Fapps%2Fdetails%3Fid%3Dgov.ny.its.healthpassport.verify) and for iOS here (https://apps.apple.com/us/app/nys-excelsior-pass-scanner/id1552709177).

Steve LaFleche, General Manager, IBM Public and Federal Markets, said, "IBM is proud to support the State of New York with its efforts to apply innovative technologies to help residents and communities respond to COVID-19. In choosing a flexible and accessible tool (https://newsroom.ibm.com/Digital-Solutions-Help-Support-New-York-State-with-Reopening-Plans) that places security and privacy at its core, the state is modeling for the rest of the country how new, technology-enabled approaches can help safely reinvigorate economies while also striving to protect public health."

Excelsior Pass is built on IBM's Digital Health Pass solution (https://www.ibm.com/products/digital-health-pass) and is designed to enable the secure verification of health credentials such as test results and vaccination records without the need to share underlying medical and personal information. The technology is flexible and built to scale, allowing other states to join and help foster a safer, trusted transition to a post-pandemic reality. The pass can also be printed and is complementary to other types of proof that patrons can use, reducing any barriers to usage.

A special emphasis has been placed on the protection of an individual's privacy. Secure technologies, like blockchain and encryption, are woven throughout Excelsior Pass to help protect the data, making it verifiable and trusted. No private health data is stored or tracked within the apps. Excelsior Pass can be used to voluntarily show a QR code as proof of COVID-19 vaccination or negative test result via a digital smartphone wallet or printed credential without sharing underlying personal health details.

Multiple security systems are in place to ensure the integrity of personal health information. Excelsior Pass was designed with equity and equal access at the forefront. With multi-language access, a robust Help Desk, and multiple ways to use Excelsior Pass — whether you have a smartphone or not — New York is committed to ensuring that all New Yorkers can participate in the safe, convenient and responsible reopening of our economy.

The following set of labs have committed to rapid reporting of COVID test results to the State Department of Health's Electronic Clinical Laboratory Reporting System (ECLRS), which will help ensure that Excelsior Pass users are able to receive their testing results in the required window of time before an event: Acutis Diagnostics, Aegis Sciences Corporation, BioReference Laboratories, Boston Heart Diagnostics, Broad Institute, Cayuga Medical Center, Clarity Lab Solutions, Lenco Diagnostic Laboratories, The Mount Sinai Hospital's Center for Clinical Laboratories, Northwell Health, Quest Diagnostics, Rapid Reliable Testing and UR Medicine Labs. The State continues to work with other labs and rapid testing sites to expand this list of partners and expedite reporting so users have timely, accurate results to participate in congregate economic and social activities.

James Dolan, Executive Chairman, MSG Sports and Executive Chairman and CEO, MSG Entertainment, said, "We are grateful the state is focused on doing everything possible to reopen businesses across our region safely and quickly. The Excelsior Pass will play an important role in allowing people to gather safely, which will be critical to New York's recovery. We were proud to be part of the Excelsior Pass pilot and look forward to participating in the program."

Bob Belber, General Manager, Times Union Center, said, "The Times Union Center looks forward to using this platform and making this excellent technology available for future events. With the convenience of Excelsior Pass, attendees will be able to easily gain access to the arena while promoting public health by showing proof of vaccinations or proof of negative test results on a mobile device. This will be a game changer for our venue's continued reopening process and for New Yorkers in the Capital Region and beyond."

James Wester, Research Director, IDC Worldwide Blockchain Strategies, said, "We are fortunate to have technologies the can play a role in securing and authenticating vaccination and health status, while putting individuals in control of what, where and when their data is shared. Having opinions in how we volunteer our health status will ultimately help us all return to normal faster."

Kathryn Wylde, President & CEO, Partnership for New York City, said, "The business community is eager to get our city's workforce back to the office, to safely re-open entertainment venues and restaurants, and much more. The Excelsior Pass is an exciting new tool that will accelerate our state's economic recovery. It is evidence of New York's forward-thinking approach to restoring jobs and moving beyond the pandemic."

Jen Lyon, Founder of NY Independent Venue Association and Owner of MeanRed Productions, said, "NYIVA is very excited that New York is leading in creating solutions for ways to open our venues and keep our audiences safe. It's been a long year of closure and we have a lot of work ahead of us until we return New York State to the arts and culture Mecca that we have always been. We look forward to continuing to work hand in hand with the Governor's re-opening team to give our members the tools and support they need to bring our arts and culture sector back to life."

Mark Dorr, President, New York State Hospitality & Tourism Association, **said,** "Excelsior Pass is a great example of the kind of innovative, forward-looking thinking that the tourism industry needs to safely get back to work as we emerge from the COVID crisis. This first-of-its-kind state app will make it easier for our members to safely hold events under the state guidance and we look forward to putting it to use for our members and guests."

Bob Provost, President & CEO, New York State Tourism Industry Association - NYSTIA, said, "New York State's Excelsior Pass will be an invaluable asset to both the tourism industry and consumers. It will ensure accuracy in verification of test and vaccination status while

streamlining the process for venues and offering increased convenience and safety to the public. Everyone wins! Kudos to New York State for setting yet another gold standard in best practice."

Melissa Fleischut, CEO of the New York State Restaurant Association, said, "It's critical to get the economy fully reopen and the app is an important tool that can help make that happen. Our members support any effort like this to ensure a safe and robust reopening of the economy."

Scott Wexler, Executive Director of the Empire State Restaurant & Tavern Association, said, "The Excelsior Pass initiative an important step towards stabilizing the State's hospitality industry. It will provide our patrons with a tool to help keep them safe while returning to arts, cultural, sports, and the other social activities that make New York a great place to live, work, and play."

Sean Willcoxon, Vice President of Catering, Mazzone Hospitality, said, "Excelsior Pass is an exciting tool providing a secure and efficient way to verify vaccination and testing records, helping caterers like Mazzone Hospitality safely host events. Safe reopening of the State and the release of this tool will be a great help as we open our doors and welcome guests and we are grateful for New York State's innovative support."

SUNY Chief Operating Officer Beth Berlin said, "It's been more than a year since New York State's first case of COVID-19, and our students, faculty, and staff—and the communities we serve—have done so much to help battle this virus. As we all remain diligent to protect one another, the innovative Excelsior Pass and other tools will help us safely resume more in-person events, which will help accelerate the return of our economy and to more normal times again."

CUNY's Executive Vice Chancellor and Chief Operating Officer Hector Batista said, "Excelsior Pass will provide our community with a convenient way to verify vaccination and testing records, helping CUNY safely resume events in line with State guidance. This state app will be an important tool as our State's safe reopening continues to move forward and we are grateful for New York State's innovative support."

Steven M. Cohen, Co-Chair of the New York Forward Reopening Advisory Board and Chair of the Empire State Development Board of Directors, said, "As we continue down the path of a safe and smart economic recovery, Excelsior Pass is a pioneering new platform that will help New Yorkers return to the activities they love. This secure, innovative and easy-to-use technology will support New York residents and businesses alike all across the state and set an example for the entire nation to follow."

MTA Chairman and CEO Patrick J. Foye said, "New Yorkers and tourists alike are beginning to return to work and social events throughout the region in larger numbers and the MTA has never been more prepared to serve them. Over the course of the last year, our heroic frontline employees have worked relentlessly to transport the city's heroic frontline workers. We have maintained safety and cleanliness on our subways, buses, and commuter railroads. The MTA remains the best way to get around New York and we are proud to serve the region as it gradually and safely returns to life after the pandemic."

Governor Cuomo also recently announced the expansion of the New York Forward Rapid Test Program (https://www.governor.ny.gov/news/governor-cuomo-announces-expansion-new-york-forward-rapid-test-program-help-businesses-venues) to help businesses, catered events, professional sports games with fans, and events, arts, and entertainment venues safely reopen, with dozens of sites now open statewide. This unique public-private partnership makes low-cost rapid testing more available to the public to support enhanced economic

activity as the State continues to reopen sectors of the economy. All participating testing providers have committed to rapid reporting of COVID-19 test results to ECLRS, enabling integration with Excelsior Pass. Learn more about the program and make an appointment here (https://forward.ny.gov/ny-forward-rapid-test-program).

Translations

Bengali Translation বাংলা অনুবাদ	(https://www.governor.ny.gov/sites/default/files/atoms/files/03.25.21.rel_.EXCELSIOR_Bengali.pdf)
Chinese Translation 中文翻譯	(https://www.governor.ny.gov/sites/default/files/atoms/files/03.25.21.rel_.EXCELSIOR_Chinese.pdf)
Haitian-Creole Translation Tradiksyon kreyòl ayisyen	(https://www.governor.ny.gov/sites/default/files/atoms/files/03.25.21.rel_.EXCELSIOR_HaitianCreole.pdf)
Korean Translation 한국어 번역	(https://www.governor.ny.gov/sites/default/files/atoms/files/03.25.21.rel_.EXCELSIOR_Korean.pdf)
Russian Translation Перевод на русский язык	(https://www.governor.ny.gov/sites/default/files/atoms/files/03.25.21.rel_.EXCELSIOR_Russian.pdf)

Spanish Translation
Traducción al español

(https://www.governor.ny.gov/sites/default/files/atoms/files/03.25.21.rel_.EXCELSIOR_Spanish.pdf)

Contact the Governor's Press Office

Contact us by phone:

Albany: (518) 474 - 8418
New York City: (212) 681 - 4640

Contact us by email:

Press.Office@exec.ny.gov

September 8, 2021 | 2:39 pm

COVID-19 Vaccines

On August 23, the FDA announced the full approval of the Pfizer-BioNTech vaccine for the prevention of COVID-19 disease in individuals age 16 and older. Read more.

DETAILS >

GOVERNOR
KATHY HOCHUL

MAY 22, 2021 | Albany, NY

Governor Cuomo Announces More Than 1 Million Excelsior Passes Retrieved Since Launch

COVID-19 VACCINE (/KI HEALTH /COVID-19-VACCINE) (/KI PUBLIC SAFETY /HEALTH) (/KI TECHNOLOGY /PUBLIC-SAFETY) (/KEYWORDS /TECHNOLOGY)

Major Venues and Businesses Across the State Integrating Excelsior Pass into Reopening After State Adopts New CDC Guidance on Mask Use for Fully Vaccinated Individuals

First-in-the-Nation Digital Pass Offers Free, Voluntary Way to Share COVID-19 Vaccination or Negative Test Status in Accordance with State Guidance

Excelsior Pass COVID-19 Vaccination Passes Now Valid for 365 Days; Those Vaccinated in NYS Can Retrieve 15 Days After Final Dose

B-Roll of Excelsior Pass Used at New York Islanders Game Available Here; Excelsior Pass Marketing Images Available Here

Governor Andrew M. Cuomo today announced that more than 1 million Excelsior Passes have been issued since New York State launched the first-in-the-nation voluntary platform in March. Excelsior Pass, which is now being utilized by venues, universities, stadiums and businesses statewide, is a free, fast, and secure way to present digital proof of COVID-19 vaccination or negative test results that's helping to get New Yorkers back to the things they love and miss — safely.

"After a long and incredibly difficult year, New Yorkers are finally returning to normal life and getting back to work amid rising vaccination rates, and the first-in-the-nation Excelsior Pass is a key part of that restoration of normalcy," **Governor Cuomo said.** "The fact that we've so quickly achieved a milestone — more than 1 million passes issued — speaks to New Yorkers' desire to resume many of the activities they've given up over the past year and is good news for bringing our economy back and building a stronger state for the future. New Yorkers are ready for the new normal, and the Excelsior Pass will help them get there until we can defeat this terrible pandemic for good."

Excelsior Pass is supporting New Yorkers building back better through NYS DOH guidance, with an over 80 percent increase in downloads this week alone. As of May 19, the State lifted capacity restrictions and adopted CDC guidance on masks and social distancing for fully vaccinated individuals. Under the new guidance (https://www.governor.ny.gov/sites/default/files/2021-05/NYS_CDCGuidance_Summary.pdf), certain businesses may choose to require proof of COVID-19 vaccination status and Excelsior Pass is an easy-to-use, verifiable option. New Yorkers can always present alternate forms of COVID-19 vaccination and negative test results — such as paper forms — directly at businesses and venues.

Major sports venues across the State are already using Excelsior Pass to safely get even more fans back into stands, including Madison Square Garden (https://www.governor.ny.gov/news/governor-cuomo-announces-launch-excelsior-pass-help-fast-track-reopening-businesses-and), Barclays Center (https://www.governor.ny.gov/news/governor-cuomo-announces-launch-excelsior-pass-help-fast-track-reopening-businesses-and), Yankee Stadium (https://www.governor.ny.gov/news/governor-cuomo-announces-large-scale-outdoor-venue-capacity-increase-new-fully-vaccinated-fan), Citi Field (https://www.governor.ny.gov/news/governor-cuomo-announces-large-scale-outdoor-venue-capacity-increase-new-fully-vaccinated-fan), the Nassau Coliseum (https://www.governor.ny.gov/news/governor-cuomo-announces-nassau-coliseum-will-have-fully-vaccinated-fan-section-islanders), Belmont Park, the Times Union Center, NBT Bank Stadium, the Carrier Dome, Sahlen Field (https://www.governor.ny.gov/news/governor-cuomo-announces-buffalos-sahlen-field-host-additional-2000-spectators-blue-jays-games) — the temporary host of the Toronto Blue Jays

— KeyBank Center, and Frontier Field.

Universities and colleges across New York — including State University of New York campuses such as the University at Buffalo, Binghamton University and Stony Brook University, as well as Syracuse University, Pace University and Long Island University — have already leveraged Excelsior Pass for in-person graduation ceremonies and large events, like sporting games, or plan to for the fall.

Users interested in opting in to use Excelsior Pass, which currently has a Vaccination Pass and two different Test Pass options, can learn more here (https://covid19vaccine.health.ny.gov/excelsior-pass); interested businesses and organizations can opt in and learn more here (https://forward.ny.gov/excelsior-pass-business) and download digital marketing assets here (https://forward.ny.gov/excelsior-pass-frequently-asked-questions#digital-assets) to help demonstrate to patrons/customers that their business accepts Excelsior Pass.

At this time, Passes may only be retrieved for COVID-19 vaccinations or negative test results received in the State of New York, though it does not require you to be a resident of New York. The State is actively working with regional and international partners to broaden its use, as well as major New York State employers to support office reopenings.

All Excelsior COVID-19 Vaccination Passes retrieved beginning today will be valid for 365 days, up from 180 days. Those who already have a Vaccination Pass may retrieve a new Pass whenever they choose to in order to take advantage of this extension. At this time, New Yorkers should know that the 365 days relates only to the length of time the Pass is valid. The duration of validity of Excelsior Vaccination Passes may continue to be updated to reflect the latest understanding from federal and state health experts and as additional science and trial data is released.

For those interested in Excelsior Pass who have received their COVID-19 Vaccinations or PCR and/or Antigen Tests in the State of New York, visit epass.ny.gov (https://epass.ny.gov/home) to get started.

Fast Facts About Excelsior Pass

- Excelsior Pass is a free, voluntary, and secure way to retrieve proof of COVID-19 vaccination or negative test results and users' data is kept confidential and secure at all times.
- At this time, Passes are only available for those who have received their COVID-19 Vaccination or PCR/Antigen tests in the State of New York.
- An Excelsior COVID-19 Vaccination Pass, available 15 days after the final dose of the vaccine was administered, is valid for 365 days.
- An Excelsior COVID-19 PCR Test Pass is valid until midnight on the third day after a test.
- An Excelsior COVID-19 Antigen Test Pass is valid for 6 hours from the time of a test.
- Each Pass contains cryptographic signatures that ensure that it is genuine and that no data-tampering has occurred.
- Excelsior Pass is accompanied by a Help Desk with extensive resources, multi-language access, and is able to be printed for those who may not own smartphones.
- New Yorkers always have the option of using other forms of proof, like a CDC card or

physical laboratory test results, directly at a business or venue.

Vaccine administrators and testing providers are directly responsible for entering COVID-19 immunization and testing data into secure New York State and New York City databases on a timely basis. Per NYS DOH guidance, all New York State vaccine administrators must have staff available to both review and correct the data they input, if data entry issues are identified.

Contact the Governor's Press Office

Contact us by phone:

Albany: (518) 474 - 8418
New York City: (212) 681 - 4640

Contact us by email:

Press.Office@exec.ny.gov

Translations

Arabic Translation
الترجمة إلى العربية

(https://www.governor.ny.gov/sites/default/files/2021-05/05.22.21.rel_.EXCELSIOR_Arabic.pdf)

Bengali Translation
বাংলা অনুবাদ

(https://www.governor.ny.gov/sites/default/files/2021-05/05.22.21.rel_.EXCELSIOR_Bengali.pdf)

SÜDWEST PRESSE

Digitaler Impfass

Viele Impfpässe gefälscht - Bayerns Innenminister Herrmann dringt auf elektronischen Impfpass

Die Einführung eines digitalen oder elektronischen Impfpasses wird angesichts vieler Fälschungen in Deutschland immer wichtiger. Bayerns Innenminister Herrmann dringt auf eine rasche Einführung.

14. Mai 2021, 12:12 Uhr • Berlin

Ein Artikel von

Tobias Knaack

Agenturen

-
- **Corona Impfung** kein **Impfpass** mehr
- Neuen Impfpass bekommen?
- Bekomme ich einen Impfpass beim **Impfzentrum**?
- Wo kann man einen Impfpass **kaufen**?
- Impfpass **Fälschung Strafe**

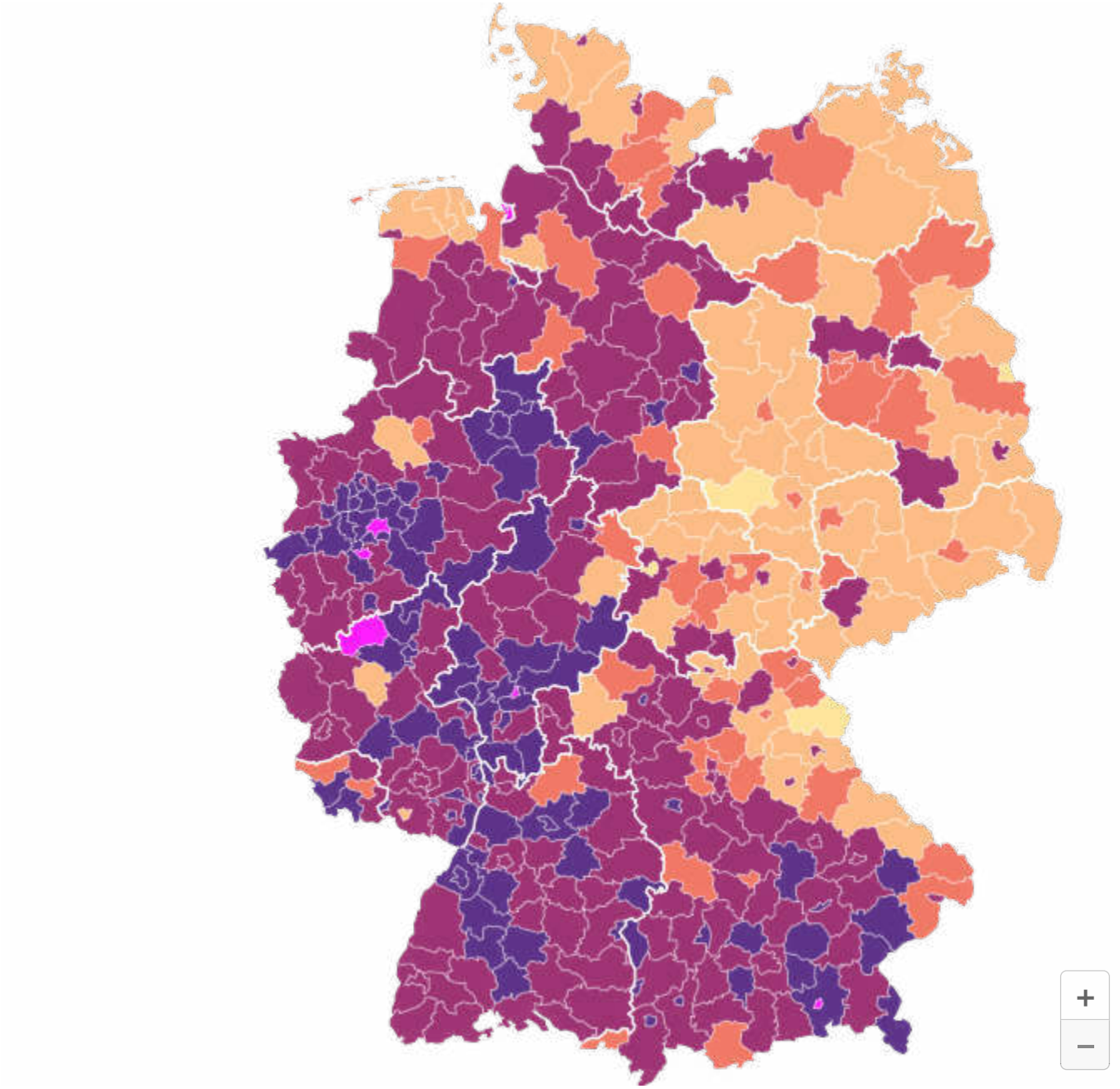
Je weiter die **Priorisierung beim Impfen in Deutschland** gegen das Coronavirus aufgehoben wird und je mehr **Impfstoff** zur Verfügung steht, desto mehr Fragen stellen die Bürgerinne

Bürger im Internet rund um die **Impfung** - und den **Impfpass**. Oben aufgeführt sind die meistgesuchten **Fragen** in den vergangenen 24 Stunden (Stand 12 Uhr, 14.05.2021) zum Begriff „Impfpass“.

Deutschland-Karte mit aktuellen Zahlen zur 7-Tage-Inzidenz

Neue Corona-Fälle pro 100.000 EinwohnerInnen binnen 7 Tagen

< 10 10–35 35–50 50–100 100–200 ≥ 200



Die Daten in der Grafik stammen vom Robert-Koch-Institut, dem die Gesundheitsämter aus ganz Deutschland ihre Corona-Zahlen schicken. Da die Verarbeitung dieser Zahlen Zeit benötigt, können sie von den aktuellen Zahlen der Gesundheitsämter abweichen.

Grafik: SÜDWEST PRESSE • Quelle: Robert Koch-Institut (RKI), dl-de/by-2-0. • Kartenmaterial: © OSM • Erstellt mit Datawrapper

Impfpass Fälschungen: Bayerns Innenminister Herrmann fordert digitalen Impfpass

Während viele schlicht organisatorische Fragen haben, gibt es aber auch eine wachsende kriminelle Energie im Versuch, schneller an eine Corona-Impfung zu gelangen. Angesichts der zunehmenden Fälschungen von Impfpässen zum Nachweis einer Immunisierung gegen das Coronavirus dringt **Bayerns Innenminister Joachim Herrmann** (CSU) auf die rasche Einführung eines elektronischen Nachweises. "Es ist höchste Zeit, dass bald ein elektronischer Impfausweis zur Verfügung steht, der fälschungssicher ist", sagte Herrmann den Zeitungen der Funke Mediengruppe (Freitagsausgaben). Er hoffe, "dass das sehr schnell auf Bundes- oder EU-Ebene realisiert" werde.

Zugleich warnte der bayerische Innenminister vor dem Vortäuschen einer Corona-Impfung. "Wer einen gefälschten Impfausweis vorlegt, muss mit einer empfindlichen Strafe rechnen", sagte er den Funke Medien. "Das ist kein Bagatelldelikt, sondern Urkundenfälschung."

Hausärzte-Chef zweifelt an schneller Einführung von elektronischem Impfpass in Deutschland

Der Vorsitzende des Deutschen Hausärzteverbands, Ulrich Weigeldt, äußerte Zweifel an der Einführung eines digitalen Impfpasses bis Ende Juni. Bislang jedenfalls deute wenig darauf hin, dass ein digitaler Impfausweis bis zum Beginn der Reisesaison im Sommer flächendeckend in Deutschland verfügbar sein werde, sagte er der "Augsburger Allgemeinen" (Freitagsausgabe).

"Digitale Impfnachweise helfen den Menschen ganz besonders dann, wenn sie nicht bloß in Aussicht gestellt werden, sondern tatsächlich auch kommen - und wenn klar ist, welche konkreten Vorteile mit ihnen verbunden sind", hob Weigeldt hervor. "Und da darf man mit Blick auf bürokratische Vorgaben und weitere leidvolle Verkomplizierungen schon Zweifel haben, ob den vollmundigen Ankündigungen dann auch zeitnah Taten folgen werden."

Auch die Digitalexpertin Anke Domscheit-Berg ist skeptisch. "Die Hürde, einen digitalen Impfpass sicher hinzubekommen, ist einfach zu hoch, um das in zwei Monaten zu schaffen", sagte die Linken-Politikerin der "Augsburger Allgemeinen". Außerdem gebe es dabei erhebliche praktische Probleme. So seien Millionen Menschen in Deutschland bereits gegen Corona geimpft worden. "Wer soll das alles nachtragen? Das kann ich von den Hausärzten und den Impfzentren nicht verlangen", sagte Domscheit-Berg.

Impfen in Hausarztpraxen: Kein weiterer bürokratischer Aufwand

Auch Weigeldt forderte, den Hausarztpraxen dürfe durch den digitalen Impfpass "keinesfalls noch mehr Bürokratie aufgebürdet werden". Die Ärzte bräuchten ihre Zeit für ihre Patienten und "ganz gewiss nicht, um uns als Passamt der Republik zu verdingen". Umso wichtiger sei es daher, "dass der über Jahrzehnte bewährte, von der Weltgesundheitsorganisation anerkannte gelbe Impfausweis weiterhin gilt, um eine Impfung nachzuweisen".

Seit einigen Tagen haben geimpfte oder von Covid-19 genesene Menschen in Deutschland wieder mehr Freiheiten. Für die Geimpften und Genesenen entfallen Kontakt- und Ausgangsbeschränkungen, sie werden zudem Menschen mit negativem Testergebnis gleichgestellt. In diesem Zusammenhang warnen Landesregierungen und Polizeivertreter vor gefälschten Impfpässen.

Fragen und Antworten rund um den Impfpass und das Impfen in Deutschland

Wie eingangs erwähnt stellen viele Menschen aktuell Fragen rund um das Impfen, den Impfpass sowie den Impfausweis. Hier eine Auswahl zur Übersicht.

Corona Impfung kein Impfpass: Geht impfen ohne Impfausweis?

Ja, Impfungen auch gegen beispielsweise das Coronavirus sind auch möglich, wenn man den **Impfpass verloren** hat. Liegt kein Impfpass vor, stellen der Arzt oder die Ärztin nach Informationen der Bundeszentrale für gesundheitliche Aufklärung (BzgA) eine Impfbescheinigung aus.

Impfpass neu: Wo bekomme ich einen neuen Impfpass her? Wer stellt Impfpass aus?

In der Regel erhält man den Impfpass als Baby vom Kinderarzt oder der Kinderärztin. Grundsätzlich kann nach Information des BzgA jeder Arzt und jede Ärztin kostenlos einen **neuen Impfpass ausstellen**, wenn man geimpft wird. Hat man den Impfausweis also verloren, wendet man sich am besten an den Hausarzt oder die Hausärztin.

Impfpass verloren - was tun?

Dennoch sollte man versuchen alle vergangenen Impfungen zu rekonstuieren. Auch dabei helfen Hausärztinnen und Hausärzte. Gibt es allerdings keine schriftlichen Nachweis über die Impfungen erhält man einen komplett leeren Impfpass. Damit gilt man als ungeimpft. In

diesem Fall soll man laut **Ständiger Impfkommission (Stiko)** die Impfungen nachholen.

Gefälschter Impfpass - Arztpraxen und Impfzentren von Fälschungen betroffen

Arztpraxen und Corona-Impfzentren sind nach Recherchen von Report Mainz häufig von Impfpass-Fälschungen betroffen, ohne es zu wissen. Die geplante Digitalisierung der Impfpässe könnte das Problem eher verschärfen als lösen, meinen Kritiker einem Bericht von tagesschau.de zufolge.

Bereits seit Längerem monieren Kritiker dem **Tagesschau-Bericht** zufolge, dass der herkömmliche Papier-Impfausweis nicht fälschungssicher sei und fordern stattdessen direkt ein digitales Impfzertifikat einzusetzen. In anderen Ländern wie in **Griechenland**, **Dänemark** oder Estland gibt es dies schon länger.

Auch für die Polizei sei eine Fälschung auf dem Papier nur äußerst schwer zu erkennen, sagt Virginie Wegner vom LKA Hessen. „Es ist klar, dass, wenn wir solche digitalen Impfpässe haben, dass nicht nur die Fälschungssicherheit erhöht wird, sondern auch der Missbrauch, der damit getrieben wird, eingedämmt werden kann."

Corona-Impfung in Deutschland: Großer Andrang vor offenem Impfstart

Vor dem Start der offenen Corona-Impfkampagne bei den Hausärzten ist das Interesse an Terminen für die von vielen ersehnte Spritze nach Einschätzung des Landesverbands der Mediziner bereits sehr groß. „Die Leute sind pandemiemüde, sie wollen diesen nächsten Schritt", sagte Verbandssprecher Manfred King am Mittwoch auf Anfrage. Allerdings sei der zeitraubende Diskussionsbedarf in den Praxen angesichts der Sorgen vor dem Wirkstoff Astrazeneca gewaltig.

Gegen das Präparat des britisch-schwedischen Pharmakonzerns gibt es teils erhebliche Vorbehalte. Es wird nach dem Auftreten von Blutgerinnseln im Gehirn bei jüngeren Geimpften nur noch für über 60-Jährige empfohlen. Andererseits gibt es viele Jüngere, die sich gern damit impfen lassen würden, aber in der Impfreihenfolge bisher noch nicht dran waren.

SCHLAGWÖRTER

Deutschland Corona-Impfung

Digitaler Impfpass Deutschland

Um die lästige Sucherei nach dem Impfpass in Zukunft zu vermeiden, hat **Deutschland** ein **digitalen Impfpass** eingeführt. Dieser ist allerdings nur ein ergänzendes Angebot. Den

Impfausweis aus Papier wird es weiter geben. Dennoch können Patientinnen und Patienten in Zukunft ihre Impfungen auch in einer App dokumentieren.

Digitaler Impfpass macht Weg frei für EU Impfpass

Eingeführt wird der digitale Impfnachweis im Zuge einer europaweiten Einführung eines „digitalen

zu können. Es soll aber auch ausgedruckt werden können. Wichtig ist, dass ein QR-Code gescannt werden kann, um die Echtheit zu prüfen. Das Dokument soll in der jeweiligen Landessprache und auf Englisch ausgestellt werden. Die deutsche Impfpass-App orientiert sich nach Angaben des Gesundheitsministeriums an diesen Vorgaben.

Zurück zur Startseite

Schutzhülle für Impfpass: Immer mehr Deutsche suchen Hülle für Impfausweis

Zum nächsten Artikel

Lag er in den vergangenen Jahren in Ordnern oder Schubladen, wird der Impfpass nun immer mehr ausgeführt. Weil viele Menschen Sorge haben, dass das wichtige Dokument im Urlaub oder auch nur zwischen Schlüsseln und Handy in der Handtasche beschädigt wird, ist das Suchinteresse nach Schutzhüllen stark gestiegen.

Kernkompetenzzentrum
Finanz- & Informationsmanagement

Fraunhofer FIT
Projektgruppe
Wirtschaftsinformatik

Mehr Sicherheit durch Open Source – Irrweg oder Zielgerade?

von

Hans Ulrich Buhl, Jochen Dzienziol

2003

in: Wirtschaftsinformatik, 45, 4, 2003, p. 474-482

Universität Augsburg, D-86135 Augsburg
Besucher: Universitätsstr. 12, 86159 Augsburg
Telefon: +49 821 598-4801 (Fax: -4899)

Universität Bayreuth, D-95440 Bayreuth
Besucher: Wittelsbacherring 10, 95444 Bayreuth
Telefon: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

WI-872

Meinung/Dialog

Mehr Sicherheit durch *Open Source* – Irrweg oder Zielgerade?

Open-Source-Software (OSS) – Software, deren Entstehung sich durch die weltweit freiwillige Mitwirkung einer Vielzahl von Programmierern deutlich von der Entwicklung proprietärer Software unterscheidet – ist in den letzten Jahren ein Thema geworden, mit dem sich Fachzeitschriften, Tagungen und wissenschaftliche Veröffentlichungen vermehrt beschäftigen. Dies steht insbesondere mit der Erfolgsgeschichte von OSS-Vertretern wie dem Apache-Webserver oder dem Betriebssystem Linux im Zusammenhang. Dabei beschreibt Open Source nicht nur die natürlich wichtige Tatsache, dass der Quellcode der betreffenden Programme zur Einsicht und Durchführung von Veränderungen offen liegt, gemäß der Open-Source-Initiative gehören auch die Freiheit zur beliebigen Nutzung und zur unveränderten oder veränderten Weitergabe der Software zu ihren Charakteristika.

Doch selbst wenn OSS insbesondere erst in den letzten 5 Jahren beständig steigende Aufmerksamkeit erfuhr, handelt es sich dabei keinesfalls um eine neue Bewegung. Vielmehr war der freie Austausch von Software sowie das gegenseitige Profitieren von Neuerungen in den Ursprüngen der Softwareentwicklung üblich. Im Zuge der rasant steigenden Bedeutung der Datenverarbeitung wurden jedoch die Entwicklung und der Verkauf von Software schnell zu einem lukrativen Geschäftsfeld, wobei in den Lizenzen die Nutzung, der Zugriff und die Weitergabe der erworbenen Software beschränkt wurden. Als bewusste Gegenbewegung und zur Wahrung der ursprünglichen Kultur entstand – insbesondere forciert durch die Bemühungen von Richard Stallman, ehemaliger Wissenschaftler am MIT und Gründer der *Free Software Foundation* – Mitte der achtziger Jahre eine Gruppierung von Programmierern, die sich mit der gemeinschaftlichen Entwicklung von „free software“ befasste. Hieraus ging 1998 – hauptsächlich wohl aus Marketinggründen gegenüber Vertretern aus der Unternehmenswelt, für welche der Begriff „freie Software“ negative Assoziationen hervorrufen könnte – die Bezeichnung „Open Source“ hervor [Krog03]. Um zu verhindern, dass in der weiteren Entwicklung der Zugriff und die Verwendung von bestimmter OSS durch die Umwandlung in proprietäre Software restringiert wird, wurde eine Lizenz geschaffen, welche die mit OSS verbundenen Freiheiten schützt: die General Public License, die aufgrund Ihrer Zielsetzung häufig als „copyleft“ anstatt als copyright bezeichnet wird [Ljun00].

Mittlerweile ist OSS in vielen Unternehmen nicht mehr wegzudenken. So arbeiten bereits 36 % der deutschen Unternehmen mit Linux [Hutt03]. Große Hardwarehersteller wie IBM, Sun und Hewlett Packard nahmen Open Source durch den Start umfangreicher Initiativen in ihre Geschäftsstrategie mit auf, und sogar in vielen öffentlichen Verwaltungen wie in Norwegen, Frankreich und auch in Deutschland wird die Verbreitung von Linux aktiv gefördert. Als einer der Gründe für den Einsatz von Linux wird in einer Befragung der Meta Group von IT-Managern – neben der Hoffnung auf Kosteneinsparungen – das Thema Sicherheit angeführt [oV02]. Interessant ist beispielsweise auch, dass die neue Sichere Inter-Netzwerk-Architektur (SINA), welche die deutschen Auslandsvertretungen miteinander verbinden wird, auf einer angepassten Linux-Plattform basiert und der Sicherheitsdienstleister VeriSign seine Produkte auf Linux migrieren will [oV03]. Auf den ersten Blick mag es verwundern, wie in einem Softwareentwicklungsprozess in der Linux-Gemeinde von freiwilligen Programmierern, welche *Eric S. Raymond* als „großer, wild durcheinander plappernder Basar von verschiedenen Zielsetzungen und Ansätzen“ [Raym98] beschreibt, Software entstehen soll, welche in Bezug auf ihre Sicherheit proprietärer Software, deren Entwicklung vermutlich eher mit dem sorgfältig geplanten Bau einer Kathedrale vergleichbar ist, überlegen sein kann. Und tatsächlich ist die Frage, ob die Sicherheit von OSS wie bspw. Linux höher als die vergleichbarer, proprietärer Softwareprodukte ist, trotz (oder gerade wegen) des Vorteils des einsehbaren und veränderbaren Quellcodes, der niedrigen Bug-Dichte und der früher seltenen, nun aber zunehmenden Anzahl an Hackerangriffen nach wie vor umstritten. Für die ausgewogene Beurteilung spielt insbesondere das Begriffsverständnis von Sicherheit eine große Rolle.

Der Begriff Sicherheit umfasst vier Bestandteile [StGr97]: Erstens erfordert die Sicherheit die grundsätzliche Betriebsbereitschaft (availability). Zweitens muss auch die Funktionsbereitschaft (reliability) gewährleistet sein, die im Gegensatz zur Betriebsbereitschaft nicht nur die grundlegende Funktionstüchtigkeit voraussetzt, sondern auch die Sicherstellung korrekter Ergebnisse. Die Forderung der Vertraulichkeit (confidentiality) stellt den dritten Aspekt des Begriffs „Sicherheit“ dar, die der Integrität (integrity), also des Datenschutzes und der Datensicherheit, schließlich den vierten.

Unter diesen Kriterien können alle Arten von Sicherheitsrisiken eingeordnet werden. Beispiele wie Schäden durch höhere Gewalt oder durch Havarien (z. B. Brand), die auch die Betriebsbereitschaft gefährden, sind zwar kaum durch die eingesetzte Software beeinflussbar, jedoch werden andere Aspekte, wie z. B. Vandalismus (durch einen Cracker) sehr wohl durch die Art der eingesetzten Software beeinflusst.

Betrachtet man die Sicherstellung der vier Aspekte über einen längeren Zeitraum, so lassen sich ebenfalls strategische/betriebswirtschaftliche Anforderungen wie Planungssicherheit und Investitionssicherheit unter dem Sicherheitsbegriff subsumieren. Beispielsweise ist für ein Unternehmen die Verfügbarkeit neuer Softwareversionen, die diese Sicherheitskriterien auch in Zukunft erfüllen, enorm wichtig.

Insgesamt bleibt zu bemerken, dass nahezu jedes Sicherheitsniveau prinzipiell erreichbar, allerdings mit einem finanziellen Trade-off in Form von höheren Kosten für Installation, Wartung und spezifische Anpassungen verbunden ist. Die Höhe dieser Kosten wird ebenfalls durch die eingesetzte Software beeinflusst. Einerseits bietet hier OSS einem Unternehmen prinzipiell die Möglichkeit, den Quelltext durch die eigene IT-Abteilung mit beliebig skalierbarem Aufwand auf Schwachstellen überprüfen zu lassen. Gegebenenfalls ist hier auch eine kostengünstige Zusammenarbeit mit den Entwicklern der OSS möglich, die für die Hilfe bei der Verbesserung ihrer Software dankbar sind. Andererseits können mit einem Anbieter kommerzieller Software Haftungs- und Wartungsverpflichtungen vertraglich vereinbart werden, während OSS-Entwickler prinzipiell zwar für ihre Hilfe bezahlt werden können, Haftung allerdings in der Regel ausschließen. Zwischen diesen beiden Extremen existieren am Markt noch weitere Alternativen, wie der professionelle Support für OSS durch spezialisierte IT-Dienstleister oder aber beispielsweise das Shared-Source-Angebot von Microsoft, das Kunden gegen Entgelt Einsicht in die Quellen der Produkte gewährt. Welche dieser Alternativen im Einzelfall vorzuziehen ist, ist von den konkreten Gegebenheiten abhängig. Allerdings ist bei OSS der Kunde in keinem Fall von einem einzigen Anbieter abhängig.

Ein Hauptgrund für die strittige Beurteilung der Sicherheitsfrage im Zusammenhang mit Open Source ist die Tatsache, dass einerseits die angesprochenen Aspekte des Sicherheitsbegriffs je nach Anwendungsgebiet unterschiedliche Bedeutung besitzen und anderer-

seits OSS und proprietäre Software unterschiedliche Eigenschaften hinsichtlich dieser Aspekte aufweisen. Dies soll in der heutigen Ausgabe von Meinung/Dialog näher diskutiert und von verschiedenen Seiten beleuchtet werden. Hierbei haben wir versucht, durch die gewonnenen Autoren eine möglichst differenzierte, von emotionalen Glaubensbekenntnissen hinsichtlich OSS oder proprietärer Software losgelöste Betrachtung zu motivieren. Lesen Sie im Folgenden die Beiträge von:

- Hermann-Josef Lamberti, Chief Operating Officer bei der Deutsche Bank AG, verantwortlich für Kosten- und Infrastrukturmanagement, Informationstechnologie, Operations, Gebäude- und Flächenmanagement sowie Einkauf,
- Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik,
- Harald Lieder, Accenture GmbH, Leiter des Bereichs Global Architecture & Core Technologies im deutschsprachigen Raum (ASG),
- Dr. Thomas Mangel, Chief Technology Officer, Postbank Systems AG und
- Richard Seibt, Chief Executive Officer, SuSE Linux AG.

Wenn auch Sie zu diesem Thema oder einem Artikel der Zeitschrift Wirtschaftsinformatik Stellung nehmen möchten, dann senden Sie Ihre Stellungnahme (max. 2 DIN A4 Seiten, gerne auch als E-Mail) bitte an den Hauptherausgeber, Prof. Dr. Wolfgang König, Universität Frankfurt am Main, E-Mail: koenig@wiwi.uni-frankfurt.de

Literatur (Auswahl)

[Raym98] *Raymond, Eric S.:* The Cathedral and the Bazaar. http://www.phone-soft.com/RaymondCathedralBazaar/catb_g.0.html, 1998-08-08, Abruf am 2003-05-17.

[Ljun00] *Ljungberg, Jan:* Open Source Movements as a Model for Organizing. In*: Bichler, M.; Hansen, H.-R.; Mahrer, H.* (Hrsg.): Proceedings of the 8th European Conference on Information Systems (ECIS) 2000. Gabler, Wiesbaden 2000, S. 501–508.

[Krog03] *von Krogh, Georg:* Open-Source Software Development. In: MIT Sloan Management Review 44 (2003) 3, S. 14–18.

[oV02] *ohne Verfasser:* Linux profitiert von der Branchenkrise. In: Computerwoche (2002) 41, S. 54.

[StGr97] Stichwort Sicherheitsmanagement. In: *Stickel, Eberhard; Groffmann, Hans-Dieter; Rau, Karl-Heinz* (Hrsg.): Gabler Wirtschaftsinformatiklexikon. Gabler, Wiesbaden 1997, S. 645–646.

[oV03] *ohne Verfasser:* Deutsche Botschaften stellen weltweit auf Linux und VPN-Tunelling um. http://www.de.internet.com/index.html?id=2018845, 2003-01-21, Abruf am 2003-05-17.

[Hutt03] *Huttenloher, Rainer:* Kostenersparnis öffnet Linux die Türen. In: Computer Zeitung 34 (2003) 6.

Prof. Dr. Hans Ulrich Buhl,
Dipl.-Kfm. Jochen Dzienziol, M.Sc.,
Lehrstuhl für Betriebswirtschaftslehre,
Wirtschaftsinformatik
& Financial Engineering,
Kernkompetenzzentrum
IT & Finanzdienstleistungen,
Universität Augsburg

Open Source – eine Alternative zu kommerziell lizenzierter Software?
von Hermann-Josef Lamberti

Open-Source-Software erobert immer breitere Einsatzbereiche in Wirtschaft und öffentlicher Verwaltung. Insbesondere das freie Betriebssystem Linux fand in den vergangenen Jahren eine zunehmende Verbreitung außerhalb seiner angestammten Einsatzgebiete im akademischen Umfeld. Aber auch andere Open-Source-Anwendungen werden teils schon seit Jahren in der Wirtschaft erfolgreich eingesetzt – allen voran der Webserver Apache mit einer weltweiten Marktdurchdringung von über 60 %. Gleiches gilt für die in der breiten Öffentlichkeit weniger bekannten Werkzeuge wie sendmail, bind oder PERL.

Wie man in den letzten Jahren beobachten konnte, entstammen die industriellen Linux-Anwender ganz unterschiedlichen Bereichen der Wirtschaft: Die Pixar Animation Studios, eine Hollywoodgröße im Bereich der Computeranimation, schafft Filmwelten auf Linux-Rechnern. VeriSign, Anbieter von sicheren Kommunikationslösungen, migriert Verschlüsselungsdienstleistungen auf das freie Betriebssystem. Und Verbrauchsgüterriese Unilever will bis zum Jahr 2006 seine IT-Landschaft im Serverbereich auf Linux umstellen – um Kosten zu sparen und die Flexibilität seiner IT-Systeme zu steigern. In den vergangenen zwei Jahren hat sich Linux auch verstärkt bei geschäftskritischen Systemen in der Finanzdienstleistungsindustrie etabliert, insbesondere im traditionell Unix-lastigen Investmentbankinggeschäft. Der Treiber für diese Entwicklung sind die geringeren Gesamtkosten, die sich (abhängig vom Einsatzgebiet) mit Linux erzielen lassen.

Diese Entwicklung spiegelt sich nicht zuletzt in den Umsätzen der IT-Branche im Serverbereich wider. Nach Zahlen von Gartner Dataquest wurden beispielsweise im vierten Quartal 2002 in den USA mit Linux-Serversystemen knapp 385 Millionen US-Dollar umgesetzt – gut 90 % mehr als im Vorjahresquartal. Der Gesamtumsatz mit Servern stieg in den USA im gleichen Zeitraum um lediglich 5 %. Allein IBM und Hewlett-Packard setzten 2002 mit Software, Hardware und Dienstleistungen für Linux weltweit 1,5 bzw. 2 Milliarden US-Dollar um. Insgesamt ist der Marktanteil installierter Linux-Systeme gegenüber Microsoft-Servern jedoch nach wie vor klein. Gleichwohl geht die Butler Group davon aus, dass sich bis 2009 ein zwischenzeitlich standardisiertes Linux als dominantes Serverbetriebssystem etabliert haben wird [BlDa02].

Im Lichte dieser Entwicklung betrachtet, ist Linux wohl weniger nur eine Alternative zu kommerziellen Betriebssystemen, als vielmehr eine klassische disruptive Technologie im Sinne von Clayton Christensen, Professor an der Harvard Business School [Clay97]. Christensen argumentiert, dass sukzessive Wellen dominanter Technologien unsere Gesellschaft durchdringen: Die jeweils nächste Welle baut auf die vorherigen auf, und scheinbar langlebige Technologien werden plötzlich durch einen neuen Herausforderer entthront. Diese disruptiven Technologien zeichnen sich zwar durch eine echte Neuerung aus, sind dabei aber anfangs gerade gut genug, um sich in einer Nische zu etablieren. Im Falle von Linux lag diese im akademischen Umfeld. In der anfänglichen Randexistenz werden disruptive Technologien jedoch kontinuierlich weiterentwickelt, wodurch sie sich dann auf breiter Ebene am Markt durchsetzen können. Dabei verdrängen sie schließlich nicht nur angestammte Konkurrenten, sie gestalten vielmehr ihren gesamten Markt in einer schöpferischen Zerstörung um. Dies betrifft insbesondere die Preismodelle und Profitmargen, die auf den betroffenen Märkten realisiert werden können. Die echte Neuerung, die mit Linux am Betriebssystemmarkt eingeführt wurde, ist die Quelloffenheit der Software. Damit wurde ein Unix-artiges Betriebssystem für verschiedenste Hardwareplattformen verfügbar. Dies gilt insbesondere für die massenhaft verbreiteten x86-Systeme, mit ihren bekannten Kostenvorteilen. Für den disruptiven Charakter von Linux spricht zudem die Tatsache, dass Industriegrößen wie IBM oder HP schon vor einigen Jahren ihr Geschäftsmodell angepasst und eine Linux-Strategie implementiert haben.

Für den Einsatz quelloffener Software hat die Deutsche Bank eine pragmatische Strategie verfolgt. Dabei kann man speziell im Falle von Linux grob in drei Phasen unterscheiden. Bis Ende 1998 wurde dieses Betriebssystem in unserer Bank hauptsächlich in wenig kritischen Bereichen eingesetzt. Dies waren beispielsweise Webserver im In-

tranet, Terminalserver in der Systemadministration oder die Datei-, Druck- oder Faxserver einzelner Abteilungen. In dieser ersten Diffusionsphase wurden wertvolle Erfahrungen im Umgang mit Linux gewonnen. Diese Erfahrungen – insbesondere im Hinblick auf Sicherheit – ermöglichten es in der zweiten Phase zwischen 1999 und 2001, Linux auch in kritischeren Bereichen einzusetzen. Hierzu zählen insbesondere Systemmanagementwerkzeuge im Rechenzentrumsumfeld, die teils eingekauft, teils selbst entwickelt wurden. Zudem wurde in dieser zweiten Phase Linux verstärkt als Plattform für den Aufbau von Firewalls zur Absicherung der Unternehmensnetze benutzt. In der zweiten Phase wurde Linux also auch für sicherheitskritische Anwendungen eingesetzt, die allerdings einen klaren Bezug zur IT-Infrastruktur haben. Man könnte daher von einer Infrastrukturphase sprechen. Dies änderte sich in der dritten Phase, die seit Ende 2001 bis heute anhält und die Diffusion von Linux in Systeme des Kerngeschäfts der Bank markiert. Seither wird Linux im Grunde für beliebige Einsatzgebiete verwendet, insbesondere auch als Plattform für geschäftskritische Anwendungen. Hierzu zählen beispielsweise die globale Risiko- und P&L Analyse für Kreditderivate [Golt03].

Der Verbreitungsprozess von Linux in der Deutschen Bank spiegelt also den jeweiligen Reifegrad und damit die erzielbare Sicherheit dieser Technologie wider. Er ist das Ergebnis eines sorgfältig geplanten Vorgehens, in dem sehr früh die besten internen und externen Linux-Projekte identifiziert und analysiert wurden. Aus dieser Analyse ergaben sich dann die strategischen Vorgaben für den weiteren Einsatz dieses Betriebssystems. Heute ist Linux eine strategische Plattform für Unixfunktionalitäten, die bislang teuren proprietären Systemen vorbehalten war. Dies umfasst einen breiten Anwendungsbereich, wie Systeme im Hochleistungsrechenbereich, die bekannten N-Schicht-Konfigurationen typischer Webapplikationen oder Anwendungen im Sicherheitsbereich.

Tatsächlich ist nach unseren Erfahrungen Linux gerade aus der Sicherheitsperspektive interessant. In Bezug auf die zugrundeliegende Sicherheitsphilosophie unterscheidet sich Linux nicht wesentlich von kommerziellen Unixderivaten. Zudem etabliert sich dieses Betriebssystem zunehmend als eine Standardplattform im Sicherheitsumfeld, da es aufgrund seiner Modularität leicht an spezielle Anforderungen angepasst werden kann. Dies gilt beispielsweise im Firewall- und VPN-Bereich. Bei der internen Sicherheitsabnahme in der Deutschen Bank wurde Linux nicht anders behandelt als kommerzielle Unixderivate. Dies betrifft insbesondere die zugrundegelegten Sicherheits- und Betriebsstandards. Im Gegensatz zu einigen anderen Betriebssystemen erfüllte Linux unsere anspruchsvollen Standards größtenteils schon ohne Modifikation der ursprünglichen Konfiguration.

Allerdings ist Sicherheit ein Prozess und kein Zustand. Deshalb ist auch die Sicherheit von Banksystemen viel weniger von den eingesetzten Plattformen wie Linux abhängig als von der Sicherheitsorganisation, die deren Einsatz steuert. Gerade im Hinblick auf die oben skizzierte zunehmende wirtschaftliche Bedeutung des Open-Source-Betriebssystems auch für unsere Bank waren die frühe Adaption von Linux und der Lernprozess, der für unsere IT-Organisation daraus resultierte, notwendige Schritte.

Neben den klassischen Sicherheitszielen wie Verfügbarkeit, Integrität und Authentizität von IT-Systemen ist im betrieblichen Umfeld zudem noch die Investitionssicherheit von besonderer Bedeutung. Diese bezieht sich sowohl auf den Schutz bereits getätigter Investitionen als auch auf die Zukunftssicherheit aktueller Investitionsentscheidungen. Im Hinblick auf die getätigten Investitionen sollte man daher nicht erwarten, dass Linux beispielsweise die mainframebasierten Systeme im Finanzsektor in naher Zukunft ersetzt. Ebenso wenig sollte man erwarten, dass sich Linux in naher Zukunft zum dominanten Desktopbetriebssystem im Finanzsektor entwickelt. Zu groß wäre der Aufwand bei der Mitarbeiterschulung für das neue Betriebssystem. In Bezug auf künftige Investitionen in Linux-basierte Systeme kann man inzwischen darauf bauen, dass dieses Betriebssystem bei einer Vielzahl von namhaften Herstellern dauerhaft verankert ist. Im Hinblick auf die bestehende (und zunehmende) Verfügbarkeit von Software, Dienstleistungen und Komplettlösungen im Linux-Umfeld erscheint es in der Tat nicht unwahrscheinlich, dass sich Linux zu einem dominanten Serverbetriebssystem entwickelt, wie die Butler Group dies prognostiziert. Aus dem gleichen Grund erscheint die Prognose von db-research nicht übertrieben, dass sich Open-Source-Kompetenz zu einem wichtigen Kriterium in Unternehmensbewertungen und Investitionsentscheidungen entwickeln könnte [Hofm02].

Ob sich diese Prognosen im vollen Umfang erfüllen, ist dabei für die Bedeutung von Linux für die Industrie von erheblicher Wichtigkeit. Allerdings hat schon die alleinige Existenz einer leistungsfähigen Alternative zu proprietären Systemen einen mäßigenden Einfluss auf die Lizenzkosten. Darüber hinaus erlaubt der Einsatz kostengünstiger Hardware unter Linux einen wichtigen Beitrag zur Kostensenkung in Unternehmen.

Literatur (Auswahl)

[BlDa02] *Blowers, Mark; Davis, Mike; Holt, Maxine:* Server Operating Systems Report – Winners & Losers in the Open/Proprietary OS Market. Butler Direct Limited, Hull, 2002.

[Clay97] *Clayton Christensen:* The Innovator's Dilemma. Harvard Business School Press, Harvard 1997.

[Golt03] *Goltzsch, Patrick:* Schneller Rechnen. In: CIO Magazin (2003) 4.

[Hofm02] *Hofmann, Jan:* Free software, big business? In: Deutsche Bank Research, E-conomics (2002) 32.

Hermann-Josef Lamberti,
Chief Operating Officer,
Deutsche Bank AG

Freie Software in der Sicherheitsstrategie der Behörden von Udo Helmbrecht

Ereignisse wie der Terroranschlag am 11. September 2001, Katastrophen wie das Elbehochwasser 2002 und erfolgreiche Angriffe wie *Loveletter* zeigen immer wieder, wie abhängig die Gesellschaft von einer reibungslos funktionierenden Informationstechnik (IT) ist. Um die Verletzlichkeit der Informationsgesellschaft zu reduzieren, gilt es, die zum Einsatz kommende IT zu diversifizieren. Es darf in Zukunft nicht möglich sein, dass durch ungewollte oder vorsätzliche Angriffe auf die IT aufgrund der globalen Vernetzung flächendeckende Ausfälle und Schäden verursacht werden können.

Dem der Biologie entlehnten Prinzip der Vermeidung von Monokulturen folgend gilt es, im Sinne der IT-Sicherheit auch die Vielfalt der Informationstechnik zu fördern. Dazu unterstützt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Bundesministerium des Innern (BMI) in dem Bemühen, den Einsatz Freier Software insbesondere im Behördenbereich zu fördern. Ziel ist es, die Nutzung der am Markt verfügbaren proprietären und Freien Software in einem integrierten, heterogenen Umfeld zu ermöglichen.

Bei der Frage, wie die IT-Sicherheit im Open-Source-Umfeld derzeit einzuschätzen ist, müssen sowohl technische als auch strategische Aspekte berücksichtigt werden.

Technische Aspekte

Technisch gesehen ist die Aufgabe jeder IT-Sicherheitsmaßnahme die Gewährleistung der Verfügbarkeit, Vertraulichkeit und Integrität der IT-Systeme und Daten. Welche Möglichkeiten bietet hier die Verwendung von Freier Software und welche nicht? Dies wird im Folgenden am Beispiel einiger zentraler Aspekte beleuchtet.

Sicherheitsprüfung

Der Zugang zum Quellcode ist eine notwendige, wenn auch keine hinreichende Voraussetzung für die Sicherheitsüberprüfung von Software. Der dafür vorgesehene internationale Standard (*Common Criteria*) zur Prüfung (Zertifizierung) von Softwareprodukten fordert z. B. für eine Reihe der vorgesehenen Prüfschritte die Offenlegung der Quellen.

Viele Softwareprodukte und einige Betriebssysteme sind bereits oder werden demnächst nach *Common Criteria* zertifiziert. Zur Zeit findet auch für das Betriebssystem Linux eine solche Prüfung statt.

Auch bei nicht zertifizierter Software können Aussagen über die Codequalität und den Sicherheitswert des Softwareprodukts getroffen werden: Die Offenlegung des Quellcodes bei Freier Software ermöglicht es einer breiten Basis von Testern, einen Blick ins „Software-Innere“ zu werfen. Darüber hinaus besteht auch die Möglichkeit, Sicherheitsanalysen auf Source-Code-Basis unabhängig vom Entwickler in Auftrag zu geben.

Sicherheitslücken

Die vielfach geäußerte Vermutung, durch die Geheimhaltung des Quellcodes von Software (Security by Obscurity) Sicherheitslücken schwerer auffindbar zu machen, hat sich leider in der Realität nicht bewahrheitet, wie die täglich in der Fachpresse veröffentlichten Beispiele zeigen. Ein sicherheitstechnisch bedenklicher Code wird nicht allein dadurch besser, dass der Quellcode nicht direkt zugänglich ist. Denn auch übersetzter Quellcode kann insbesondere durch Profis in vielen Fällen mit genügend hohem Aufwand analysiert werden.

Das Vorhandensein von Sicherheitslücken und Softwarefehlern ist ein Sicherheitsrisiko, das durch den Einsatz von sogenannten Sicherheitsanalysen (Audits) im Quelltext am einfachsten minimiert werden kann.

Ein weiterer wichtiger Aspekt nach dem Auffinden von Sicherheitslücken ist eine kurze Reaktionszeit bis zur Bereitstellung einer Fehlerbehebung. Hersteller proprietärer Software sowie Entwickler Freier Software bemühen sich, Sicherheitsupdates zeitnah zur Verfügung zu stellen.

Mit Freier Software ist die Anwendergemeinde zudem in der Lage, Fehler selbst zu beheben – ein Vorgehen, dass bei proprietärer Software aus lizenzrechtlichen Gründen meist untersagt ist.

Selbst wenn der öffentlichen Verwaltung der Einblick in proprietäre Software von den Herstellern relativ leicht gewährt wird, so ist dies ein Privileg, das der Wirtschaft, vor allem dem Mittelstand, oft nicht zuteil wird.

Härtung des Systems

Je „minimaler“ und übersichtlicher ein System aufgebaut ist, desto sicherer kann es gemacht und umso besser kontrolliert werden. Dies gilt auch für Software. Der zentrale Aspekt ist hier die Modularität: Sie ermöglicht eine Minimierung der Funktionen und reduziert so die Fläche für potentielle Angriffe. Gleichzeitig wird die Ausfallsicherheit erhöht.

Freie Software wird durch den Entwicklungsprozess sehr modular entwickelt und kann daher meist leicht minimiert werden. Das Gleiche gilt für einen Teil der proprietären Software.

Ein Beispiel für die Modularisierung und die damit mögliche Minimierung bietet der Linux-Kernel. Das BSI hat diese Möglichkeiten genutzt, um eine Sichere-Inter-Netzwerk-Architektur (SINA) zu schaffen. SINA ermöglicht PC-Anwendern die verschlüsselte Übertragung von Informationen mit sehr hohem Schutzbedarf über öffentliche, ungeschützte Netze und so die exklusive private Kommunikation zwischen verschiedenen Zugangspunkten. Zum Einsatz im SINA Projekt wurde der Linux-Kern auf die wesentlichen, absolut notwendigen Teile reduziert, überprüft, verbessert und gesichert. Das SINA-System dient unter anderem zur Vernetzung der deutschen Botschaften und Auslandsvertretungen.

Softwarevielfalt

Ein wichtiger Aspekt in einer großen IT-Umgebung ist der Aspekt der Softwarevielfalt. Ein homogenes IT-System ist genauso angreifbar durch Viren wie eine Monokultur durch Schädlinge. Nur so konnte es passieren, dass durch den *Loveletter*-Virus ein derart großer Schaden angerichtet wurde.

Freie Software schützt zwar nicht automatisch vor Viren, zur Zeit sind jedoch meist proprietäre Systeme Ziel der Virenattacken. Dies könnte sich in Zukunft mit der Verbreitung Freier Software auf dem Desktop relativieren.

Insgesamt wird durch Softwarevielfalt die Sicherheit in der Informationstechnik erhöht, gleichzeitig aber auch die Komplexität des Systems. Zudem muss die Kommunikation der verschiedenen Systeme sichergestellt werden.

Strategische Aspekte

Interoperabilität

Wichtig bei der Auswahl der IT-Systeme ist die Interoperabilität der Systeme. Um die Kommunikation der Softwarekomponenten untereinander und mit anderen Systemen zu gewährleisten, ist die Verwendung offener Standards und Schnittstellen unabdingbar. Um vielfältige Programme einsetzen zu können und die Kompatibilität sicherzustellen, sollten Standards frei zugänglich dokumentiert und einsetzbar sein – wobei nur von offenen Standards gesprochen werden kann, wenn unabhängige Implementierungen realisiert werden können.

Erst offene Standards und Schnittstellen ermöglichen, dass eine Produktpalette im Sinne der Diversifizierung zur Verfügung steht – sowohl als Freie Software als auch als kompatible proprietäre Software.

Die erreichbare Marktbreite von Entwicklungsfirmen, die die offenen Schnittstellen nutzen können, erhöht darüber hinaus die Verfügbarkeit der notwendigen Produkte. Letztlich fördert die Stabilität eines offenen Standards auch die Qualität der Software.

Support

Support für Freie Software kann genau wie für proprietäre Software bei qualifizierten Unternehmen eingekauft werden. Ein Unterschied ist der Umfang des Supports für Freie Software.

Auf der einen Seite ist der Support für Installation und Wartung der Software bei Freier und proprietärer Software gleich. Man kann beliebige Unternehmen damit beauftragen oder den Support selbst übernehmen.

Anders sieht es bei der Behebung von Sicherheitslücken aus. Hier ist man bei proprietärer Software auf den Hersteller angewiesen und darauf, dass dieser die Lücken schnell behebt. Bei Freier Software kann die Behebung der Sicherheitslücken direkt durch die Softwareentwickler geschehen. Der Anwender hat aber auch die Möglichkeit, diese bei einem beliebigen qualifizierten Softwareunternehmen zu beauftragen. Beispiele haben gezeigt, dass beide Verfahren gut in der Praxis funktionieren können, wobei hervorzuheben ist, dass auch bei proprietärer Software in der Regel kein An-

spruch auf die Behebung von Sicherheitslücken besteht.

Das Gleiche gilt für die Anpassung und Weiterentwicklung von Software: Bei proprietären Produkten übernimmt dies der Hersteller. Dies sichert meistens regelmäßige Releasezyklen mit neuen Funktionalitäten. Der Anwender hat begrenzt Einfluss darauf. Auch Freie Software hat Releasezyklen, in denen neue Funktionalitäten in die Software einfließen. Weiterentwicklungen, die nicht durch die Entwickler aufgegriffen werden, aber den Einsatz im eigenen Unternehmen verbessern, können jedoch bei unabhängigen Softwareunternehmen in Auftrag gegeben werden.

Investitionssicherheit
Ein wichtiges Kriterium bei der Auswahl von Software ist die Herstellerunabhängigkeit. Die Insolvenz eines Softwareherstellers bedeutet für den Nutzer von dessen Software in der Regel den Kauf und die Einführung eines neuen Softwareproduktes. Wie die Praxis zeigt, müssen heutzutage nicht nur kleine und mittelständische Unternehmen Insolvenz anmelden, sodass Investitionen in deren Software verloren sind.

Um herstellerunabhängig zu bleiben, gibt es mehrere Möglichkeiten, so z. B. den Einsatz Freier Software oder die Sicherstellung des Zugriffes auf den Quellcode proprietärer Software im Insolvenzfall.

Eine Möglichkeit, die immer häufiger eingesetzt wird, ist die Hinterlegung des Quellcodes proprietärer Software bei einem Notar. Bei Insolvenz wird dem Lizenznehmer voller Zugriff auf die Quellen gewährt. Dies erfordert allerdings die Einwilligung des Herstellers. Die Lizenzen Freier Software sichern den Zugang zum Quellcode sowie das Recht, diesen zu verändern und einzusetzen. Mit dem Besitz des Quellcodes und dem Recht, diesen zu ändern und in der veränderten Form auch einzusetzen, ist ein Investitionsschutz erreicht.

Planungssicherheit
Über das hinaus, was bereits im Abschnitt Investitionssicherheit gesagt wurde, ist ein zusätzlicher Aspekt der Planungssicherheit die Verfügbarkeit abwärtskompatibler Versionen von Software. Die meisten Hersteller achten darauf, dass ihre Software abwärtskompatibel ist. Dies gelingt meistens solange, bis ein Redesign stattfindet oder wesentliche Funktionen geändert werden. Das ist auch bei Freier Software der Fall.

Die Wartung von älteren Versionen entfällt meistens nach einiger Zeit. Bei Freier Software lässt sie sich im Bedarfsfall noch über Supportverträge einkaufen. Das Gleiche gilt für die Weiterentwicklung von älteren Versionen.

Fazit: Sicherheit ist ein Prozess.
Der erfolgreiche Erhalt von IT-Sicherheit bedingt die genaue Kenntnis des IT-Systems sowie eine regelmäßige Wartung und eine schnelle Behebung von Sicherheitslücken. Der Einsatz Freier Software hat in diesem Prozess einige strategische Vorteile, bietet jedoch keine Gewähr für ein sicheres System. Das notwendige IT-Sicherheits-Know-how sowie gute, an die jeweiligen Anforderungen angepasste Lösungen sind unumgänglich.

Unabhängigkeit und Softwarevielfalt sowie die Verwendung offener Standards sind eine Basis für IT-Sicherheit. Diese sollten als zentrale Aspekte in den Auswahlprozess für Softwareprogramme eingehen.

Dr. Udo Helmbrecht,
Präsident des Bundesamtes für Sicherheit
in der Informationstechnik

Die Sicherheit von Software wird nicht allein durch deren Quellcode bestimmt
von Harald Lieder

Vielfach wird behauptet, Open-Source-Software (OSS) sei grundsätzlich sicherer als proprietäre Software. Als Beleg hierfür werden Statistiken angeführt, die zeigen, dass z. B. Microsofts Webserver IIS im Verhältnis öfter erfolgreich attackiert wurde als das Open-Source-Gegenstück Apache. Aus meiner Sicht ist grundsätzlich fraglich, ob solche Statistiken tatsächlich den direkten Rückschluss auf die Sicherheit des Produkts erlauben. Zum einen wird mit wachsender Verbreitung von OSS im kommerziellen Bereich diese auch für Hacker immer interessanter, zum anderen können die Ursachen erfolgreicher Angriffe nicht ausschließlich auf das Entwicklungsmodell (Open/Closed Source) der Software reduziert werden. Zudem sollte das Thema „Sicherheit“ bei Software nicht nur unter dem Gesichtspunkt einer Offenlegung des Quellcodes diskutiert werden.

Weder das Offenlegen des Quellcodes alleine noch dessen Geheimhaltung schafft mehr Sicherheit
In den Diskussionen über den Zusammenhang von frei zugänglichem Quellcode und der Sicherheit von Software tauchen immer wieder die beiden folgenden Argumente für und wider Open Source auf: Auf der einen Seite ist zu hören, dass OSS sicherer sei, da eine Vielzahl von Entwicklern den Quellcode auf Sicherheitslücken hin untersuchen. Auf der anderen Seite wird genau diese Offenheit als Argument gegen OSS verwendet: Es wird argumentiert, dass Hacker im Quellcode nach sicherheitsrelevanten Schwachstellen suchen und diese gezielt ausnutzen könnten. Aus meiner Sicht müssen beide Argumente relativiert werden:

Die Tatsache, dass der Quellcode eines Programms einseh- und veränderbar ist und von einer Vielzahl von Entwicklern geprüft werden kann, macht ein Programm noch lange nicht sicher. Es kann sogar dazu führen, dass sich ein falsches Sicherheitsgefühl einstellt. Das „Viele-Augen-Prinzip“ hat nur Erfolg, wenn tatsächlich Security-Reviews durchgeführt werden und die Entwickler, die sich den Code ansehen, entsprechend fundierte technische Kenntnisse im Bereich Softwaresicherheit besitzen. Dass dies nicht selbstverständlich ist, zeigen Open-Source-Programme wie GNU Mailman und wu-ftp, bei denen gravierende Sicherheitslücken auch über eine lange Zeit hinweg trotz diverser Reviews Bestand hatten. Mitwirkende in Open-Source-Projekten untersuchen zudem einen fremden Code meist aus eigenem Interesse und weniger aus altruistischen Beweggründen. Deshalb haben Programme im Open-Source-Bereich, deren Quellcode nur schwer entwirrbar ist oder in einer unpopulären Programmiersprache geschrieben wurde, oft nur eine geringe Anzahl von Reviewern. Dies sollten Anwender von OSS bei der Softwareauswahl beachten, da bei zu wenigen Reviewern ein sicheres Kontrollverfahren nicht garantiert ist.

Auf der anderen Seite wird Software jedoch nicht automatisch dadurch sicherer, dass der Quellcode unveröffentlicht bleibt. Durch Reverse Engineering ist es heute jedem Hacker möglich, die Binärdateien in der einen oder anderen Form lesbar zu machen und nach Mustern für Sicherheitslücken zu durchsuchen.

Ein Problem von Closed-Source-Software ist sicherlich die potenzielle Möglichkeit der Programmierer, sich Hintertürchen für administrative oder andere Zwecke offen zu lassen und damit in Bezug auf die Sicherheit der Software Lücken zu schaffen. Bei in einer Versionskontrolle befindlichen Open-Source-Projekten ist dies eher unwahrscheinlich. Die Gefahr, dass andere Entwickler solche „Kuckuckseier“ entdecken und dass der entsprechende Programmierer seinen in der Open-Source-Gemeinschaft so wichtigen eigenen guten Ruf verliert, ist sehr hoch. Deshalb tauchen in der Praxis auch fast ausschließlich in proprietärer Software solche für den Anwender sicherheitsrelevanten Disfunktionalitäten auf. Aus eben diesem

Grund versuchen in letzter Zeit die Hersteller proprietärer Software das Misstrauen, das vor allem Regierungsinstitutionen dem Closed-Source-Modell entgegenbringen, durch teilweise oder komplette Offenlegung des Quellcodes abzubauen. Ein Beispiel ist die Shared-Source-Initiative von Microsoft. Nachdem Microsoft bereits seit zehn Jahren akademischen Institutionen den Windows-Quellcode für Forschungszwecke zur Verfügung gestellt hat, richtet sich diese neue Initiative nun hauptsächlich an Großkunden, Regierungsinstitutionen und Systemintegratoren mit dem Ziel, eine größere Transparenz bezüglich des Quellcodes zu erreichen.

Eine Ungewissheit über mögliche Sicherheitslücken im Quellcode besteht damit sowohl bei Open als auch bei Closed Source. Werden an eine Software durch den Nutzer extreme Sicherheitsanforderungen gestellt und traut der Nutzer weder den Reviewprozessen der Open-Source-Entwickler noch den Standards kommerzieller Softwareanbieter, so bleibt als Ausweg nur das selbstständige Durchsuchen des Codes auf mögliche Schwachstellen.

Kleinere Unternehmen oder Konzerne, die die Softwareauswahl den einzelnen Abteilungen überlassen, können sich aber den Aufwand, Tausende von Zeilen Quellcode auf Herz und Nieren zu prüfen, aus Mangel an Zeit, Geld und Ressourcen oft nicht leisten. In diesem Fall ist es letzten Endes eine Frage des Vertrauens, ob man die Überprüfung des Codes vielen, unabhängigen Entwicklern der Open-Source-Gemeinde oder aber wenigen, dafür auf Sicherheitsfragen spezialisierten Mitarbeitern eines Softwareherstellers überlässt.

Viele Angriffe auf IT-Systeme waren letztendlich nur deshalb erfolgreich, weil versäumt wurde, rechtzeitig die aktuellsten Servicepacks einzuspielen

Beurteilt man Software unter Sicherheitsgesichtspunkten, so sollte man sich aber grundsätzlich nicht nur mit der Frage der Öffentlichkeit des Programmcodes beschäftigen. Genauso wichtig ist es zu überprüfen, wie viele entdeckte Sicherheitslücken veröffentlicht wurden, wie lange es dann gedauert hat, bis die entsprechenden Korrekturen zur Verfügung standen, und wann diese schließlich von Systemadministratoren eingespielt wurden.

Open-Source-Projekte reagieren auf öffentlich bekannt gewordene Sicherheitslücken im Allgemeinen schneller als Hersteller proprietärer Software; die anschließende Verteilung der Software in den Unternehmen läuft dann aber meist nicht mehr so problemlos. Grund hierfür ist, dass die Existenz neuer Patches meist über Mailinglisten oder Userforen bekannt gegeben wird. Dies erfordert ein ständiges, aktives Überwachen dieser Kommunikationskanäle.

Dagegen brauchen Hersteller kommerzieller Software mit ihrer Reaktion meist etwas länger, allerdings haben einige von ihnen schon Verfahren, bei denen die aktuellsten Servicepacks und Korrekturen sofort nach deren Freigabe automatisch heruntergeladen werden können.

Schwer zu konfigurierende Software, unzureichende Dokumentation und fehlende Schulung bergen weitere Sicherheitsrisiken

Nicht selten ist aber auch eine fehlerhafte Konfiguration eines Programms für Sicherheitslücken in der Software eines Unternehmens verantwortlich. Der Grund hierfür ist die oft unzureichende Schulung der Administratoren und eine mangelhafte Dokumentation. Hier hat OSS eindeutig Nachteile, denn oft ist die Dokumentation von OSS nur für Experten verständlich. Gerade für eher unerfahrene Entwickler und Administratoren ist das Verständnis über Funktionsweise und Konfiguration sicherheitsrelevanter Systeme aber von grundlegender Bedeutung. Auch Schulung bzw. Training wird oft nur für populäre OSS angeboten und dann meist von lokal tätigen Anbietern. Für globale Unternehmen, die eine einheitliche Ausbildung ihrer Administratoren anstreben sollten, kann dies keine befriedigende Lösung sein.

Investitionssicherheit ist weitgehend unabhängig von der Frage, ob es sich um Open-Source- oder proprietäre Software handelt

Neben den sicherheitsrelevanten Punkten technischer Natur muss die Frage nach der Investitionssicherheit des Produkts geklärt werden. Aufgrund des Marktdrucks sind die Hersteller proprietärer Software gezwungen, in immer kürzeren Zeitzyklen neue Versionen ihrer Programme auf den Markt zu bringen. Sind für ein Unternehmen die Kosten der Umstellung auf eine neuere Version zu hoch, leidet es dann in der Folge unter auslaufenden Supportverträgen oder höheren Wartungskosten für ältere Versionen. Das gleiche Problem stellt sich auch für Nutzer von Open-Source-Produkten, sogar noch in einer verschärften Form. Bei großen Open-Source-Projekten werden vor allem in der Anfangsphase neue Versionen in sehr kurzen Zeitabständen zur Verfügung gestellt. Entscheidet man sich nun aus Kosten-, Stabilitäts- oder sonstigen Gründen dafür, ein Release länger beizubehalten, sieht man sich mit einem ständig sinkenden Interesse der Entwicklergemeinde konfrontiert, sich Problemen zurückliegender Releases anzunehmen und dafür passende Lösungen anzubieten.

Die Angst, die Weiterentwicklung von Open-Source-Produkten sei nicht gesichert, ist allerdings für populäre OSS mit großer, aktiver Entwicklergemeinde unbegründet. Zusätzlich versuchen Konzerne wie IBM, HP oder Sun durch eigene oder gesponserte Open-Source-Projekte Investitionssicherheit zu gewährleisten.

Fazit

Die Frage nach der Sicherheit von Software kann nicht pauschal durch die Empfehlung des Open- oder Closed-Source-Modells beantwortet werden. Ob der Anwender von offenem und veränderbarem Quellcode überhaupt profitieren kann, richtet sich nach seinem Sicherheitsbedürfnis und nach der Möglichkeit, den Code in einem ökonomisch vertretbaren Rahmen selbst zu überprüfen. Daneben sind noch andere Punkte bei der Entscheidungsfindung für Software unter Sicherheitsaspekten wichtig, die zum Teil unabhängig vom Entwicklungsmodell sind. Hierzu gehören vor allem folgende Punkte:

- Welche formalen Securityreviews für die Software wurden durchgeführt?
- Wer hat diese Reviews durchgeführt?
- Auf welchem Weg soll die Versorgung mit aktuellen Patches bzw. Servicepacks erfolgen?
- Mit welchem Aufwand und mit welchen Kenntnissen ist eine sichere Konfiguration und Handhabung der Software möglich?
- Ob und in welchem Umfang sind Dokumentation und Schulungen für das entsprechende Produkt verfügbar?
- Ist der Support auch älterer Releases der eingesetzten Software in Zukunft gesichert?

Jeder dieser Punkte sollte sowohl nach Relevanz für den Anwender als auch nach dessen zur Verfügung stehenden Möglichkeiten, wie z. B. Zeit, Budget und Expertise der eigenen Mitarbeiter bewertet werden. Erst dann kann die Auswahl für ein passendes Produkt getroffen werden – ohne vorher grundsätzlich pro oder contra Open Source entschieden zu haben.

Harald Lieder,
Leiter des Bereichs Global
Architecture & Core Technologies ASG,
Accenture GmbH

Offen, transparent . . . sicher?
von Thomas Mangel

Die aktuellen Diskussionen um Open-Source- versus Closed-Source-Systemen scheinen stark von subjektiven Argumenten geleitet und führen in einigen Bereichen zu einer gewissen Zurückhaltung gegenüber der euphorischen Begrüßung von Open-Source-Systemen in einer breiten Anwenderschicht. Dennoch stützen Veröffentlichungen wie [BaRe00] die Erfahrung, dass Open-Source-Systeme in Bezug auf geschäftsorientierte Werte eines Unternehmens, wie z. B. Wirtschaftlichkeit, Verfügbarkeit und nicht zuletzt Sicherheit mehr zu bieten haben, als nur ein politisches Statement.

Als Bank sind wir dem Vertrauen unserer Kunden besonders verpflichtet, als Multikanalbank hat die Verfügbarkeit unserer Leistungen eine immense Bedeutung, als Internetbank müssen unsere elektronischen Transaktionen mit entfernten Geschäftspartnern absolut integer sein, und diese Partner müssen wir als solche auch sicher identifizieren können. Somit lassen sich die Grundwerte der IT-Sicherheit für die Postbank festhalten als Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit und Verfügbarkeit.

Bezieht man diese Grundwerte in die Diskussion um die Sicherheit in Open-Source-Systemen ein, ergibt sich ein Bild, aus dem man die objektiven Werte für die Bank sehr wohl herauslesen kann. Und so sind Open-Source-Produkte bereits ein unverzichtbarer Bestandteil der IT-Infrastruktur der Postbank. Auch in sicherheitssensiblen Bereichen werden Open-Source-Produkte gezielt eingesetzt.

Institutionen mit besonders hohen Sicherheitsanforderungen haben seit längerem erkannt, dass die Möglichkeit, die Funktions- und Verarbeitungsabläufe in einem System einsehen zu können, Grundlage zur Beurteilung der Sicherheit von Software ist [BaRe00; BSIT03; BMWT01]. Als Kunde eines Softwareprodukts ist dies naturgemäß nur bei Open Source der Fall. Die gleichzeitig geführte Argumentation, dass dann natürlich auch Hacker den Code verändern können und nicht jeder den Code versteht, um die Sicherheit beurteilen zu können, wurde durch die faktische Erfahrung der letzten Jahre im wesentlichen entschärft.

Eine Offenlegung des Quellcodes einer Software ist aber kein Garant für die Sicherheit und Qualität dieser Software. Denn die Erkenntnisse über Fehler und Verbesserungen der Software müssen wieder kontrolliert in das System einfließen. Auch wenn „tausende Augen“ jederzeit die Software bis auf die Fundamente einsehen und daran arbeiten, ist im Gegensatz zu oft zitierten Aussagen keine Sicherheit für das Vertrauen in diese Software ableitbar [Raym98].

Daher schützen viele Open-Source-Projekte ihre Programmentwicklung inzwischen durch die Nutzung zentraler Entwicklungsplattformen. Dort können viele Entwickler, die meist namentlich bekannt und persönlich erreichbar sind, gemeinsam arbeiten, die Veränderung werden immer automatisch sichtbar und Kollisionen in der Entwicklung können vermieden werden. Bei diesen Systemen führt der Synergieeffekt hunderter bis tausender Expertisen zu ungeheueren Innovationsschüben auch in Punkten der Sicherheit.

Im Gegensatz dazu lässt sich diese Transparenz bei der Entwicklung und Einführung von Closed-Source-Systemen nicht aufweisen. Hier führen Abhängigkeiten von Wiederverwertbarkeit, Marktanteilen, Imagewerten und Zeithorizonten der Partnerschaften zu komplexeren Vertrauensstrukturen die meist langjährig erarbeitet werden. Qualität und Sicherheit wird den Erfordernissen entsprechend aus beiderseitigen Kosten- und Nutzenrechnungen eingestellt. Steuerungsmittel sind die definierten Vertragsverhältnisse.

Da es diese Vertragsverhältnisse bei Open-Source-Systemen nicht gibt, scheint ein nicht berechenbarer Zustand vorzuliegen. Hierzu existieren jedoch interessante Erhebungen, in denen z. B. aufgezeigt wird, wie die Anzahl der Fehler in einer Software während der Programmentwicklung durch Alpha- und Betatests reduziert wird und vergleicht diesen Prozess bei offenen und proprietären Systemen. Das Ergebnis ist erstaunlich: Während in der Theorie dieser Prozess für beide Systeme von unterschiedlichen Ausgangspunkten auf das gleiche Niveau läuft, führen langjährige Analysen realer Projekte zu einer Begünstigung von Open-Source-Systemen.

Die Ursachen hierfür sind äußerst vielschichtig und daher in kaum einem Modell wiederzufinden. Stark vereinfacht lässt sich sagen, dass bei Closed-Source-Systemen Kunde und Hersteller aufgrund ihrer Interessenlage oftmals gegensätzliche Standpunkte beziehen müssen und die Entwicklung quasi ein Verhandlungsprozess ist. Im Gegensatz dazu stehen bei Open-Source-Systemen Kunde und Entwickler nicht nur auf der selben Seite, sie sind ebenso oft identisch. Der sich daraus ergebende Aspekt zur Beurteilung der IT-Sicherheitsrisiken muss daher die Interessen der Beteiligten einbeziehen. Grundvoraussetzung und somit Limitierung des Open-Source-Systems ist selbstverständlich das Vorhandensein eines breiten Interesses der gebotenen Funktionalität. „Kundenspezifische“ Anforderungen und Lösungen sind nicht im Modell vorgesehen.

Als Argument gegen den Einsatz von Open-Source-Software wird häufig der Investitionsschutz angeführt. Hierbei wird angenommen, dass ein Open-Source-Produkt nur solange weiterentwickelt wird, solange es „Hype“ ist und dann der Anwender eine evtl. fehlerbehaftete veraltete Anwendung betreiben muss, für die er keinen Support mehr bekommt, wohingegen Closed-Source-Software durch Pflegeverträge, in denen die Hersteller sich zur Weiterentwicklung verpflichten, gegen solche Unwägbarkeiten abgesichert sei. Die Vergangenheit hat aber leider gezeigt, das auch Closed-Source-Produkte dieses bei Open-Source-Systemen befürchtete Schicksal erleiden. Denn ist eine Software – gerade für ein Großunternehmen mit breitem Portfolio – unrentabel, dann wird sie häufig nicht mehr weiterentwickelt. Bei einigen Produkten hat dies zu Firmenausgründungen geführt, die dann die Betreuung der „Altkunden“ übernommen haben.

Im Open-Source-Bereich werden bestimmte Produkte auch „abgekündigt“, dann jedoch häufig durch andere Entwicklergruppen übernommen. Wegen der Open-Source-Lizenzen ist eine Übernahme und Betreuung durch andere Gruppen bzw. eigenes Knowhow auch wesentlich leichter möglich. Ein besonderes Beispiel ist hier die Weiterentwicklung des CERN-HTTP-Servers. Als dieses Projekt stockte, wurde kurzerhand ein neues Projekt geschaffen: Apache. Heute ist der Apache-HTTP-Server der im Internet am weitesten verbreitete und weltweit am häufigsten eingesetzte Webserver.

Will man die IT-Ressourcen des Unternehmens langfristig effektiv nutzen und gleichzeitig die Geschäftsprozesse bezüglich der Grundwerte der IT-Sicherheit zuverlässig schützen, ist man auf eine umfassende Kontrolle über die eingesetzten IT-Werkzeuge angewiesen. Bei Programmen z. B. zur Wahrung der Vertraulichkeit ist es seit einigen Jahrzehnten schon so, dass ausschließlich offene Standards eingesetzt werden; in vielen Fällen, wie z. B. bei Behörden, ist der Einsatz gar zwingend.

Um die Sicherheit der IT eines Unternehmens zu gewährleisten, werden auch in Zukunft immer neue Herausforderungen zu bewältigen sein. Open-Source-Systeme bieten mit hoher Innovationsrate und naturgegebener Flexibilität eine Chance, die zwar ihren Preis hat, aber sicher kein „Irrweg“ im

Streben nach verlässlicheren IT-Systemen ist.

In sicherheitssensiblen Bereichen können Open-Source-Systeme durchaus mit Vorteilen gegenüber Closed-Source-Systemen aufwarten. Sie fördern offene Standards und vermeiden Softwaremonokulturen. Die Entscheidung zwischen funktionsgleichen Open-Source- und Closed-Source-Produkten ist jedoch in jedem Einzelfall auf Basis von Analysen der Wirtschaftlichkeit, der Absicherung der betrieblichen Verfügbarkeit und des angestrebten IT-Sicherheitsniveaus zu treffen.

Open-Source-Systeme werden schon heute vielfach in der Postbank-IT eingesetzt, die Tendenz ist steigend. Der Skill unserer IT-Mitarbeiter im Open-Source-Bereich ist inzwischen beeindruckend. Somit liegen alle Vorraussetzungen vor, sich des Themas Open Source innerhalb der Postbank geschäftsorientiert anzunehmen, eine Integration dieser Themen in unsere Organisationsstrukturen zur Bündelung von Kompetenzen und Verantwortungen findet statt.

Literatur (Auswahl)

[BaRe00] *Bahr, Rudolf E.; Reiländer, Ralf; Troles, Egon:* Open Source Software in der Bundesverwaltung. In: KBSt. Brief Nr. 2/2000.

[BSIT03] Bundesamt für Sicherheit in der Informationstechnik: Open Source Software. http://www.bsi-fuer-buerger.de/11/, Abruf am 2003-05-21.

[BMWT01] Bundesministerium für Wirtschaft und Technologie: Open Source Software – Leitfaden für kleine und mittlere Unternehmen.

[Raym98] *Raymond, Eric S.:* The Cathedral and the Bazaar. http://tuxedo.org/~esr/writings/cathedral-bazaar/cathedral-bazaar.html, 1998-08-08, Abruf am 2003-05-14.

[Möll01] *Möller, Erik:* Die Reformation zum Anfassen: GNU/Linux und Open Source. http://www.heise.de/tp/deutsch/inhalt/te/9786/1.html, 2001-10-12, Abruf am 2003-05-21.

[Ande02] *Anderson, Ross:* Security in Open versus Closed Systems The Dance of Boltzmann, Coase and Moore. http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf, 2002-06-18, Abruf am 2003-05-21.

[NSA03] *National Security Agency:* Security-Enhanced Linux Frequently Asked Questions. http://www.nsa.gov/selinux/faq.html, Abruf am 2003-05-21.

[Pesc03] *Pescatore, John:* Nimda Worm Shows You Can't Always Patch Fast Enough. http://www3.gartner.com/resources/101000/101034/101034.pdf, 2001-09-19, Abruf am 2003-05-22.

Dr. Thomas Mangel,
Chief Technology Officer,
Postbank Systems AG

Transparenz schafft Sicherheit
von Richard Seibt

Software – gleich, ob lizenziert, gekauft oder selbst entwickelt – verhält sich sicherheitstechnisch ungleich anders als anfassbare Maschinen, Werkzeuge, Büromöbel oder Verbrauchsmaterialien. Wer sich an Werbeaussagen der EDV-Frühzeit erinnert: „Dieser Schnellrechner erledigt in einer Minute die gleiche Arbeit, für die 5000 Mathematiker 13 Jahre bräuchten!", bekommt ein Gefühl für das Problem.

Natürlich erledigt der Schnellrechner überhaupt nichts, die Software tut's. Und wenn wir sicher sein wollen, dass sie genau das tut, was sie soll? Mit 5000 Mathematikern hätten wir es in 13 Jahren nachgerechnet. Oder sollen wir Testsoftware einsetzen, die selbst nur ziemlich fehlerfrei ist? Es ist eine nichttriviale und unexakte Wissenschaft, Software noch während ihrer Lebenszeit auf korrekte Funktion zu testen; Softwaretesting stellt eine eigene Industrie dar.

Wirtschaftlich sinnvolles Softwaretesting bringt zwar fehlerarme, doch kaum fehlerfreie Produkte auf den Markt. Dabei geht es nicht nur um unbeabsichtigte Fehler. Bei genügend kriminell untermauertem Marktmachtstreben könnte beispielsweise ein Unternehmen der Kosmetikindustrie ein Softwarepaket zur molekularen Modellierung von Faltenglättungssubstanzen anbieten, das garantiert nur Stoffe entwirft, die auf der Haut einen ausgeprägten Faltenwurf erzeugen. Bis der Wettbewerber dieses bemerkt, ist der Anbieter des quasi trojanischen Stoffpferdes längst Marktführer.

Mit dem industriellen Einsatz des Internets nun bringen Softwarefehler ein ganz neues Schadenspotenzial mit sich. Denn solch ein Fehler kann

- Beeinträchtigungen auf Fremdrechnern hervorrufen, für die wir zumindest zivilrechtlich haftbar sind,
- Informationen, deren Vertraulichkeit geschäftsentscheidend ist, über das Netz kompromittieren, bis wir wettbewerbsunfähig gemacht sind.

Es ist nicht Paranoia, an kriminelle Softwarefehler zu denken. Die National Security Agency (NSA) in den USA betreibt seit Jahren versteckte und direkte Finanzierungen von Unternehmen im Bereich Computersicherheit. Zuweilen dringen solche Bemühungen bis an die Oberfläche der Öffentlichkeit, wenn beispielsweise Autoren bestimmter Verschlüsselungsverfahren gerichtlich oder anderweitig bedroht oder größere Schlüssellängen einfach per Gesetz verboten werden. In Frankreich dürfen Unternehmen ihre Daten nur dann verschlüsselt übertragen, wenn Regierungsbehörden einen Zweitschlüssel erhalten. Und in Hongkong (wie in der restlichen Chinesischen Volksrepublik) ist Datenverschlüsselung unter Androhung drakonischer Strafen generell untersagt; einige Unternehmen haben deswegen ihre Hauptverwaltungen aus dem chinesischen Einflussbereich heraus verlagert.

Software auf (absichtlich oder unabsichtlich) versteckte Fehler zu untersuchen, gestaltet sich ungleich schwieriger, wenn der Quellcode nicht zu Verfügung steht und der übersetzte Binärcode analysiert werden muss. Das Ausmaß dieser Schwierigkeiten kann ermessen, wer als Veterinär Krankheiten eines Lebewesens diagnostizieren muss, dessen Anatomie ihm unbekannt ist.

Die traditionelle Softwareindustrie hat – ursprünglich, um geistiges Eigentum zu schützen – ein Übriges getan, Softwarepflege und Schutz vor Softwarefehlern weitgehend zu erschweren. Denn Software wird in aller Regel nicht verkauft, sondern eingeschränkte Nutzungsrechte werden lizenziert. Im Kleingedruckten der Lizenzierungsverträge werden bestimmte Rechte ausdrücklich ausgenommen, insbesondere das Recht, den Quellcode aus dem Binärcode zu restaurieren. Der Kunde verpflichtet sich also zu Schadenersatz, wenn er herausfinden möchte, was eine Software so alles bei ihm anstellt. Im selben Vertrag stellt sich der Softwareanbieter von der Haftung aus Fehlfunktionen frei.

Die Machtlosigkeit des traditionellen Softwarekunden zeigt sich besonders drastisch, wenn bei Online-Update-Prozeduren ein Fenster aufscheint: „Der Anbieter überträgt keine privaten Daten währen des Updates." Woher weiß denn der Anbieter, welche Daten privat sind? Hat er uns gefragt? Oder schon ausspioniert und vormundlich für uns entschieden, was wir als privat bezeichnen dürfen?

Das Minimum, was ein Kunde aus seinem eigenen Sicherheitsbedürfnis heraus von der Softwareindustrie erwarten darf, ja fordern muss:

- Der Anbieter muss Hilfsmittel mitliefern, die Fehlfunktionen aufspüren und beseitigen helfen. Das schlichtweg wichtigste Hilfsmittel ist der Quellcode.
- Will der Softwareanbieter den Quellcode nicht offen legen, so kann er die Haftung für Softwarefehler nicht auf den Kunden abwälzen. Die Lizenzverträge müssen das widerspiegeln.

Open Source als Geschäftsprinzip bestärkt somit die Kundenrechte deutlich. Der Kunde erhält uneingeschränkten Zugang zum Quellcode, kann ihn selbst nach Gutdünken analysieren und weiterverwenden. Open Source bringt als erwünschten Nebeneffekt durch das Prinzip, eine Vielzahl von Programmierern weltweit in jeder Projektphase Einblick in den Quellcode nehmen und die Programme schon in embryonaler Phase testen zu lassen, in aller Regel stabilere und weniger fehlerbehaftetere Programme. Bereits in den Anfangsjahren der Linux-Entwicklung wiesen deshalb Linux-Server legendäre unterbrechungsfreie Einsatzzeiten auf; Systeme, die in der traditionellen Softwarewelt auf Neustarts im Stunden- oder Tagesrhythmus angewiesen waren, liefen mit Linux Monate, sogar Jahre ohne softwarebedingte Unterbrechungen.

Sicherheit rund um Software erfordert Grundsatzentscheidungen. Auf die Auswahl der Lieferanten kommt es an. Die richtigen Lieferanten können folgende Fragen zufriedenstellend beantworten:

- Hast Du schon während der Softwareentwicklung eine breite, internationale Öffentlichkeit zum Testen eingesetzt?
- Darf ich deine Antworten nachprüfen (lassen) und mir deine Software im Quellcode ansehen?

Damit die Rechte der Kunden – insbesondere die Sicherheitsbedürfnisse – respektiert werden, hat sich SuSE unwiderruflich für Open Source als Geschäftsgrundlage entschieden. Mit Binärcode allein ist der Sicherheit kaum zu dienen.

Richard Seibt,
Chief Executive Officer,
SuSE Linux AG

Aus den Hochschulen

Prof. Harald Eichsteller, Jahrgang 1961, der als Manager E-Business und Geschäftsführer der Aral Online GmbH tätig war und nach der Fusion mit BP das Online-Business verantwortete, hat in der Hochschule der Medien (HdM) in Stuttgart eine Professur für Internationales Medienmanagement übernommen. Seine Arbeitsschwerpunkte sind Medienproduktion, Online-Marketing und E-Business.

Mario Jeckle, Jahrgang 1974, der bislang als Forschungsgruppenleiter bei DaimlerChrysler in Ulm beschäftigt war, hat an der Fachhochschule Furtwangen im Fachbereich Wirtschaftsinformatik den Ruf auf eine Professur für Software-Engineering angenommen. Seine Forschungsschwerpunkte sind Datendarstellung und -modellierung, insbesondere objektorientierte Modellierung mit UML sowie Weiterentwicklung und Anwendung der Metasprache XML (http://www.jeckle.de).

Das E-Finance Lab Frankfurt a. M., ein von der Wirtschaftspraxis (z. B. Accenture, Deutsche Bank, Deutsche Postbank, Microsoft, Siemens, T-Systems) für zunächst drei Jahre finanziertes und gemeinsam von den Universitäten Frankfurt a. M. und Darmstadt getragenes Forschungsprogramm, wurde mit einem Symposium, in dessen Rahmen der Hessische Ministerpräsident Koch und weitere Wissenschaftler und Praktiker das Wort ergriffen haben, eröffnet. Ziel ist die Entwicklung und Erprobung von Verfahren, um Finanzdienstleistungsunternehmen bei der Industrialisierung ihres Geschäfts zu unterstützen, z. B. hinsichtlich des Aufbrechens von bislang weitgehend hausintern realisierten Wertschöpfungsketten und deren neuartigen Zusammensetzung unter Einbezug von qualitätsgesicherten Zulieferungen. Seitens der Universitäten Frankfurt und Darmstadt tragen die **Professoren König**, **Skiera**, **Wahrenburg** und **Steinmetz** die Verantwortung (http://www.efinancelab.de).

Dr. sc. nat. Christopher Lueg, Jahrgang 1966, der seit seiner Promotion an der Universität Zürich als Senior Lecturer in Information Systems an der University of Technology, Sydney, Australien, tätig ist, hat einen Ruf auf den Stiftungslehrstuhl E-Business (Chair in E-Business, der von Computer Sciences Corp. (CSC) unterstützt wird) an der in Gründung befindlichen Charles Darwin University in Darwin, Australien, erhalten.

Prof. Dr. Thomas Myrach, Jahrgang 1961, vorher als Lehrstuhlvertreter an der RWTH Aachen tätig, hat einen Ruf auf eine ordentliche Professur für Wirtschaftsinformatik an der Universität Bern angenommen und ist seit Ende 2002 Mitdirektor des dortigen Instituts für Wirtschaftsinformatik. Seine Forschungsschwerpunkte sind Informationsmanagement mit dem Fokus auf Datenbanksystemen sowie die betriebliche Nutzung von Internettechnologien im Zuge des E-Business (http://www.im.iwi.unibe.ch/).

Prof. em. Dr. Dieter Preßmar, Jahrgang 1936, der an der Universität Hamburg bis 2002 das Institut für Wirtschaftsinformatik leitete, wurde von der Fakultät für Wirtschaftswissenschaften der Universität Siegen die Würde eines Doktors ehrenhalber verliehen. Die Laudatio betonte seine besonderen Leistungen bei Gründung und Aufbau des Fachs Wirtschaftsinformatik in der Bundesrepublik Deutschland.

Prof. Dr.-Ing. Rainer Schmidt, Jahrgang 1965, hat einen Ruf an die Fachhochschule Aalen auf eine Professur für Wirtschaftsinformatik angenommen. Zuvor war er in einer Unternehmensberatung sowie als Professor an der Berufsakademie Lörrach tätig. Seine Forschungsgebiete sind unternehmensübergreifende Geschäftsprozesse und deren Optimierung sowie IT-Management.

Prof. Dr. Eberhard Stickel, Jahrgang 1958, der an der Wirtschaftswissenschaftlichen Fakultät der Europa-Universität Frankfurt (Oder) die Professur für Allgemeine Betriebswirtschaftslehre, insbesondere Wirtschaftsinformatik, Finanz- und Bankwirtschaft, bekleidet, hat als Gründungsrektor die Leitung der Hochschule der Sparkassen-Finanzgruppe – University of Applied Sciences – in Bonn übernommen. Prof. Stickel wurde für seine neue Tätigkeit beurlaubt. Informationen über die Hochschule der Sparkassen-Finanzgruppe, die im Juli 2003 mit den ersten zwei Bachelor-Studiengängen, darunter ein Studiengang „Bachelor of Financial Information Systems“, startet, findet man unter http://www.s-hochschule.de.

Press Releases

Minister of Health Edelstein: "This Is What Your First Step on the Way Back to Normal Life Is Going to Look Like"

Subject: Coronavirus , Vaccines
Secondary topic : Ministry of Health , Updates , Coronavirus
Publish Date : 18.02.2021

The Green Pass, which will take effect this Sunday, has been presented in a press conference

Health Minister Edelstein: " This is what your first step on the way back to normal life is going to look like. Counterfeiters may also end up in prison".

He further said: "If we keep up the fast vaccination rate and follow the guidance – there might be no need for a fourth lockdown".

Minister of Health Yuli (Yoel) Edelstein, the Ministry of Health's Director General Prof. Chezy Levy abd top Ministry of Health officials presented today (Thursday) the Green Pass which will take effect this Sunday. In the press conference the issuing methods for the vaccination certificate were also presented, with a special emphasis on the certificate's security using QR code. The Ministry of Health will also launch a Green Pass campaign on Sunday.

Below are the Health Minister's words:

"Today we bring tremendous news to the vaccinated – this is what your first step on the way back to nearly normal life is going to look like.

Starting Sunday, vaccinated individuals and recovered coronavirus patients could go to gyms, shows, hotel and synagogues that will be registered as supporting the Green Pass.

Soon there will be workplaces where the employees will be required to vaccinate or to test for coronavirus every 48 hours in order to work.

The vaccination is a national task of the highest importance. Everyone is coming forward to lend a hand in this task, from the stage of bringing the vaccines, through the preparation stage and up to the public education campaign that the Ministry of Health has been working on for the last few months.

There is no and there will be no compulsory vaccination in Israel. Anyone has a right to choose to not vaccinate. Neither will there be any personal sanctions against anyone who will not vaccinate. You need to understood that each and every one of us has been given a great privilege to vaccinate, something that many countries around the world have not yet reached.

It is our duty to protect the health of all Israeli citizens, and we are not going to make any compromises on that.

Unfortunately, many of those vaccinated have decided that masks are no longer necessary. I ask you once again: Keep your masks on, even if you vaccinated. There is no other way to protect our health.

Someone may be sitting and feeling disappointed that he has not been vaccinated yet. It is not too late. We are also vaccinating 11th and 12th grade pupils. A class where everyone is vaccinated could be permitted to go on special activities during Passover that other classes might not be permitted to do. It's not too late to do so.

Over the next two weeks we will be launching a pilot run. For this transitory period, we consider the option to also allow the use of the vaccination certificate. I want to say to anyone dealing in counterfeiting – Know that we know about this possibility. Anyone thinking that this is child's play and print a vaccination certificate despite not having vaccinated will be caught eventually, and this game could also land him in prison. There is a long list of legal provisions that do not allow for the use of counterfeit certificates. You better be very careful.

As for what's next, this is up to all of us. If we keep up the fast vaccination rate and follow the guidance – there might be no need for a fourth lockdown."

Ministry of Health's Director General, Prof. Chezy Levy: "In a place where people vaccinate they could go to restaurants and to gyms, and in the future to also hold international activities"

We call upon the public to get vaccinated in order for us to come out of the situation that we're currently in, resume activities and go

back to our daily lives. We want everyone to be healthy. We do not know yet how much a vaccinated person could infect others. We know that they are less infectious – but we live with family members who cannot vaccinate and we want to protect our children's health.

As for counterfeit vaccination certificates or Green Passes: Today we held a meeting with senior police officials discussing enforcement and uncompromising punishments against providers and users of counterfeit Green Passes".

More on the subject

The Official COVID-19 Website of the Ministry of Health

All news

The green pass, certificate of recovery and vaccination certificate

This page was last updated on 18.02.2021

English

What is the Green Pass Scheme?

The Green Pass Scheme applies to everyone 3 years of age or older:
entry to venues that must comply with the Green Pass Scheme is permitted only if you show the Green Pass or a valid negative test result.
The limit on the Green Pass will be updated on 1.10.2021.

How is the Green Pass issued?

Entry to venues that comply with the Green Pass Scheme

You can enter a venue that complies with the Green Pass Scheme if you show one of the two documents below:

Green Pass with an I.D.
Negative test results (a rapid test or a privately-funded PCR test)

Access shall be denied to anyone who must stay in isolation or confirmed COVID-19 patients (if confirmed by contact tracing or positive PCR test result).

NOTE: Children 12 years and 3 months of age or younger with a quick access card (queue jumping) are exempt from presenting a Green Pass.

Showing the Green Pass

• Digital copy : You need to show the App screen with the animation. The venue can scan the Green Pass code with a special feature for venues in the Traffic Light App.
• Printed Green Pass , including the QR code.

The Pass should be presented with a document of identification (ID, driver's license, passport).

Minors who do not have an identification document yet may present their parent's identification document (or a photocopy thereof), including the slip, and their Green Pass (either on the application or in printed form).

Showing Test Results

You can show the QR code that you received after testing negative in one of the following tests as an alternative to the Green Pass:

Rapid test (antigen): valid for 24 hours from sampling time.
Everyone 3 to 12 years and three months of age and people with a contraindication to vaccination with the COVID-19 vaccine are eligible for

a publicly-funded rapid test in the stations accredited by the Ministry of Health.
Privately-funded PCR test: valid for 72 hours.

Further information on tests and rapid tests.

In hotels: When you check in, it will be possible to show PCR test results from the last 72 hours and these shall remain effective for the entire duration of the stay (children aged 3-12 and people with a contraindication to the COVID-19 vaccine who wish to take a vacation in a hotel in Israel may take a PCR test free of charge in HMO clinics or in Home Front Command's stations).

Information for business owners: "Green Pass guide for business owners"

How is the Green Pass issued?

Who is eligible for a Green Pass and what is its limit?

Vaccinated individuals

People who received three doses of the vaccine and a week has passed from the date of the third dose – the Green Pass is valid for six months from the date of the third dose.
People who received two doses of the vaccine and a week has passed (two weeks in case of the Moderna vaccine) from the date of the second dose – the Green Pass is valid until 31.12.2021. Effective 1.10.2021, the Green Pass shall become valid for six months from the date of the second dose.

Recovered individuals

People who have recovered from COVID-19 – the Green Pass is valid until 31.12.2021. Effective 1.10.2021, the Green Pass shall become valid for six months from the date of issuance of the recovery certificate.
People who have recovered from COVID-19 and received one dose of the vaccine – the Green Pass is valid for six months from the date of vaccination.

Effective 1.10.2021: to receive a Green Pass with updated limits, request the Green Pass again.

Tested individuals

Everyone 12 years of age or younger with a negative PCR test result taken as part of the Magen Education program – the Green Pass is valid for 7 full days after testing, i.e. until the end of the 7th day.

Who else can get the Green Pass?

When parents are issued a Green Pass, children under 18 will be included in their pass. If the children are eligible for a Green Pass due to being in the status of vaccinated or recovered individuals or due to testing negative for coronavirus (PCR swab test) in the last 72 hours, they will be included in their parents' Green Pass.

What is the jurisdiction of the Green Pass?

The Pass only applies within Israeli territories, in accordance with the Ministry of Health's policy, allowing access to services and places that must comply with the Green Pass restrictions.

Who issues the Green Pass, and what is the guidance?

The only agency authorized to issue the Green Pass is the Ministry of Health. Neither HMOs nor employers may issue Green Passes. Guidance for business owners about admitting Green Pass holders will be published in the Traffic Light website and application under "Guidance according to areas of interest" in the Traffic Light Local Councils page.

What details are required to have the Green Pass issued?

Please make sure that the details that you enter in this form are the same as your updated details that you registered with your insuring HMO:
• Identification number
• Mobile phone number
• Date of birth
Anyone registered with the HMO through their passport or visa number instead of an identification document number will enter these numbers instead of the identification document number.

How to get a Green Pass?

The Green Pass is issued in Hebrew and it can be issued in one of the channels below:

- The Traffic Light website
- The Ministry of Health Hotline at *5400

If you do not have internet access, you can apply for a green pass via:

- The Ministry of Health's hotline at *5400
- Self-service, accessible government stations available nationwide
- Interactive voice response system 02-5082000

Issuing the Pass with the interactive voice response system

Holders of kosher phones or those who are unable to have the Pass issued on the application are welcome to use the interactive voice response system at 02-5082000.

To use this service, you are required to under a two-stage identification process:

- Enter your identification details: Your identification number and date of birth. The system will verify your data.
- The system will call you back (to your phone number that was registered with the HMO).

If you will be found to be eligible for a Pass, you will be required to enter a fax number and the Pass will be sent to you within a few hours. If you will not bot found to be eligible for a Pass – the interactive voice response system will inform you accordingly and end the call.

The service will be available in the following languages: Hebrew, English, Arabic and Russian.

Please note: The interactive voice response service will only be available for callers from non-unlisted numbers.

An example of a Green Pass

FAQs Regarding Requesting Documents https://corona.health.gov.il/en/local-councils-traffic-light-model/

Download "Ramzor" App

GET IT ON Google Play

Download on the App Store

Frequently Asked Questions on Co-WIN

A. Registration

1. Where can I register for COVID-19 vaccination?

You can log into the Co-WIN portal using the link www.cowin.gov.in and click on the "Register/Sign In yourself" tab to register for COVID-19 vaccination.

2. Is there a mobile app that needs to be installed to register for vaccination?

There is no authorised mobile app for registering for vaccination in India except Aarogya Setu. You need to log into the Co-WIN portal. Alternatively, you can also register for vaccination through the Aarogya Setu App and Umang app.

3. Which age groups can register for vaccination on the Co-WIN portal?

All beneficiaries aged 18 years and above can register for vaccination.

4. Is online registration mandatory for Covid 19 vaccination?

Vaccination Centres provide for a limited number of on-spot registration slots every day. Beneficiaries aged 45 years and above can schedule appointments online or walk-in to vaccination centres. Beneficiaries aged 18 years and above can schedule appointments online or walk-in to Government vaccination centres. However, beneficiaries aged 18-44 years should mandatorily register themselves and schedule appointment online before going to a Private vaccination centre.

In general, all beneficiaries are recommended to register online and schedule vaccination in advance for a hassle-free vaccination experience.

5. How many people can be registered in the Co-WIN portal through one mobile number?

Up to 4 people can be registered for vaccination using the same mobile number.

6. How can beneficiaries with no access to smart phones or computers manage online registration?

Up to 4 people can be registered for vaccination using the same mobile number. Beneficiaries can take help from friends or family for online registration.

7. Can I register for vaccination without Aadhaar card?

Yes, you can register on Co-WIN portal using any of the following ID proofs:

a. Aadhaar card
b. Driving License
c. PAN card
d. Passport
e. Pension Passbook
f. NPR Smart Card
g. Voter ID(EPIC)
h. Unique Disability ID (UDID)
i. Ration Card

8. Is there any registration charge to be paid?

No. There is no registration charge.

B. <u>Scheduling Appointment</u>

9. Can I book an appointment for vaccination in the Co-WIN portal?

Yes, you can book appointment for vaccination through Co-WIN portal after logging-in to the Co-WIN Portal through your registered mobile number.

10. What are the options if one beneficiary is aged 45 or above and other is aged 18 or above?

If one beneficiary is aged 45 or above and other beneficiary is aged 18 to 44 years and both want to schedule a combined appointment, then only private paid vaccination centres or vaccination centres as per State's policy will be made available. However, it may happen that some hospitals which are catering to people with 45 years or more may not allow the booking of appointments for people with lesser age. In that case you may make bookings one by one.

11. Can I check the vaccine being administered at each vaccination centre?

Yes, while scheduling an appointment for vaccination, the system will show vaccination centre names along with the name of the vaccine that will be administered.

12. Can I download appointment slip?

Yes, the appointment slip can be downloaded after the appointment has been scheduled.

13. How can I find the nearest vaccination centre?

You can search in Co-WIN portal (or Aarogya Setu or Umang) for the vaccination centre nearest to your location by either searching through Map, PIN code or by choosing the State and the District.

14. What if I cannot go for vaccination on the date of appointment? Can I reschedule my appointment?

The appointment can be rescheduled at any time. In case you are not able to go for vaccination on the date of appointment, you can reschedule the appointment by clicking on "Reschedule" tab.

15. Do I have an option for cancellation of appointment?

Yes, you can cancel an appointment already scheduled. You can also reschedule the appointment and choose another date or time slot of your convenience.

16. Where will I receive confirmation of date and time of vaccination?

Once an appointment is scheduled, you will receive the details of the vaccination centre, date and time slot chosen for appointment in an SMS sent to your registered mobile number. You can also download the appointment slip and print it or keep it on your smart phone.

17. Can I get vaccination without appointment?

Beneficiaries aged 45 years and above can schedule appointments online or walk-in to vaccination centres. Beneficiaries aged 18-44 years can schedule appointment or walk-in for vaccination in Government vaccination centre. However, they should mandatorily register

themselves and schedule appointment online before vaccination in Private vaccination centres.

However, all beneficiaries are recommended to register online and schedule vaccination in advance for a hassle-free vaccination experience.

18. When I click on vaccination centre it shows 'No appointments are available in this period'. What to do?

In case of no availability of slots for scheduling appointment for vaccination in the searched vaccination centre, you may try scheduling appointment in other nearby centres. The portal gives you the feature of searching vaccination centres using your PIN code and District.

19. What is the 4-digit secret code on the Account Details page of self-registration portal on Co-WIN?

At the time of vaccination, you may be asked for the 4-digit secret code. This is to ensure that the rightful beneficiary receives the vaccine dosage and there is no misuse.

C. 2nd dose scheduling

20. Is it necessary to take 2nd dose of vaccination?

Yes. It is recommended that both doses of vaccine should be taken for realising the full benefit of vaccination. Both doses must be of the same vaccine type.

21. When should I take the 2nd dose of vaccination?

It is recommended that the 2nd dose of COVAXIN should be administered in the interval of 28 days to 42 days after the 1st dose. The 2nd dose of COVISHIELD should be administered in the interval of 84 days to 112 days after the 1st dose. The second dose of SPUTNIK V should be administered in the interval of 21 days to 90 days after the 1st dose.

22. Will my 2nd dose appointment be automatically scheduled by Co-WIN system?

No. You have to take an appointment for the 2nd dose vaccination. The Co-WIN system will help you book an appointment in a Vaccination Centre where the same vaccine is being administered as the vaccine type (COVAXIN, COVISHIELD or SPUTNIK V) of the 1st dose.

23. Whom can I contact if I have some problems related to my online registration of appointment?

You can call on the national helpline '1075' for information and guidance on COVID-19 vaccination and Co-WIN software related queries.

D. <u>Vaccination</u>

24. Is vaccination free at all vaccination centres?

No. Currently, vaccination is free at Government hospitals and charged at INR 250 in Private hospitals for beneficiaries aged 45 years and above.

From 1st May onwards, the Vaccination for people of 45 years or more will continue to be free at the Government facilities. For people between 18 to 44 years the States will announce the policy relating to payment. Vaccination will be priced by private facilities and you can see the price of each vaccine at the time of booking.

25. Can I check the price of the vaccine?

Yes. The System will show the price of the vaccine below the name of the vaccination centre at the time of scheduling an appointment.

26. Can I choose the vaccine?

System will show the vaccine being administered in each vaccination centre at the time of scheduling an appointment. Beneficiary can choose the vaccination centre as per their choice of vaccine being administered.

27. What precautions should I take at the time of 2nd dose vaccination?

The Vaccination Centres have been directed to ensure that if a beneficiary is being vaccinated with 2nd dose, they should confirm that the first dose vaccination was done with the same vaccine as is being offered at the time of second dose and that the first dose was administered more than 28 days ago for COVAXIN, 84 days ago for COVISHIELD and 21 days ago for SPUTNIK V. You should share the correct information about the vaccine type and the date of 1st dose vaccination with the vaccinator. You should carry your vaccine certificate issued after the first dose.

28. I have taken the first dose of Covid Vaccination through on-spot registration. When I tried to book a second dose online, it asked me to schedule an appointment for the first dose. What to do?

Please ensure that you are using the same mobile number for second dose online appointment booking which you had used at the time of first dose.

29. Can I get vaccinated with 2nd dose in a different State/District?

Yes, you can get vaccinated in any State/District. The only restriction is that you will be able to get vaccinated only on those centres which are offering the same vaccine as was administered to you on your first dose.

30. Which documents should I carry with me for vaccination?

You should carry your identity proof specified by you at the time of registration on the Co-WIN portal and a printout/screenshot of your appointment slip.

31. I have registered myself on Co-Win portal. However, I am not able to make any booking as I do not see any vaccination facility near my location? What should I do?

Yes, it is possible that no facility near your place has published their vaccination program as yet. You may wait for some time till vaccination facilities near your place are onboarded on Co-Win platform, become active and start their services.

E. <u>Vaccine Certificate</u>

32. Why do I need a vaccination certificate?

A COVID Vaccine Certificate (CVC) issued by the government offers an assurance to the beneficiary on the vaccination, type of vaccine used, and the provisional certificate also provides the next vaccination due. It also is an evidence for the beneficiary to prove to any entities which may require proof of vaccination specially in case of travel. Vaccination not only protects individuals from disease, but also reduces their risk of spreading the virus. Therefore,

there could be a requirement in future to produce certificate for certain kind of social interactions and international travel.

In this context the certificate issued by Co-WIN has built in security features to guarantee genuineness of the certificate which can be digitally verified using approved utilities which are provided in Co-WIN portal.

33. Who is responsible for providing the vaccination certificate?

The Vaccination Centre is responsible for generating your certificate and for providing a printed copy post vaccination on the day of vaccination itself. Please do insist on receiving the certificate at the Centre. For Private Hospitals, the charges for providing a printed copy of the certificate are included in the service charge for vaccination.

34. Where can I download vaccination certificate from?

You can download vaccination certificate from the Co-WIN portal (cowin.gov.in) or the Aarogya Setu app or through Digi-Locker by following the simple steps. You may do so by using the mobile number used at the time of registration.

35. How can I access COVID Vaccination Certificate from DigiLocker?

You can find vaccination certificate in DigiLocker under Ministry of Health and Family Welfare under Health category. Click on Covid Vaccine certificate and enter Beneficiary Reference ID to access the certificate.

F. <u>Reporting Side effects.</u>

36. Whom do I contact in case of side effects from vaccination?

You can contact on any of the following details:

a. Helpline Number: +91-11-23978046 (Toll free- 1075)

b. Technical Helpline Number: 0120-4473222

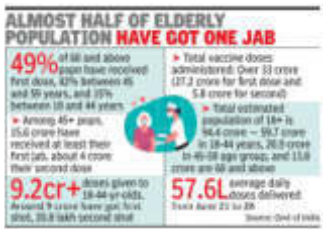
You may also contact the Vaccination Centre where you took vaccination, for advice.

Printed from
THE TIMES OF INDIA

DCGI gives emergency use nod to Moderna's vaccine

TNN | Jun 30, 2021, 08.32 AM IST

Indian pharma major Cipla will "facilitate" the import of Covid vaccines donated by US biotech major Moderna, possibly in the near future, under licence for restricted use by India's drug regulator DCGI. In parallel, Cipla is also pursuing a separate tie-up with the US firm to undertake large-scale fill-and-finish, distribution and commercialisation of Moderna's messenger or mRNA vaccines. Moderna's vaccine becomes the fourth to get emergency authorisation in the country after Serum Institute's Covishield, Bharat Biotech's Covaxin and Russia's Sputnik V.



Niti Aayog member (health) V K Paul told a media briefing on Tuesday that the regulatory clearance potentially opens up a clear possibility of the vaccine being imported to India in the near future. "An application received from Moderna through their Indian partner Cipla has been granted new drug permission for restricted use which is commonly known as emergency use authorisation," Paul said. "Our efforts to invite and to have other internationally developed vaccines, specifically Pfizer and J&J, also continue. Those processes are on," Paul added.

ALSO READ
Covid-19: All you need to know about mRNA vaccine

Elaborating on the development, Cipla's global CEO Umang Vohra told TOI, "This is not a commercial or supply deal, and we do not distribute this consignment either."

Hertie School
Data Science Lab

respondi
CLOSE TO PEOPLE

Studienbericht

Ein Jahr digitale Kontaktpersonennachverfolgung mit der Corona-Warn-App

Nutzung – Popularität – Verständnis

16. Juni 2021

Prof. Simon Munzert, Hertie School

Myrto Papoutsi, respondi AG

Holger Nowak, respondi AG

#COVID-19
#CoronaWarnApp
#LucaApp

Nachdem es zwischenzeitlich ruhig um die Corona-Warn-App geworden war, nahm die Diskussion um digitale Kontaktpersonennachverfolgung im Frühjahr 2021 wieder Fahrt auf. Die Corona-Warn-App wurde mit lange erwarteten Zusatzfeatures zur Eventregistrierung und Erfassung von Schnelltestergebnissen ausgestattet, während die Luca-App aufgrund von Sicherheitslücken und Datenschutzmängeln zunehmend in die Kritik geriet.

In unserem Bericht dokumentieren wir, wie populär diese Apps mittlerweile in der deutschen Bevölkerung sind. Nach wie vor gilt: Für die Wirksamkeit dieser Technologien ist die breitflächige Nutzung in der Bevölkerung entscheidend. In unserer Erhebung, einem Smartphone-basierten Nutzertracking, das zwischen dem 19. Mai und 01. Juni 2021 durchgeführt wurde, zeigt sich nach wie vor deutliche Unterschiede in der Nutzung der beiden bekanntesten Apps – Corona-Warn-App und Luca-App. Im Vergleich zur vorherigen Befragung (März/April 2021) sind jedoch einige Verschiebungen beobachtbar: Die Luca-App ist bekannter geworden, gleichzeitig steigt die Sorge um den Datenschutz der App allenfalls leicht an. Bei vielen Befragten besteht nach wie vor große Unklarheit über die Unterschiede in Funktionsweise und Zweck dieser Apps.

1 Einsatz von Digital Contact Tracing zur Pandemiebekämpfung

Weltweit suchen Staaten weiterhin Strategien, um die COVID-19-Pandemie wirksam einzudämmen. Virusmutationen, unentschlossenes oder ineffektives staatliches Handeln, Nichteinhaltung präventiver Maßnahmen und Widrigkeiten in der Impfstoffvergabe stehen dem jedoch entgegen. Als unterstützendes Werkzeug zur Bekämpfung wurde frühzeitig der Einsatz digitaler Technologien vorgeschlagen. Beispielsweise ist mithilfe der in Smartphones integrierten Bluetooth-Schnittstelle digitale Kontaktverfolgung *(Digital Contact Tracing, DCT)* möglich. Mobile Apps sollen dabei helfen Kontakte zwischen infizierten Personen zu protokollieren und diese zu benachrichtigen, um eine fortgesetzte Übertragung zu verhindern.

Im Juni 2020 wurde dafür in Deutschland die Corona-Warn-App zum Download bereitgestellt, die von SAP und Deutscher Telekom entwickelt und vom Robert-Koch-Institut herausgegeben wird.

Nachdem die Downloadzahlen anfänglich stark nach oben schnellten, stagnierte das Wachstum der Nutzerbasis seit der zweiten Jahreshälfte 2020 bis heute. Aktuell berichtet das Robert-Koch-Institut eine Gesamtdownloadzahl von 28,3 Mio. (Stand: 11.06.2021). Die Anzahl der Nutzer dürfte aufgrund mehrfacher Downloads, Nutzung auf unterschiedlichen Geräten, Deinstallation oder Nicht-Nutzung niedriger liegen.

Neben der „offiziellen" App existiert mittlerweile ein breites Angebot weiterer Apps, wobei in den letzten Monaten insbesondere die von privaten Investoren finanzierte Luca-App medial Aufmerksamkeit erregte. Hier steht die Erfassung von Kontakten verschiedener Locations im Vordergrund, um die in verschiedenen Bundesländern vorgeschriebene Dokumentation von Location-Kontakten zu gewährleisten. Über diese und andere Apps sollen Nutzer die Möglichkeit erhalten, sich aktiv über das Einscannen von QR-Codes einzuchecken und sich dabei zu registrieren.

Jüngste Erkenntnisse zur Luca-App weisen sowohl auf gravierende Datenschutzprobleme, teilweise im Zusammenhang mit der Zentralität der Datenspeicherung, als auch auf zweifelhafte Effektivität hin.[1][2] Für die Corona-Warn-App wurde am 21. April ein Update veröffentlicht, durch das die App nun ebenfalls eine Check-in-Funktionalität bei gleichzeitig dezentraler Datenspeicherung zur Verfügung stellt.[3] Seit Anfang Mai ist außerdem die Integration von Schnelltestergebnissen möglich. Im am 9. Juni veröffentlichten Update wurde zudem die Möglichkeit integriert, das digitale Impfzertifikat in der App zu hinterlegen.

---

[1] Linus Neumann. Luca-App: CCC fordert Bundesnotbremse. https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse (Stand: 11.06.2021)
[2] Florian Alt et al. Gemeinsame Stellungnahme zur digitalen Kontaktnachverfolgung. https://digikoletter.github.io/ (Stand: 11.06.2021)
[3] Hanna Heine. Das Projektteam veröffentlicht Corona-Warn-App 2.0 mit Eventregistrierung. https://www.coronawarn.app/de/blog/2021-04-21-corona-warn-app-version-2-0/ (Stand: 11.06.2021)

2 Breitflächige Nutzung entscheidend für Wirksamkeit

Ein für die Wirksamkeit der Apps entscheidender Faktor ist die breitflächige Nutzung durch die Bevölkerung. Dem stehen sowohl mangelnde Bekanntheit als auch mögliche Bedenken zur Effektivität und Datenschutzsicherheit entgegen sowie eine allgemeine Skepsis gegenüber der Bedrohung durch die Pandemie und staatlichem Handeln in diesem Kontext.

Um die Wirksamkeit der App aus Nutzerperspektive zu beurteilen und durch gezielte Bewerbung und Anpassung zu steigern, sind Erkenntnisse über tatsächliches Nutzungsverhalten entscheidend. Nutzungsmuster sind jedoch grundsätzlich schwer zu ermitteln – dies gilt insbesondere für Apps wie die Corona-Warn-App, die nach *Privacy-by-design*-Grundsätzen entwickelt wurden und somit kaum Nutzungsinformationen liefern. Zusätzlich ist das App-Angebot im Laufe der letzten Monate größer und damit unübersichtlicher geworden, was eine ganzheitliche Nutzungsevaluation erschwert.

3 Bestandsaufnahme ein Jahr nach der Veröffentlichung der Corona-Warn-App

Wir berichten die Ergebnisse einer Studie, für die wir Befragungsdaten in Kombination mit Smartphone-Trackingdaten erhoben haben, um die Nutzung von Contact-Tracing-Apps im Mai und Juni 2021 zu untersuchen. Wir bauen dabei direkt auf einer Vorgängerstudie auf, die im März und April 2021 im Feld war.[4] Dazu wurden zwischen dem 19. Mai und dem 01. Juni 2021 1.719 Mitglieder eines kommerziellen Access-Panels zu Verhalten und Einstellungen im Kontext der Corona-Pandemie im Allgemeinen und zu Contact-Tracing-Apps im Besonderen befragt. Für etwa die Hälfte der Befragten (n = 891) sowie weiteren Teilnehmern aus der ersten Erhebung wurde zusätzlich das Verhalten auf mobilen Geräten erfasst, womit die Nutzung (und Nicht-Nutzung) von Apps direkt beobachtet werden konnte.

Die Studie aktualisiert des Weiteren die Bestandsaufnahme einer früheren Erhebung, die zwischen Juni und September 2020 durchgeführt wurde und auf das Nutzerverhalten von CWA-Nutzern fokussierte.[5]

[4] Munzert, S., Papoutsi, M., Nowak, H. (2021). Nutzung von digitalen Tools zur Unterstützung von COVID-19-Kontaktverfolgung. Wie populär sind Corona-Warn-App und Luca-App in der dritten Pandemiewelle? https://opus4.kobv.de/opus4-hsog/frontdoor/index/index/docId/3830

[5] Munzert, S., Selb, P., Gohdes, A. et al. (2021). Tracking and promoting the usage of a COVID-19 contact tracing app. *Nature Human Behaviour* 5:247—255. https://doi.org/10.1038/s41562-020-01044-x

4 Ergebnisse

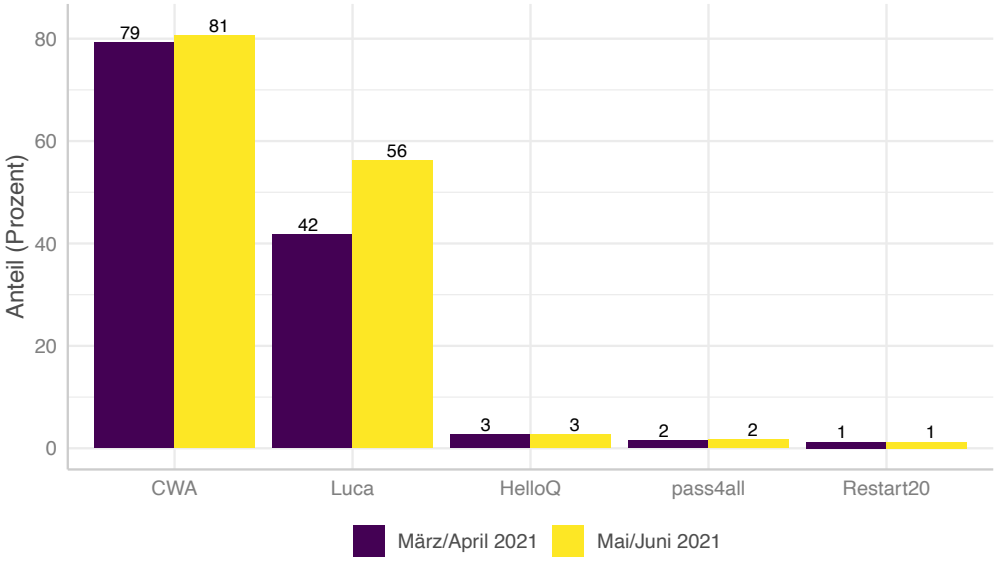
Zusammenfassung

1. **Corona-Warn-App (CWA)** und **Luca-App** sind **der Mehrheit der Befragten bekannt**, andere Angebote so gut wie nicht.
2. Die **CWA** wird nach wie vor **um ein Vielfaches häufiger genutzt als die Luca-App.** Die Luca-App hat jedoch im Verlauf der letzten Monate in der Nutzerzahlen aufgeholt.
3. Luca-App-Nutzer haben in den meisten Fällen auch die CWA installiert – eine **Ausweitung der App-Nutzerbasis seit Veröffentlichung der Luca-App ist kaum zu beobachten.**
4. **CWA-Nutzung** ist **ungünstig mit Risikoverhalten korreliert**: Diejenigen, die sich an AHA-Regeln halten, nutzen auch die App relativ häufiger. Dies trifft jedoch nicht mehr im gleichen Maße für die Luca-App zu.
5. **Vertrauen in Regierung und Wissenschaft** sowie Befürwortung härterer Anti-COVID-Maßnahmen sind **starke Prädiktoren für CWA-Nutzung**. Auch hier zeigen sich diese Unterschiede nicht mehr bei der Luca-App-Nutzung.
6. Im Vergleich zur letzten Befragung hat die **Luca-App** etwas an Popularität eingebüßt. Gleichzeitig steigen die Datenschutzbedenken gegenüber der App marginal an, wobei sich keine Unterschiede zur CWA finden.
7. Knapp ein Jahr nach Einführung der CWA zeigt sich in der Befragung immer noch deutlich eine **mangelnde Kenntnis über die Funktionsweise der CWA**. Auch bezüglich der Luca-App wird die Funktionsweise häufig nicht verstanden; die **Kritik von IT-Sicherheitsforschern an der Luca-App** ist den meisten Befragten **nicht bekannt**.
8. Dem **digitalen Impfpass** steht die Mehrheit der Befragten positiv gegenüber.

Bekanntheit der Apps

Zunächst erfassen wir die Bekanntheit unterschiedlicher Apps unter den Befragten (vgl. **Abbildung 1**). Wenig überraschend ist die Corona-Warn-App weithin bekannt (81% geben in der neuen Befragung an, von der App bereits gehört zu haben); dahinter folgt die Luca-App mit einem Bekanntheitsgrad von 56%. Andere abgefragte Apps – HelloQ, pass4all, Restart20 – sind so gut wie unbekannt. Auch in den Metered-Daten können wir nahezu keine Nutzungsaktivitäten jenseits der CWA und der Luca-App beobachten. Gegenüber der vorangegangenen Befragung im März/April 2021 hat im Befragtenpool insbesondere die Luca-App an Bekanntheit zugenommen. Nicht auszuschließen ist, dass Befragte erst in der Vorgängerbefragung von der Luca-App erfuhren und somit die Zunahme der Bekanntheit in Teilen auf die Befragung selbst zurückzuführen ist. Dagegen spricht jedoch die nur marginale (CWA) Veränderung bzw. Konstanz (HelloQ, pass4all, Restart20) der Bekanntheit anderer Apps.

Abbildung 1: Nennungen in Prozent bei der Frage „Von welchen der folgenden Apps haben Sie bereits gehört?" (N = 1.719).



App-Nutzung im Vergleich

Befragt man die Teilnehmer zur Installation von COVID-19-Apps auf ihrem Smartphone, zeigt sich, dass die CWA (46% im Sample; vgl. **Abbildung 2**) nach wie vor um ein Vielfaches häufiger genutzt wird als die Luca-App (20%). Luca-App-Nutzer haben in den meisten Fällen auch die CWA installiert – eine Ausweitung der App-Nutzerbasis ist kaum zu beobachten. Lediglich fünf Prozent berichten mittlerweile, ausschließlich die Luca-App zu nutzen.

Über die Verknüpfung der gemessenen (metered) Daten- mit den Befragungsdaten können weitere Rückschlüsse darauf gezogen werden, welche Faktoren wie stark mit der Nutzung bestimmter Apps zusammenhängen. Außerdem umgehen wir mit den hoch aufgelösten Verhaltensdaten zur App-Nutzung mögliche Verzerrungen der berichteten Nutzung, die durch sozial erwünschtes Verhalten zustande kommen können. So finden sich für 31% (44%) der Nutzer, die angeben, die Corona-Warn-App (Luca-App) installiert zu haben, keine App-Nutzungsspuren in den getrackten Smartphone-Daten.

Abbildung 3 stellt die metered (bzw. für die nicht getrackten Teilnehmer berichtete) App-Nutzung jeweils für die Corona-Warn-App und für die Luca-App über verschiedene Subgruppen hinweg dar (Mittelwerte). In Panel (a) werden verschiedene soziodemographische Merkmale verglichen. Für beide Apps zeigen sich höhere Nutzungsraten bei den Älteren, wohingegen hinsichtlich des Geschlechts, der Bildung und des Einkommens kaum Unterschiede bestehen. In Bundesländern, in denen die Luca-App frühzeitig lizensiert wurde (Mecklenburg-Vorpommern, Saarland, Schleswig-Holstein), sind höhere Adoptionsraten zu beobachten. Panel (b) schlüsselt Nutzung nach Risiko- und Verhaltensmerkmalen auf. Während sich in der dritten Pandemiewelle noch ein ungünstiger Zusammenhang zwischen Nutzung und risikobehafteten Verhaltensweisen (ÖPNV-Nutzung, Restaurantbesuch, private Treffen) zeigte, sind diese Unterschiede nun kaum noch sichtbar. Weiterhin zeigt sich jedoch, dass diejenigen, die sich weniger

an die AHA-Maßnahmen halten, die Corona-Warn-App (nicht jedoch die Luca-App) seltener nutzen. Vorerkrankungen und COVID-19-Fälle im persönlichen Netzwerk hingegen hängen mit einer höheren Nutzungsrate zusammen. In Panel (c) werden schließlich Einstellungen mit der App-Nutzung verglichen. Hier zeigen sich starke Unterschiede in Nutzungsraten der CWA. Diese sind höher für Befragte, die sich besorgt über COVID-19 zeigen, eine Ausweitung der staatlichen Maßnahmen zur Bekämpfung der Pandemie fordern, Bereitschaft zur Impfung zeigen und sich häufig zu COVID-19 informieren. Hohes Vertrauen in Regierung, Wissenschaft und Gesundheitssystem hängen ebenfalls stark mit einer Nutzung zusammen. Hier haben sich die Unterschiede zur ersten Welle jedoch abgebaut. Dies gilt noch stärker beim Blick auf die Adoptionsraten der Luca-App. Hier sind kaum nennenswerte Subgruppenunterschiede bezüglich Einstellungen zu beobachten.

Abbildung 2: Nennungen in Prozent bei der Frage „Haben Sie oder hat jemand für Sie eine der folgenden Apps auf Ihrem Smartphone installiert?" (N = 1.719).

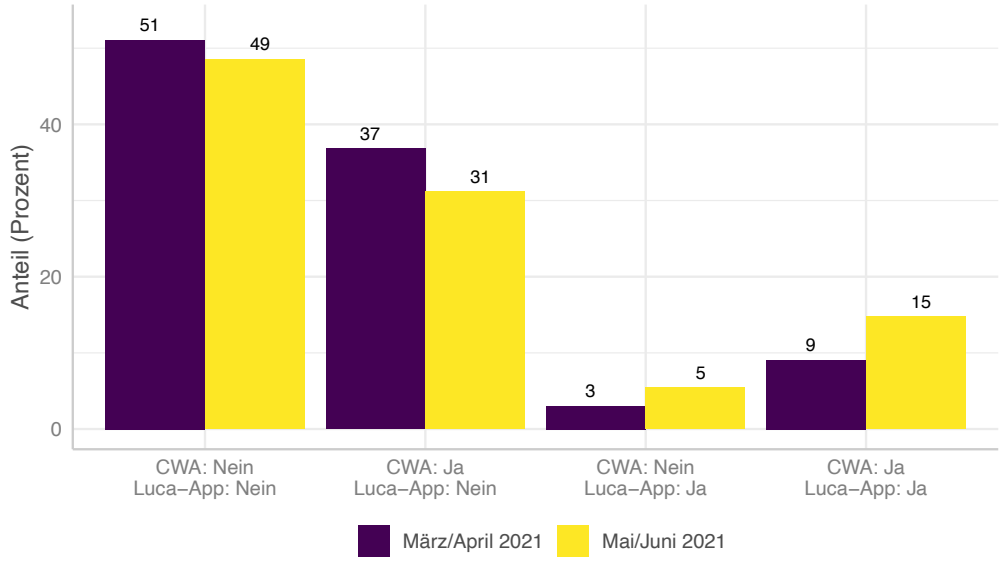
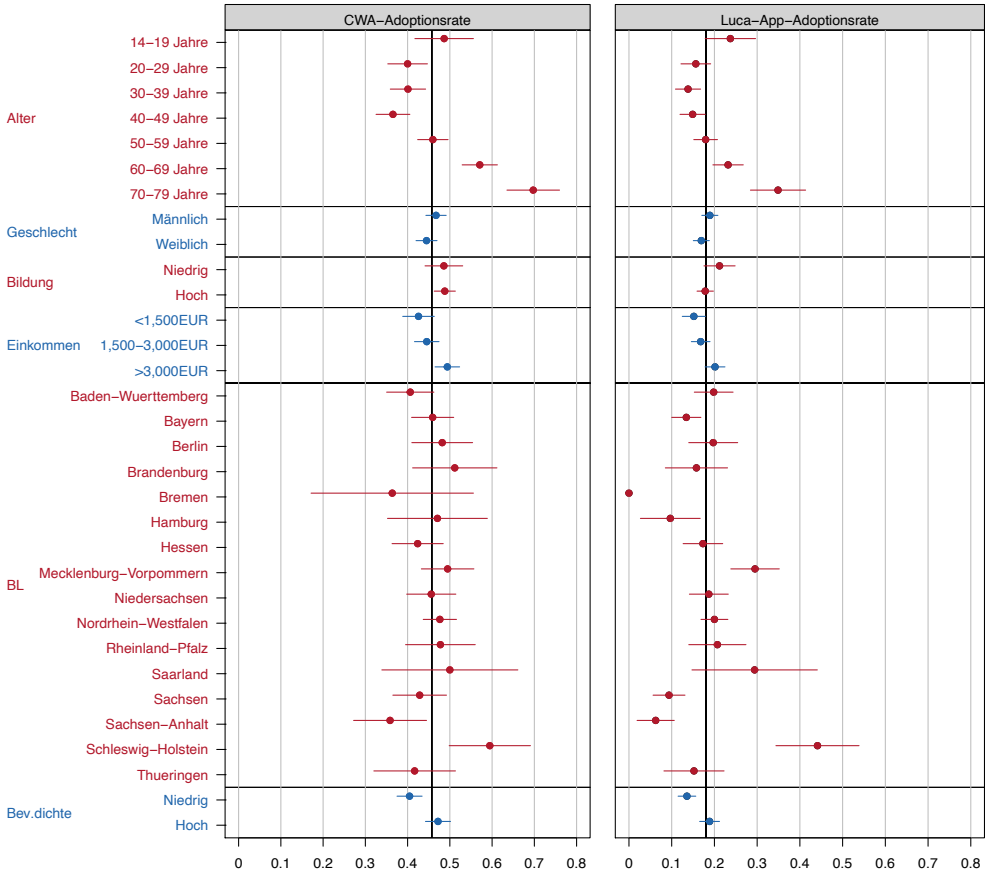


Abbildung 3: Nutzungsraten der Corona-Warn-App und der Luca-App (getrackt) nach Subgruppe (N = 1.719, Messzeitraum: 1.1-31.5.2021).

(a) Soziodemographische Merkmale



(b) Risikostatus und Verhalten

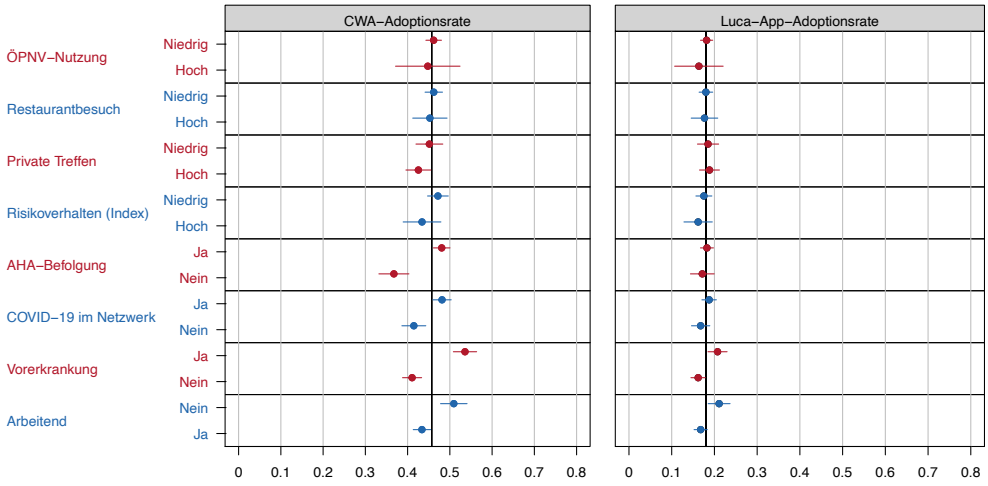
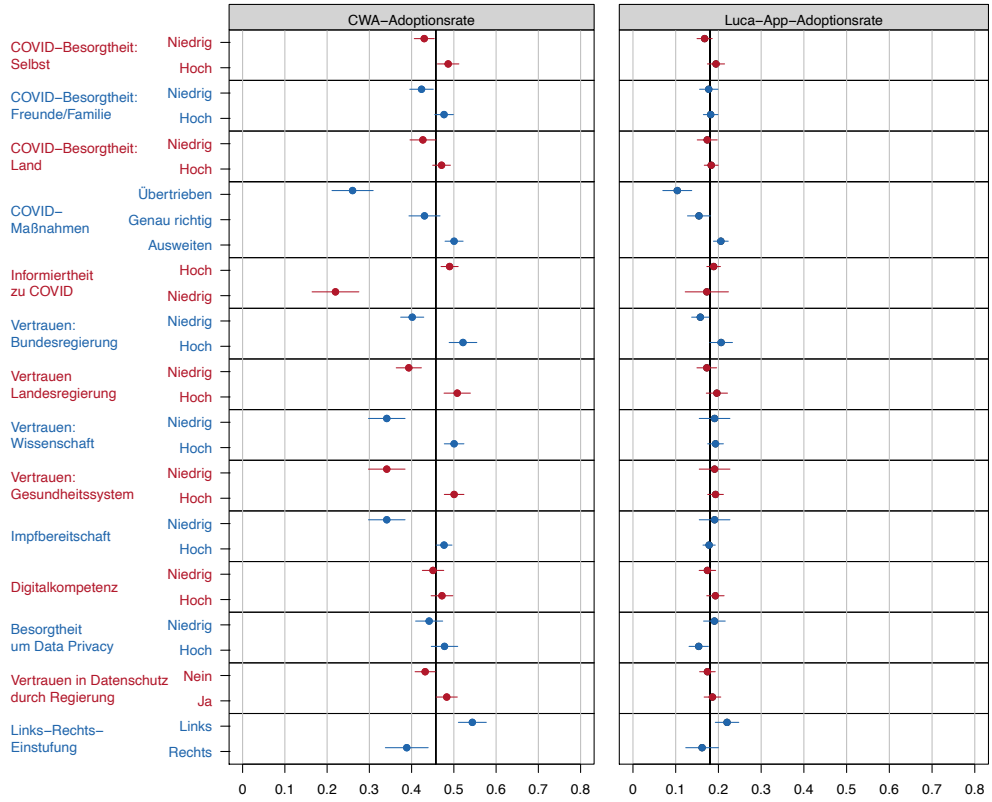


Abbildung 3, fortgesetzt: Nutzungsraten der Corona-Warn-App und der Luca-App (getrackt/berichtet) nach Subgruppe (N = 1.719, Messzeitraum: 1.1-31.5.2021).

(c) Einstellungen



App-Nutzung im Zeitverlauf

Die hochaufgelösten metered Daten erlauben auch eine Betrachtung der App-Nutzung im Zeitverlauf. **Abbildung 4** zeigt für den Zeitraum zwischen 1. Februar und 6. April die kumulative Adoptionsrate, die misst, wie viele Befragte zu einem bestimmten Zeitpunkt die jeweilige App mindestens einmal auf ihrem Smartphone geöffnet hatten (Abweichungen von den oben gezeigten berichteten und getrackten Nutzungsraten können sich unter anderem dadurch ergeben, dass die Apps zwischenzeitlich wieder deinstalliert wurden). Es zeigt sich nur eine marginale Steigerung der Rate für die CWA und ein moderates, anfänglich lineares Wachstum für die Erstnutzung der Luca-App seit Anfang März.

In Abbildung 5 sind daneben die täglichen Nutzungsraten abgetragen (Anteil derjenigen, die die jeweilige App an einem bestimmten Tag geöffnet haben, unter allen getrackten Personen). Hier zeigt sich eine eher rückläufige Zahl durchschnittlicher täglicher Nutzungen der Corona-Warn-App auf der einen Seite und ein deutlicher Anstieg der Nutzungszahlen der Luca-App im Mai. Der Rückgang bei der Corona-Warn-App muss jedoch nicht auf ein gesunkenes Interesse an der App generell hindeuten. So könnte beispielsweise ein Rückgang der Kontakte im Kontext der Bundesnotbremse dazu geführt haben, dass für Nutzer der App weniger Anlass bestand, den Risikostatus regelmäßig zu überprüfen.

Abbildung 4: Kumulative App-Nutzungsraten im Zeitverlauf, Corona-Warn-App und Luca-App. N = 1076, Trackingzeitraum: 1.1-31.5.2021, Betrachtungszeitraum 1.2.-31.5.2021).

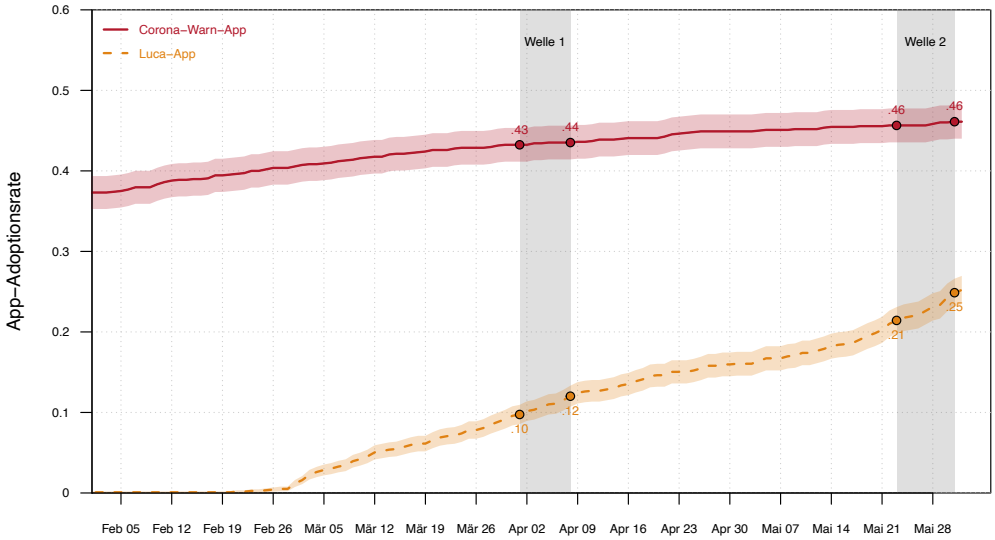
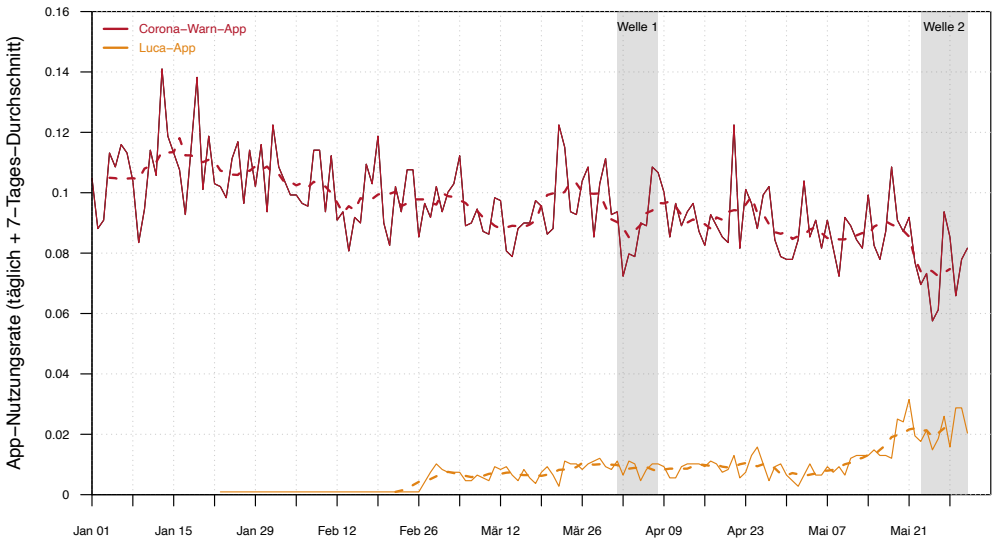


Abbildung 5: Tägliche App-Nutzungsraten im Zeitverlauf (täglich + 7-Tages-Durchschnitt), Corona-Warn-App und Luca-App. N = 1076, Trackingzeitraum: 1.1-31.5.2021, Betrachtungszeitraum 1.1.-31.5.2021).



Warum werden die Apps nicht genutzt?

Im nächsten Schritt der Analyse berichten wir App-spezifische Einstellungen und selbstberichtete Gründe dafür, die jeweiligen Apps nicht zu nutzen. **Abbildung 6** zeigt Zustimmungsraten zu Statements bezüglich des Datenschutzes, Informiertheit und wahrgenommener Effektivität sowohl im App-Vergleich als auch im Vergleich zwischen den Befragungswellen. Es zeigt sich ein leichter Rückgang in der positiven Bewertung der Luca-App hinsichtlich ihrer Wirksamkeit („sinnvolles

Zusatzinstrument zur Nachverfolgung", „nützt für die Bekämpfung der Pandemie"). Gleichzeitig äußern die Befragten im Mittel etwas mehr Bedenken bezüglich des Datenschutzes der App. Dies stellen mutmaßlich Folgen der medial präsenten Diskussionen um Sicherheitslücken und Datenschutzprobleme der Luca-App dar. Ein Großteil der (negativen) Berichterstattung über Datenschutzprobleme der App fand zwischen den beiden Erhebungszeiträumen statt. Insofern ist es bemerkenswert, dass sich die Befragten unverändert schlecht über die App informiert fühlen.

Abbildung 7 berichtet Gründe der Nichtnutzung der Corona-Warn-App und der Luca-App. Grundlage hierbei sind selbstverständlich nur die jeweiligen selbstberichteten Nichtnutzer, die über die Wellen hinweg nicht deckungsgleich sind. Bezüglich der CWA scheint weiterhin insbesondere Skepsis hinsichtlich des Nutzens zu bestehen (genannt von 50% der selbstberichteten Nichtnutzer), außerdem zweifeln Nichtnutzer trotz dezentralisierter Datenspeicherung und *Privacy by design* am Datenschutz der App (27%) und möchten nicht, „dass sie der Staat überwacht" (25%). Auch die Voraussetzung, Bluetooth dauerhaft aktiv zu halten, scheint einige abzuschrecken (25%). Luca-App-Nichtnutzer fühlen sich in erster Linie noch nicht gut genug informiert (29%) und möchten erst die Erfahrung von anderen abwarten (13%). Ein (im Vergleich zur CWA deutlich geringerer, aber nach der ersten Befragung gestiegener) Teil zweifelt am Nutzen der App (26%) oder sorgt sich um den Datenschutz (23%).

Abbildung 6: Einstellungen zur Corona-Warn-App und zur Luca-App („Inwiefern stimmen Sie den folgenden Aussagen zu den folgenden Tracing-Apps zu?", N = 1.719).

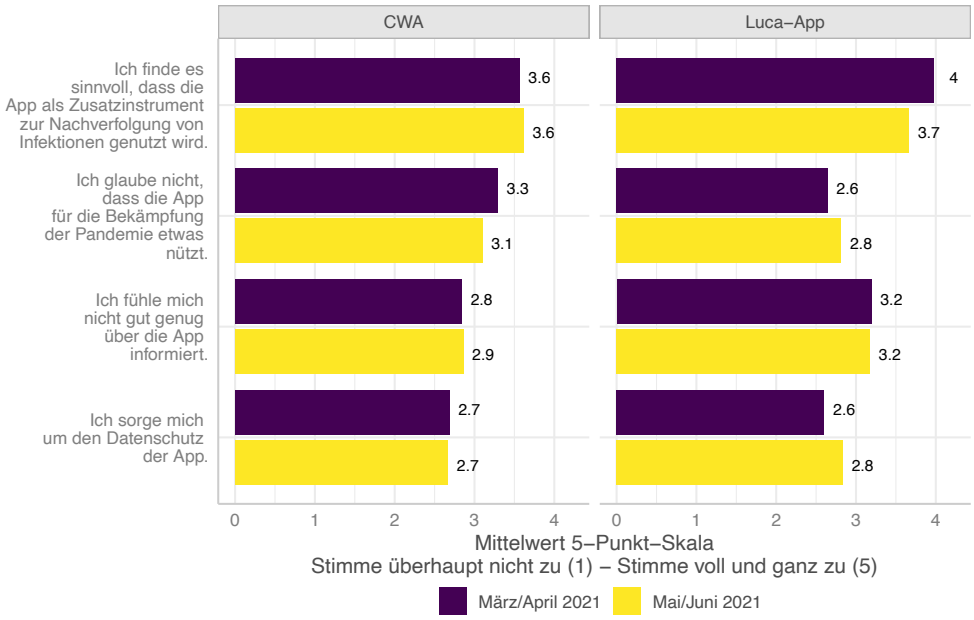
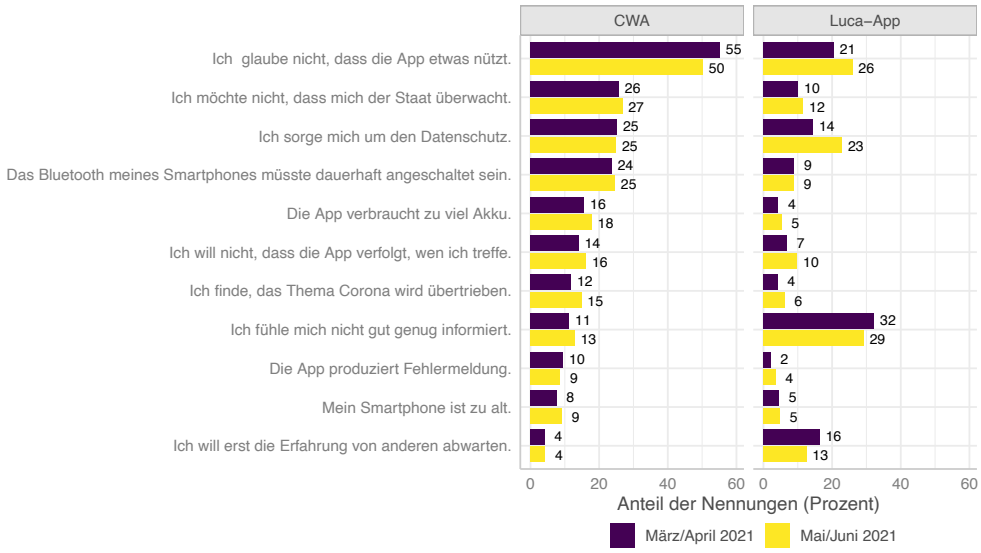


Abbildung 7: Gründe der Nichtnutzung der Corona-Warn-App und der Luca-App („Können Sie uns sagen, weshalb sie die App nicht mehr installiert haben?", N = 1.719).



Wie ist es um das Wissen zur Funktionsweise der Apps bestellt?

Bereits in der Frühjahrsbefragung deutete sich an, dass nicht alle Befragten ausreichend über die Funktionsweise der Kontaktverfolgungsapps Bescheid wissen. Während die Corona-Warn-App Bluetooth-Signale nutzt, um die Nähe zu anderen Smartphone-Haltern zu schätzen, und nutzungsbezogene Daten im Wesentlichen dezentral speichert und verarbeitet, baut die Luca-App auf einer Registrierungslogik auf, bei der sich Nutzer durch das Einscannen von an Locations zur Verfügung gestellten QR-Codes mit ihren Daten registrieren können. Diese Daten werden zentral auf Luca-Servern gespeichert und können prinzipiell an Gesundheitsämter weitergegeben werden. Zahlreiche IT-Sicherheitsforscher hatten sich in einer gemeinsamen Stellungnahme gegen dieses System ausgesprochen, da sowohl der Nutzen der Anwendung zweifelhaft bleibe als auch zahlreiche konzeptionelle Sicherheitslücken entdeckt worden seien.[6] Diese Informationen wurden vor der aktuellen Befragungswelle durch verschiedene Medien wiederholt berichtet.

In der aktuellen Befragung wurden die Befragten um Einschätzungen gebeten, inwiefern bestimmte Aussagen zur Corona-Warn-App und zur Luca-App richtig oder falsch seien. Sowohl die jeweiligen Statements als auch die jeweiligen Anteile von „Richtig"-, „Falsch"- und „Weiß nicht"-Nennungen sind in **Abbildung 8** aufgeschlüsselt.

Beim Blick auf das Wissen zur Corona-Warn-App ergibt sich ein differenziertes Bild. In den meisten Fällen wird die faktisch richtige Antwort auch von der Mehrheit der Befragten gewählt. Etwa 70% der Befragten wissen beispielsweise über die Nutzung von Bluetooth-Signalen durch die App. Immerhin 35% wissen auch über

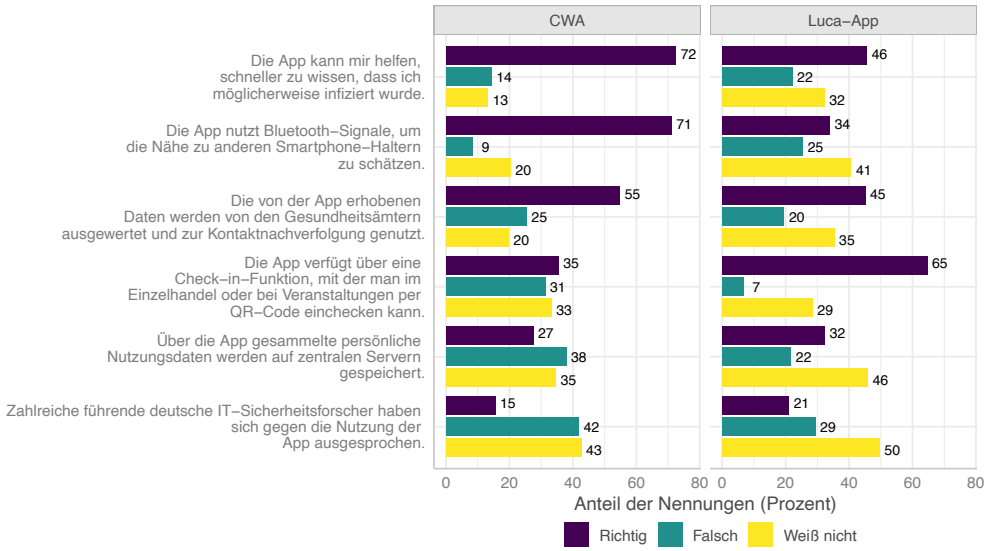
[6] Florian Alt et al. Gemeinsame Stellungnahme zur digitalen Kontaktnachverfolgung. https://digikoletter.github.io/ (Stand: 11.06.2021)

die Check-in-Funktionalität, die erst kurz vor Befragungsbeginn eingeführt worden war. Gleichzeitig gehen immerhin 27% der Befragten davon aus, dass durch die Corona-Warn-App gesammelte persönliche Nutzungsdaten auf zentralen Servern gespeichert werden; 35% trauen sich keine Einschätzung zu. Sogar 55% der Befragten gehen davon aus, dass die von der App erhobenen Daten von den Gesundheitsämtern ausgewertet und zur Kontaktverfolgung genutzt werden. Dies steht im direkten Widerspruch zur eigentlichen Funktionsweise der App.

Bezüglich der Luca-App ist einem Großteil der Befragten die Kernfunktionalität - die Check-in-Funktion – bekannt (65%). Allerdings kommt es auch bezüglich der Luca-App zu Fehleinschätzungen eines signifikanten Teils der Befragten. Nur 25% widersprechen der Aussage, dass die App Bluetooth-Signale benutze. Eine Mehrheit der Befragten (46%) geht außerdem davon aus, dass die App helfen kann, schneller über eine mögliche Infektion Bescheid zu wissen. Das darf auf Basis aktueller Erkenntnisse zum Einsatz der App in der Praxis zumindest bezweifelt werden. Ebenso ist einer Mehrheit weder das zentrale Datenspeicherungskonzept bewusst, noch haben sie Kenntnis vom Statement der IT-Sicherheitsforscher.

Insgesamt lässt sich zusammenfassen, dass das Wissen über die Funktionsweise und den Nutzen der beiden populärsten Apps zur Pandemiebekämpfung in Deutschen unter den Befragten beschränkt ist.

Abbildung 8: Einschätzungen von Statements zur Corona-Warn-App und der Luca-App („Welche dieser Aussagen über die Corona-Warn-App/Luca-App halten Sie für richtig und welche für falsch?", N = 1.719).



Wie stehen die Befragten zum digitalen Impfpass und zu Impfprivilegien?

Im Winter 2020 kündigte das Bundesgesundheitsministerium die Einführung eines digitalen Corona-Impfpasses an. Dieser wird ab 14. Juni unter anderem von teilnehmenden Apotheken ausgestellt. Das digitale Impfzertifikat kann dann entweder in der eigens dafür entwickelten „CovPass-App" oder auch in der Corona-

Warn-App gespeichert werden. Auch die Luca-App soll mit dieser Funktionalität nachgerüstet werden.

Der Impfpass – sowohl in analoger als auch digitaler Form – kann dann unter anderem dafür genutzt werden, um den Besuch bestimmter Länder, Orte oder Ereignisse, der vom Impfstatus der Besucher abhängig gemacht wird, zu erleichtern. Er hängt damit mittelbar auch mit Privilegien zusammen, die Geimpften gegenüber Ungeimpften zuteilwerden können.

In der Befragung haben wir sowohl den Impfstatus der Befragten erfasst als auch ihre Einstellungen zum digitalen Impfpass und zu Privilegien für Geimpfte und Genesene abgefragt. **Abbildung 9** berichtet die Einstellungen zum digitalen Impfausweis nach Impfstatus. Es zeigt sich ein positiver Zusammenhang zwischen Impfstatus und Befürwortung des digitalen Impfausweises. Gleichzeitig befürwortet jedoch die Mehrheit aller, die eine Impfung geplant haben, den Impfpass eher oder stark. Lediglich die Gruppe derer, die keine Impfung geplant haben, lehnt den Impfpass mehrheitlich völlig oder eher ab.

Ein ähnliches Muster zeigt sich beim Blick auf die Zustimmung zu Privilegien für Geimpfte und Genesene (siehe **Abbildung 10**). Hier befürwortet eine Mehrheit derer, die sich zur Impfung angemeldet haben oder bereits einfach oder vollständig geimpft sind, diese Privilegien.

Abbildung 9: Einstellung zum digitalen Impfpass nach („Bald sollen Corona-Genesene und gegen Corona Geimpfte ihren Status in einem digitalen Corona-Impfausweis dokumentieren können. Wie stehen Sie der Einführung dieses digitalen Impfausweises gegenüber?", N = 1.719).

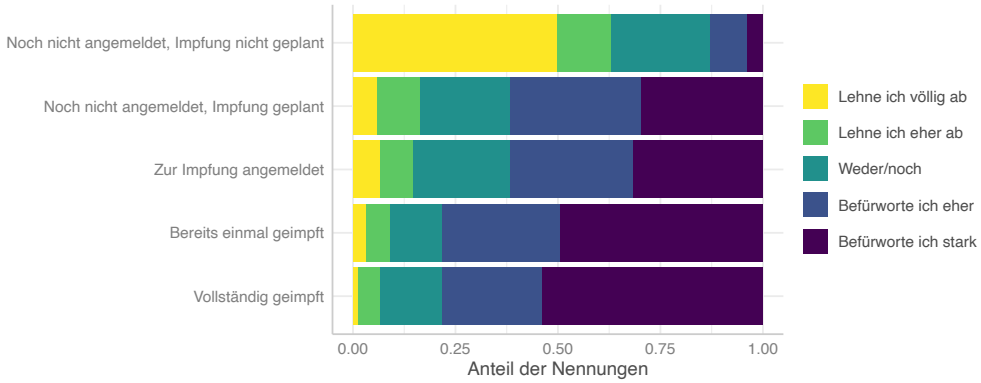
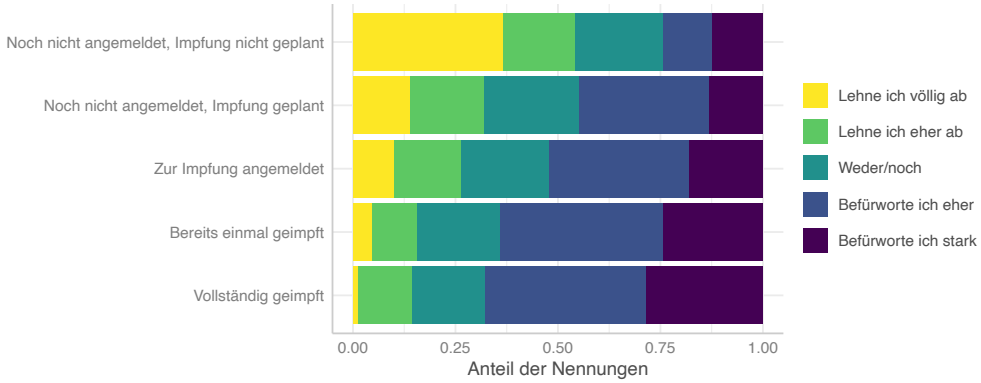


Abbildung 10: Einstellung zu Privilegien für Geimpfte und Genesene („Für vollständig Geimpfte und Genesene gelten seit kurzem keine Ausgangsbeschränkungen mehr. Sie müssen sich also nicht mehr an die lokalen Ausgangssperren halten. Auch die Kontaktbeschränkungen im privaten Umfeld sind für sie aufgehoben. Wie stehen Sie diesen Lockerungen gegenüber?", N = 1.719).



5 Zusammenfassung

Digitale Technologien können in der Pandemie einen wichtigen Beitrag leisten, um die Kontaktnachverfolgung zu unterstützen und Virusübertragungen zu verhindern. Sie sind in erster Linie Werkzeuge für den Einzelnen, um sich zu informieren und eigenverantwortliches Handeln zu stärken.

Die Nutzung dieser Tools im Privaten entzieht sich in einer liberalen Demokratie staatlicher Kontrolle. Umso wichtiger ist es jedoch zu verstehen, welche Faktoren die Nutzung beeinflussen und wie die Tools noch attraktiver gemacht werden können, um eine möglichst breite Nutzerbasis zu schaffen.

Die hier berichteten Ergebnisse deuten darauf hin, dass die Corona-Warn-App nahezu ein Jahr nach Einführung einen hohen Bekanntheitsgrad genießt und im internationalen Vergleich und mit Berücksichtigung der Freiwilligkeit der Nutzung auf eine solide Nutzerbasis bauen kann. Obwohl sie gegenüber privaten Lösungen entscheidende Vorteile hinsichtlich des Datenschutzes, aber auch der Effektivität genießt, überwiegen unter Nichtnutzern die Skepsis bezüglich dieser Merkmale.

Nun gilt es, durch klare Kommunikation und weitere Bewerbung der Funktionalität bisherige Nichtnutzer zu überzeugen. Die hinzugefügte Check-in-Funktionalität sowie das Hinterlegen von Schnelltestergebnissen und Impfstatus kann dabei ein wichtiger Baustein sein, da sie die potenzielle Effektivität und Nützlichkeit unmittelbarer vermittelt als das im Wesentlichen passive Bluetooth-gestützte Contact Tracing.

Informationen zu Befragung und Smartphone-Tracking

Die hier präsentierten Ergebnisse basieren auf einer zwei-welligen Befragung, die anfänglich 2.099 Teilnehmer eines durch die respondi AG rekrutierten Access-Panels umfasste. In der zweiten Welle nahmen noch 1.719 der ursprünglich rekrutierten Befragten teil. Die Teilnahme war freiwillig. Teilnehmer mussten zwischen 14 und 74 Jahre alt sein, in Deutschland wohnen und mindestens wöchentlich Zugriff auf ein Smartphone haben. Dies traf auf 98% der eingeladenen Teilnehmer zu. Teilnehmer wurden nach Geschlecht (2 Gruppen), Alter (7 Gruppen) und Bundesland ausgewählt, um Randverteilungen der 2020 Best-for-Planning-Studie (Strukturanalyse der Wohnbevölkerung in DE: Onliner exkl. Mobile Nicht-Nutzer zwischen 14-74 Jahre) zu approximieren. Mecklenburg-Vorpommern hat im März 2021 als erstes Bundesland eine Lizenz zur Nutzung des Luca Systems zur Kontaktnachverfolgung erworben. Um die Effekte dieser Maßnahme der Landesregierung besser einschätzen zu können, wurde die Stichprobengröße für dieses Bundesland bewusst höher angelegt. Statt der in der B4P Verteilung benötigten Fallgröße von etwa 2% für Mecklenburg-Vorpommern wurden insgesamt 8% Teilnehmer aus diesem Bundesland in der Stichprobe zugelassen.

Mobile Trackingdaten

respondis Metered-Panel verwendet die Wakoopa-Software, die Daten über Web-Besuche und mobile App-Nutzung auf allen Geräten sammelt, die vom Teilnehmer registriert wurden. Die gesammelten Daten werden über eine sichere Verbindung an eine Cloud-Umgebung geschickt. Teilnehmer erklären ihre Einwilligung und es wird ihnen angeboten, das Daten-Sharing jederzeit zu unterbrechen oder zu beenden. Die von uns genutzten Metered Daten beziehen sich auf den Zeitraum 01. Januar bis 31. Mai 2021. Von den 1.078 im Metered-Panel erfassten Nutzern identifizierten wir 682 Nutzer, die am Ende des Befragungszeitraums die Corona-Warn-App installiert und mindestens einmal genutzt hatten; außerdem 300 Luca-App-Nutzer. Insgesamt verzeichnete die Software 29.557 Interaktionen mit einer aktiven Median-Nutzungsdauer von 10 Sekunden pro App-Interaktion (d.h. Dauer der Öffnung der App) für die Corona-Warn-App und 2.973 Interaktion (durchschnittlich 15 Sekunden Interaktion) für die Luca-App.

Einwilligung und Umgang mit den Daten

Das Verknüpfen von passiven Verhaltensdaten mit Umfragedaten zur Untersuchung des Verhaltens bei Nutzung von Kontaktverfolgungs-Apps, die so konzipiert sind, dass keine Nutzungsdaten in Kombination mit Zusatzdaten über den Nutzer mit Dritten geteilt werden, erfordert besondere Vorsicht. Personen, die dem Passiv-Metered-Panel beitreten, werden über die Art der gesammelten Daten aufgeklärt. Die Daten werden anonymisiert und nicht an Dritte weitergegeben. Die Panelteilnehmer werden außerdem darüber informiert, dass die Software jederzeit gelöscht oder das Tracking unterbrochen werden kann.

Allgemeine Hinweise zur Interpretation

Das Studiendesign bietet hohe Genauigkeit und Granularität in der Messung der App-Nutzung. Gleichzeit schränkt die Natur des Samples die Verallgemeinerbarkeit der Ergebnisse auf die Zielpopulation ein, da die Teilnehmer unter anderem überdurchschnittlich digitalaffin sind. Absolute Anteile sollten deshalb nicht als repräsentativ für die Population– Smartphone-Nutzer in Deutschland, deren Handys technische Mindeststandards erfüllen (mindestens Android 6 und iOS 12) – interpretiert werden. Die berichteten bedingten Verteilungen (z.B. Unterschiede in CWA-Nutzung zwischen verschiedenen Altersgruppen) sind hingegen zwischen Population häufig leichter zu vergleichen. Bei der Interpretation der in diesem Studienbericht vorgestellten Ergebnisse kommt hinzu, dass diese sich lediglich auf Befragte beziehen, die an beiden Befragungen teilnahmen. Deshalb ergeben sich auch bei Zahlen zur ersten Welle kleine Abweichungen zum ersten Studienbericht.

frontiers in Digital Health

OPINION
published: 25 June 2021
doi: 10.3389/fdgth.2021.594124

Digital COVID Credentials: An Implementation Process

Mayssam Nehme[1], Laurent Kaiser[2,3], Philippe Gillet[4], Philippe Thevoz[4], Silvia Stringhini[1,2,5] and Idris Guessous[1,2]*

[1] Division of Primary Care Medicine, Geneva University Hospitals, Geneva, Switzerland, [2] Faculty of Medicine, University of Geneva, Geneva, Switzerland, [3] Division of Infectious Diseases, Geneva University Hospitals, Geneva, Switzerland, [4] SICPA, Prilly, Switzerland, [5] University Centre for General Medicine and Public Health, University of Lausanne, Lausanne, Switzerland

Keywords: digital, blockchain, COVID-19, decentralized governance, free movement, immunity, certificate, vaccination

Edited by:
Constantinos S. Pattichis, University of Cyprus, Cyprus

Reviewed by:
Gary Matkin, University of California, Irvine, United States
Joshua Coyne, University of Memphis, United States

****Correspondence:***
Mayssam Nehme
mayssam.nehme@hcuge.ch

Specialty section:
This article was submitted to Health Technology Innovation, a section of the journal Frontiers in Digital Health

Received: *25 August 2020*
Accepted: *04 June 2021*
Published: *25 June 2021*

Citation:
Nehme M, Kaiser L, Gillet P, Thevoz P, Stringhini S and Guessous I (2021) Digital COVID Credentials: An Implementation Process. Front. Digit. Health 3:594124. doi: 10.3389/fdgth.2021.594124

Initial public health responses to the COVID-19 pandemic have focused on non-pharmaceutical interventions including stringent physical distancing measures, lockdowns, and restriction to free movement. This comes at significant costs however, both economically and socially (1, 2). As authorities begin to ease existing measures, governments are looking into specific alternatives to lockdown, such as phased mobilization of the economy (3), less stringent physical distancing measures, or immunity passports that would determine individual access or restrictions (4). Immunity passports vs. certificates differ in the rights related to their use and their issuing authority. Immunity passports have been cautioned against by the WHO and at international levels (5, 6) citing a lack of reliable interpretability of the presence or absence of COVID-19 antibodies, as well as ethical risks (7). With the advent of vaccines, these risks are potentially mitigated while other risks arise such as universal access to vaccination, and the debate around immunity passports is once again justifiably revived (8). COVID credentials could be an answer to facilitate some of the currently difficult scenarios in society and everyday life (travel, large gatherings, etc.). The need for a non-falsifiable solution is of utmost importance, especially with reports of fraud increasingly emerging (9).

Reflecting on the digital aspects of such a solution is important to ensure the implementation of adequate safeguards, display the right amount of information and use digital health systems to society's advantage. The European Union has recently published open source material detailing a potential trust framework and technical specificities that would be used in establishing a European Union Digital COVID Certificate that would be uniform and interoperable (10). COVID credentials taking into account vaccination, serology, PCR testing, and self-reported symptoms can employ algorithms to certify an individual's most recent COVID-related status. Certification would take into account results from pre-certified laboratories and pre-certified vaccination centers only, thus decreasing the prospect of false positive results and individuals inadvertently foregoing protective measures, putting themselves and others at risk (11). In addition, information could further assist individuals in making the right decisions and can also provide reminders to get tested or retested, vaccinated or re-vaccinated; which would also accommodate continually evolving aspects of the current COVID-19 pandemic and virus response. An example is setting reminders for individuals who received a vaccination to receive a booster shot, depending on the duration of the immune response (once defined), but also for individuals who received a specific vaccine to follow specific measures if a new variant turned out resistant to that vaccine. The presence of symptoms should also be part of the algorithm and could determine the need for fast-track testing or the implementation of isolation measures.

Here, we propose a very practical decentralized secured digital solution (**Figure 1**). The solution is securing the original data provided from a certified vaccination center, a certified laboratory or testing center. A digital security seal protects and guarantees the integrity of the data to be secured, through an unforgeable mathematical link between the hash of the data and the seal. To

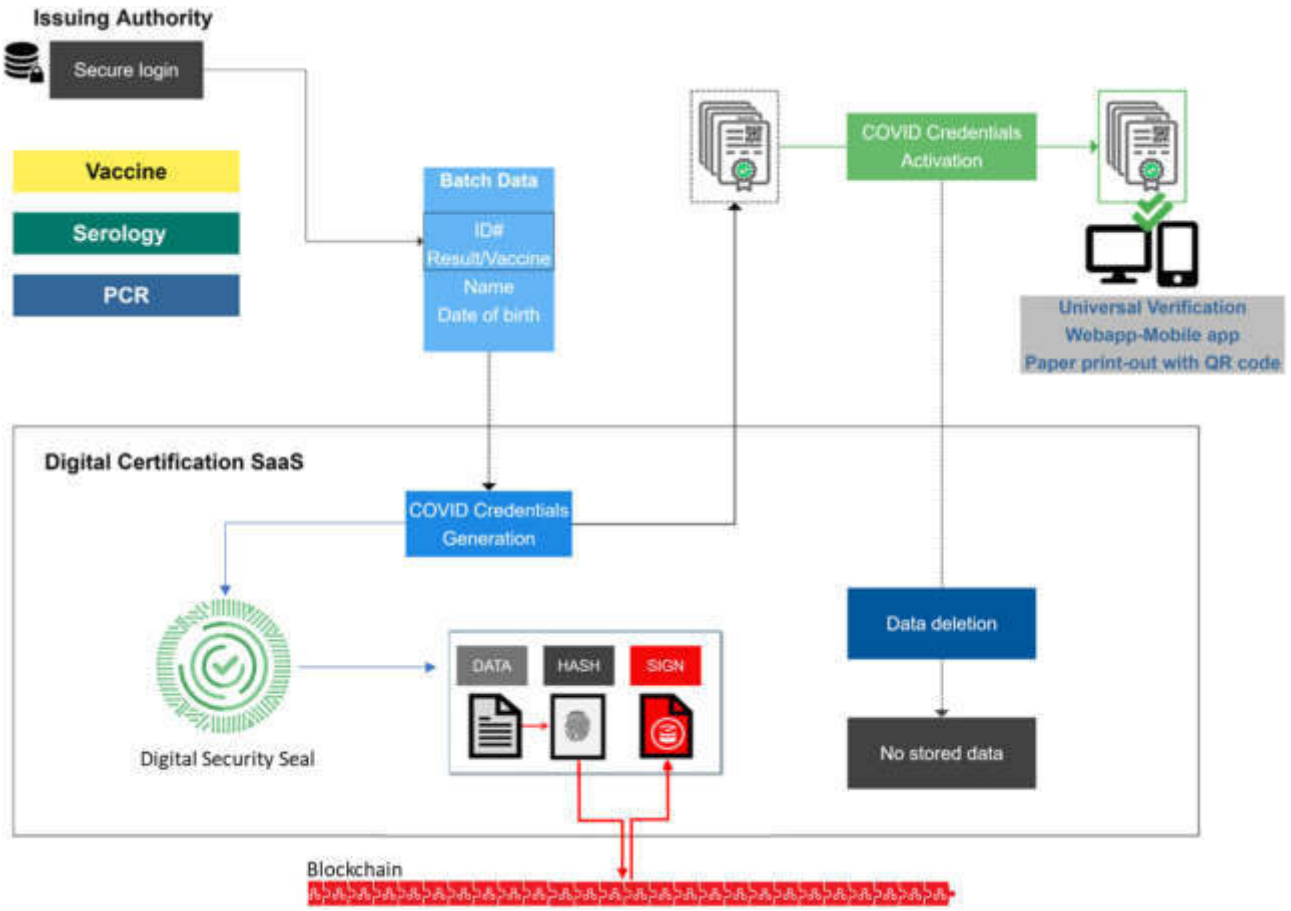


FIGURE 1 | Digital process for COVID credentials.

ensure the immutability, the digital security seal is timestamped on a blockchain. As the digital security seal contains only metadata, it guarantees privacy protection of the holder with personal and medical data only on the credential (QR code) itself. The blockchain is acting only as a secure "Trust Anchor," in the form of an undisputable timestamp. Thus, no data are ever exposed or stored on the blockchain. Unlike the European Union Digital COVID Certificate, this solution does not need to handle the complex management of cryptographic keys, thus avoiding the risk of having some of these keys being compromised or stolen.

The individual presents him or herself to the certified vaccination or testing center. His or her identity is verified (using an official ID) prior to testing, vaccination or determination of recovery. The information on vaccination status, or the test result or the recovery status is secured as COVID credentials. The COVID credentials consist of a certificate, secured by its QR code, containing the name of the person (previously verified), the medical information (vaccine, test result, recovery etc.) as well as the name and identification of the issuing authority. The COVID credentials are issued in batches (in the form of secured QR-codes) by the issuing authority (certified vaccination or testing center) using a Digital Certification SaaS. This Digital Certification SaaS is accessible online by the issuing authority only, with a secure login. Once the QR codes are generated, they are activated by the issuing authority and all information used to issue the credentials is deleted from the Digital Certification SaaS. This process reinforces the decentralized approach by removing the need for a central database that could be easily targeted, and safeguards are important to ensure only certified testing and vaccination centers are capable of issuing such credentials while respecting data protection and privacy regulations. The data remains in the issuing authority medical records (like any other laboratory or vaccination result and for a defined period of time if needed), enabling individuals to have their credentials re-issued when necessary (lost QR code for example). The secure QR code can be stored on an individual's phone or delivered as a print-out to reduce the digital divide. The secure QR code reduces the risk of forgery or tampering, and can be universally verifiable via a web-based portal or a mobile app, without the need to access a database containing personal or medical information. The individual has access to the web-based portal to verify his or her own credentials. The individual can choose to disclose information in specific contexts (airport control, access to a

venue, nursing home, etc.) and interpretation of the result ensues, based on the context-related requirements (for example negative PCR within the last 72 h to enter a specific country vs. 24 h etc.). Individuals can selectively decide who to show this information to and how many identifying details to reveal depending on the context. Selective disclosure and decentralized information can further assist in preserving privacy and confidentiality. A digitally secured solution can also reduce the risk of loss, identity theft and forgery while ensuring accessibility, bidirectional information and the possibility to revoke the credentials or update the expiration information when needed. In order to ensure more universal access, a paper version of the digital certificate and QR code is also available. This paper version provides the same level of security as the digital one, as its content is certified via the QR code which can be universally verified with the same security as the digital credential. QR code verification acting as a digital unforgeable stamp remains a cornerstone of certification in order to avoid any fraud or falsification. The QR code verification can also be performed offline as the verification keys (digital security seals) can be periodically replicated locally on the verification device when connected.

CONCLUSION

Immunity passports, certificates or COVID credentials will be increasingly at the forefront of medical and public policy discussions in the months and years to come. The adequate safeguards around a digital COVID credential should be discussed, and a non-falsifiable solution should be implemented especially if rights are linked to such credentials. The solution presented here provides a decentralized approach to databases as well as a secure certification process in line with the European Commission's recommendations (10). This solution also provides a secure approach, ensuring the integrity and validity of the information and respecting data protection regulations on privacy and confidentiality. The question of COVID credentials, now at the forefront, should be also be addressed at a policy level involving discussions between medical and public health actors, technology experts, ethicists and governing bodies. It is also of utmost importance to actively engage the public on the options and opinions connected with this issue in order to assess their trust and needs when proposing a digital health solution.

AUTHOR CONTRIBUTIONS

MN, PG, PT, LK, SS, and IG contributed to the writing of the manuscript. MN, PT, and IG contributed to the figures. All authors contributed to the article and approved the submitted version.

FUNDING

This work was supported by the Edmond J. SAFRA Foundation for clinical research in internal medicine.

REFERENCES

1. OECD. *Evaluating the Initial Impact of COVID-19 Containment Measures on Economic Activity*. OECD (2020). Available online at: http://www.oecd.org/coronavirus/policy-responses/evaluating-the-initial-impact-of-covid-19-containment-measures-on-economic-activity-b1f6b68b/ (accessed July 18, 2020).
2. Correia S, Luck S, Verner E. *Pandemics Depress the Economy, Public Health Interventions do Not: Evidence From the 1918 Flu*. (2020). Available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561560 (accessed July 27, 2020).
3. Edmond Safra Center for Ethics, Harvard University. *Roadmap to Pandemic Resilience*. (2020). Available online at: https://ethics.harvard.edu/covid-roadmap (accessed July 18, 2020).
4. Persad G, Emanuel EJ. The ethics of COVID-19 immunity-based licenses ("immunity passports"). *JAMA*. (2020) 323:2241–2. doi: 10.1001/jama.2020.8102
5. WHO. *"Immunity Passports" in the Context of COVID-19 Scientific Brief*. WHO (2020). Available online at: https://www.who.int/publications-detail/immunitypassports-in-the-context-of-covid-19 / (accessed April 30, 2020).
6. National COVID-19 Science Task Force (NCS-TF) ELSI report. *Ethical, Legal, and Social Issues Associated With "Serological Passports"*. (2020). Available online at: https://ncs-tf.ch/en/policy-briefs (accessed June 15, 2020).
7. Olivarius K. Immunity, capital, and power in antebellum New Orleans. *Am Hist Rev*. (2019) 124:425–55. doi: 10.1093/ahr/rhz176
8. Hall MA, Studdert DM. "Vaccine passport" certification - policy and ethical considerations. *N Engl J Med*. (2021). doi: 10.1056/NEJMp2104289. [Epub ahead of print].
9. Europol. *Europol Warning on the Illicit Sale of False Negative COVID-19 Test Certificates*. Available online at: https://www.europol.europa.eu/newsroom/news/europol-warning-illicit-sale-of-false-negative-covid-19-test-certificates
10. European Commission. *EU Digital COVID Certificate*. Available online at: https://ec.europa.eu/health/ehealth/covid-19_en (accessed April 21, 2021).
11. Phelan AL. COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges. *Lancet Lond Engl*. (2020) 395:1595–8. doi: 10.1016/S0140-6736(20)31034-5

Conflict of Interest: PG and PT has a patent WO2020011447 pending, and a patent WO2020030382 pending. SICPA has developed the CERTUS digital solution certificates with digital seal technology.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Excelsior Pass: Frequently Asked Questions

Excelsior Pass Frequently Asked Questions

Please continue reading to find frequently asked questions regarding Excelsior Pass. For frequently asked questions regarding Excelsior Pass *Plus*, please click the button below.

Excelsior Pass Plus FAQs

About Excelsior Pass

ESPAÑOL

What is Excelsior Pass?

Excelsior Pass is a free, voluntary platform that provides secure, digital proof of COVID-19 vaccination or negative test results.

Excelsior Pass can be accessed and stored through the NYS Excelsior Pass Wallet app, or through the Excelsior Pass Web Portal and printed. The NYS Excelsior Pass Wallet app can be downloaded at no cost from the Apple App Store and Google Play Store.

Excelsior Pass is currently available in more than 10 languages, including English, Spanish, Chinese, Russian, Haitian-Creole, Korean, Bengali, Arabic, Italian, Polish and Yiddish.

Are there different Excelsior Pass types?

There are currently three Excelsior Pass types:

- Excelsior Vaccination Pass (available 15 days after the final dose of the vaccine was administered: valid for 365 days)
- Excelsior PCR Pass (valid until midnight on the third day after a test)
- Excelsior Antigen Pass (valid for 6 hours from the time of a test)

Retrieving an Excelsior Pass

Retrieving an Excelsior Pass

How do I know if I am eligible to retrieve an Excelsior Vaccination Pass?

You are eligible to retrieve your Excelsior Vaccination Pass if:

- It has been 15 days or longer since you received the final dose in your vaccine series and you have not tested positive for COVID-19 in the last 10 days; and
  - You have been fully vaccinated in the State of New York OR
  - You are a New York resident who has been fully vaccinated in the state of New Jersey OR
  - You are a New York resident and your New York State healthcare provider has entered

your out-of-state immunization information into the New York State and/or New York City databases.

Please note that you must have received one of the COVID-19 vaccines authorized by the Food and Drug Administration (FDA) in the United States in order to retrieve your Excelsior Vaccination Pass. At this time, this includes the Pfizer-BioNTech COVID-19 vaccine, which has received full FDA approval, and the Moderna and Johnson & Johnson/Janssen COVID-19 vaccines, which have been authorized for emergency use.

If I was vaccinated outside of New York State but meet the eligibility requirements for an Excelsior Vaccination Pass, how do I retrieve my Excelsior Vaccination Pass?

For New York State residents who were fully vaccinated outside of New York State or New Jersey, your New York healthcare provider must input your vaccination information into the secure New York State and New York City immunization databases, and they must be administering the COVID-19 vaccine. Please note that when you go to retrieve your Excelsior Vaccination Pass from the Excelsior Pass Web Portal, you will need to enter the county where your provider who entered the information is located, not the county where you received your COVID-19 vaccine.

How do I know if I am eligible to retrieve an Excelsior PCR Pass?

You are eligible to retrieve your Excelsior PCR Pass if your PCR test was conducted in the State of New York, administered within 3 days of attempting to retrieve your Excelsior PCR Pass, and your results came back negative. An Excelsior PCR Pass is typically available within a few hours of receiving your negative test results from your testing laboratory.

How do I know if I am eligible to retrieve an Excelsior Antigen Pass?

You are eligible to retrieve your Excelsior Antigen Pass if your antigen test was conducted in the State of New York, administered within 6 hours of attempting to retrieve your Excelsior Antigen Pass, and your results came back negative. An Excelsior Antigen Pass is typically available within a few hours of receiving your negative test results from your testing laboratory.

I have children under 18 years old. Do they need an Excelsior Pass? How can they get an Excelsior Pass?

Anyone who has received a COVID-19 vaccine or negative test result in the State of New York is eligible for an Excelsior Pass, including children under 18 years old. You may retrieve and store Excelsior Passes on behalf of your children if desired.

Can I access and retrieve an Excelsior Pass if I am not a New York resident?

You do not have to be a New York resident to retrieve an Excelsior Pass. However, if you are not a New York resident, you must have received a COVID-19 vaccine or negative COVID-19 test results in the State of New York.

What information do I need to provide to retrieve my Excelsior Pass?

To retrieve your Excelsior Pass, you will need to provide basic personal information, including your first and last name, date of birth, ZIP code, and phone number. You will also need to verify your information with three "challenge questions" whose answers are unique to you. You'll need to enter this information every time you retrieve an Excelsior Pass.

How is my Excelsior Pass generated?

Your Excelsior Pass is generated based on data provided by your vaccine administrator or testing laboratory to the secure New York State and New York City immunization and COVID-19 testing databases.

Some entities that are not under the regulatory authority of the State of New York (e.g., federal entities, first nations, and jurisdictions outside of New York State) may not report into these systems, which may make an Excelsior Pass unavailable at this time.

What do I do if I am not able to retrieve an Excelsior Pass?

First, be sure to review the different Excelsior Pass types to ensure you are eligible. After confirming eligibility, if you are still having issues, please make sure that the information you are entering matches the information (e.g., name, date of birth, and ZIP code) from your CDC Vaccination Card or test results, as you will need to match this information accurately to retrieve your Excelsior Pass.

I am still unable to retrieve my Excelsior Pass, what should I do?

If you are still unable to retrieve your Excelsior Pass, please submit a record review, and our team will provide you with steps to take to get the issue fixed. Be sure to describe the problem and correction needed (e.g., first name spelled incorrectly) in the “Describe Your Situation” field.

You are also encouraged to reach out to your vaccine administrator and/or testing laboratory directly to ensure the information entered is accurate. Please know that per New York State Department of Health (DOH) guidance, all New York State vaccine administrators must submit vaccination data to the secure New York State and City immunization databases and have staff available to both review and correct the data they input, if data entry issues are identified.

Using Excelsior Pass

How do I show my Excelsior Pass to participating organizations?

You can present your Excelsior Pass on your smartphone, through the NYS Excelsior Pass Wallet app, or you can print your Excelsior Pass from the Excelsior Pass Web Portal and present the printed version.

Organizations who accept Excelsior Pass will use the NYS Excelsior Pass Scanner app to prove that the QR Code on your Excelsior Pass is valid.

If you are an adult aged 18+, you will also need to present a photo ID with name and date of birth alongside each unique Excelsior Pass. Adults can hold Excelsior Pass for children under 18 years old.

Am I required to use Excelsior Pass?

No, participation is voluntary. Excelsior Pass empowers you to be in control of your health information. Even after retrieving an Excelsior Pass, you decide if, when, or how to use and show it.

How much does it cost to use Excelsior Pass?

Excelsior Pass is free.

Can I show more than one type of Pass on the same device?

Yes. You may retrieve, store, or show as many Passes as you may be eligible for. This includes:

- Excelsior Vaccination Pass
- Excelsior PCR Pass
- Excelsior Antigen Pass
- Excelsior Vaccination Pass *Plus*
- Excelsior PCR Pass *Plus*
- Excelsior Antigen Pass *Plus*

For more information on Excelsior Pass *Plus*, please visit the Excelsior Pass *Plus* FAQs.

Can I show Excelsior Passes for more than one individual on the same device?

Yes, multiple Excelsior Passes for adults aged 18+ and children under 18 can be stored on the same device.

My Excelsior Vaccination Pass expired. Can I get another one?

Your Excelsior Vaccination Pass is currently valid for 365 days after the final dose of the vaccine was administered. For a secure, digital copy of your COVID-19 vaccination record, please visit the Excelsior Pass Web Portal to retrieve your Excelsior Vaccination Pass *Plus*.

My Excelsior PCR or Antigen Pass expired. Can I get another one?

After an Excelsior PCR or Antigen Pass expires, you will need to follow the requirements for retrieving a new Excelsior PCR or Antigen Pass:

- **Excelsior PCR Pass:** Valid until midnight on the third day after your test. After your Excelsior PCR Pass expires, a new test is required to retrieve a new Excelsior PCR Pass.
- **Excelsior Antigen Pass**: Valid for 6 hours after your test. After your Excelsior Antigen Pass expires, a new test is required to retrieve a new Excelsior Antigen Pass.

Can I get a refund if I bought a ticket to an event, but my Excelsior Pass is not valid?

Refund policies are unique to the organization you are visiting. It is recommended that you consult with the organization directly as to their refund policies.

Can I use one Excelsior Pass in multiple places?

Yes. Each Excelsior Pass can be used for as long as it remains active, at as many places as you would like.

Accessibility

How can I retrieve an Excelsior Pass if I don’t have access to a smartphone?

Participation in Excelsior Pass is voluntary and designed to be inclusive of all New Yorkers, regardless of access to a smartphone. You can easily print your Excelsior Pass via the Excelsior Pass Web Portal.

You can also show alternate proof of COVID-19 vaccination or negative test results, like a paper

form, directly at an organization.

Is Excelsior Pass available in multiple languages?

Yes. Excelsior Pass and its companion apps are available in more than 10 languages including English, Spanish, Chinese, Russian, Haitian Creole, Korean, Bengali, Arabic, Italian, Polish, and Yiddish.

Is Excelsior Pass accessible to people who may have hearing or vision impairments?

Yes. The application has gone through thorough accessibility testing to ensure it is easy to use for those who may have hearing or vision impairments.

Policies

What is the difference between a PCR test and an antigen test?

According to the Food and Drug Administration (FDA), PCR tests are molecular tests that detect the virus' genetic materials, and antigen tests detect specific proteins from the virus. You can read more about testing in the FDA's Coronavirus Disease 2019 Testing Basics.

Where can I get tested for COVID-19?

Testing for COVID-19 is widely available throughout New York State. Individuals who have questions about COVID-19 testing should call the New York State COVID-19 Hotline at 1-888-364-3065 or visit NYS Find A Test Site Near You.

If I tested positive for COVID-19 antibodies, can I retrieve an Excelsior Pass?

At this time, Excelsior Pass is only available for COVID-19 vaccination or negative COVID-19 diagnostic test results in accordance with New York State Department of Health (DOH) guidance.

Security and Privacy

Is my data private and secure?

Your data is private, secure, and only used to retrieve your Excelsior Pass. Your personal data will not be used for sales or marketing purposes or shared with a third party, other than for the sole purpose of validating COVID-19 vaccination or negative test results.

Excelsior Pass gives you the ability to maintain control of your personal data and share it in a manner that is secure, verifiable, and trusted. Your Excelsior Pass contains cryptographic signatures that ensure that it is genuine and that no data tampering has occurred.

If you choose to use the NYS Excelsior Pass Wallet app, only the Excelsior Passes you save will be stored on your mobile device. You may delete an Excelsior Pass at any time.

What health information can Excelsior Pass access?

When you receive a COVID-19 vaccine or test in the State of New York, the New York State Department of Health (DOH) receives a copy of your records from your vaccine administrator, provider, or testing laboratory. Using the information you provide, Excelsior Pass searches the New York State Department of Health's (DOH) records for your COVID-19 vaccination or COVID-19

negative test results and then provides you an Excelsior Pass showing your name, date of birth, Pass type, and Pass expiration. No other information is accessed or stored.

Will my personal information be stored on the NYS Excelsior Pass Wallet app?

If you choose to use the NYS Excelsior Pass Wallet app to store your Excelsior Pass, the only personal identification information saved on your Excelsior Pass is your first name, last name, and date of birth. You may delete an Excelsior Pass at any time.

Answers to the "challenge questions" used to verify your identity will not be stored, which is why you need to verify your identity every time you retrieve a new Excelsior Pass.

When your Excelsior Pass is scanned, the NYS Excelsior Pass Scanner app collects analytics about the type of Excelsior Pass and the result of the scan. No personal information from an Excelsior Pass is collected or stored.

What personal information can organizations see when they scan my Excelsior Pass?

The only information the organization can see when they scan your Excelsior Pass is your name, date of birth, Pass type, and Pass expiration date. Additionally, the NYS Excelsior Pass Scanner app lets an organization know if your Excelsior Pass is valid.

A valid Excelsior Pass indicates that you have either been fully vaccinated against COVID-19 or that you had a recent negative COVID-19 test. An invalid or expired Excelsior Pass is not an indication that you have COVID-19.

Will those who scan my Excelsior Pass be able to save or store my personal information?

No. The NYS Excelsior Pass Scanner app does not download or store your information, which is why your Excelsior Pass must be scanned again if you leave and return to a participating organization.

Does Excelsior Pass track my location?

No. Excelsior Pass does not track your location.

Will New York State or anyone else be notified if I attempt to retrieve an Excelsior Pass after a positive COVID-19 test result?

No. Excelsior Pass does not share your data with anyone. And, an Excelsior Pass cannot be retrieved if you receive a positive test result.

Can I use this app to see if someone else has been fully vaccinated or tested negative?

No. Excelsior Pass is intended for personal use only.

Where can I read the Excelsior Pass Privacy Policy?

You can read the Excelsior Pass Privacy Policy by visiting the Excelsior Pass Privacy Webpage.

Technical Support

What are the basic requirements for using Excelsior Pass applications?

Excelsior Pass applications are compatible with smartphones running iOS 13.0+ or Android 7.0+.

If preferred, you may also retrieve your Excelsior Pass via the Excelsior Pass website and print a paper copy.

What should I do if my vaccination or test information couldn't be confirmed?

For an Excelsior Vaccination Pass: Please check that you entered your information exactly as it appears on your CDC Vaccination Card, as you will need to match that information accurately to retrieve your Excelsior Pass. This includes:

- The county where you received your vaccine (for New Yorkers vaccinated outside of New York State or New Jersey, this would be the county in which your healthcare provider who is entering your information is located).
- The date you received the last dose of your vaccine series (one dose of Johnson & Johnson/Janssen vaccination series or the second of the two dose Pfizer or Moderna series).
- The type of vaccine you received.

For an Excelsior PCR or Antigen Pass: Please check that you entered your information exactly as it appears on your test results, as you will need to match that information accurately to retrieve your Excelsior Pass. This includes: your first name, last name, the location where you received your test, the date you were tested, and the type of test you received.

If you still can't get your Excelsior Pass, you can:

- Contact your vaccine administrator or testing laboratory to confirm your correct information was submitted. All vaccine administrators must have staff dedicated and available to correct these issues. Once a testing laboratory has submitted test result information to the State, it cannot be modified.
- If you were vaccinated at a city-run site within New York City and require a change to a vaccination record, you can call 311 from within the City or 212-639-9675 from outside New York City or email cir@health.nyc.gov. Additionally, if you are a New York City resident and fully vaccinated but lost your CDC Vaccination Card, you can request a copy of your COVID-19 vaccination record by calling 311.
- Submit a record review request form. Please note that this form is for vaccination records only, not test result records.
- Call the Excelsior Pass Help Desk at (844) 699-7277 for general inquiries/to receive support in submitting a record review request to help resolve the issue.

In the meantime, you can always present alternate proof of COVID-19 vaccination or negative test results, like a paper form, directly to an organization.

How do I remove an Excelsior Pass from the NYS Excelsior Pass Wallet app?

Please review how to remove an Excelsior Pass in the step-by-step instructional guide that is most relevant for you:

- NYS Excelsior Pass Wallet for iOS
- NYS Excelsior Pass Wallet for Android

What do I do if I have questions about Excelsior Pass?

For general questions or technical inquiries about Excelsior Pass, including how to navigate the website or retrieve an Excelsior Pass, you can fill out the support form or reach out to the Excelsior

Help Desk at 844-699-7277 from 8 a.m. to 8 p.m. EST daily.

How do I submit feedback about the app or Excelsior Pass?

If you have feedback about Excelsior Pass, please share it via our support form.

If you are having trouble, please consult one of our helpful, step-by-step instructional guides:

- Excelsior Pass Website | español
- NYS Excelsior Pass Wallet for iOS | español
- NYS Excelsior Pass Wallet for Android | español

If you are still unable to solve your problem, you can always use an alternate form of proof, like a paper form, of your COVID-19 vaccination or negative test results.

For Providers

As a provider, what COVID-19 vaccination data am I responsible for providing?

You are responsible for reporting complete and accurate COVID-19 vaccination data to the appropriate data system (CIR for New York City providers, NYSIIS for all other providers) within 24 hours of vaccine administration. All required and critical fields must be completed at the time the data is entered. For more information on data reporting guidelines, please visit the NYSIIS and CIR Requirements for Providers.

As someone who administers COVID-19 vaccines, what do I do when customers/patients tell me they are having trouble retrieving an Excelsior Pass?

The provider who administered the vaccine is responsible for entering all vaccine data correctly into NYSIIS (or CIR if provider is located in New York City). If one of your customers/patients is having trouble retrieving an Excelsior Pass, your first action should be to check their information in NYSIIS/CIR (don't just look in your system/electronic medical record). For more information on what to look for and how to fix data errors, please visit the Excelsior Pass Fact Sheet for Vaccine Providers.

If I am a New York State healthcare provider, can I submit COVID-19 vaccination information for patients who are residents of New York State, but received their vaccine outside of the State?

If you have patients who were vaccinated outside of New York State who can show proof of vaccination, you should enter those patients' immunization records into the secure New York State and New York City immunization databases. You will submit these as historical doses to reflect that you did not administer the dose to the patient. If you are a New York State provider, please visit the NYSIIS and CIR Requirements for Providers for more information on COVID-19 vaccination data entry.

Translations

The New York Times https://www.nytimes.com/2021/06/01/nyregion/excelsior-pass-vaccine.html

Will the Excelsior Pass, New York's Vaccine Passport, Catch On?

More than one million Excelsior passes have been downloaded since they were introduced, but officials are hoping they will be adopted more widely.

By Sharon Otterman

Published June 1, 2021 Updated Aug. 19, 2021

On the Upper East Side in Manhattan, a well-heeled crowd flashed it to get into a socially distanced dance performance at the Park Avenue Armory. In Chelsea, people showed it to attend a John Mulaney stand-up set at City Winery. And in Troy, N.Y., patrons are using it to enter an intimate, speakeasy-style bar that only admits vaccinated guests.

This magic ticket is New York State's Excelsior Pass, which was introduced in March as the first and only government-issued vaccine passport in the country, accessible, for now, only to people who have been vaccinated in the state.

Officials are hoping that it can help New Yorkers feel confident about the safety of businesses and jump-start a statewide economy that is still reeling from losses experienced during the pandemic. But in order for that to happen, they will need more people and businesses to start using it and vaccine passports to become more universally accepted.

Though it is basically just a QR code on your phone that indicates your vaccine status, the pass, and vaccine passports more generally, have become a political flash point among conservatives and others who say the passports violate privacy concerns.

About 1.1 million Excelsior Passes had been downloaded onto phones and computers as of last week, according to the state. But so far, 9.1 million New Yorkers have been fully vaccinated.

Officials are hopeful that the pass will catch on more widely.

Eric Piscini, the vice president of emerging business networks at I.B.M., which developed the Excelsior Pass for the state, said New York was in discussions with other states so the pass could be used by out-of-state residents in New York and by New Yorkers elsewhere.

"In the application space, when you reach a million people, that's a pretty good threshold to pass," Mr. Piscini said. "That is a really good indication that people find value in this."

Many businesses, like the City Winery in Chelsea, are using the Excelsior Pass to monitor whether clients have been vaccinated. Victor J. Blue for The New York Times

Nationally, a range of states including Georgia, Alabama, Arizona and Florida have already banned the use of vaccine passports, presenting the bans as measures to protect individual privacy and vaccination choice.

In New York, some lawmakers are backing new legislation that would provide additional privacy protections.

But though major sports venues and a growing number of smaller New York businesses are embracing using the app, the vast majority of businesses are not requiring any proof of vaccination to enter. (The state would not say how many businesses had signed up.)

For those that take the Excelsior Pass, paper vaccine cards must also be accepted as a form of proof, the state said.

Some businesses — especially those catering to adult audiences, like arts venues — are jumping into the world of verification. Aside from accepting the Excelsior Pass, City Winery in Chelsea, for example, also uses the CLEAR Health Pass as a way to verify health and vaccination status. Gov. Andrew M. Cuomo has encouraged the move toward fully vaccinated crowds by permitting businesses to disregard social distancing if everyone is vaccinated.

But civic technology experts warn that the passes can be gamed relatively easily, just like the paper vaccine card itself.

It took Albert Fox Cahn, executive director of the Surveillance Technology Oversight Project, a nonprofit watchdog group, just 11 minutes to download someone else's Excelsior Pass using information they had posted on social media and Google searches, he said. Many people have posted pictures of their vaccination cards, which include a person's name, birthday, date of vaccination and type of shot.

Some patrons prefer to bring along their paper vaccination cards instead of downloading the app. Victor J. Blue for The New York Times

And each pass can be uploaded to a limitless number of devices, or printed out and copied. The Excelsior Pass, which cost the state $2.5 million to develop, contains no biometric data for privacy reasons, so it needs to be compared against an ID, an extra step that, in practice, sometimes isn't taken.

"We need to realize that as much as we want a magic piece of software to be able to tell us whether the person next to us is vaccinated, these apps really can't," Mr. Cahn said. "At the end of the day, it's largely built on trust."

The Coronavirus Pandemic ›

Latest Updates ›

Updated Sept. 8, 2021

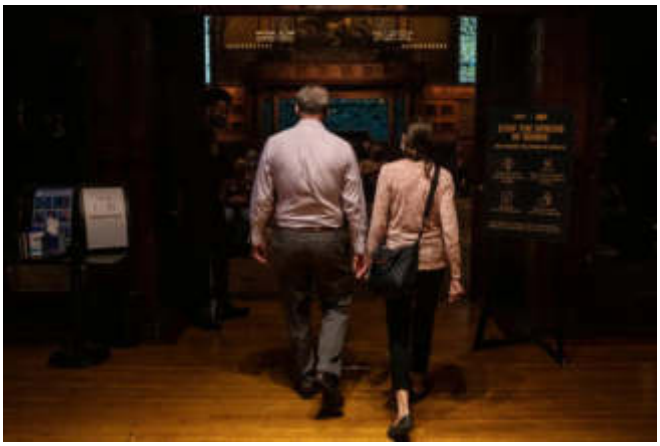
- Elizabeth Warren asks Amazon to 'stop peddling misinformation about Covid vaccines and treatments.'
- L.A. is set to become the first major U.S. school district to require vaccinations for students.
- President Biden is expected to lay out a plan on Thursday to push broad vaccination mandates.

At the City Winery on Wednesday, outdoor hosts sometimes asked for ID when people flashed their Excelsior Pass or paper vaccination cards to gain entry, but sometimes they didn't. At the Armory, Covid compliance officers in face shields carefully checked IDs, but they just eyeballed the pass's QR code, instead of scanning it to double-check its veracity.

There is no law mandating such steps be taken.

"We trust our audience," said Michael Dorf, the chief executive of City Winery, adding that his employees use their discretion to make those choices.

Accessibility is another worry. New York's vaccine rollout was marred by a heavy reliance on a complex internet appointment system, which gave tech-savvy people an advantage. Many older New Yorkers and those without good internet access struggled.



The Park Avenue Armory required that all patrons be vaccinated to attend a recent performance. Victor J. Blue for The New York Times

Now those same people face another technological hurdle if the pass becomes popular. Noel Hidalgo, executive director of BetaNYC, a nonprofit public interest technology organization, said he didn't think the state should be investing millions in a vaccine passport at a time when more time and effort could be spent on things

like helping improve vaccination rates among Black and Hispanic New Yorkers and figuring out how people could quickly replace a lost or damaged paper card.

"Why are we focusing on providing a tech tool to a small group of New Yorkers who are digitally literate and understand how to get access?" he asked.

Delays in entering data and data entry mistakes are also limiting who gets the pass. About 4 percent of people who tried to get passes were unable to do so, said Jennifer Givner, a state spokeswoman.

Understand Vaccine and Mask Mandates in the U.S.

- **Vaccine rules**. On Aug. 23, the Food and Drug Administration granted full approval to Pfizer-BioNTech's coronavirus vaccine for people 16 and up, paving the way for an increase in mandates in both the public and private sectors. Private companies have been increasingly mandating vaccines for employees. Such mandates are legally allowed and have been upheld in court challenges.
- **Mask rules**. The Centers for Disease Control and Prevention in July recommended that all Americans, regardless of vaccination status, wear masks in indoor public places within areas experiencing outbreaks, a reversal of the guidance it offered in May. See where the C.D.C. guidance would apply, and where states have instituted their own mask policies. The battle over masks has become contentious in some states, with some local leaders defying state bans.

SEE MORE

The pass pulls its information from the state and city immunization databases. If the information is entered incorrectly — for example, with misspellings or a wrong initial — the pass cannot be found.

I.B.M. recently added a phone number check to the identification field of the app to make it easier to find someone's vaccination. Only four of the five fields — including first and last name, date of birth and ZIP code — need to match for someone to get a pass.

A thread on Reddit dedicated to helping people who could not get passes noted that sometimes putting in an old ZIP code seemed to work.

"Yeah, for me it was a ZIP code I hadn't used in 14 years," one user wrote on the thread.

People who can't get a pass can fill out a complaint form and call a state hotline, but for the most part, the organization that vaccinated them has to correct the data, which is not always easy. The Excelsior Pass also does not have access to federal vaccination data, so people who got their vaccines at veterans' hospitals, like John Taylor, a 77-year-old Vietnam War veteran who lives in Pleasant Valley, N.Y., are out of luck.

"I had it laminated," said Mr. Taylor of his paper vaccine card. "I'm just going to forget about the pass."

State officials emphasized that the paper card could always be used, so the Excelsior Pass was not essential. Mr. Cuomo himself recently said that he still shows his paper card.

Outside shows at the Park Avenue Armory and City Winery on recent days, it seemed that about half of the patrons waiting in line to enter flashed their Excelsior Passes to prove vaccination and that the rest used their cards or photos of their cards. Both venues had additional alternatives for unvaccinated guests, such as rapid testing on site, or accepted proof of recent negative coronavirus tests.

"I'm proud of it," Scott Hernandez, 42, said of his Excelsior Pass as he waited to see if there was room for him and friends to have dinner at the winery. "There needs to be more education about it."

But the extent of social acceptance of the Excelsior Pass may vary around the state. In more conservative areas, the blowback can be severe.

In Auburn, N.Y., a tiny five-table chocolate store, Gretchen's Confections and Cafe, was inundated with social media hate from around the country after photos of a sign asking people to be vaccinated to sit indoors went viral. The store decided to take down its sign, and it now welcomes everyone.

"It is very polarizing," said Gretchen Christenson, the owner. "They have been calling us Hitler and fascists, 'Segregation Cafe.' I think the number of people against it is tiny, but they are just extra loud and threatening."

And when Matt Baumgartner announced that one of his bars, the Berlin Lounge in Troy, N.Y., would allow only vaccinated guests because of its small size and lack of outdoor space, he was also hit with social media hate.

In both cases, loyal customers rallied in support, and the lounge and the shop have been doing well in recent weeks.

"I'm someone who very strongly who believes in the vaccine, and part of me feels like getting to visit more places is kind of a reward," Mr. Baumgartner said.

On an innovative architecture for digital immunity passports[1] and vaccination certificates

John C. Polley[2], Ilias Politis[3], *Member, IEEE*, Christos Xenakis[4], *Member, IEEE*, Adarbad Master[5], and Michał Kępkowski[6]

***Abstract* — With the COVID-19 pandemic entering a second phase and vaccination strategies being applied by countries and governments worldwide, there is an increasing expectation by people to return to normal life. There is currently a debate about immunity passports, privacy, and the enablement of individuals to safely enter everyday social life, workplace, and travel. Such digital immunity passports and vaccination certificates should meet people's expectations for privacy while enabling them to present to 3rd party verifiers tamper-evident credentials. This paper provides a comprehensive answer to the technological, ethical and security challenges, by proposing an architecture that provides to individuals, employers, and government agencies, a digital, decentralized, portable, immutable, and non-refutable health status cryptographic proof. It can be used to evaluate the risk of allowing individuals to return to work, travel, and public life activities.**

***Index Terms* — biometric strong authentication, digital immunity passports, real-time id verification, vaccination certificates, verifiable credentials**

I. Introduction

The urgency to contain the COVID-19 pandemic has led governments to implement various restrictions to day to day life. The development of several vaccines approved by the World Health Organization (WHO) [1], which are currently available to the public, assists in ending this societal health threat. While the number of people being vaccinated is increasing, the need for a carefully designed system of digital immunity passports is evident.

The adoption of a worldwide system that verifies people's COVID-19 status, including vaccination records, centers around the solution of digital immunity passports. This system would enable the holders of such passports to re-enter social life, work, and travel in safety. However, the nature of what information should be held on an immunity passport fuels debates among proponents of the solution and right-to-privacy advocates. Additionally, the technical challenges facing the successful integration of digital immunity passports in everyday life are yet unsolved. Most countries currently depend on paper-based systems in which people receive a test result or a vaccination record card with basic information on it. These paper records lack the security features that would render them trusted official certificates. Nothing prevents these documents from being lost or stolen, and thus, the opportunities for fraud are high [2].

In addition to the technical, legal, and societal issues, digital immunity passports are going to face possibly the most demanding scientific challenges. The development of new vaccines for COVID-19 and the beginning of general public vaccinations, signals the need for a revision on WHO recommendations for the COVID-19 Public Health Emergency of International Concern (PHEIC) [3], which would include the COVID-19 vaccination certificates. Therefore, it is evident that there is a need for a digital credentials proofing system, which would offer immutable proof of a vaccination status. In this study the focus is placed on providing an answer to the technological challenges that the application of digital immunity passports and vaccination certificates is facing, ensuring that such answers would also address the privacy and ethical concerns, which have been raised recently [7].

This paper is introducing a holistic solution for addressing the challenges that digital immunity passports and vaccination certificates are facing. The solution is a mobile service that maps a person's vetted identity and biometrics to the phone and then, cryptographically binds it with their COVID-19 test and vaccination records. The person can then prove their status by utilizing the credentials with a QR code, Bluetooth transfer or NFC single tap. The basis of the solution lies on the premise that users can have their identity vetted online with no personal contact, and thus, creating a digital identity that is bounded to their mobile phone. The proposed Digital Immunity Passport (DIPA) solution allows users to access test-laboratory or central government portals, utilizing their own account credentials. This solution also generates an access token, to be used by third parties to access the user's COVID-19 test results or vaccination records. These results and records are securely transferred to the mobile application and their anonymized

[1] This work has been funded in part with Federal funds from the National Institutes of Health, Department of Health and Human Services, under Contract No. 75N91020C00035 and in part by the European Union's Horizon 2020 Stimulating innovation by means of cross-fertilisation of knowledge program under Grant 824015 (H2020-MSCA-RISE-2018-INCOGNITO) and the Grant 826404 (H2020-SC1-FA-DTS-2018-1-CUREX).

[2] John C. Polley at Systems Security Lab of the University of Piraeus, Greece (email: j.c.polley@ssl-unipi.gr).

[3] Ilias Politis at InQbit Innovations SRL., Bucharest, 041386 Romania and with the Systems Security Lab of the University of Piraeus, Greece (email: ilias.politis@inqbit.io, ipolitis@ssl-unipi.gr).

[4] Christos Xenakis at the Systems Security Lab of the University of Piraeus, Greece (email: xenakis@unipi.gr).

[5] Adabard Master at iCrypto, Inc., Santa Clara, CA 95054 U.S.A. (email: info@icrypto.com).

[6] Michał Kępkowski at Computing, Macquarie University, Sydney Australia (email: michal.kepkowski@students.mq.edu.au).

version can be immutably logged. The information that is securely stored in the mobile application can be presented to verifiers upon user's biometric identification and consent.

The rest of the paper is organized as follows. Section II presents the main challenges that need to be addressed before immunity passports can be widely adopted by society. The emphasis is placed on the technological challenges that currently limit the wide implementation of digital immunity passports. In Section III, the platforms stakeholders are introduced along with the overall description of the proposed DIPA solution. The key innovations are discussed in Section IV, while main components and functionalities are described in Section V. A description of the use case that is considered for this paper is presented in Section VI. Section VII summarizes the benefits and added value gained by national health care organizations and governments from incorporating the proposed platform into their workflows. Last, Section VIII concludes the paper.

II. Challenges for a Successful Adoption of Digital Immunity Passports

Recently, the discussion on the issuing and applicability of digital immunity passports have raised concerns regarding the technological, scientific, and ethical problems such certificates are encountering [3]. Any plan for incorporating a digital immunity passport for daily use should offer completely anonymous and untraceable information to prevent being accessed without the consent of the user by 3rd party verifiers such as individuals, public health organizations and others. Furthermore, the digital immunity passports and the vaccination certificates should be in the heart of a holistic automated real-time policy enforcement strategy. This strategy could keep public health organization employees, first responders, individuals, and other stakeholders, aware of the current status and any policy updates. Such a strategic decision is expected to minimize the risk of exposure.

For a technological proposal to be adopted as a successful solution for addressing the portability, immutability, privacy and security aspects of the digital immunity passports and vaccination certificates, it should address the following challenges:

1. Individuals (users) should be able to remotely register in an easy and expeditious manner.
2. Users' identities should be automatically and securely verified leading to a seamless onboarding experience.
3. Users should be able to access the solution upon verification via state-of-the-art strong authentication (preferably biometric based).
4. Individuals must be able to prove their test result or vaccination status in their work environment, travel, etc., minimizing the probability of unintentionally endangering others.
5. The proof should be regularly updated to ensure that individuals are always presenting the most updated results, since earlier negative tests may not be indicative of their present health status.
6. The proof itself and the mechanism that produces it, needs to possess such properties that render it indisputably, unsusceptible to fraud, collusion, and misrepresentation.
7. The proposed solution must be seamlessly integrated to the COVID-19 testing ecosystem, eliminating the need for modifications and upgrades of the existing workflows required to produce immutable proofs.
8. The proof must be portable and easy to convey to any requesting authority.
9. Multiple proof types must be supported – positive or negative infection status, antibody presence, vaccination records, etc.
10. The proposed solution should not store any Personally Identifiable Information (PII).
11. The proposed solution should support an "anonymous mode" to enable use cases such as entering restaurants, cinemas, public venues, etc. without the user being required to reveal his identity to the verifier.
12. The proposed solution should be able to operate with machine verifiers (no human agent present).
13. The proposed solution supports use cases that require less than a second verification (mass-transit, stadiums, etc.).
14. The proposed solution should not require any specialized hardware. Leverage existing widely adopted smartphone technologies.
15. The proposed solution should support consumer and person to person use cases (food delivery, uber, entry to private residence, etc.)
16. Dynamic context must be collected at proof points to facilitate data collection and contact tracing.

III. Digital Immunity Passport Solution

A. *Stakeholders and Entities*

Figure 1 Stakeholders and Entities

The stakeholders and entities involved in the solution are depicted in Figure 1. The users of the mobile application are onboarded into the system and activated for usage of the service. The consumers of the service could include public and private organizations whose operation requires the immunity and vaccination status of the travelers, employees, etc. The testing laboratories and vaccination centers are also stakeholders of the proposed solution, which could convey the test results of the users to the application. The identity management and access infrastructure support the assignment

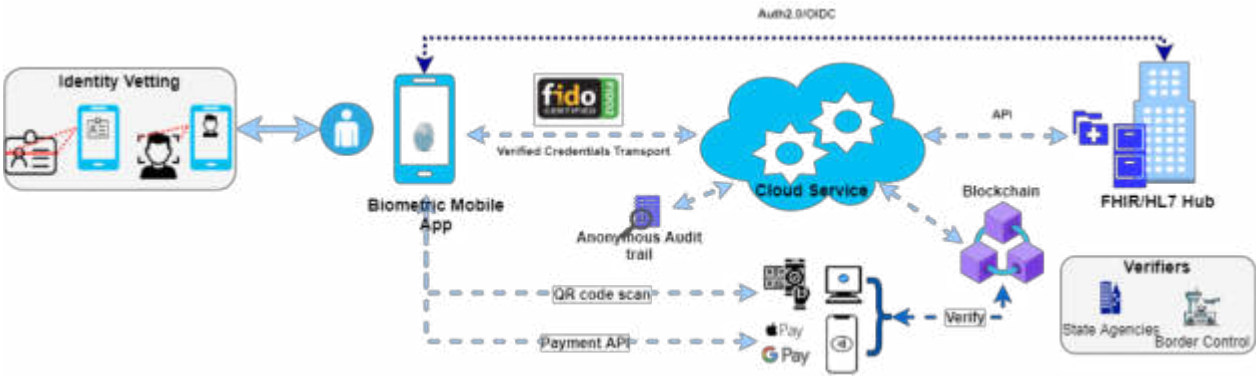


Figure 2 Overview of DIPA proposed architecture

of user identities and access privileges as well as the strong authentication of users. Moreover, the overall ecosystem displays the test and vaccination status and includes key entities, such as the mobile application responsible for interaction with the user to facilitate identity vetting, onboarding, and biometric authentication. The distributed ledger is utilized to create immutable audit trails and provide cryptographic proof of the immutability of the user verifiable credentials. The solution incorporates the integration of native mobile wallets to allow proofs to be in alternate portable formats, thus, ensuring quick validation based on existing widely adopted payment mechanisms. The solution is implemented as a software-as-a-service (SaaS) virtual private cloud to provide secure infrastructure services for building applications which store, process and share sensitive health-related information, in accordance with GDPR and other national security and privacy regulatory frameworks (i.e., HIPAA, etc.) [4]. The proposed solution does not store any PII of the user.

B. *Overview*

An overview of the overall architecture, including the key protocols and actions described in the DIPA solution is shown in Figure 2. The solution allows a user to prove the status of their COVID-19 testing to provide verifiers (individuals, small business, authorities, etc.) with non-repudiated proof of vaccination records, current virus infection status and presence of antibodies to safely return to work, travel or socialize. Furthermore, the solution provides the user with the means to instantiate a trusted identity, using the current trusted institutional identities by leveraging a smartphone. Transport and application layer encryption along with state-of-the-art channel biding and certificate pinning techniques, establish secure transactions between the user and relevant stakeholders (i.e., test kit manufacturers, test laboratories, etc.).

The proposed technological solution ensures that the user's test status proof will remain resistant to fraud and cyberattacks, by incorporating a Keyless Signature Infrastructure (KSI) blockchain [8] (or any other Distributed Ledger technology), which record new events that are cryptographically linked to the previous ones in a distributed and immutable manner. Moreover, the solution allows the proof to be carried in a portable mobile wallet on the user's personal phone, by using security technologies such as, threshold cryptography and secure mobile storage. The smartphone's on-board fingerprint, face, and iris readers, in parallel to face recognition services, are utilized to ensure the user's identity proof and provide high degree of security. To minimize the need for modifications of the existing workflows of health care services and sufficiently address the ethical issues associated with the immutable proofs, the DIPA solution is designed to be fully compliant with the latest standards and regulations of health care, user privacy and data usage. One of the core principles in the designing and implementation of the proposed technological solution is that no personal and sensitive data of any kind is stored anywhere in the ecosystem, except the proof of status. Such data remains with the appropriate authoritative sources (i.e., vaccination centers, healthcare providers, government, and enterprise identity providers, etc.). The platform's seamless integration with current networks and services is ensured by leveraging widely established and well-known technologies/standards of identity, access management, trusted storage (OAuth2.0 [9] and Open ID Connect - OIDC [10], data storage {Federal Information Processing Standard – FIPS}, Transport Layer Security {TLS} [11], cryptographic proofs {hash functions} and distributed storage {KSI Blockchain}).

IV. Key Innovations

Several key innovations have been introduced in the DIPA solution to ensure the digital immunity passport's integrity, the holder's privacy and the procedure's security.

A. *Digital onboarding*

The proposed solution allows users to leverage powerful aspects of technology such as mobility and privacy-preserving information sharing. The security in such environment begins with onboarding, that is the intuitive provisioning of individuals into the described ecosystem. Its implementation allows seamless onboarding of users, accompanied with assurances. Specific focus has been given on ensuring that there is no user manual data entry through this stage, thus, increasing its potential adoption by the community. Additionally, the digital onboarding allows the timely registration of biometrics, which will be used later, by the FIDO2 protocol [12]. A key advantage of the digital onboarding is the ability to perform online real-time identity verification, by exploiting the OCR and MRZ extractions along with performing checksum validations. The ID verification procedure is also enhanced with face matching between the ID and a selfie (with liveness detection - anti-spoofing), along with validating the ID data against the database of the identity issuer (i.e., government agencies,

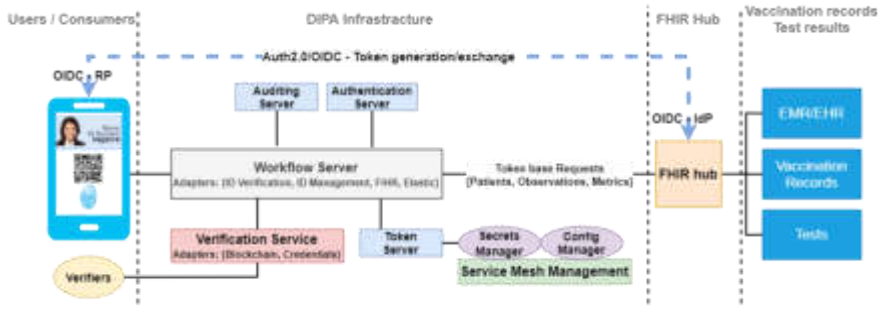


Figure 3 DIPA key components and functionalities

enterprise HR, etc.), in accordance with the use case and the national policies. Moreover, digital onboarding facilitates the creation of verifiable credential for the user identity signed by the identity management server and stored only on the user's phone. An immutable proof of all transactions is stored on the distributed ledger. The service has a built-in consent service, which capture user acceptance in a signed digital attestation.

B. Verifiable credentials

To address the immunity passport holders' demand for privacy and anonymity while assuring third party verifiers of the user's identity validity, the system design faces the following conundrum:

- Validate a user identity such that it is unquestionably associated with a person whose results are being requested from the health system.
- Do not keep any identifiable personal and health data on the solution servers.

DIPA is based on the implementation of the W3C Verifiable Credentials standard [14]. Essentially, the identity of the user and their status are represented as portable blocks of data that have incorporated cryptography mechanisms based on zero-knowledge proof. The generated credentials are sent to the mobile device over a secure channel. The mobile application then presents the credentials directly to any application (3rd party verifier) requesting the data.

Utilizing the verifiable credentials protocol, the system can store portable digital credentials on the mobile device only. Thus, it eliminates the need for keeping identity and test data on servers and allows the users to prove their identity and status directly to the requesting verifying party without any mediation of third-party servers. Furthermore, the user can select between identified or de-identified presentation of credentials. Such decision preserves the users' privacy and makes information disclosure a transaction directly between the holder (i.e., the user of the application) and the verifier (i.e., consumers), as in Figure 2. Firstly, the system ensures that the credentials themselves contain proofs of authenticity, since they are signed by the identity management server. Secondly, the system succeeds on guaranteeing the immutability of the verifiable credentials by deploying a distributed ledger that registers identifiers and user schemas. The verifiable credentials designed for the proposed system have a built-in expiration for protection against reuse, while they are specifically designed to be extensible enough to account for any credential claims. The scalability and easy incorporation of the solution to existing platforms is also supported by the wide interoperability of the W3C standard.

C. Enhanced FIDO2

One of the challenges the DIPA solution is facing is the establishment of a cryptographically secure communications with the solution server that would allow the data to be sent with the biometric consent of the user. The selected solution to this challenge is the utilization of an enhanced FIDO2 based authentication. Specifically, the FIDO2 protocol is configured to utilize the extensions mechanism from WebAuthN [15]. The utilization of FIDO2/WebAuthN extensions allows the cryptographically signed data to be conveyed between application and server. Therefore, the data to and from the mobile device will be encapsulated within signed packets of binary objects. The signature will be generated via biometric authentication and will be verified by the server.

In parallel, the compliance to the standards facilitates an extensible architecture which can be easily enhanced with new verification methods and additional data elements. Finally, the extended FIDO2 creates a secure tunnel between mobile application and the authentication server with perfect forward secrecy.

D. FHIR Interface

Instead of requesting from laboratories to integrate OIDC servers to provide users with the ability to allow authorization for third party applications to access their test results, the Health Level Seven International (HL7) standards body [16] has already proposed a standard which leverages OIDC/OAuth2 as an option for Web authentication, named Fast Healthcare Interoperability Resources (FHIR) [13]. The FHIR is a standard which describes data formats and elements, including an API for exchanging EHRs.

The implementation of FHIR within the proposed architecture offers an easier way to integrate mobile applications, such as the Digital Immunity Passport. Additionally, FHIR is ready for use and comes with out-of-the-box interoperability, thereby, reducing the Capital expenditures (CAPEX) and Operating expenses (OPEX). The supported user control over their data in FHIR forms the basis for the establishment of the user consent to share and self-report as envisioned in the DIPA solution. User consent is explicitly obtained when they request results from the vaccination centers or test labs. This consent is given online and is captured in digital format with all the context available to the DIPA system (i.e., geolocation of the mobile device, device data and time of day, etc.). The standard common target data format of the provided API ensures data integrity,

accuracy, and consistency for a wide range of national health organizations data hubs, while it supports machine learning and artificial intelligent techniques for better data mining from these organizations.

E. *Workflow engine*

The workflow engine, incorporated into the design of the DIPA's technology framework, allows the integration of the implemented microservices into a scalable and distributed workflow engine. In parallel, it provides detailed visibility into how a workflow is performing so that it can identify potential problems. In addition, the workflow engine supports the orchestration of microservices to fulfill a defined workflow and ensures that all workflow instances are completed according to plan. Within this concept, it also allows the easy addition, update, and deletion of elements of a workflow, based on changes to user registration, FHIR data acquisition and verification flows. At the same time, it is capable to handle complex multi-stage registration and data acquisition workflows in scale with resilience and high performance.

V. Main Components and Functionalities

The main architectural components and functionalities are illustrated in Figure 3. In detail, the mobile application is responsible first, for providing the user interface for the collection of the identity data. Secondly, for secure (encrypted) storage, the user's identity information as a verifiable credential and displaying the user, attributes whenever prompted. Moreover, it facilitates the communication with the FHIR hub to provide user access to the Electronic Medical or Health Records (EMR/EHR) portal, through the OAuth2/OIDC protocol, as well as, transporting the vaccination status or test results. The application is also charged with storing (encrypted) and displaying the test and the immunity status as verifiable credential.

The workflow server is offering web services to the mobile application. The role of this server is the provisioning of identity and biometric registration services using FIDO2/WebAuthN protocol and the facilitation of encrypted and signed transactions to/from the mobile device. The server is also providing various adapters for service operations, such as identity proofing and acquisition of vaccination status and test results. It handles the communications with the FHIR hub to register users as HL7 patient resource, while it provides observation interfaces that filter and log user and test result data, anonymously, on behalf of various National Health Organizations (NHO - e.g., NIH).

An identity management server is empowered with responsibilities associated with the processing and communication of the user's identity data. Specifically, this server receives image captures, optical character recognition (OCR) data and barcode readouts of identity documents and user selfie images from mobile application. Upon the reception of these data, it is extracting faces from the identity document and user selfies, submitting them to a face matching server. Furthermore, the server is used for capturing data such as name, date of birth and address from the ID document and deriving new identity data including city, state, age, etc. Finally, it is responsible for verifying ID documents with external authorities, creating identity verified credentials and inserting verification signatures into the distributed ledger. It is worth mentioning that no personal data is stored on any of the solution servers and after processing all sensitive data are discarded.

A token server is utilized to store and manage user tokens and keys. It is in control of storing push tokens for notification delivery to the mobile application and the public key management for the verification of the credential holder signatures from the mobile application. In addition, the token server is managing the symmetric keys for the QR code generation and verification.

The proposed architecture also incorporates an auditing server for providing high capacity and reliable indexed log storage services. The server is responsible for intaking audit trails for user registration and test results acquisition. It can retrieve data with text search and support raw and aggregated data visualization, while generating reports for data uploads to available data repositories of the various NHOs.

A verification service is designed for generating and validating verifiable credentials for users, test results and immutability statuses. Moreover, it is interfacing with the blockchain to create and verify transaction proofs. To offer a centralized service level configuration of all applications in the architecture, as well as a security module for storing and retrieving secrets (i.e., passwords, certificates, encryption keys, PKI, etc.) a specific component is defined in the architecture, namely the Service Mesh Management. It constitutes a set of infrastructure level services that provide core application and secrets management. It is designed to provide a policy engine for managing test results rationalization and access control.

Finally, the FHIR hub is envisioned as an external service, which interfaces with various EMR/EHR and proxies the HL7 interfaces to these entities. A wide section of EMR/EHR is compliant to the new HL7/FHIR standard, but this is not universal. As such, the component acts towards homogenizing the interface to EMR/EHR into a consistent set of REST APIs. In addition. it provides the required rationalization of HL7 observation resources into a consistent FHIR compliant JSON structure, while it can handle any security and compliance issues related to patient data acquisition.

As a result, the described architectural components constitute a holistic approach for allowing users to prove the status of their testing with respect to COVID-19, to provide 3rd party verifiers (individuals, enterprises, relevant authorities, etc.) with non-repudiated proof of current virus infection, presence of antibodies, vaccination records, and any other condition necessary to return to work, travel or socialize.

VI. Use case

A. *Onboarding and Authentication*

As a first step, the user downloads and installs the mobile application associated with the proposed solution. Upon the completion of these two actions, the user is called to enable the device-based biometrics and is guided through an identity vetting process, which validates the identity of the user and cryptographically binds it to the device. DIPA guarantees that no PII data is stored on a server (privacy-preserving).

During this phase, DIPA registers user biometrics (PIN, fingerprint, face) on the phone using FIDO2. It then, requests

the user to take a camera capture of the front and back of their government ID card. The user is then, requested to take a selfie of their face with liveness detection built in. The system verifies that the picture on the ID matches the selfie. All data from this process is conveyed to the backend where additional databases may be consulted for verification based on the ID type.

The result of this procedure is that a user identity verifiable credential is created. This is represented by a W3C Verifiable Credential with the associated decentralized identifier (DID) stored at a distributed ledger. This credential is portable and verifiable by any system that supports the appropriate standards. The credential is securely stored on the mobile. The user may also be asked to enter additional information such as email address. This information will be verified in the standard manner.

B. Digital immunity test and vaccination certificate

Although the procedure of obtaining a vaccination or COVID-19 test certificate may slightly differ per country, the user eventually is required to create an account at the specific EMR/EHR online portal, or similar systems provided by the various jurisdictions.

Using the mobile application, the user logs in to the EHR portal using a commercially available FHIR aggregation service. During this procedure, the login credentials are not exposed or stored neither in the mobile application, nor in the cloud-based servers. The FHIR hub provides an access token that is stored in the user's mobile phone secure storage. The mobile application will then call on the health system via the FHIR hub using FHIR protocols to retrieve the user's test results (i.e., observations). In this case, the access token is presented as a proof of authorization. The transaction is cryptographically signed and stored in an immutable audit trail using blockchain technology (i.e., immutable ledger). The proposed solution ensures that only the proof of status is stored on the distributed ledger – not the actual results data. The results, which constitute the actual data, are securely stored on the user's phone, and sent to the log database in anonymized format.

C. Person-to-person fast presentation and verification of certificates

The advantage of the existence of the mobile application is that it can hold the verifiable credentials (i.e., government ID, passenger location form, COVID-19 test, etc.) and utilize them in multiple ways depending on the use case. The solution support smartphone to smartphone verification without the need for specialized hardware. Upon entering the user biometrics, the application will cryptographically generate a QR code. Third party verifiers will be able to scan the QR code, which verifies in a tamper evident manner the user's test results on the immutable ledger.

Depending on the use case, DIPA supports different verification modalities with biometric authentication, verifiable credentials generation, cryptographic signature verification, and DL attestation. Moreover, to allow for seamless scalability and integration with an amalgam of communication modes and channels, DIPA supports dynamic and static QR code scan, NFC, Bluetooth, WiFi and mobile pass.

VII. Platform's Added Value

The proposed Digital Immunity Passport provides a formal, provable, trust framework and ecosystem with integrated mobile applications, quick plug-in SDKs and componentized software microservices. These characteristics render this technology solution capable of rapid integration in operational healthcare facilities and COVID-19 testing services for issuing digitally signed credentials about a patient's COVID-19 status directly to their smartphones. With a quick biometric fingerprint or face scan, individuals can prove that they are currently virus-free or have been vaccinated. True to the spirit of verifiable credentials, this certificate does not contain personally identifiable information, hence, privacy and confidentiality can always be preserved while still providing strong cryptographic proof that the credential belongs to the specific individual. The proposed DIPA technology framework achieves:

- Peer to Peer tamper-evident COVID-19 test status and vaccination record verification.
- Privacy preserving, with credentials (government ID, test results, vaccination records) securely (encrypted) stored in the user's smartphone and only anonymized data for general purpose queries be allowed.
- Anonymous Verification by proving test results or vaccination status without shared ID information.
- Remote Onboarding with real-time ID verification by generating decentralized ID with Digital ID credentials stored on the smartphone.
- Biometric strong authentication with device biometrics.
- Extensible digital proofing framework based on the smartphone's secure credentials wallet.
- Future Proof Solution leveraging Industry open standards.

From the national healthcare organization's point of view, the DIPA solution presents the means for a secure drop-in solution deployable on-premises or in a private cloud as a SaaS. The numerous benefits that national health organizations, governments and others are gaining by incorporating the DIPA solution, include:

- Mapping the identity of the user to vaccination records and test results with an immutable digital certificate.
- Eliminating the uncertainty, fraud, repudiation, collusion, and impersonation by other individuals.
- Provision of security and frictionless experience easily adopted by users.
- Seamless integration into current workflows by test providers, laboratories, and enterprise systems.
- Compliance with privacy and consent collection hence, fostering user's trust in a seamless user experience.
- The implementation of mobile biometric and state-of-the-art open-source standards, which provides a modern and future-proof approach for test verification, scalable to new use cases.
- Digitally signed attestations with immutable audit logs, which provides compliance, accountability, and non-repudiation.

VIII. Conclusion

As the world is experiencing the effects of the COVID-19 pandemic which affects almost every aspect of life (emotional, physical, financial, social), the debate about the introduction of an immunity passport that will allow a quicker return to a more familiar everyday life is heating up. Although privacy and ethical issues have been raised regarding the digital immunity passports, the existence of a digital certification for proof of COVID-19 status (i.e., testing, recovery, vaccination) may be necessary. The paper presents and discusses a framework solution for a scalable and commercially viable verifiable certificate augmented with non-repudiation and integrity. The proposed Digital Immunity Passport complies with the emerging worldwide regulations on privacy, trust, and accountability. It incorporates well studied and widely adopted by the industry standards (OAuth2/OIDC, FIDO2/WebAuthN, VC, FHIR/HL7, etc.) to empower national health care organizations and governments worldwide with the most robust technology for a next generation ubiquitous digital proofing solution, having a seamless access control and intuitive transactional verification.

References

[1] https://extranet.who.int/pqweb/sites/default/files/documents/Status_COVID_VAX_16Feb2021.pdf . Accessed on 01 March 2021.

[2] Brown, Rebecca CH, Dominic Kelly, Dominic Wilkinson, and Julian Savulescu. "The scientific and ethical feasibility of immunity passports." The Lancet Infectious Diseases (2020).

[3] World Health Organization. "COVID 19 Public Health Emergency of International Concern (PHEIC). Global research and innovation forum: towards a research roadmap." (2020).

[4] Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." A Practical Guide, 1st Ed., Cham: Springer International Publishing 10 (2017): 3152676.

[5] Annas, George J. "HIPAA regulations-a new era of medical-record privacy?." New England Journal of Medicine 348, no. 15 (2003): 1486-1490.

[6] Davahli, M.R.; Karwowski, W.; Sonmez, S.; Apostolopoulos, Y. The Hospitality Industry in the Face of the COVID-19 Pandemic: Current Topics and Research Methods. Int. J. Environ. Res. Public Health 2020, 17, 7366.

[7] Natalie Kofler, Françoise Baylis, “Ten reasons why immunity passports are a bad idea,” Nature 581, 379-381 (2020)

[8] Nagasubramanian, Gayathri, Rakesh Kumar Sakthivel, Rizwan Patan, Amir H. Gandomi, Muthuramalingam Sankayya, and Balamurugan Balusamy. "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud." Neural Computing and Applications 32, no. 3 (2020): 639-647.

[9] D. Hardt, "The oauth 2.0 authorization framework", IETF2012, 2012.

[10] Sakimura, Natsuhiko, John Bradley, Mike Jones, Breno De Medeiros, and Chuck Mortimore. "Openid connect core 1.0." The OpenID Foundation (2014): S3.

[11] Dierks, Tim, and Eric Rescorla. "The transport layer security (TLS) protocol version 1.2." (2008): 5246.

[12] FIDO-specs (2020). Fido specifications overview. https://fidoalliance.org/specifications.

[13] FHIR Overview, in: FHIR Release 4 (Technical Correction #1) (v4.0.1). Accessed October 12, 2020. http://www.hl7.org/fhir/overview.html.

[14] Manu Sporny et al., "Verifiable Credentials Data Model 1.0", W3C Rec, Nov 2019, [online] Available: https://www.w3.org/TR/vc-data-model/.

[15] Dirk Balfanz, et. al.,“Web Authentication: An API for accessing Public Key Credentials Level 1”, W3C Recommendation, 4 March 2019

[16] Health Level Seven International – Homepage | HL7 International. Accessed October 12, 2020. https://www.hl7.org/.

ROBERT KOCH INSTITUT

Häufig gestellte Fragen

- Die aktuell häufigsten Fragen
- Allgemeine Fragen
- Fragen zur CovPass-App
- Fragen zur CovPassCheck-App
- Fragen zum Impfzertifikatsservice
- Fragen zu den technischen Details

Bei allen Fragen rund um den Impfnachweis wenden Sie sich gern telefonisch oder per E-Mail an uns:

Für die CovPass-App:

0800-4747-001

support@covpass-app.de

ROBERT KOCH INSTITUT

support@covpasscheck-app.de

Für Zertifikatsaussteller:

0800-4747-003

aussteller-support@covpass-app.de

Für sonstige Anfragen:

info@covpass-app.de

Die aktuell häufigsten Fragen

Ist mein Zertifikat gültig für die Einreise in ein EU-Land?

Ich war an COVID-19 erkrankt und bin genesen. Wie kann ich einen vollständigen Immunschutz nachweisen?

Warum lässt sich mein QR-Code nicht einscannen?

In welchen App Stores ist die CovPass-App erhältlich?

Ab wann gilt der vollständige Impfschutz?

ROBERT KOCH INSTITUT

obwohl mehr als zwei Wochen nach der letzten Impfung vergangen sind. Was kann ich tun?

Gibt es die App auch auf Englisch?

Wie kann ich den QR-Code scannen, wenn meine Smartphone-Kamera kaputt ist oder eine schlechte Auflösung hat?

Allgemeine Fragen

Was ist der digitale Impfnachweis?

Wie funktioniert der digitale Impfnachweis?

Warum machen wir das?

Wie erhalte ich die digitalen COVID-Zertifikate der EU?

ROBERT KOCH INSTITUT

Wie lange ist das digitale COVID-Zertifikat der EU gültig?

Ist der gelbe Impfpass weiterhin gültig?

Ja. Der gelbe Impfpass der Weltgesundheitsorganisation WHO ist ein international anerkanntes Dokument, das Sie weiterhin benutzen können, um Ihre Impfungen zu belegen.

Der digitale Impfnachweis in der CovPass-App ist lediglich ein freiwilliges und ergänzendes Angebot.

Sie können Ihre Corona-Impfungen alternativ auch mit dem ausgedruckten digitalen COVID-Zertifikat der EU oder mit einer Impfbescheinigung vom Impfzentrum bzw. der impfenden Stelle nachweisen.

Muss ich in der Apotheke für das Impfzertifikat bezahlen?

Kann auch nach einmaliger Impfung mit dem Impfstoff von Johnson & Johnson ein Zertifikat erstellt werden?

Nein, es ist keine zentrale Speicherung geplant. Die Speicherung erfolgt freiwillig auf dem Smartphone. Jeder kann so selbst entscheiden, ob und wann er diese Daten löscht.

Durch wen wird die Gesamtlösung angeboten?

Der digitale Impfnachweis ist ein Projekt im Auftrag des Bundesministeriums für Gesundheit. Die Anwendung wurde von den Unternehmen UBIRCH, IBM Deutschland, govdigital und Bechtle entwickelt. Das Robert Koch-Institut ist als Herausgeber verantwortlich für die Ausgestaltung der Anwendung sowie für die sorgfältige Prüfung der Anforderungen an Datenschutz und Datensicherheit.

ROBERT KOCH INSTITUT

ausgeschrieben?

Eine gemeinsame EU-Ausschreibung hätte zu viel Zeit benötigt und wäre aufgrund der unterschiedlichen Impfinformationssysteme in den Mitgliedstaaten auch schwierig umzusetzen gewesen. Beim EU-Ansatz geht es um die Regelung eines Anerkennungsrahmens. Etwaige

Fragen zur CovPass-App

Warum brauche ich die CovPass-App?

Impfnachweises in Deutschland werden die EU-Vorgaben von vornherein

Wie funktioniert die CovPass-App?

Bin ich verpflichtet, die CovPass-App zu nutzen?

Wo kann ich die CovPass-App herunterladen?

Mit welchen Smartphones kann man die CovPass-App nutzen?

Welchen QR-Code kann ich mit der CovPass-App einscannen?

Kann ich Zertifikate auch für mehrere Personen in der App speichern?

ROBERT KOCH INSTITUT

Impfschutz erst nach zwei Wochen gültig?

Welche personenbezogenen Daten werden in der CovPass-App gespeichert?

Wo werden meine Daten gespeichert?

Welche Daten sind im QR-Code hinterlegt?

Wie wird ein Missbrauch meiner Daten verhindert?

Werden meine Daten beim Löschen der CovPass-App entfernt?

Kann ich den QR-Code auch ohne Internetverbindung vorzeigen?

Welche Daten werden bei der Überprüfung des QR-Codes angezeigt?

Wieso sehe ich im Startbildschirm der CovPass-App nur einen QR-Code, obwohl ich mehrere Zertifikate von mir gespeichert habe?

ROBERT KOCH INSTITUT

Was mache ich, wenn ich mein Smartphone verloren habe?

Was ist mit Personen, die kein Smartphone besitzen?

Muss ich die Ausdrucke der digitalen COVID-Zertifikate der EU aufheben?

Kann ich mein Zertifikat als PDF herunterladen?

Fragen zur CovPassCheck-App

Wann brauche ich die CovPassCheck-App?

Was macht die CovPassCheck-App?

Wie funktioniert die CovPassCheck-App?

ROBERT KOCH INSTITUT

Wo kann ich die CovPassCheck-App herunterladen?

Welche Voraussetzungen benötige ich für die CovPassCheck-App?

Durch wen wird die Lösung angeboten?

Kann ich den Corona-Impfstatus auch ohne Internetverbindung prüfen?

Wie barrierefrei ist die CovPassCheck-App?

Fragen zum Impfzertifikatsservice

Wie stelle ich als Ärztin oder Arzt ein Genesenenzertifikat aus?

Wie bekommen Arztpraxen und Apotheken die Zugangsdaten für den Zertifikatsservice?

ROBERT KOCH INSTITUT

Können wir Materialien von der Webseite verwenden?

Wie kann man als Aussteller sicher sein, dass der Impfpass ein echtes Dokument ist?

Wie können Ärzte den Komfort-Client nutzen?

Wie installiere und nutze ich den Impfzertifikatsservice?

Welche Daten muss ich im Impfzertifikatsservice erfassen?

Wie kann ich als Betriebsärztin oder Betriebsarzt den Impfzertifikatsservice nutzen?

Fragen zu den technischen Details

ROBERT KOCH INSTITUT

Für die Erstellung des digitalen COVID-Zertifikats der EU sowie des digitalen Impfnachweises werden keine Daten zentral gespeichert.

Welche Daten werden erhoben und verarbeitet?

Für die Erstellung des digitalen COVID Zertifikats der EU werden in den Impfzentren, Arztpraxen und Apotheken die minimal notwendigen Daten, wie Vorname(n), Nachname, Geburtsdatum, Impfstoff, Impfdatum und Impfdosis erfasst und kodiert. Weitere Informationen wie Krankheitserreger, Produkt, Hersteller, Land, Gesamtanzahl der Impfungen und Aussteller des technischen Zertifikats werden vom Impfzertifikatsservice automatisch ergänzt.

Wie ist die Struktur des QR-Codes definiert?

Der QR-Code ist ein CBOR Web Token, welches das Zertifikat mit den persönlichen Informationen, wie Name und Geburtsdatum, sowie die Impfinformationen enthält. Die genaue Struktur ist durch eine Richtlinie der eHealth Gruppe der EU definiert.

Die Daten werden in einem besonders gesicherten System von UBIRCH im Auftrag des Robert Koch-Instituts digital signiert. Zugriff darauf haben nur autorisierte Personen und Erfassungssysteme. Es werden keine personenbezogenen Daten bei UBIRCH gespeichert.

Warum wird ein Open-Source-Ansatz verfolgt?

Wir sind der Auffassung, dass der Erfolg der Lösung unmittelbar von der Akzeptanz und dem Vertrauen der nutzenden Personen abhängt.

Durch den gewählten Open-Source-Ansatz sind der vollständige Quelltext für die Apps und die Infrastruktur frei und ohne Zugangsbeschränkungen verfügbar. So möchten wir die für eine starke Vertrauensbasis notwendige Transparenz schaffen. Der Open-Source-Ansatz ermöglicht der Öffentlichkeit und der Entwicklungs-Community außerdem, aktiv zu dem Erfolg der Lösung beizutragen, zum Beispiel in Form von Reviews und Pull Requests.

ROBERT KOCH INSTITUT

keine Gefahr für die Cybersecurity?

Die Open-Source-Community erhöht die Sicherheit der Software, da der

Digitaler Impfnachweis

Services

CovPass-App

CovPassCheck-App

Impfzertifikatsservice

Hilfe

Häufige Fragen

Technische Details

Kontakt

Materialien zum Download

Rechtliches

Impressum

Datenschutzerklärung

Erklärung zur digitalen Barrierefreiheit

Sprache

Deutsch

English

Co-funded by
the European Union

ROBERT KOCH INSTITUT

Die CovPass-App

COVID-Zertifikate der EU digital nachweisen

Verwalten Sie Ihre digitalen COVID-Zertifikate der EU ganz einfach mit dem Smartphone.

Laden im App Store | JETZT BEI Google Play | ENTDECKEN BEI HUAWEI AppGallery

Kompatibel ab iOS Version 12 und Android Version 6

ROBERT KOCH INSTITUT

So funktioniert die CovPass-App

1

Lassen Sie sich ein digitales COVID-Zertifikat der EU ausstellen

Impfzertifikate erhalten Sie in Impfzentren, Apotheken, Arztpraxen und Gesundheitsämtern. Genesenenzertifikate werden von Arztpraxen, Apotheken und Gesundheitsämtern ausgegeben.

ROBERT KOCH INSTITUT

2

Scannen Sie den QR-Code

Sie können sowohl Impfzertifikate als auch Genesenenzertifikate in der App speichern und bei Bedarf als PDF-Dokument herunterladen und ausdrucken.

3

Lassen Sie den QR-Code beispielswesie beim Einlass zu Veranstaltungen, in Hotels oder Restaurants scannen

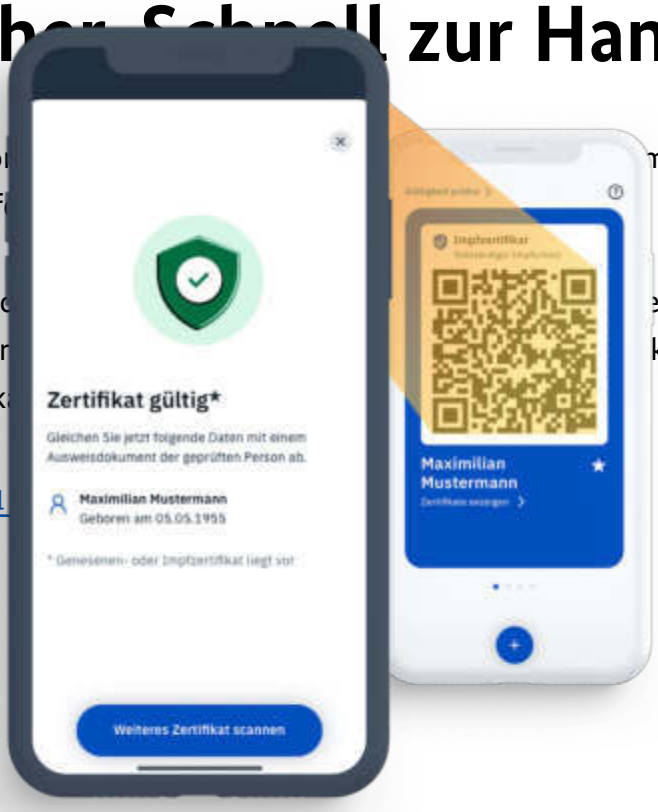
Halten Sie zudem ein Ausweisdokument bereit. Die prüfende Person wird mit der CovPassCheck-App Ihren Nachweis prüfen.

ROBERT KOCH INSTITUT

Einfach. Sicher. Schnell zur Hand.

Mit Hilfe der CovPass-App kö mpfung wie auch eine Genesung von der Corona-Inf

Bitte beachten Sie, dass die Co en kann, die den europäischen Vorgaben entspr kat an der Überschrift „Digitales COVID-Impfzertifik

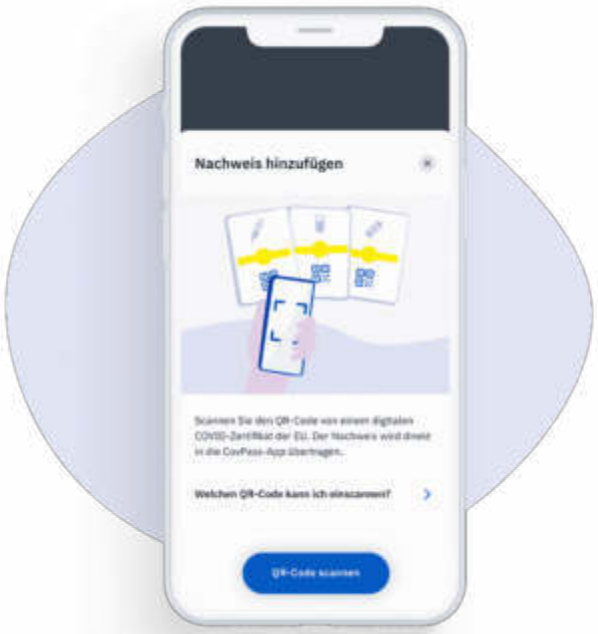


[Alle Informationen zu]

Kompatibel ab iOS Version 12 und Android Version 6

ROBERT KOCH INSTITUT

Die CovPass-App im Detail



1 Fügen Sie ein digitales COVID-Zertifikat der EU in der App hinzu

Laden Sie die CovPass-App auf Ihr Smartphone und öffnen Sie die App. Drücken Sie auf das blaue Plus-Symbol und scannen Sie den QR-Code Ihres Zertifikats. Das Zertifikat wird zusammen mit dem QR-Code auf das Smartphone geladen und auf der Startseite der App angezeigt.

Sofern das Zertifikat in der CovPass-App hinterlegt ist, können Sie es jederzeit

ROBERT KOCH INSTITUT

Verwalten Sie mehrere Zertifikate an einem Ort

2

In der CovPass-App können Sie bei Bedarf mehrere Impf- und Genesenenzertifikate verwalten: Für sich und für andere Personen, wie zum Beispiel Familienangehörige.

Erfahren Sie, ab wann der QR-Code für den vollständigen Impfschutz gilt

ROBERT KOCH INSTITUT

Überprüfen Sie bei Auslandsreisen die Gültigkeit des Zertifikats

Sollten Sie eine Reise planen, können Sie in der CovPass-App unverbindlich vorab prüfen, ob Ihr Zertifikat in dem entsprechenden Land gültig ist. Dafür werden die geltenden Einreiseregeln des gewählten Reiselands berücksichtigt.

3

Die Einreiseregeln können sich jederzeit ändern. Informieren Sie sich zur Sicherheit immer auch auf der Seite Re-open EU. Dort finden Sie die aktuellsten Regelungen. Sie finden Ihr Reiseland nicht? In einem mehrstufigen Prozess werden nach und nach mehr Länder verfügbar gemacht.

Erfahren Sie mehr über die Einreiseregeln

ROBERT KOCH INSTITUT

Den QR-Code bei Bedarf vorzeigen

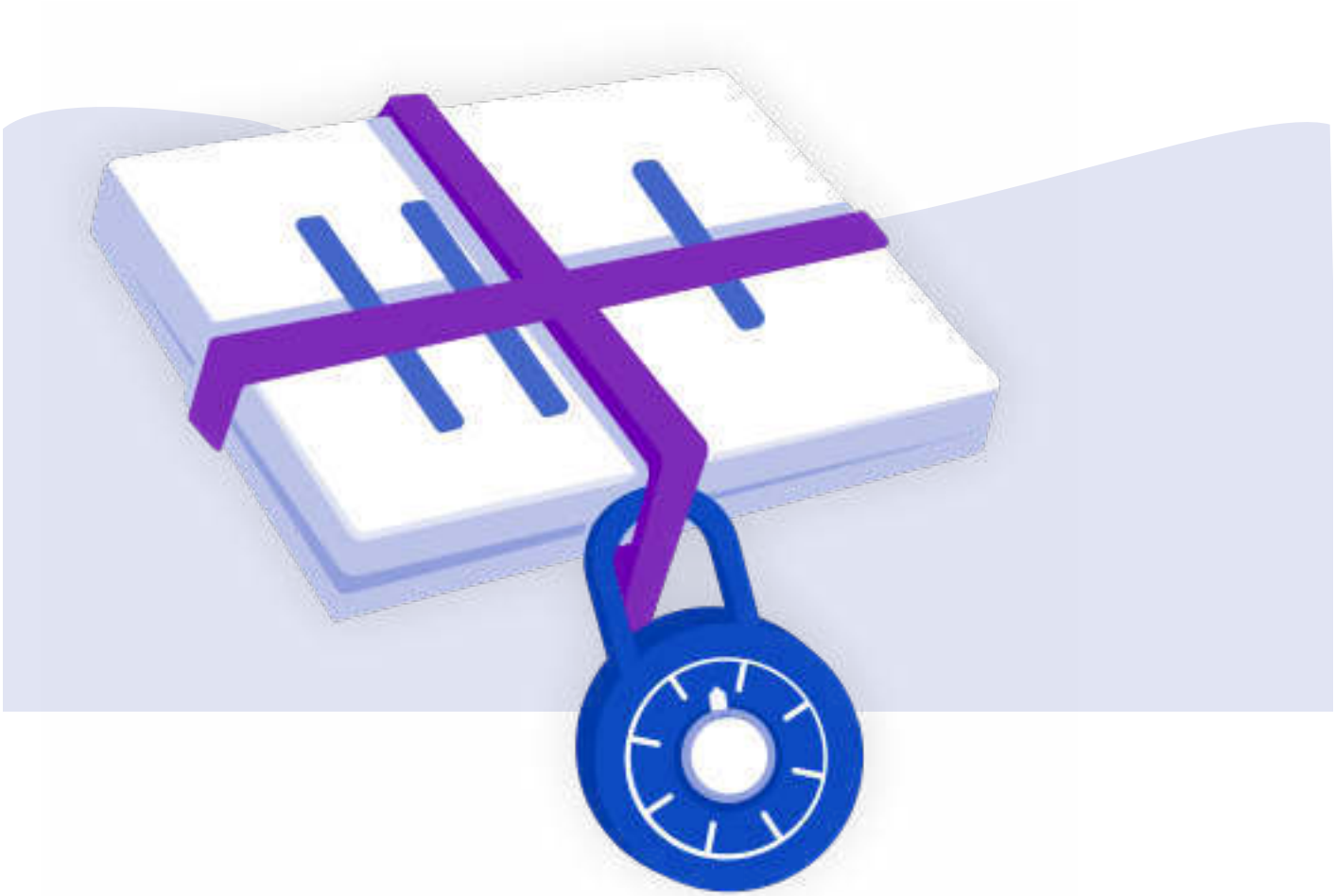
Lassen Sie den QR-Code in der CovPass-App von der prüfenden Person scannen. Bitte halten Sie ergänzend Ihr Ausweisdokument bzw. das Ausweisdokument der geimpften, getesteten oder genesenen Person bereit.

Für die Nutzung der CovPass-App ist keine bestehende Internetverbindung notwendig.

Erfahren Sie mehr über den Prüfvorgang

Jetzt die kostenlose App herunterladen

ROBERT KOCH INSTITUT



Ihre Daten bleiben Ihre Daten

Nur Sie entscheiden, wann und wem Sie den digitalen Impfnachweis vorzeigen möchten.

Lokale Datenspeicherung

Ihre vollständigen Impfdaten sind nur auf Ihrem Smartphone gespeichert.

ROBERT KOCH INSTITUT

Die Daten im QR-Code sind mit einer Signatur abgesichert, die Fälschungen verhindert.

Mehr erfahren

Ein Nachweis, zwei Möglichkeiten

Zeigen Sie Ihr Impfzertifikat ganz einfach mit der CovPass-App oder mit der Corona-Warn-App vor.

ROBERT KOCH INSTITUT

Haben Sie noch Fragen?

Wie erhalte ich die digitalen COVID-Zertifikate der EU?

Warum brauche ich die CovPass-App?

Bin ich verpflichtet, die CovPass-App zu nutzen?

Welchen QR-Code kann ich mit der CovPass-App einscannen?

Wo werden meine Daten gespeichert?

Zu den häufigen Fragen →

ROBERT KOCH INSTITUT

Digitaler Impfnachweis

Services

CovPass-App

CovPassCheck-App

Impfzertifikatsservice

Hilfe

Häufige Fragen

Technische Details

Kontakt

Materialien zum Download

Rechtliches

Impressum

Datenschutzerklärung

Erklärung zur digitalen Barrierefreiheit

Sprache

Deutsch

English

Co-funded by
the European Union

INDIA NEWS

Data of millions on CoWIN portal safe, assures govt, denies reports of 'hacking'

Reports of CoWIN being hacked surfaced after a website called Data Leak Market said it was selling a database for Covid-19 vaccination in India.

By hindustantimes.com | Written by Shankhyaneel Sarkar | Edited by Avik Roy, Hindustan Times, New Delhi
PUBLISHED ON JUN 10, 2021 11:11 PM IST

(MietY) are currently investigating the matter.

"There have been some unfounded media reports of the CoWIN platform being hacked. Prima facie, these reports appear to be fake," the government said in a release.

Dr RS Sharma who heads the CoWIN portal and is also the chairman of the empowered group on vaccine administration also clarified that the reports of hacking of the CoWIN portal are false. "Our attention has been drawn towards the news circulating on social media about the alleged hacking of the CoWIN system. In this connection we wish to state that CoWIN stores all the vaccination data in a safe and secure digital environment," Sharma said.

"No CoWIN data is shared with any entity outside the CoWIN environment. The data being claimed as having been leaked, such as geo-location of beneficiaries, is not even collected at CoWIN," he further added.

Reports of CoWIN being hacked surfaced after a website called Data Leak Market said it was selling a database for Covid-19 vaccination in India. The website also said that the data of 150 million people also included their name, Aadhaar number, and location. They also clarified that they did not originally leak the data and were merely reselling the data.

Security of open source and closed source software: An empirical comparison of published vulnerabilities

ABSTRACT

Reviewing literature on open source and closed source security reveals that the discussion is often determined by biased attitudes toward one of these development styles. The discussion specifically lacks appropriate metrics, methodology and hard data. This paper contributes to solving this problem by analyzing and comparing published vulnerabilities of eight open source software and nine closed source software packages, all of which are widely deployed. Thereby, it provides an extensive empirical analysis of vulnerabilities in terms of mean time between vulnerability disclosures, the development of disclosure over time, and the severity of vulnerabilities, and allows for validating models provided in the literature. The investigation reveals that (a) the mean time between vulnerability disclosures was lower for open source software in half of the cases, while the other cases show no differences, (b) in contrast to literature assumption, 14 out of 17 software packages showed a significant linear or piecewise linear correlation between time and the number of published vulnerabilities, and (c) regarding the severity of vulnerabilities, no significant differences were found between open source and closed source.

Keywords

Vulnerabilities, security, open source software, closed source software, empirical comparison

INTRODUCTION

Over the last few decades we have got used to acquiring software by procuring licenses for a proprietary, or binary-only, immaterial "object". We have, then, come to regard software as a good we have to pay for just as we would pay for material objects, such as electronic devices, or food. However, in more recent years, this widely cultivated habit has begun to be accompanied by a new model, which is characterized by software that comes with a compilable source code (open source code). Often, such a source code is free of charge and may be modified and/or redistributed. The family of software of this kind is referred to as the umbrella term "open source software". When discussing this alleged innovation in software distribution, we are reminded by (Glass, 2004) that, essentially, free and open source software dates right back to the origins of the computing field, as far back in fact as the 1950s, when all software was free, and most of it open. (Schwarz and Takhteyev, 2008) provide detailed insights into the history and the evolvement of open source software.

The application fields of open source software are manifold. Internet programs, such as the mail transfer agent *Sendmail* and the operating system *Linux* are some of the most popular examples. In the business sector, open source software is nowadays part of the core infrastructure of sophisticated technology companies, such as Amazon, Google, and Yahoo (Schwarz and Takhteyev, 2008). Obviously, open source software has arrived in the world of important and critical software environments that need security protection against attacks. Its increasing availability and deployment makes it appealing for hackers and others who are interested in exploiting software vulnerabilities, which become even more dangerous when software is not applied in a closed context, but interconnected with other systems and the Internet (this argument is valid for closed source software as well).

While there is consensus that opening source code to the public increases the potential number of reviewers, its impact on finding security flaws is controversially debated. Proponents of open source software stress the strength of the resulting review process (Payne, 2002) and argue in the sense of (Raymond, 2001) that, *"Given enough eyeballs, bugs are shallow."* (p. 19), while some opponents follow the argument of (Levy, 2000), who remarks *"Sure, the source code is available. But is anyone reading it?"* Interestingly, both parties essentially agree that open source basically makes it easy to find vulnerabilities; they only differ in their conclusions with regard to the resulting impact on security. For a detailed discussion of the arguments, see (Schryen and Kadura, 2009).

In order to have an unbiased discussion on open source and closed source security, it is helpful, if not necessary, to transparently measure the empirical security of software – be it open source or closed source software (Wolfe, 2007). However, measuring security is a challenging task, because security is somehow invisible. Despite an increasing number of quantitative research papers on measuring software security in the past years, it is still true what (Witten, Landwehr and Caloyannidis, 2001) observed: what the discussion on software security specifically lacks is appropriate metrics, methodology and hard data.

Addressing this research gap, this paper analyzes and compares published vulnerabilities of eight open source software and nine closed source software packages, all of which are widely deployed. More specifically, this empirical study statistically analyses vulnerabilities in terms of the mean time between vulnerability disclosures, the development of disclosure over time, and the severity of vulnerabilities. This paper thereby allows for validating models provided in the literature.

The rest of this paper is structured as follows: The next section presents the basic background on open and closed source software and work related to software vulnerabilities. Section 3 provides the methodology of this empirical study. The used data are described in Section 4. Section 5 presents the empirical findings, before Section 6 provides conclusions.

BACKGROUND AND RELATED WORK

Open and closed source software

Generally, the availability of source code to the public is a precondition for software being denoted as "open source software". Beyond this requirement, the Open Source Initiative (OSI) has defined a set of criteria that software has to comply with (OSI, 2006). The definition particularly includes permission to modify the code and to redistribute it. However, it does not govern the software development process in terms of who is eligible to modify the original version. When what is called "bazaar style" by (Raymond, 2001) is in place, any volunteer can provide source code submissions. Software development is then often based on informal communication between the coders (Gonzalez-Barahona, 2000). In a more closed environment, software is crafted by individual wizards and the development process is characterized by a relatively strong control on design and implementation. This style is referred to as "cathedral style" (Raymond, 2001). The implementation of this modification procedure might have an impact on the security of software, so that a detailed discussion of open source security would need to consider it.

A plethora of OSD-compliant licenses have come into operation, such as the *Apache License*, *BSD license*, and *GNU General Public License (GPL)*, which is maintained by the Free Software Foundation (FSF). The FSF provides a definition of " *'free software' [as] a matter of liberty, not price.*" (FSF, 2007). In contrast to the OSD definition, the FSF definition explicitly focuses on the option of releasing the improvements to the public (freedom 3), thereby rejecting a strong supervision of the modification process. Software is usually regarded as being "closed", if the source code is not available to the public.

Vulnerabilities

When software is executed in a way different from what the original software designers intended, this misbehaviour is rooted in software bugs. (Anderson, 2001) assumes the ratio of bugs and software lines of code (SLOC) to be about 1:35, i.e. Windows 2000 with its 35 Mio. SLOC would then have included one million bugs. The portion of bugs that are security-critical ("vulnerabilities") is assumed to be 1% (Anderson, 2001), resulting to an amazingly high figure of 350,000 vulnerabilities in Windows 2000. Detected vulnerabilities can further be divided into those being published and unpublished. An overview of the classification of bugs provides

Figure 1, which also shows that in this work only published vulnerabilities are considered.

Vulnerabilities are (software) product-related weaknesses, for which publicly accessible databases are available. Rooted in these are concrete security incidents (breaches), which are system-related and cause the actual harm. Breaches are much more difficult to investigate, because data is scarcer. For a detailed discussion of breaches, see (Jonsson, Strömberg and Lindskog, 2000; Kimura, 2006).

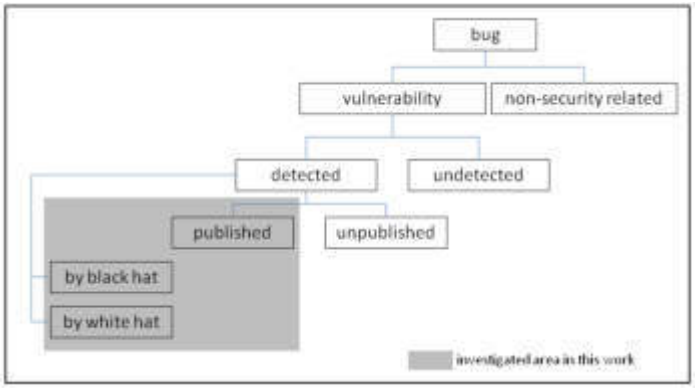


Figure 1. Classification of software bugs and vulnerabilities

(Alhazmi, Malaiya and Ray, 2005; Alhazmi, Malaiya and Ray, 2007) assume that the development of vulnerability discovery can be split up into three different phases. In phase 1, software testers gather sufficient knowledge of the system to break into it successfully. In phase 2, discovering vulnerabilities will be most rewarding for both white hat and black hat finders. Finally, in phase 3, vulnerability detection effort will then start shifting to the succeeding version of the software. These phases form an "S" shape that is assumed to follow the principle that the vulnerability discovery rate is linear in both the momentum gained by the market acceptance of the product and in the saturation due to a finite number of vulnerabilities. The

model also implies that the total number of vulnerabilities that would eventually be found is limited. (Rescorla, 2004) adopts the probabilistic G-O model (Goel and Okumoto, 1979), but finds no significant empirical evidence for its appropriateness. A model that relates the number of vulnerabilities to the total effort spent on detecting vulnerabilities is proposed by (Alhazmi and Malaiya, 1995).

Once a vulnerability is detected, the question arises whether to disclose it or not. (Rescorla, 2004) argues against disclosure unless vulnerabilities are correlated. However, investigating the operating system *FreeBSD* (Ozment, 2005) finds vulnerabilities being correlated regarding its' rediscovery and argues in favour of disclosure. Using game-theoretic models, (Nizovtsev and Thursby, 2007; Arora, Krishnan, Nandkumar, Telang and Yang, 2004; Arora, Telang and Xu, 2004) address the question of when software vulnerabilities should be disclosed and conclude that neither instant disclosure nor non-disclosure is optimal.

In a theoretical paper, (Anderson, 2005) draws on software reliability models and statistical thermodynamics and conclude that, under ideal conditions, open and closed systems are equally secure.

METHODOLOGY

Software Packages and Data Sources

The selection of software packages to get investigated is driven by the goals to

- have open and closed source software systems that serve the same purpose (for the sake of comparability),
- include both open source software developed in cathedral style and in bazaar style
- have a sufficiently large set of vulnerability data available,
- consider software that is known and relevant to the community, and
- cover a broad range of services provided by the overall set of software packages.

Following these guidelines, I chose to include the software listed in

Table 3 (see Annex) and described in the data section. Overall, the software sample contains nine closed source software bundles and eight open source software bundles.

Each of the selected software bundles is analyzed regarding its vulnerabilities, as published in the National Vulnerability Database (NVD) of the National Institute of Standards and Technology (NIST). This database is one of the most comprehensive vulnerability databases. I analyze each software product regarding the number of vulnerabilities, the disclosure rate, the development of disclosure over time, and the severity of vulnerabilities. The statistical analysis focuses on the detection of differences between open source and closed source software.

Vulnerability Measurement

I define the "mean time between vulnerability disclosures" (MTBVD) as the *number of days since software release* divided by the *number of published vulnerabilities*. With regard to determining the MTBVD, I consider only those vulnerabilities that have been published after the release date.[1]

A simple comparison of MTBVD is not assumed to provide reliable results regarding the level of security, because vulnerability detection and publication are probably correlated with market and with software factors. For example, an important market factor is the attractiveness of the software for "vulnerability searchers", an important software factor is software size, as given by "software lines of code" (SLOC[2]). While SLOC values can be used at cardinal level, market share values are regarded at ordinal level (low, medium, high) in this paper for two reasons: (1) in some cases no precise values are available, (2) market share values change over time so that data on the continuous development of market shares would be

[1] Vulnerabilities that have been published earlier than the release date and that also affect the version under consideration are due to the development process of earlier versions.

[2] SLOC as a meaningful measure for software size is discussed controversially. One argument is that it does not distinguish code generated automatically from hand-written code, another one is that a single SLOC does not necessarily correspond to a single instruction in a high-level programming language. In this work, I ideally assume that no characteristic differences between open and closed source software exist in this regard.

needed for a reasonable consideration at cardinal level. Each of the application types is discussed separately with regard to its MTBVD, SLOC and market share.

DATA

Considered software

In the few empirical studies on software security (for example, see (Rescorla, 2004; Alhazmi et al. 2007)), the application types mainly considered are operating systems, web browsers, web servers, email clients, and database management systems. Adopting this focus, this study considers five operating systems (Windows 2000, Windows XP, MAC OSX, Red Hat Enterprise Linux 4, Debian 3.1), two web browsers (Internet Explorer 7, Firefox 2), two web servers (IIS 5, Apache 2), two email clients (MS Outlook Express 6, Thunderbird 2), four database management systems (mySQL 5, PostgreSQL 8, Oracle 10g, DB2 v3), and, in addition, two office products (MS Office 2003, OpenOffice 2). Details on these packages are provided in

Table **3** (see Annex).

Vulnerability sources

I consider those vulnerabilities that have been accepted as Common Vulnerabilities and Exposures (CVE) by MITRE (http://cve.mitre.org)[3]. Each of these vulnerabilities has a unique identifier, e.g. CVE-1999-0067. CVE identifiers are also used as references in many other vulnerability databases; for a list of such databases see (MITRE, 2009). Among these databases, the NIST NVD (http://nvd.nist.gov/) is one of the most comprehensive ones, which provides (xml) data feeds for each year; vulnerabilities prior to and including 2002 are stored in a single xml file. In contrast to the data feeds provided by MITRE (http://cve.mitre.org/cve/cve.html), the NVD feeds contain data on the severity and type of vulnerabilities. I do not consider any misconfigurations (CCE = Common Configuration Enumeration), because the NVD database is still being set up in this regard.

Overall, I consider two types of vulnerabilities: those that are explicitly applicable to the software version under consideration, and those that affect all versions of the particular software and that have been published after the release date of the considered version. The data used in this work refer to vulnerabilities that have been published prior to 01 February 2009.

Content of the NIST national vulnerability database (NVD)

Each vulnerability entry listed in the NIST xml files includes the following data (and even more that are not used here):

- **CVE identifier**, e.g. CVE-1999-0067
- **Affected software and versions**: The NVD applies the structured naming scheme CPE (Common Platform Enumeration) provided by MITRE (http://cpe.mitre.org/index.html). An example is “cpe:/o:redhat:enterprise_linux:3”.
- **(Base) Score**: The NVD provides vulnerability scores for almost all published vulnerabilities using the “Common Vulnerability Scoring System” (CVSS) 2.0 (FIRST, 2007; http://nvd.nist.gov/cvsseq2.htm.). The scores are between 0 and 10 (highest severity) and the particular value depends on several characteristics of the vulnerability, such as the level of authentication needed to exploit the vulnerability and the impact of a security breach on confidentiality and integrity.
- **Vulnerability references**: strings that provide references to sources with additional information on the vulnerability, such as links to available patches
- **Original release date**: This date refers to the particular NVD release day. In some cases, the corresponding CVE entry in the MITRE database contains another date, labeled as “assigned date”. I could not find any specific explanation of this date, nor for the differences between corresponding dates. Neither of these dates necessarily mirrors the point of time when the vulnerability was detected. However, as this paper aims at comparing data on open source and closed source software and I assume that no relevant statistical difference between the (detection, publication) time gaps of open source and closed source software vulnerabilities exist, I use the publication date as included in the comprehensive NVD data feeds.

[3] A good overview of enumerations, standards, and languages for software security provides the MITRE site (http://makingsecuritymeasurable.mitre.org/).

EMPIRICAL RESULTS

Development of vulnerabilities over time

As

Table **3** shows, for some of the closed source software packages I could not get reliable SLOC data. As data on market share are at ordinal level (see section on methodology), it is not possible to compute and (statistically) compare weighted MTBVD values. I therefore discuss each of the application types separately (see Table 1):

- **Browser**: Although *Internet Explorer 7* (IE 7) has had a much higher market share and its SLOC is presumably not lower than that of *Firefox 2*, the MTBVD of *IE7* is more than two times higher that of *Firefox 2*.
- **Email client**: Although I could not find any reliable data on the market shares of email clients, MS Outlook Express 6 has been probably much more deployed than *Thunderbird 1*. As in the case of browsers, no data on the SLOC of *MS Outlook Express* is available, but if we reasonably assume that *MS Outlook Express 6* has not considerably fewer SLOC, then the MTBVD of the closed source software is about eight times higher than that of the open source software. As this result seems surprising, I doublechecked the analyzed data.
- **Web server**: The market shares of the considered web servers are in the medium range, with *Apache 2* having been more widely deployed than *IIS 5*. Again, I have no information on the SLOC of *IIS 5*. The MTBVD values of both software bundles are quite close to each other.
- **Office**: In the case of office software, the open source software shows a MTBVD that is about three times higher than that of the closed source software. However, the market share of *MS Office 2003* is medium or even high, in contrast to that of *OpenOffice 2*. Overall, this result is not surprising.
- **Operating system**: The analysis of five operating systems surprisingly reveals that the widely deployed *Windows* operating systems have shown a MTBVD that is about two times higher than tose of the open source operating systems and *MAC OSX*. On the other hand, the SLOC of *MAC OSX* and *Debian 3.1* are higher than those of the Windows operating systems.
- **DBMS**: In the case of database management systems, none of the systems dominates the market. Overall, the results show a mixed picture.

Summing up the MTBVD results, in three of six application types, closed source software shows higher mean times, while in three cases no significant differences occur (if we also consider market shares and SLOC). However, this result might be biased and not representative, as in all but one case (databases) software of Microsoft is involved so that a company bias might be included. On the other hand, the software packages under consideration belong to the most deployed ones and cover a large part of worldwide installed software systems. The result does not mean that closed source software features less vulnerabilities or that less vulnerabilities have been detected, it only refers to vulnerabilities that have been published (see

Figure 1).

While the discussion above provides a static picture of the history of vulnerabilities, I now address the development of vulnerabilities over time (see Figure 2-Figure 7 in the Annex for a graphical representation). For ten out of 17 considered software packages, a significant linear correlation between time and the number of vulnerabilities is found. For each package, the shape of its curve is given in Table 1, with R^2 (adj.) denoting adjusted R^2 when applying ordinary least squares (OLS). Four other packages either show a piecewise linear correlation – which, presumably, indicates the occurrence of specific events – or a linear correlation, for which, however, statistical evidence is weak due to the small number of data points. Three packages show a development that in the beginning follows an S-shape, as suggested by (Alhazmi, Malaiya and Ray, 2005), but finally changes its characteristics with the second derivation becoming positive again. Therefore, the results do not support their model regarding the qualitative development of vulnerability detection.[4] The results also show that (Alhazmi, Malaiya and Ray, 2005) underestimate the number of vulnerabilities that will eventually be found in Windows XP (88) and Windows 2000 (163), because the NVD lists 297 and 385 published ones, respectively, by the end of January 2009.

[4] To be more precisely, (Alhazmi, Malaiya and Ray, 2005; Alhazmi, Malaiya and Ray, 2007) model the development of the number of detected vulnerabilities, while in this paper the number of published vulnerabilities is analyzed. On the other hand, (Alhazmi, Malaiya and Ray, 2007) use data on published vulnerabilities to show that their model fits.

Overall, there is no observable difference between open source and closed source software with regard to the (qualitative) development of vulnerabilities over time, and there is also no observable difference between open source software developed in bazaar and in cathedral style. The reason why three out of 17 packages show a different behaviour is not clear at this level of aggregation. An analysis of the particular types of vulnerabilities might reveal more facts.

Application type	**Product**	**#vuln**	**MTBVD [days]**	**Development of vulnerability disclosure over time**		
				Curve shape	**R^2 (adj.)**	**Remark**
Browser	Internet Explorer 7	74	13.29	Linear	0.99	
	Firefox 2	167	5.16	Linear	0.99	
Email client	MS Outlook Express 6	23	120.73	Linear	0.97	
	Thunderbird 1	110	13.79	S-shape, then strong increase		
Web server	IIS 5	83	40.90	Piecewise linear		
	Apache2	80	40.63	Linear	0.99	
Office	MS Office 2003	99	19.22	S-shape, then strong increase		
	OpenOffice 2	19	63.16	Linear	0.95	
Operating system	Windows 2000	385	9.35	Linear	0.99	
	Windows XP	297	8.97	Linear	0.98	
	MAC OSX	300	4.64	Linear	0.96	
	Red Hat Enterprise Linux 4[1)]	54 +284[2)] =338	4.32	Linear	0.95	
	Debian 3.1[1)]	22 +244[2)] =266	5.02	linear	0.96	
Database Management System	mySQL 5	33	46.00	linear		Too few data points available for any reliable statistic conclusion
	PostgreSQL 8	25	58.96	linear		
	Oracle 10g	63	29.72	S-shape, then strong increase		
	DB2 v8	13	136.38	linear		

[1)] The NVD lists linux kernel vulnerabilities separately from vulnerabilities of specific Linux distributions. Both *Red Hat Enterprise Linux 4* and *Debian 3.1* contain *Linux kernel 2.6*. As many consecutive versions of *Linux kernel 2.6* have been released, in each case I consider only those kernel 2.6 vulnerabilities that were published after the release date of *Red Hat Enterprise Linux 4* and *Debian 3.1*, respectively.

[2)] Linux kernel

Table 1. Published vulnerabilities in terms of MTBVD and development over time

Severity of vulnerabilities

I analyzed the severity of vulnerabilities for each software package in terms of mean, median, standard deviation, and proportion of highly severe vulnerabilities. For each application type, also the median of medians is given (see Table 2). The analysis provides the following results:

- The medians of medians reveal that the vulnerabilities of office products are much more severe (8.45) than those of web servers (5.0), while the values of the other application types are close to each other. However, the number of investigated software bundles is still too low to deduce general hypotheses. An investigation of the type of vulnerabilities might reveal the reasons for the observed differences.
- When we determine the medians of medians of open source software (5.7) and closed source software (6.8) and also the corresponding medians of the proportions of highly severe vulnerabilities (30.28% and 45.95%, respectively), the first impression is that open source software is more secure in terms of the level of severity. However, applying statistical analysis (Mann-Whitney U-test), no statistically significant differences can be found: the two-tailed test provides a high number for P (P=0.1139). Applying the same test to the proportion figures, the test, again, does not indicate that the samples are significantly different (P=0.06). Summing up, I find no significant difference between the severity of vulnerabilities in open source and closed source software.
- Comparing open source software developed in bazaar style with that developed in cathedral style, no significant difference in terms of median (P=0.25) and also no significant difference in terms of the proportion of highly severe vulnerabilities occur (P=0.39).

Application type	Product	Severity (range=[0;10])				
		mean	median	std. dev.	Proportion of highly severe vuln. ([7;10])	Median of medians
Browser	Internet Explorer 7	6.65	6.80	2.07	45.95%	6.6
	Firefox 2	6.38	6.40	2.11	36.53%	
Email client	MS Outlook Express 6	6.18	5.10	1.76	39.13%	5.95
	Thunderbird 1	6.53	6.80	2.23	47.27%	
Web server	IIS 5	6.00	5.00	1.55	36.14%	5.00
	Apache2	5.36	5.00	1.50	18.75%	
Office	MS Office 2003	8.11	9.30	1.91	67.72%	8.45
	OpenOffice 2	7.61	7.60	1.79	63.16%	
Operating system	Windows 2000	6.58	7.20	2.10	57.92%	6.8
	Windows XP	6.67	7.20	2.16	58.92%	
	MAC OSX	6.18	6.80	2.13	41.33%	
	Red Hat Enterprise Linux 4[2)]	4.81	4.90	2.20	24.56%	
	Debian 3.1[2)]	4.79	4.90	2.15	22.93%	
Database Management Systems	mySQL 5	5.05	4.90	2.02	12.12%	5.7
	PostgreSQL 8	6.17	6.80	1.89	36.00%	
	Oracle 10g	5.96	5.50	2.05	33.33%	
	DB2 v8	6.22	7.2	2.75	53.85%	

[1)] compliant with CVSS severity ratings

Table 2. Severity of published vulnerabilities

CONCLUSIONS

Reviewing literature on open source and closed source security reveals research lacks in applying appropriate metrics, methodology and hard data. This paper contributes to solving this problem by analyzing and comparing published vulnerabilities of widely deployed open source software and closed source software packages.

The empirical investigation shows that the mean time between vulnerability disclosures was lower for open source software in three out of six cases, while the other cases show no differences. This means that only if vulnerability disclosure supports software security, open source software would (tend to) be more secure. It should be also noted that the presented analysis does not cover detected, but unpublished vulnerabilities. This gap leads to the interesting research question of the relevance of this gap.

A surprising result of the empirical analysis is that for 14 out of 17 considered software packages, an (in most cases) significant linear or piecewise linear correlation between the number of published vulnerabilities and time occurs, while in only three cases the development follows an S-shape (at least in the beginning), as assumed in the literature. This does not only mean that the detection of vulnerabilities in the beginning of a software lifecycle is underestimated, it also shows that the detection of vulnerabilities does not level off during years. Consequently, addressing vulnerabilities must not be neglected in any phase of the software lifecycle. However, it is still an open question why some software packages show an S-shape. An analysis of the particular type of vulnerabilities might reveal more facts.

The empirical analysis shows differences in terms of vulnerability severity for different application types. Again, an investigation of the vulnerability type might reveal the reasons. However, no significant differences in terms of vulnerability severity were found between open source and closed source.

ANNEX

Software

Application type	Product (Vendor/Community)	Devel. type[0)]	Released	SLOC[1)]	Market share
Browser	Internet Explorer 7 (Microsoft)	Closed	2006-10-18	--	High(≈67.6%)[3)]
	Firefox 2 (Mozilla)	Open (BS)	2006-10-24	≈63,000[4)]	Low (≈21.5%)[3)]
Email client	MS Outlook Express 6 (Microsoft)	Closed	2001-10-25	--	--
	Thunderbird 1 (Mozilla)	Open (CS)	2004-12-07	≈320,000[4)]	--
Web server	IIS 5 (Microsoft)	Closed	2000-02-17	--	Medium (≈34.6%)[8)]
	Apache2 (Apache Software Foundation)	Open (CS)	2000-03-10	≈200,000[4)]	Medium (≈50.2%)[8)]
Office	MS Office 2003 (Microsoft)	Closed	2003-11-17	--	Medium/High[8)]
	OpenOffice 2 (Openoffice.org)	Open (CS)	2005-10-20	≈9 Mio[4)]	Low[9)]
Operating System	Windows 2000 (all versions) (Microsoft)	Closed	2000-02-17	≈ 35 Mio.[5) 6)]	High (≈ 90%)[3)]
	Windows XP (Microsoft)	Closed	2001-10-25	≈ 40 Mio.[5)]	
	MAC OSX 10.4 (Tiger) (Apple)	Closed [20)]	2005-04-29	≈ 86 Mio [7)]	Low (≈8.2%)[3)]
	Red Hat Enterprise Linux 4 (Red Hat)	Open (CS)	2005-02-14	≈7 Mio (kernel), rest unknown	Low (< 1%, all Linux derivates))[3)]
	Debian 3.1 (Debian Project)	Open (BS)	2005-06-06	≈50 Mio.[4)]	
Database Management System	mySQL 5 (Sun)	Open (BS)	2005-10-24	≈ 15,000[4)]	Low (none of the databases is assumed to have more than 33% market share)[10)11)]
	postgreSQL 8 (PostgreSQL Global Development Group)	Open (CS)	2005-01-19	≈580,000[4)]	
	Oracle 10g (Oracle)	Closed	2004-01-15[2)]	--	
	DB2 v8 (IBM)	Closed	2004-03-26	--	

BS: Bazaar style CS: Cathedral style --: no reliable data found

0) Regarding the identification of the particular open source development style (cathedral vs. bazaar) I checked the particular community web site. Reading their different contribution rules, in some cases I found elements of both styles. The binary classification in the table reflects the personal assessment of the rules according to whether they are more "cathedral" or "bazaar style".

1) SLOC=Source lines of code (excl. comments and blanks)

2) Oracle provides as released date only "January 2004", but no specific date. For computing the age of vulnerabilities I use 15 January 2004, as this date minimizes the expected error under the assumption of uniform distribution.

3) http://marketshare.hitslink.com

4) http://www.ohloh.net

5) (http://www.dwheeler.com/sloc/)

6) (Anderson, 2001)

7)(http://www.engadget.com/2006/08/07/live-from-wwdc-2006-steve-jobs-keynote/

8) http://survey.netcraft.com/Reports/200811/

9) http://www.it-director.com/business/change/content.php?cid=9453

10)http://www.mysql.com/why-mysql/marketshare/

11)http://docs.huihoo.com/postgresql/mysql-vs-pgsql.html

12) Some open source components are included.

Table 3. Investigated open and closed source software

Vulnerability disclosure

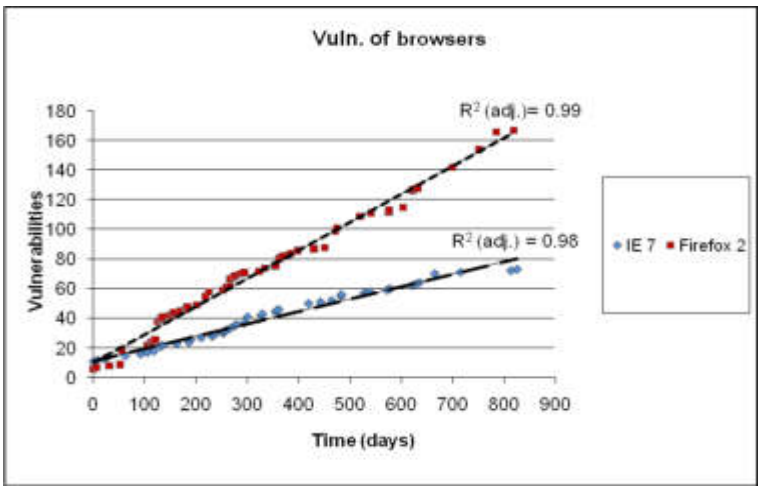


Figure 2. Vulnerability disclosure of browsers over time

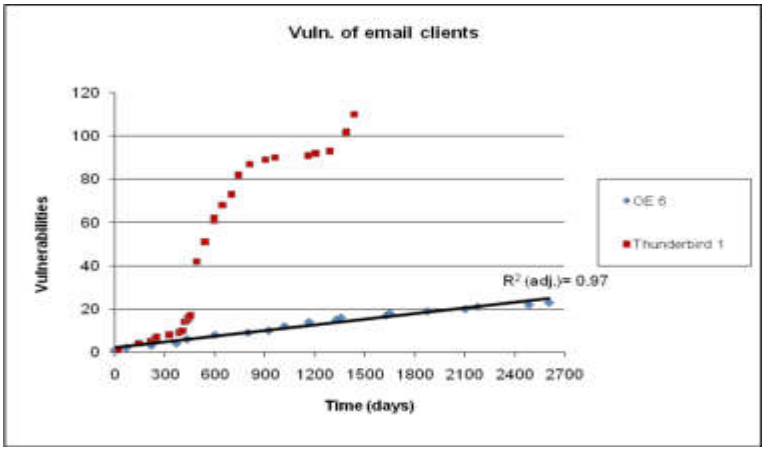


Figure 3. Vulnerability disclosure of email clients over time

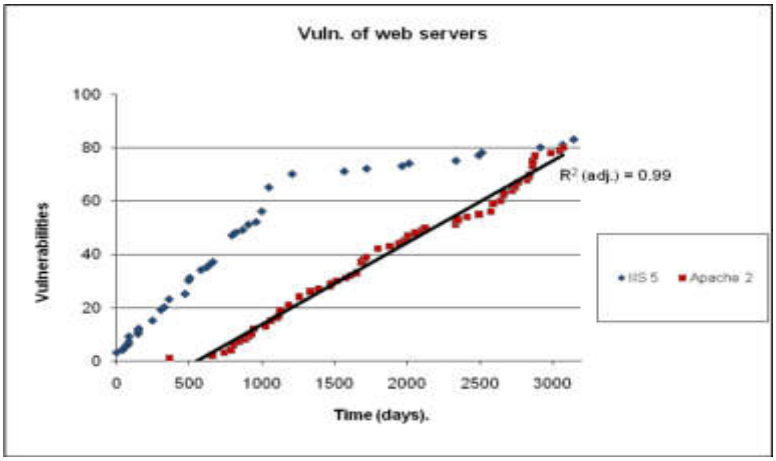


Figure 4. Vulnerability disclosure of web servers over time

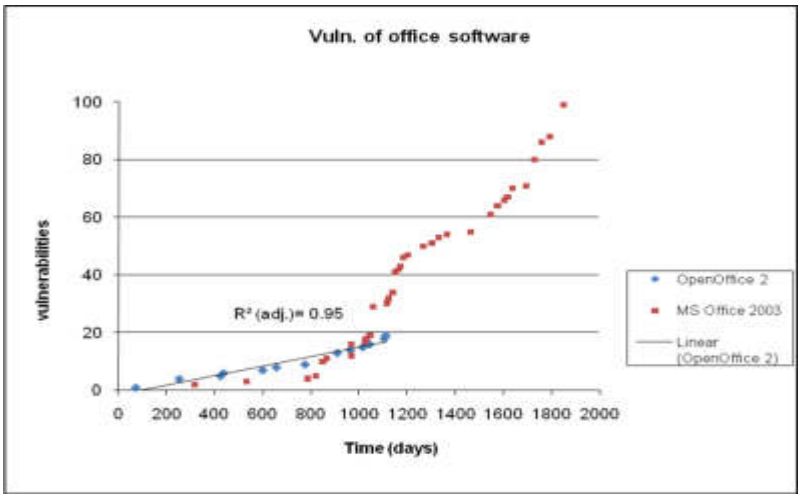


Figure 5. Vulnerability disclosure of office software over time

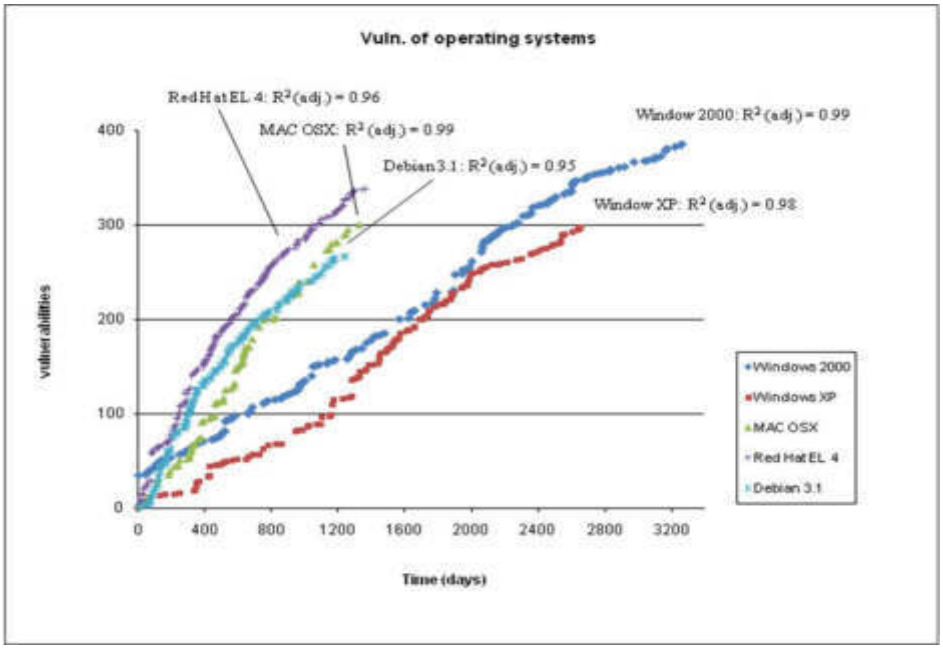


Figure 6. Vulnerability disclosure of operating systems over time

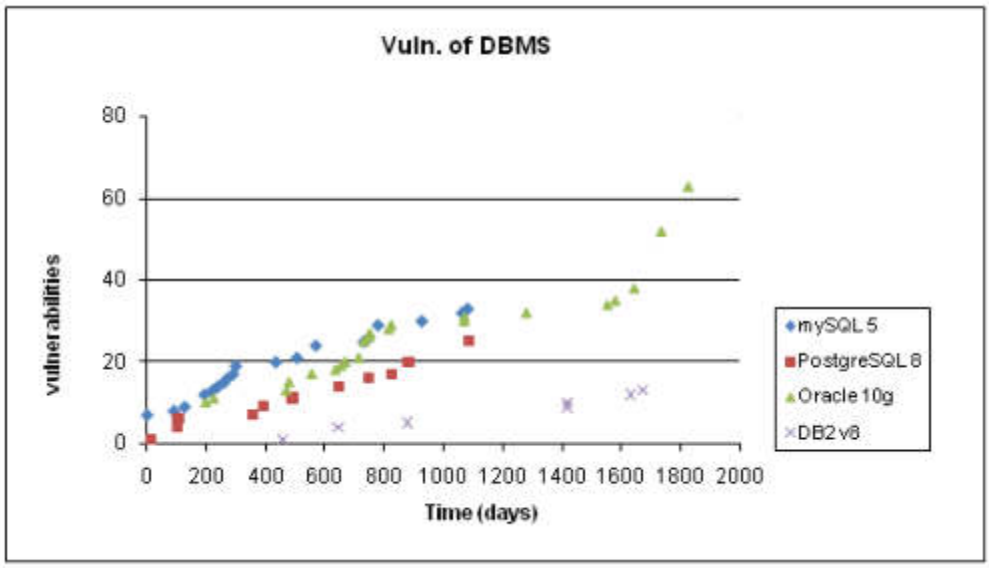


Figure 7. Vulnerability disclosure of DBMS over time

REFERENCES

1. Alhazmi, O., Malaiya, Y. and Ray, I. (2005) Security Vulnerabilities, in *Software Systems: A Quantitative Perspective in Data and Applications Security 2005,* LNCS 3654, 281-294.
2. Alhazmi, O., Malaiya, Y., Ray, I. (2007) Measuring, analyzing and predicting security vulnerabilities in software systems, in *Computers & Security*, 26, 3, 219-228.
3. Anderson, R. (2005) Open and Closed Systems are Equivalent (that is, in an ideal world), in Feller, J., Fitzgerald, B., Hissam, S. A. and Lakhani, K.R. (Eds.) *Perspectives on Free and Open Source Software*, MIT Press, Cambridge, 127–142.
4. Anderson, R. (2002) Security in Open versus Closed Systems – The Dance of Boltzmann, Coase and Moore, in *Proceedings of the Conference on Open Source Software Economics*, Toulouse, France, June 20-21, 1-13.
5. Anderson, R. (2001) Why Information Security is Hard – An Economic Perspective, in *Proceedings of the Seventeenth Computer Security Applications Conference*, New Orleans, December 10-14, 358-365.
6. Arora, A., Krishnan, R., Nandkumar, A., Telang, R. and Yang, Y. (2004) Impact of Vulnerability Disclosure and Patch Availability – An Empirical Analysis, in *Proceedings of the Third Workshop on the Economics of Information Security*, University of Minnesota, May 13-14, 1-20.
7. Arora, A., Telang, A. and Xu, H. (2004), "Optimal Policy for Software Vulnerability Disclosure", in *Proceedings of the Third Annual Workshop on Economics and Information Security*, University of Minnesota, May 13-14, 52-59.
8. FIRST (2007) A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0, http://www.first.org/cvss/cvss-guide.html.
9. Free Software Foundation (FSF) (2007) The Free Software Definition, http://www.fsf.org/licensing/essays/free-sw.html.
10. Glass, R.L. (2004) A look at the economics of open source, in *Comm. of the ACM,* 47,2, 25-27.
11. Goel, A.L. and Okumoto, K. (1979) Time-Dependent Error-Detection Rate Model for Software and Other Performance Measures, in *IEEE Transactions on Reliability*, 28, 3, 206-211.
12. Gonzalez-Barahona, J. M. (2000) Free Software/Open Source: Information Society Opportunities for Europe?, Working group on Libre Software, http://eu.conecta.it/paper/cathedral_bazaar.html.
13. Jonsson, E., Strömberg, L. and Lindskog, S. (2000) On the functional relation between security and dependability impairments, in *Proceedings of the 1999 Workshop on New Security Paradigms*, Caledon Hills, Ontario, Canada, September 22 – 24, 104-111.
14. Kimura, M. (2006) Software vulnerability: definition, modelling, and practical evaluation for e-mail transfer software, in *International Journal of Pressure Vessels and Piping*, 83, 4, 256-261.

15. Levy, E. (2000) Wide open source, http://www.securityfocus.com/news/19.
16. Messmer, E. (2005) Open source vs. Windows: security debate rages, in *Network World*, 22, 26, 26-27.
17. MITRE (2009) Vulnerability Management Products & Services by Product Type, http://cve.mitre.org/compatible/vulnerability_management.html.
18. Naraine, R. (2006) DHS backs open-source security, in *eWeek*, 23, 3, 20.
19. Open Source Initiative (OSI) (2006) The Open Source Definition, http://www.opensource.org/docs/osd.
20. Ozment, A. (2005) The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting, in *Proceedings of the Fourth Workshop on the Economics of Information Security*, Harvard University, June 2-3, Cambridge, Massachusetts, 1-21.
21. Nizovtsev, D. and Thursby, M. (2007) To disclose or not? An analysis of software user behavior, in *Information Economics and Policy*, 19, 1, 43-64.
22. Payne, C. (2002) On the security of open source software, in *Information Systems Journal*, 12, 1, 61-78.
23. Raymond, E.S. (2001) The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary, O'Reilly, Beijing, China.
24. Rescorla, E. (2004) Is finding security holes a good idea?, in *Proceedings of the Third Annual Workshop on Economics and Information Security*, University of Minnesota, May 13-14.
25. Schryen, G. and Kadura, R. (2009) Open Source vs. Closed Source Software: Towards Measuring Security, in *Proceedings of the 2009 ACM Symposium on Applied Computing*, Honolulu, Hawaii, USA, March 8-12, 2016-2023.
26. Schwarz, M. and Takhteyev, Y. (2008) Half a Century of Public Software Institutions: Open Source as a Solution to Hold Up Problem, http://www.takhteyev.org/papers/Schwarz-Takhteyev-2008.pdf.
27. Witten, B., Landwehr, C. and Caloyannidis, M. (2001) Does open source improve system security?, in *IEEE Software*, 18,5, 57-61.

CoWIN open-source version to be given to 50 nations

Bindu Shajan Perappadan

Countries from Central Asia, Africa and Latin America have indicated interest in the technology, says NHA CEO

India would soon provide an open-source version of its CoWIN application to nearly 50 countries from Central Asia, Africa and Latin America that have indicated an interest in the technology, R.S. Sharma, CEO, National Health Authority (NHA) and CoWIN platform, said on Monday at the 2nd Public Health Summit 2021 — 'Emerging Imperative in Strengthening Public Health for India', organised by the Confederation of Indian Industry (CII).

India was getting ready to share its information globally and on July 5 would participate in an international conclave where the technology would be presented. While India continued to grapple with the devastating second wave of the pandemic, vaccines seemed to be the best way forward, he stated.

CoWIN is an extension of electronic vaccine intelligence network – eVIN – which is used to collect real-time feedback of the vaccination programmes. CoWIN is a cloud-based IT solution for planning, implementing, monitoring, and evaluating COVID-19 vaccination in the country.

According to the operational guidelines for COVID-19 vaccination prepared by the Union Health Ministry, the CoWIN system, on a real-time basis, tracks not only the beneficiaries but also the vaccines at the national, State and district levels. It monitors the utilisation, wastage and coverage of vaccination. Also every detail, from the sites where vaccinations are carried out to the number of beneficiaries and even the batch number, doses per vial and schedule of the vaccine, are uploaded on it.

Dr. Sharma said the NHA was constantly working at improving the reach and coverage of the health care services "and in that context, would be bringing in an e-voucher system that allows immediate payment to the service provider for specific medical services. This will greatly improve the service delivery for patients".

Prepare for outbreaks: Dr. Guleria

Speaking at the meet, Randeep Guleria, Director, All India Institute of Medical Sciences (AIIMS), pointed out that the pandemic had stressed the health care system and disrupted the medical care eco-system. "But what this has also taught us is that we have to be prepared for outbreaks. We have seen bird-flu, swine-flu, Ebola and Zika outbreaks in the past and now it's time that we understand the

importance of prevention," he said.

The country had to work at getting health a greater share in the GDP and ensure that the human resources were available and trained. "The challenges we face include underinvestment in the health care sector, lack of the public health system being driven by technology and data and slow paced development of infrastructure. COVID-19 has taught us that the way forward is partnership and we have to undertake this in a big way," he urged.

Doses for States

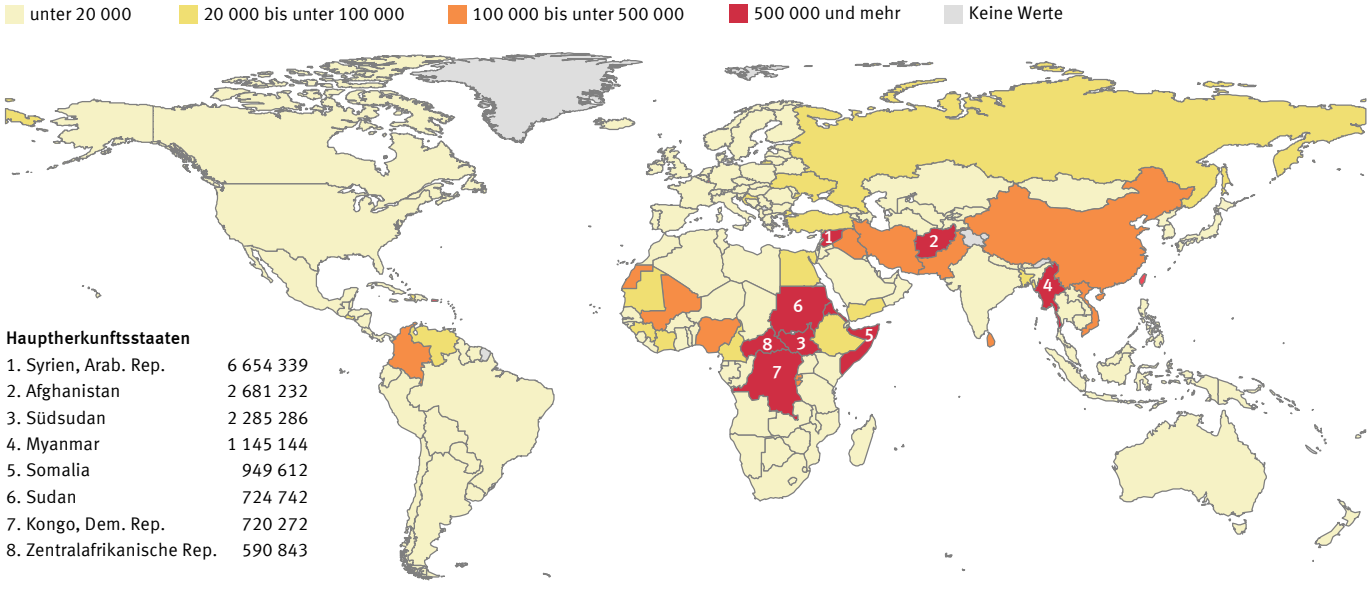
The Union Health Ministry said on Monday that more than 31.69 crore (31,69,40,160) vaccine doses had been provided to the States through the free of cost channel and through direct State procurement category. Of this, the total consumption, including wastage, was 30,54,17,617 doses (as per data available at 8 a.m. on Monday). More than 1.15 crore (1,15,22,543) balance and unutilised vaccine doses were still available with the States/UTs, it added.

A Internationales

In Deutschland kommen auf 100 Personen **41** feste **Breitbandanschlüsse** | **15 %** aller EU-Erwerbstätigen arbeiten regelmäßig oder gelegentlich im **Home-Office** | **Lebenshaltungskosten** in der **Türkei** um **16 %** gestiegen | 26 % der **Weltbevölkerung unter 15 Jahre** alt | **Selbstständigenquote** in China bei 48 % | Energiebedarf: **Australien** deckt **8 %** aus **erneuerbaren Energien** | 38 % der **Landfläche** von Tansania als **Naturschutzgebiet** ausgewiesen

A.0 Auf einen Blick

Anzahl Geflüchtete nach Herkunftsstaaten 2018

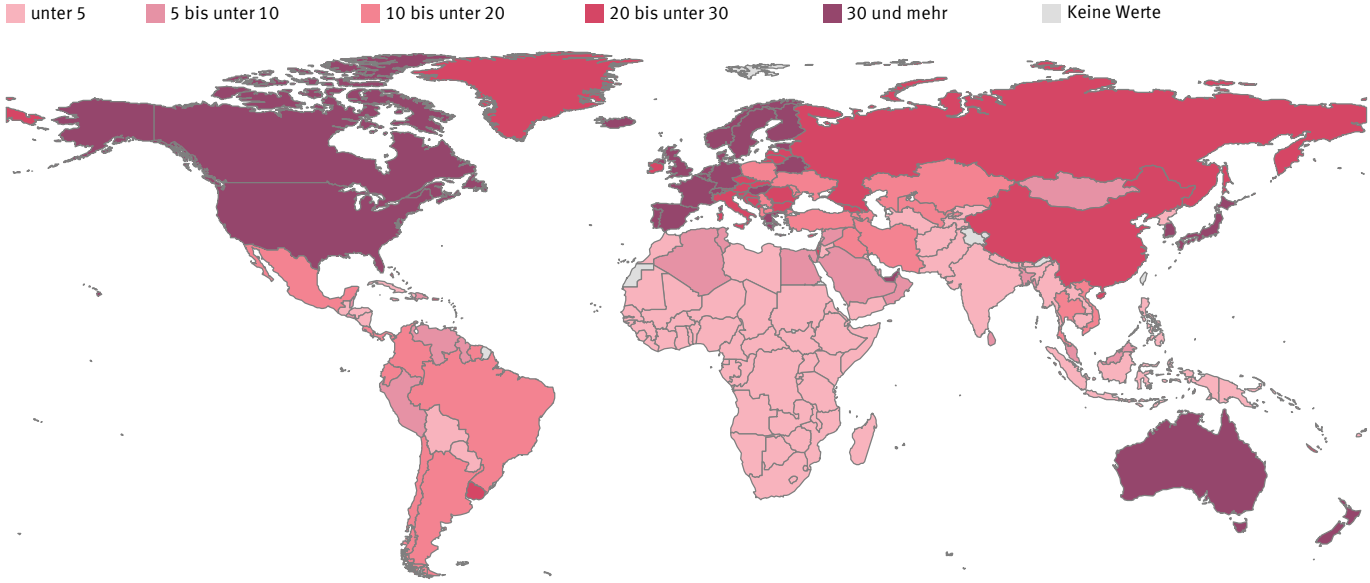


Hauptherkunftsstaaten

1. Syrien, Arab. Rep.	6 654 339
2. Afghanistan	2 681 232
3. Südsudan	2 285 286
4. Myanmar	1 145 144
5. Somalia	949 612
6. Sudan	724 742
7. Kongo, Dem. Rep.	720 272
8. Zentralafrikanische Rep.	590 843

Kartengrundlage: © EuroGeographics bezüglich der Verwaltungsgrenzen
Quelle: Flüchtlingshilfswerk der Vereinten Nationen (UNHCR)

Festinstallierte Internet-Breitbandanschlüsse 2018
im Abonnement, je 100 Einwohner/-innen



Kartengrundlage: © EuroGeographics bezüglich der Verwaltungsgrenzen
Quelle: Internationale Fernmeldeunion (ITU), Vereinte Nationen

2019 - 01 - 0308

A.0 Auf einen Blick: Bevölkerung und Wirtschaft weltweit

	Bevölkerung insgesamt [1]	Bevölkerungsanteil unter 15 Jahren [1]	Bruttoinlandsprodukt (BIP) je Einwohner/-in [2]	Reale Veränderung des BIP gegenüber Vorjahr [2]
	2018			
	1 000	%	Internat. US$ [3]	%
Welt	**7 594 270**	***25,8***	**.**	***+ 3,6***
Europa				
Europäische Union	513 213	*15,4*	*43 148*	*+ 2,1*
Albanien	2 866	*17,1*	*13 345*	*+ 4,2*
Andorra	77	.	.	.
Belarus	9 485	*17,0*	*20 003*	*+ 3,0*
Belgien	11 422	*17,2*	*48 245*	*+ 1,4*
Bosnien und Herzegowina	3 324	*14,2*	*13 491*	*+ 3,1*
Bulgarien	7 024	*14,4*	*23 156*	*+ 3,2*
Dänemark	5 797	*16,4*	*52 121*	*+ 1,2*
Deutschland	**82 928**	***13,1***	***52 559***	***+ 1,5***
Estland	1 321	*16,6*	*34 096*	*+ 3,9*
Finnland	5 518	*16,5*	*46 430*	*+ 2,4*
Frankreich	66 987	*18,0*	*45 775*	*+ 1,5*
Griechenland	10 728	*14,1*	*29 123*	*+ 2,1*
Irland	4 854	*21,5*	*78 785*	*+ 6,8*
Island	354	*20,0*	*55 917*	*+ 4,6*
Italien	60 431	*13,4*	*39 637*	*+ 0,9*
Kroatien	4 089	*14,7*	*26 221*	*+ 2,7*
Lettland	1 927	*15,6*	*29 901*	*+ 4,8*
Liechtenstein	38	.	.	.
Litauen	2 790	*15,0*	*34 826*	*+ 3,4*
Luxemburg	608	*16,5*	*106 705*	*+ 3,0*
Malta	484	*14,5*	*45 606*	*+ 6,4*
Moldau, Republik	3 546	*15,8*	*7 305*	*+ 4,0*
Monaco	39	.	.	.
Montenegro	622	*18,0*	19 043	*+ 4,5*
Niederlande	17 231	*16,2*	*56 383*	*+ 2,5*
Nordmazedonien	2 083	*16,6*	*15 709*	*+ 2,7*
Norwegen	5 314	*17,8*	*74 356*	*+ 1,4*
Österreich	8 847	*14,1*	*52 137*	*+ 2,7*
Polen	37 979	*14,9*	*31 939*	*+ 5,1*
Portugal	10 282	*13,4*	*32 006*	*+ 2,1*
Rumänien	19 474	*15,2*	*26 447*	*+ 4,1*
Russische Föderation	144 478	*17,8*	*29 267*	*+ 2,3*
San Marino	34	.	*60 313*	*+ 1,1*
Schweden	10 183	*17,7*	*52 984*	*+ 2,3*
Schweiz	8 517	*14,9*	*64 649*	*+ 2,5*
Serbien [4]	6 982	*16,3*	*17 555*	*+ 4,4*
Slowakei	5 447	*15,5*	*35 130*	*+ 4,1*
Slowenien	2 067	*15,1*	*36 746*	*+ 4,5*
Spanien	46 724	*14,6*	*40 139*	*+ 2,5*
Tschechische Republik	10 626	*15,5*	*37 371*	*+ 2,9*
Türkei	82 320	*24,6*	*27 956*	*+ 2,6*
Ukraine	44 623	*15,8*	*9 283*	*+ 3,3*
Ungarn	9 769	*14,3*	*31 903*	*+ 4,9*
Vereinigtes Königreich	66 489	*17,8*	*45 705*	*+ 1,4*
Zypern [5]	1 189	*16,8*	*39 973*	*+ 3,9*
Afrika				
Ägypten	98 424	*33,3*	*13 366*	*+ 5,3*
Algerien	42 228	*29,5*	*15 440*	*+ 2,1*
Angola	30 810	*46,6*	*6 814*	*– 1,7*
Äquatorialguinea	1 309	*37,0*	*22 710*	*– 5,7*
Äthiopien	109 225	*40,0*	*2 332*	*+ 7,7*
Benin	11 485	*42,4*	*2 426*	*+ 6,5*
Botsuana	2 254	*31,2*	*17 965*	*+ 4,6*
Burkina Faso	19 752	*44,9*	*1 996*	*+ 6,0*
Burundi	11 175	*45,1*	*733*	*+ 0,1*
Cabo Verde	544	*29,8*	*7 316*	*+ 4,7*
Côte d'Ivoire	25 069	*42,3*	*4 178*	*+ 7,4*
Dschibuti	959	*30,6*	*3 786*	*+ 6,7*
Eritrea	5 110 [6]	*42,8* [6]	*1 657*	*+ 4,2*
Eswatini [7]	1 136	*37,0*	*11 020*	*+ 0,2*
Gabun	2 119	*35,9*	*18 496*	*+ 1,2*
Gambia	2 280	*45,1*	*2 792*	*+ 6,6*
Ghana	29 767	*38,3*	*6 452*	*+ 5,6*
Guinea	12 414	*42,0*	*2 310*	*+ 5,8*
Guinea-Bissau	1 874	*41,3*	*1 937*	*+ 3,8*
Kamerun	25 216	*42,5*	*3 828*	*+ 4,0*
Kenia	51 393	*40,1*	*3 691*	*+ 6,0*
Komoren	832	*39,5*	*1 632*	*+ 2,8*
Kongo	5 244	*42,1*	*6 799*	*+ 0,8*
Kongo, Dem. Republik	84 068	*46,2*	*767*	*+ 3,9*
Lesotho	2 108	*35,3*	*3 394*	*+ 1,5*
Liberia	4 819	*41,5*	*1 418*	*+ 1,2*
Libyen	6 679	*27,9*	*11 469*	*+ 17,9*
Madagaskar	26 262	*40,7*	*1 630*	*+ 5,2*
Malawi	18 143	*43,7*	*1 199*	*+ 3,2*
Mali	19 078	*47,5*	*2 384*	*+ 4,9*
Marokko	36 029	*27,2*	*8 933*	*+ 3,1*
Mauretanien	4 403	*39,7*	*3 990*	*+ 3,0*
Mauritius	1 265	*17,9*	*23 699*	*+ 3,8*
Mosambik	29 496	*44,5*	*1 291*	*+ 3,3*
Namibia	2 448	*36,5*	*11 229*	*– 0,1*
Niger	22 443	*50,1*	*1 217*	*+ 5,2*
Nigeria	195 875	*43,8*	*6 027*	*+ 1,9*
Ruanda	12 302	*39,8*	*2 280*	*+ 8,6*
Sambia	17 352	*44,5*	*4 104*	*+ 3,5*
São Tomé und Príncipe	211	*42,4*	*3 324*	*+ 3,0*
Senegal	15 854	*42,7*	*3 651*	*+ 6,2*
Seychellen	97	*22,4*	*30 505*	*+ 3,6*
Sierra Leone	7 650	*41,7*	*1 620*	*+ 3,7*
Simbabwe	14 439	*41,0*	*2 788*	*+ 3,4*
Somalia	15 008	*46,3*	.	*+ 3,1*
Südafrika	57 780	*28,8*	*13 675*	*+ 0,8*
Sudan	41 802	*40,5*	*4 232*	*– 2,1*
Südsudan	10 976	*41,5*	*1 502*	*– 1,2*
Tansania, Ver. Republik	56 318	*44,7*	*3 444*	*+ 6,6*
Togo	7 889	*41,3*	*1 746*	*+ 4,7*
Tschad	15 478	*46,9*	*2 415*	*+ 3,1*
Tunesien	11 565	*24,0*	*12 372*	*+ 2,5*
Uganda	42 723	*47,4*	*2 498*	*+ 6,2*
Zentralafrik. Republik	4 666	*42,8*	*712*	*+ 4,3*

A.0 Auf einen Blick: Bevölkerung und Wirtschaft weltweit

	Bevölkerung insgesamt [1]	Bevölkerungsanteil unter 15 Jahren [1]	Bruttoinlandsprodukt (BIP) je Einwohner/-in [2]	Reale Veränderung des BIP gegenüber Vorjahr [2]
	2018			
	1 000	%	Internat. US$ [3]	%
Amerika				
Antigua und Barbuda	96	23,6	27 981	+ 5,3
Argentinien	44 495	24,7	20 537	– 2,5
Bahamas	386	20,5	33 494	+ 2,3
Barbados	287	18,9	18 534	– 0,5
Belize	383	30,9	8 501	+ 3,0
Bolivien, Plurinat. Staat	11 353	31,3	7 477	+ 4,3
Brasilien	209 469	21,4	16 154	+ 1,1
Chile	18 729	20,1	25 978	+ 4,0
Costa Rica	4 999	21,4	17 559	+ 2,7
Dominica	72	.	9 886	– 12,0
Dominikanische Republik	10 627	29,0	18 425	+ 7,0
Ecuador	17 084	28,2	11 718	+ 1,1
El Salvador	6 421	27,1	8 041	+ 2,5
Grenada	111	26,3	16 167	+ 4,8
Guatemala	17 248	34,4	8 436	+ 3,1
Guyana	779	28,6	8 519	+ 3,4
Haiti	11 123	32,6	1 864	+ 1,5
Honduras	9 588	31,0	5 212	+ 3,7
Jamaika	2 935	22,6	9 447	+ 1,4
Kanada	37 059	16,1	49 651	+ 1,8
Kolumbien	49 649	23,1	14 943	+ 2,7
Kuba	11 338	15,9	.	.
Mexiko	126 191	26,3	20 602	+ 2,0
Nicaragua	6 466	28,6	5 683	– 4,0
Panama	4 177	27,1	25 675	+ 3,9
Paraguay	6 956	29,1	13 395	+ 3,7
Peru	31 989	27,1	14 224	+ 4,0
St. Kitts und Nevis	52	.	29 820	+ 3,0
St. Lucia	182	18,5	14 355	+ 1,0
St. Vincent u. d. Grenadinen	110	23,5	11 956	+ 2,0
Suriname	576	26,2	15 105	+ 2,0
Trinidad und Tobago	1 390	20,5	32 254	+ 0,3
Uruguay	3 449	20,9	23 274	+ 2,1
Venezuela, Bol. Republik	28 870	27,3	.	– 18,0
Vereinigte Staaten	327 167	18,8	62 606	+ 2,9
Asien				
Afghanistan	37 172	42,6	2 017	+ 2,3
Armenien	2 952	20,1	10 176	+ 5,0
Aserbaidschan	9 942	23,3	18 076	+ 1,4
Bahrain	1 569	19,2	50 057	+ 1,8
Bangladesch	161 356	27,8	4 620	+ 7,7
Bhutan	754	26,2	9 540	+ 5,8
Brunei Darussalam	429	22,6	79 530	– 0,2
China [8]	1 392 730	17,6	18 110	+ 6,6
Georgien	3 731	19,4	11 485	+ 4,7
Indien	1 352 617	27,4	7 874	+ 7,1
Indonesien	267 663	27,0	13 230	+ 5,2
Irak	38 434	40,2	17 659	+ 0,6
Iran, Islamische Republik	81 800	23,7	19 557	– 3,9
Israel [9]	8 884	27,8	37 972	+ 3,3
Japan	126 529	12,8	44 227	+ 0,8
Jemen	28 499	39,6	2 377	– 2,7
Jordanien	9 956	35,2	9 433	+ 2,0
Kambodscha	16 250	31,2	4 335	+ 7,3
Kasachstan	18 276	28,3	27 550	+ 4,1
Katar	2 782	13,9	130 475	+ 2,2
Kirgisistan	6 316	32,1	3 844	+ 3,5
Korea, Dem. Volksrepublik	25 550	20,4	.	.
Korea, Republik	51 635	13,4	41 351	+ 2,7
Kuwait	4 137	21,2	67 000	+ 1,7
Laos, Dem. Volksrepublik	7 062	32,5	7 925	+ 6,5
Libanon	6 849	22,6	14 684	+ 0,3
Malaysia	31 529	24,0	30 860	+ 4,7
Malediven	516	23,4	21 760	+ 7,0
Mongolei	3 170	29,9	13 447	+ 6,9
Myanmar	53 708	26,3	6 511	+ 2,1
Nepal	28 088	30,2	2 905	+ 6,3
Oman	4 829	21,6	46 584	+ 2,1
Pakistan	212 215	34,7	5 680	+ 5,2
Philippinen	106 652	31,5	8 936	+ 6,2
Saudi-Arabien	33 700	24,9	55 944	+ 2,2
Singapur	5 639	14,7	100 345	+ 3,2
Sri Lanka	21 670	23,7	13 397	+ 3,0
Syrien, Arabische Republik	16 906	35,7	.	.
Tadschikistan	9 101	35,3	3 416	+ 7,0
Thailand	69 429	17,0	19 476	+ 4,1
Timor-Leste	1 268	43,5	5 242	+ 0,8
Turkmenistan	5 851	30,8	19 527	+ 6,2
Usbekistan	32 955	28,0	7 665	+ 5,0
Ver. Arabische Emirate	9 631	13,9	69 382	+ 1,7
Vietnam	95 540	23,0	7 511	+ 7,1
Australien und Ozeanien				
Australien	24 992	19,1	52 373	+ 2,8
Fidschi	883	28,3	10 234	+ 3,2
Kiribati	116	35,3	2 086	+ 2,3
Marshallinseln	58	.	3 697	+ 2,4
Mikronesien, F. Staaten von	113	32,7	2 955 [10]	– 0,2 [10]
Nauru	13	.	12 326	– 2,4
Neuseeland	4 886	19,8	40 135	+ 3,0
Palau	18	.	14 952	+ 0,4
Papua-Neuguinea	8 606	35,6	3 662	.
Salomonen	653	38,5	2 242	+ 3,4
Samoa	196	36,4	5 890	+ 0,7
Tonga	103	35,4	6 111	+ 1,8
Tuvalu	12	.	4 052	+ 4,3
Vanuatu	293	35,8	2 862	+ 3,2

1 Quelle: World Development Indicators, Weltbank.
2 Quelle: World Economic Outlook, Internationaler Währungsfonds (IMF). Zum Teil IMF Schätzungen.
3 Weitere Informationen zu dieser Währungseinheit siehe Erläuterungen auf Seite 674.
4 Ohne Kosovo.
5 Einschl. Nordzypern.
6 2014.
7 Frühere Bezeichnung Swasiland.
8 Ohne Taiwan, Macau, Hongkong.
9 Ohne Palästinensische Gebiete. Einschl. Ost-Jerusalem.
10 2015.

A.1 Geografie und Klima

	Landfläche [1]	Hauptstadt (in Klammern: Standort Wetterstation, sofern nicht Hauptstadt)	Mittlere Lufttemperatur [2]			Mittlere tägliche Sonnenscheindauer [2]			Mittlerer Niederschlag [2]		
			Jahresdurchschnittswert	des kältesten Monats	des wärmsten Monats	Jahresdurchschnittswert	des Monats mit der niedrigsten Sonnenscheindauer	des Monats mit der höchsten Sonnenscheindauer	durchschnittlicher Jahresgesamtwert	des nassesten Monats	des trockensten Monats
	2016		Referenzperiode 1996 bis 2010								
	km²		°C			Stunden			l/m²		
Europa											
Europäische Union	4 238 694	.	.	.	.	.	.	.	.	.	.
Belgien	30 280	Brüssel	10,8	3,3 Jan	18,4 Jul	4,3	1,4 Dez	7,1 Jun	863	100 Aug	49 Apr
Bulgarien	108 560	Sofia	10,5	– 0,6 Jan	21,5 Jul	6,1	1,9 Dez	10,1 Jul	629	73 Jun	35 Feb
Dänemark	41 990	Kopenhagen	9,2	1,4 Jan	18,1 Aug	.	.	.	539	78 Aug	26 Apr
Deutschland	**349 360**	**Berlin**	**9,7**	**0,4 Jan**	**19,2 Jul**	**4,8**	**1,5 Dez**	**7,8 Jun**	**594**	**75 Aug**	**27 Apr**
Estland	43 470	Tallinn	6,2	– 4,2 Feb	17,8 Jul	5,2	0,7 Dez	9,8 Jul	672	99 Jul	31 Apr
Finnland	303 910	Helsinki	5,7	– 5,7 Feb	18,3 Jul	5,0	0,8 Dez	9,2 Jul	666	87 Okt	30 Mrz
Frankreich	547 557	Paris	11,7	4,1 Jan	19,8 Jul	5,1	1,6 Nov	8,0 Jun	612	66 Aug	40 Sep
Griechenland	128 900	Athen	18,7	9,9 Jan	29,2 Jul	7,9	3,7 Dez	12,4 Jul	435	81 Dez	5 Jun
Irland	68 890	Dublin	9,6	5,1 Dez	15,2 Jul	4,1	1,8 Dez	6,6 Mai	780	85 Okt	45 Mrz
Island	100 250	Reykjavík	5,2	0,0 Feb	11,7 Jul	3,8	0,4 Dez	7,0 Mai	837	94 Dez	38 Jun
Italien	294 140	Rom	16,2	8,8 Jan	24,7 Aug	7,1	3,8 Dez	11,3 Jul	614	97 Dez	10 Jun
Kroatien	55 960	Zagreb	12,5	1,8 Jan	22,5 Jul	5,4	1,6 Dez	8,9 Jul	883	100 Sep	39 Feb
Lettland	62 180	Riga (Libau)	7,7	– 2,3 Feb	18,3 Jul	5,4	0,7 Dez	10,1 Jun	.	.	.
Litauen	62 642	Wilna	6,9	– 4,2 Jan	18,6 Jul	4,9	0,9 Dez	8,9 Jun	690	101 Jul	38 Mrz
Luxemburg	2 430	Luxemburg	9,6	0,8 Jan	18,2 Jul	5,0	1,4 Dez	8,4 Jun	864	84 Aug	53 Apr
Malta	320	Valletta	19,4	12,5 Feb	27,2 Aug	8,2	5,2 Dez	11,9 Jul	566	98 Nov	‹ 1 Jul
Niederlande	33 690	Amsterdam (De Bilt)	10,4	3,1 Jan	18,0 Jul	4,6	1,9 Dez	7,2 Jun	863	91 Aug	43 Apr
Norwegen	365 123	Oslo	5,2	– 4,5 Jan	16,4 Jul	.	.	.	866	100 Okt	46 Feb
Österreich	82 523	Wien	10,7	0,1 Jan	20,8 Jul	5,6	1,7 Dez	8,7 Jun	698	84 Jul	40 Okt
Polen	306 190	Warschau	8,6	– 2,3 Jan	19,5 Jul	6,3	1,1 Dez	11,5 Jul	558	91 Jul	29 Jan
Portugal	91 606	Lissabon	17,1	11,5 Jan	23,1 Aug	7,9	4,7 Dez	11,2 Jul	832	130 Dez	3 Jul
Rumänien	230 080	Bukarest	10,8	– 1,7 Jan	23,0 Jul	6,0	1,8 Dez	10,0 Jul	632	79 Sep	33 Feb
Russische Föderation	16 376 870	Moskau	6,1	– 6,9 Feb	20,2 Jul	.	.	.	701	85 Jul	34 Apr
Schweden	407 310	Stockholm	7,7	– 1,4 Feb	18,7 Jul	1,4	0,8 Mrz	2,2 Jul	523	67 Jul	25 Apr
Schweiz	39 516	Bern (Zürich)	9,6	0,5 Jan	18,5 Jul	4,5	1,4 Dez	7,1 Jun, Jul	1 133	132 Aug	52 Jan
Slowakei	48 080	Pressburg	.	.	.	.	.	.	.	.	.
Slowenien	20 142	Laibach	11,2	0,3 Jan	21,4 Jul	5,3	1,7 Dez	9,2 Jul	1 382	159 Sep	69 Feb
Spanien	499 564	Madrid	14,6	5,7 Jan	25,2 Jul	7,8	4,3 Dez	12,0 Jul	397	61 Okt	7 Jul
Tschechische Republik	77 220	Prag	8,6	– 1,6 Jan	18,2 Jul	4,9	1,5 Dez	7,9 Jun	495	84 Jul	19 Feb
Türkei	769 630	Ankara	12,7	1,0 Jan	24,7 Jul	6,7	2,5 Dez	11,1 Jul	411	53 Apr	11 Aug
Ungarn	90 530	Budapest	11,2	– 0,4 Jan	22,1 Jul	5,8	1,9 Dez	9,5 Jul	580	73 Jun	27 Feb
Vereinigtes Königreich	241 930	London	11,8	5,7 Dez	18,7 Jul, Aug	4,4	1,8 Dez	6,9 Jun	639	72 Nov	41 Mrz
Zypern	9 240	Nikosia	20,1	12,2 Jan	28,4 Aug	9,3	5,8 Dez	12,9 Jun	324	84 Jan	‹ 1 Jul, Aug

A.1 Geografie und Klima

	Landfläche [1]	Hauptstadt (in Klammern: Standort Wetterstation, sofern nicht Hauptstadt)	Mittlere Lufttemperatur [2]			Mittlere tägliche Sonnenscheindauer [2]			Mittlerer Niederschlag [2]		
			Jahresdurchschnittswert	des kältesten Monats	des wärmsten Monats	Jahresdurchschnittswert	des Monats mit der niedrigsten Sonnenscheindauer	des Monats mit der höchsten Sonnenscheindauer	durchschnittlicher Jahresgesamtwert	des nassesten Monats	des trockensten Monats
	2016		Referenzperiode 1996 bis 2010								
	km²		°C			Stunden			l/m²		
Afrika											
Ägypten	995 450	Kairo	22,3	13,9 Jan	29,1 Jul, Aug	9,5	7,1 Jan	11,6 Jul	23	6 Dez	0 Jun–Sep
Äthiopien	1 000 000	Addis Abeba	17,0	15,5 Dez	18,9 Mai	7,3	3,8 Jul	10,0 Dez	1 225	294 Aug	12 Dez
Kenia	569 140	Nairobi	19,7	17,4 Jul	21,5 Mrz	6,5	3,6 Jul	9,5 Feb	749	140 Nov	10 Aug
Kongo, Dem. Republik	2 267 050	Kinshasa	25,3	23,5 Jul	26,5 Mrz	.	.	.	1 365	220 Apr	‹ 1 Aug
Nigeria	910 770	Abuja (Lagos)	27,3	25,6 Aug	29,4 Mrz	.	.	.	1 574	314 Jun	5 Jan
Südafrika	1 213 090	Pretoria	18,9	11,9 Jul	22,9 Dez–Feb	8,6	7,8 Jan	9,4 Aug	684	134 Jan	1 Jul
Tansania, Ver. Republik	885 800	Dodoma	22,9	20,1 Jul	24,8 Nov	9,1	7,7 Feb	10,2 Okt	587	154 Dez	0 Jul, Aug
Amerika											
Argentinien	2 736 690	Buenos Aires	17,9	11,5 Jul	24,2 Jan	7,0	4,4 Jun	9,6 Jan	1 053	151 Jan	42 Jun
Brasilien	8 358 140	Brasília	21,4	19,3 Jun	23,0 Okt	6,7	4,4 Dez	9,0 Aug	1 482	246 Dez	2 Jul
Chile	743 532	Santiago de Chile	14,8	8,5 Jul	21,4 Jan	7,0	3,5 Jun	10,6 Jan	342	97 Jun	‹ 1 Dez
Kanada	9 093 510	Ottawa (Montreal)	7,3	– 9,0 Jan	21,4 Jul	5,9	2,4 Dez	8,7 Jul	1 020	99 Okt	62 Feb
Kolumbien	1 109 500	Bogotá	13,3	12,9 Jan	13,7 Apr, Mai	4,2	3,3 Apr, Mai	5,6 Jan	901	119 Mai	33 Jan
Mexiko	1 943 950	Mexiko-Stadt	17,1	14,4 Dez	19,6 Mai	7,0	4,7 Sep	8,6 Apr	803	190 Aug	3 Feb
Vereinigte Staaten	9 147 420	Washington, D.C.	14,6	2,6 Jan	26,2 Jul	.	.	.	1 046	118 Jun	63 Feb
Asien											
Bangladesch	130 170	Dhaka	26,0	18,6 Jan	29,2 Mai	.	.	.	2 101	417 Jul	4 Dez
China	9 424 700	Peking	13,1	– 3,0 Jan	27,2 Jul	6,7	5,5 Dez	8,5 Mai	470	128 Jul	2 Dez
Indien	2 973 190	New-Delhi	25,3	13,8 Jan	32,8 Jun	5,8	3,8 Dez	7,9 Apr	785	212 Aug	5 Nov
Indonesien	1 811 570	Jakarta	27,5	26,8 Feb	27,9 Mai	.	.	.	1 743	374 Feb	30 Dez
Iran, Islamische Republik	1 628 760	Teheran	18,5	4,6 Jan	31,1 Jul	8,2	5,1 Dez	11,1 Jun	239	40 Mrz	1 Aug
Israel	21 640	Jerusalem (Tel Aviv)	20,9	13,5 Jan	27,9 Aug	.	.	.	498	145 Jan	0 Jul, Aug
Japan	364 560	Tokio	16,6	6,4 Jan	27,5 Aug	5,2	4,2 Jun	6,2 Jan	1 582	221 Okt	52 Feb
Korea, Republik	97 489	Seoul	12,9	– 1,9 Jan	25,8 Aug	5,3	3,3 Jul	6,4 Mai	1 550	424 Jul	18 Dez
Malaysia	328 550	Kuala Lumpur	27,7	27,1 Dez	28,6 Mai	.	.	.	2 805	339 Nov	136 Jun
Myanmar	653 080	Naypyidaw (Rangoon)	27,1	24,6 Jan	30,4 Apr	.	.	.	.	.	.
Pakistan	770 880	Islamabad	22,3	10,6 Jan	31,4 Jun	.	.	.	1 179	283 Aug	14 Nov
Philippinen	298 170	Manila	27,5	25,7 Jan	29,3 Mai	.	.	.	2 631	505 Sep	19 Feb
Saudi-Arabien	2 149 690	Riad	26,3	13,8 Jan	36,3 Aug	8,7	7,1 Jan	10,5 Jul	125	28 Apr	0 Jun, Jul
Thailand	510 890	Bangkok	29,0	27,4 Dez	30,8 Apr	6,5	4,6 Sep	8,3 Feb	1 706	326 Sep	9 Dez
Ver. Arab. Emirate	71 020	Abu Dhabi	28,1	18,9 Jan	35,9 Aug	9,7	8,1 Dez	11,3 Jun	47	12 Jan	0 Jun–Sep
Vietnam	310 070	Hanoi	24,5	17,4 Jan	29,8 Jun, Jul	3,6	1,4 Mrz	5,4 Jun	1 639	317 Jul	19 Jan
Australien und Ozeanien											
Australien	7 692 020	Canberra	13,4	5,8 Jul	20,9 Jan	8,0	5,6 Jun	9,8 Dez	582	68 Nov	27 Apr
Neuseeland	263 310	Wellington (N. Plymouth)	13,8	9,9 Jul	18,3 Feb	5,8	4,5 Mai, Jun	7,5 Jan	1 368	147 Jun	71 Mrz

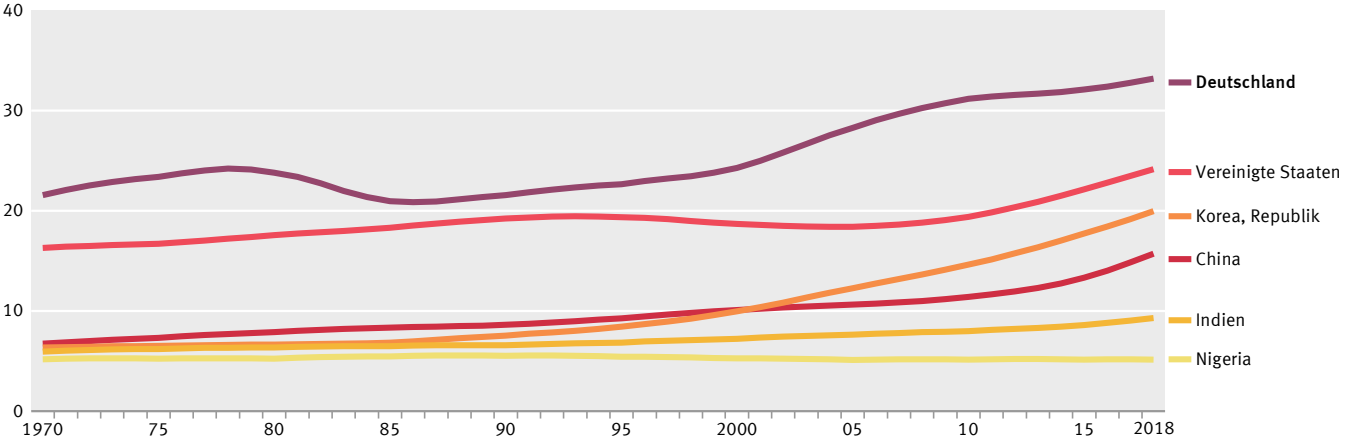
1 Quelle: Welternährungsorganisation (FAO), Vereinte Nationen.
2 Quelle: Deutscher Wetterdienst (DWD).

A.2 Bevölkerung

	Bevölkerung insgesamt [1]	Überschuss der Geborenen (+) bzw. Gestorbenen (–) [1]	Überschuss der Zuzüge (+) bzw. Fortzüge (–) [1]	Bevölkerungszunahme (+) bzw. -abnahme (–) [1]	Bevölkerungsvorausberechnung [2]	Lebenserwartung bei Geburt [3]		Zusammengefasste Geburtenziffer [3]	Asylbewerber/-innen [1]	
						Frauen	Männer		Personen	Anteil der unter 18-Jährigen [4]
	2018				2050	2017			2018	
	1 000					Jahre		Kinder je Frau	Anzahl	%
Europa										
Europäische Union	512 379	– 354	+ 1 457	+ 1 102	496 796 [5]	83,8	78,4	*1,59*	646 385	*30,6*
Belgien	11 399	+ 8	+ 62	+ 69	12 221	84,0	79,0	*1,68*	22 565	*29,3*
Bulgarien	7 050	– 46	– 4	– 50	5 385	78,5	71,3	*1,54*	2 535	*33,3*
Dänemark	5 781	+ 6	+ 19	+ 25	6 245	82,9	79,2	*1,79*	3 600	*30,8*
Deutschland	**82 792**	**– 167**	**+ 394**	**+ 227**	**80 104**	**83,5**	**78,6**	***1,57***	**184 235**	***46,1***
Estland	1 319	– 1	+ 7	+ 6	1 158	82,2	73,3	*1,60*	95	*21,1*
Finnland	5 513	– 7	+ 12	+ 5	5 486	84,4	78,6	*1,57*	4 515	*24,8*
Frankreich	66 926	144	– 43	+ 102	67 587	85,7	79,5	*1,92*	120 425	*20,1*
Griechenland	10 741	– 34	+ 15	– 19	9 029	84,0	78,9	*1,38*	66 975	*32,5*
Irland	4 830	+ 30	+ 44	+ 74	5 678	83,8	80,2	*1,81*	3 670	*23,3*
Island	348	+ 2	+ 7	+ 9	377	84,1	80,4	*1,74*	775	*23,2*
Italien	60 484	– 193	+ 69	– 124	54 382	85,6	81,0	*1,34*	59 950	*17,0*
Kroatien	4 105	– 16	– 13	– 29	3 365	80,9	74,9	*1,42*	800	*28,1*
Lettland	1 934	– 10	– 5	– 14	1 479	79,7	69,9	*1,74*	185	*21,6*
Litauen	2 809	– 11	– 3	– 15	2 121	80,1	69,5	*1,69*	405	*30,9*
Luxemburg	602	+ 2	+ 10	+ 12	790	85,4	80,1	*1,41*	2 335	*26,3*
Malta	476	+ 1	+ 17	+ 18	427	84,4	80,6	*1,37*	2 130	*21,6*
Niederlande	17 181	+ 15	+ 86	+ 101	17 165	83,2	80,0	*1,66*	24 025	*22,9*
Norwegen	5 296	.	.	.	6 600	84,2	80,9	*1,71*	2 685	*30,0*
Österreich	8 822	+ 2	+ 35	+ 37	9 131	84,1	79,3	*1,53*	13 745	*49,1*
Polen	37 977	– 26	+ 22	– 4	33 295	82,0	73,9	*1,39*	4 115	*45,4*
Portugal	10 291	– 26	+ 12	– 14	9 085	84,3	78,1	*1,36*	1 285	*23,7*
Rumänien	19 531	– 75	– 54	– 129	16 260	79,1	71,7	*1,64*	2 135	*25,8*
Russische Föderation	144 478 [3]	.	.	.	135 824	77,4	67,1	*1,76*	.	.
Schweden	10 120	+ 24	+ 86	+ 110	11 389	84,1	80,6	*1,85*	21 600	*29,6*
Schweiz	8 484	+ 19	+ 40	+ 58	9 818	85,6	81,7	*1,54*	15 235	*41,1*
Slowakei	5 443	+ 3	+ 4	+ 7	4 984	80,7	73,8	*1,48*	175	*25,7*
Slowenien	2 067	– 1	+ 15	+ 14	1 940	84,3	78,2	*1,58*	2 875	*27,7*
Spanien	46 658	– 56	+ 332	+ 276	43 637	86,3	80,5	*1,34*	54 060	*20,8*
Tschechische Republik	10 610	+ 1	+ 39	+ 40	10 546	82,6	76,5	*1,63*	1 700	*15,9*
Türkei	80 811	+ 823	+ 371	+ 1 193	97 140	79,2	72,8	*2,03*	.	.
Ungarn	9 778	– 38	+ 32	– 6	8 470	79,7	72,6	*1,53*	670	*53,7*
Vereinigtes Königreich	66 274	+ 115	+ 258	+ 374	74 082	83,0	79,4	*1,79*	37 805	*24,3*
Zypern	864	+ 4	+ 8	+ 12	1 355	82,8	78,5	*1,34*	7 765	*14,1*

Altenquotient

Zahl der Personen im Alter ab 65 Jahren je 100 Personen im erwerbsfähigen Alter (15 – 64 Jahre)



Quelle: World Development Indicators, Weltbank

2019 - 01 - 0309

A.2 Bevölkerung

	Bevölkerung insgesamt [1]	Bevölkerungsvorausberechnung [2]	Lebenserwartung bei Geburt [3]		Zusammengefasste Geburtenziffer [3]
			Frauen	Männer	
	2018	2050	2017		
	1 000		Jahre		Kinder je Frau
Afrika					
Ägypten	98 424	159 957	74,0	69,5	*3,21*
Äthiopien	109 225	205 411	67,8	64,0	*4,08*
Kenia	51 393	91 575	69,7	64,9	*3,79*
Kongo, Dem. Republik	84 068	194 489	61,5	58,5	*6,02*
Nigeria	195 875	401 315	54,7	53,1	*5,46*
Südafrika	57 780	75 518	67,0	59,9	*2,43*
Tansania, Ver. Republik	56 318	129 387	68,1	64,6	*4,95*
Amerika					
Argentinien	44 495	54 867	80,4	73,0	*2,28*
Brasilien	209 469	228 980	79,3	72,1	*1,71*
Chile	18 729	20 319	82,1	77,2	*1,77*
Kanada	37 059	45 669	84,4	80,7	*1,50*
Kolumbien	49 649	55 958	78,2	71,0	*1,83*
Mexiko	126 191	155 151	79,7	74,9	*2,15*
Vereinigte Staaten	327 167	379 419	81,1	76,1	*1,77*
Asien					
Bangladesch	161 356	192 568	74,6	71,2	*2,08*
China	1 392 730	1 402 405	78,0	74,9	*1,63*
Indien	1 352 617	1 639 176	70,4	67,3	*2,30*
Indonesien	267 663	330 905	71,6	67,3	*2,34*
Iran, Islamische Republik	81 800	103 098	77,3	75,1	*1,64*
Israel	8 884	12 720	84,6	80,7	*3,11*
Japan	126 529	105 804	87,3	81,1	*1,43*
Korea, Republik	51 635	46 830	85,7	79,7	*1,05*
Malaysia	31 529	40 550	77,9	73,3	*2,02*
Myanmar	53 708	62 253	69,1	64,4	*2,19*
Pakistan	212 215	338 013	67,7	65,6	*3,41*
Philippinen	106 652	144 488	72,8	65,9	*2,89*
Saudi-Arabien	33 700	44 562	76,5	73,4	*2,49*
Thailand	69 429	65 940	79,3	71,8	*1,47*
Ver. Arab. Emirate	9 631	10 425	78,9	76,7	*1,73*
Vietnam	95 540	109 605	81,0	71,8	*1,95*
Australien und Ozeanien					
Australien	24 992	32 814	84,7	80,4	*1,77*
Neuseeland	4 886	5 608	83,4	80,0	*1,81*

1 Quelle: Statistisches Amt der Europäischen Union (Eurostat).
2 Quelle: World Population Prospects – The 2019 Revision, Vereinte Nationen (Population Division, UN DESA). Mittlere Variante.
3 Quelle: World Development Indicators, Weltbank.
4 Eigene Berechnungen basierend auf Eurostat Daten.
5 Eigene Berechnungen basierend auf UN DESA Daten.

Bevölkerungsvorausberechnungen liefern Erkenntnisse darüber, wie sich die Bevölkerungszahl entwickeln würde, wenn bestimmte Annahmen zur künftigen Entwicklung der Geburtenhäufigkeit, der Lebenserwartung sowie der Migration einträfen. Die Vereinten Nationen (UN) berechnen hierzu verschiedene Varianten. Die vorliegenden Daten entsprechen der mittleren Variante der UN-Bevölkerungsvorausberechnung. Weitere Informationen unter *population.un.org/wpp*

Die **zusammengefasste Geburtenziffer** eines Kalenderjahres ist ein Maß dafür, wie viele Kinder durchschnittlich je Frau zur Welt kamen. Sie charakterisiert das Geburtenverhalten der Frauen im jeweiligen Kalenderjahr. Die zusammengefasste Geburtenziffer wird auch als durchschnittliche Kinderzahl beschrieben, die eine Frau im Laufe ihres Lebens gebären würde, wenn die altersspezifischen Geburtenziffern, die im betrachteten Kalenderjahr nachgewiesen wurden, von ihrem 16. bis zu ihrem 50. Lebensjahr (Alter 15 bis 49) gelten würden. Die altersspezifische Geburtenziffer zeigt für jedes einzelne Altersjahr zwischen 15 und 49 Jahren die Relation zwischen der Zahl der von Müttern eines bestimmten Alters geborenen Kinder und der Gesamtzahl der Frauen dieses Alters. Durch die Addition der altersspezifischen Geburtenziffern ergibt sich die zusammengefasste Geburtenziffer.

A.3 Bildung

	Schüler/-innen je Lehrkraft (Sekundarstufe) [1]	Anteil der 20- bis 24-Jährigen ohne Erwerbstätigkeit und nicht in Ausbildung [2]	PISA-Studie: Vergleich der Schülerleistungen im Bereich [3]			Studierende und Schüler/-innen an Einrichtungen des Tertiärbereichs		Anteil der 25- bis 34-Jährigen mit tertiärem Bildungsabschluss [3]	Öffentliche Bildungsausgaben [1]	Bruttoinlandsausgaben für Forschung und Entwicklung [1]
			Mathematik	Naturwissenschaften	Lesekompetenz					
	2016	2018	2015			2016		2017	2015	2017
	Anzahl	%	Durchschnittliche Punktzahl			je 100 000 Einwohner/-innen [4]	Frauenanteil, in % [1]	%	% des BIP	
Europa										
Europäische Union	.	*15*	.	.	.	.	.	.	.	.
Belgien	*9*	*14*	507	502	499	*4 485*	*56*	*46*	*6,6*	*2,6*
Bulgarien	13	*18*	441	446	432	*3 742*	*54*	.	*4,1* [5]	*0,8*
Dänemark	11 [6]	*10*	511	502	500	*5 496*	*56*	*47*	*7,6* [6]	*3,1*
Deutschland	**12**	***9***	**506**	**509**	**509**	***3 695***	***48***	***31***	***4,8***	***3,0***
Estland	*9*	*12*	520	534	519	*3 883*	*59*	*43*	*5,2*	*1,3*
Finnland	13	*12*	511	531	526	*5 408*	*53*	*41*	*7,1*	*2,8*
Frankreich	13 [5]	*17*	493	495	499	*3 710*	*54*	*44*	*5,5*	*2,2*
Griechenland	8	*21*	454	455	467	*6 584*	*49*	*43*	.	*1,1*
Irland	.	*13*	504	503	521	*4 593*	*52*	*54*	*3,8*	*1,0*
Island	.	*6*	488	473	482	*5 542*	*64*	*47*	*7,7*	*2,2*
Italien	10	*27*	490	481	485	*2 995*	*56*	*27*	*4,1*	*1,4*
Kroatien	*7*	*18*	464	475	487	*3 881*	*57*	.	*4,6* [5]	*0,9*
Lettland	*8*	*13*	482	490	488	*4 301*	*59*	*42*	*5,3*	*0,5*
Litauen	*8*	*13*	478	475	472	*4 663*	*57*	*56*	*4,2*	*0,9*
Luxemburg	*9*	*8*	486	483	481	*1 195*	*51*	*51*	*3,9*	*1,3*
Malta	*7*	*8*	479	465	447	*2 927*	*56*	.	*5,3*	*0,5*
Niederlande	14	*6*	512	509	503	*4 914*	*52*	*47*	*5,4*	*2,0*
Norwegen	*9*	*7*	502	498	513	*5 300*	*58*	*48*	*7,6*	*2,1*
Österreich	*9*	*9*	497	495	485	*4 935*	*53*	*40*	*5,5*	*3,2*
Polen	*9*	*14*	504	501	506	*4 214*	*59*	*44*	*4,8*	*1,0*
Portugal	10	*13*	492	501	498	*3 323*	*53*	*34*	*4,9*	*1,3*
Rumänien	12	*20*	444	435	434	*2 717*	*54*	.	*3,1*	*0,5*
Russische Föderation	.	.	494	487	495	*4 283*	*53*	*60* [7]	*3,8*	*1,1*
Schweden	13	*9*	494	493	500	*4 295*	*59*	*47*	*7,6*	*3,3*
Schweiz	10	*7*	521	506	492	*3 525*	*50*	*50*	*5,1*	*3,4* [7]
Slowakei	11 [7]	*14*	475	461	453	*3 080*	*59*	*35*	*4,6*	*0,9*
Slowenien	10	*10*	510	513	505	*3 913*	*58*	*45*	*4,9*	*1,9*
Spanien	12	*18*	486	493	496	*4 235*	*53*	*43*	*4,3*	*1,2*
Tschechische Republik	12 [5]	*9*	492	493	487	*3 520*	*57*	*34*	*5,8*	*1,8*
Türkei	18 [7]	*32*	420	425	428	*8 413*	*46*	*32*	*4,3*	*1,0*
Ungarn	10	*15*	477	477	470	*3 009*	*54*	*30*	*4,6*	*1,4*
Vereinigtes Königreich	19	*14*	492	509	498	*3 639*	*56*	*52*	*5,6*	*1,7*
Zypern	10 [7]	*18*	437	433	443	*3 201* [7]	*57* [7]	.	*6,4*	*0,6*

A.3 Bildung

	Schüler/-innen je Lehrkraft (Sekundarstufe) [1]	PISA-Studie: Vergleich der Schülerleistungen im Bereich [3]			Studierende und Schüler/-innen an Einrichtungen des Tertiärbereichs		Öffentliche Bildungsausgaben [1]	Bruttoinlandsausgaben für Forschung und Entwicklung [1]
		Mathematik	Naturwissenschaften	Lesekompetenz				
	2016	2015			2016		2015	2017
	Anzahl	Durchschnittliche Punktzahl			je 100 000 Einwohner/-innen [4]	Frauenanteil in % [1]	% des BIP	
Afrika								
Ägypten	15	.	.	.	*2 915*	*50*	.	*0,6*
Äthiopien	.	.	.	.	*778* [6]	*32* [6]	*4,7*	*0,6* [5]
Kenia	.	.	.	.	*1 114*	*41*	*5,3*	.
Kongo, Dem. Republik	14 [7]	.	.	.	*590*	*36*	*2,2*	*0,4* [7]
Nigeria	.	.	.	.	.	.	.	.
Südafrika	27	.	.	.	*1 881*	*58*	*6,0*	*0,8* [8]
Tansania, Ver. Republik	.	.	.	.	*321*	*37*	*3,5* [6]	*0,5* [5]
Amerika								.
Argentinien	.	.	.	.	*6 981*	*62*	*5,8*	*0,5* [8]
Brasilien	17	377	401	407	*4 006*	*57*	*6,2*	*1,3* [8]
Chile	19 [7]	423	447	459	*6 905*	*52*	*4,9*	*0,4* [8]
Kanada	.	516	528	527	*4 394*	*56*	.	*1,6*
Kolumbien	26	390	416	425	*4 921*	*53*	*4,5*	*0,2*
Mexiko	16	408	416	423	*3 328*	*50*	*5,2*	*0,5* [8]
Vereinigte Staaten	15 [7]	470	496	497	*5 970*	*56*	*5,0* [6]	*2,8*
Asien								.
Bangladesch	36	.	.	.	*1 657*	*40*	*2,0* [5]	.
China	13	.	.	.	*3 183*	*52*	.	*2,1*
Indien	28	.	.	.	*2 446*	*48*	*3,8* [5]	*0,6* [7]
Indonesien	14	386	403	397	*2 352*	*52*	*3,6*	*0,2*
Iran, Islamische Republik	19	.	.	.	*5 417*	*46*	*2,8*	*0,3* [5]
Israel	12 [6]	470	467	479	*4 421*	*57*	*5,9*	*4,6*
Japan	11	532	538	516	*3 029*	*48*	*3,6* [6]	*3,2*
Korea, Republik	14	524	516	517	*6 253*	*41*	*5,3*	*4,6*
Myanmar	13	.	.	.	*4 286*	*53*	*5,0*	*1,4* [8]
Malaysia	24	.	.	.	.	.	.	.
Pakistan	21	.	.	.	*961*	*45*	*2,7*	*0,2*
Philippinen	24	.	.	.	*3 560* [6]	*55* [6]	.	*0,1* [5]
Saudi-Arabien	11 [6]	.	.	.	*5 027*	*49*	.	*0,8* [5]
Thailand	27	415	421	409	*3 501*	*58*	*4,1* [5]	*0,8* [8]
Ver. Arab. Emirate	10	427	437	434	*1 721*	*55*	.	*1,0* [8]
Vietnam	.	495	525	487	*2 440*	*54*	*5,7* [5]	*0,5*
Australien und Ozeanien								
Australien	.	494	510	503	*7 931*	*58*	*5,3*	*1,9* [7]
Neuseeland	14	495	513	509	*5 784*	*57*	*6,3*	*1,2* [7]

1 Quelle: Organisation der Vereinten Nationen für Bildung, Wissenschaft und Kultur (UNESCO), teilweise Schätzungen bzw. vorläufige Daten.
2 Quelle: Eurostat.
3 Quelle: Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD).
4 Eigene Berechnungen basierend auf UNESCO und Weltbank Daten.
5 2013.
6 2014.
7 2015.
8 2016.

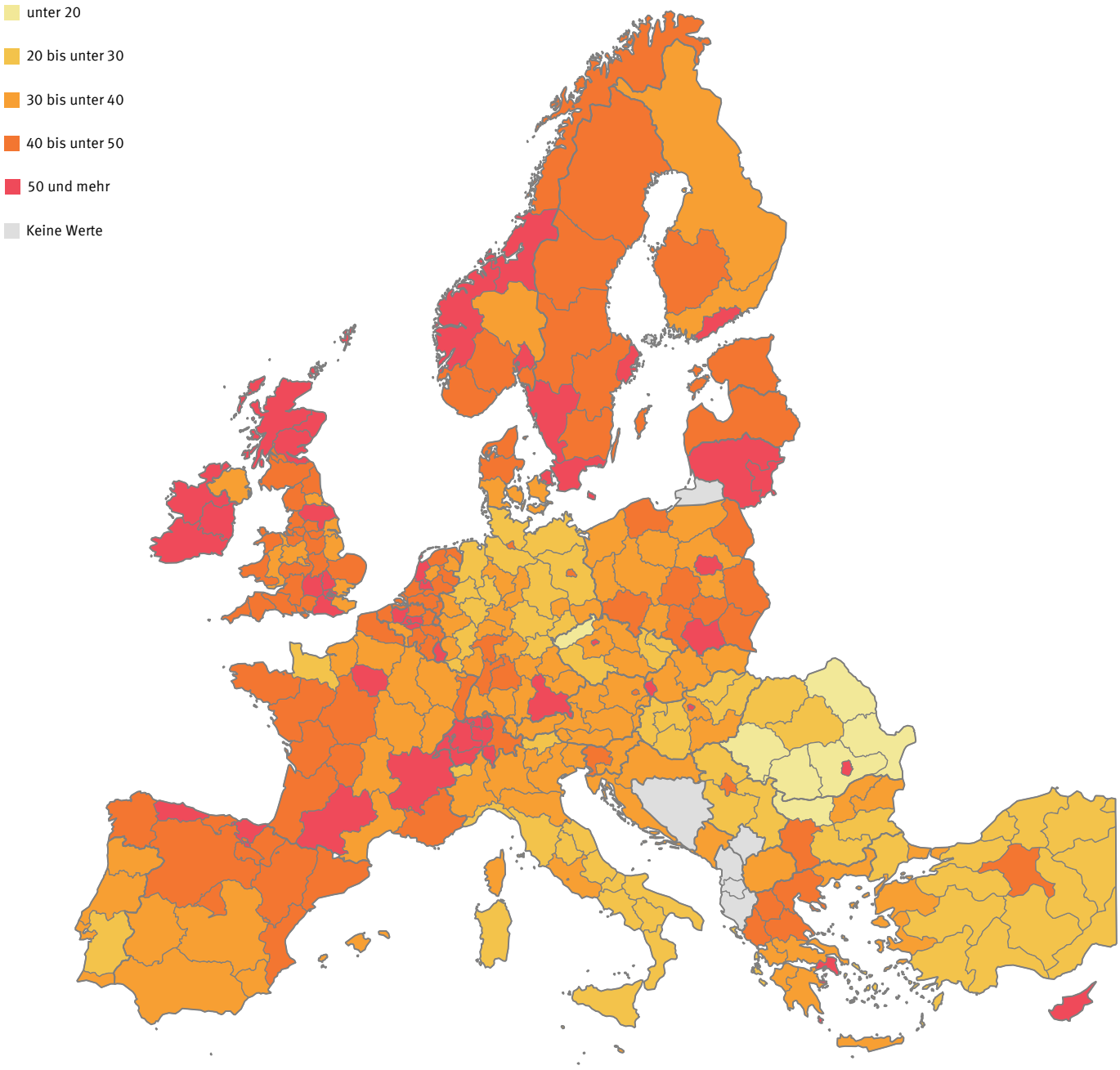
Der **Anteil junger Erwachsener ohne Erwerbstätigkeit und nicht in Aus- oder Fortbildung** wird international auch als NEET-Rate (Not in Education, Employment or Training) bezeichnet.

Das **Programme for International Student Assessment (PISA)** ist die internationale Schulleistungsstudie der OECD. An der 2015 durchgeführten Studie nahmen insgesamt 540 000 Schülerinnen und Schüler in 72 Ländern teil. Der OECD-Durchschnittswert liegt in jedem Kompetenzbereich (bzw. Fach) bei 500 Punkten, die Standardabweichung bei 100 Punkten.

Bei den **Studierenden und Schüler/-innen an Einrichtungen des Tertiärbereichs** werden die Bildungsstufen ISCED 5 (z. B. berufsspezifische tertiäre Bildung), ISECD 6 (Bachelor und vergleichbare Abschlüsse), ISCED 7 (Master und vergleichbare Abschlüsse) und ISCED 8 (Promotion und vergleichbare Abschlüsse) berücksichtigt. ISCED ist die Internationale Standardklassifikation für das Bildungswesen.

Die **Bruttoinlandsausgaben für Forschung und Entwicklung** umfassen alle zur Durchführung von Forschung und Entwicklung (FuE) im Inland verwendeten Mittel, ungeachtet der Finanzierungsquellen. Eingeschlossen sind auch Mittel aus dem Ausland sowie Mittel internationaler Organisationen für im Inland durchgeführte Forschungsarbeiten.

Anteil der 30- bis 34-Jährigen mit tertiärem Bildungsabschluss nach Regionen (NUTS-2-Ebene) 2018
in %

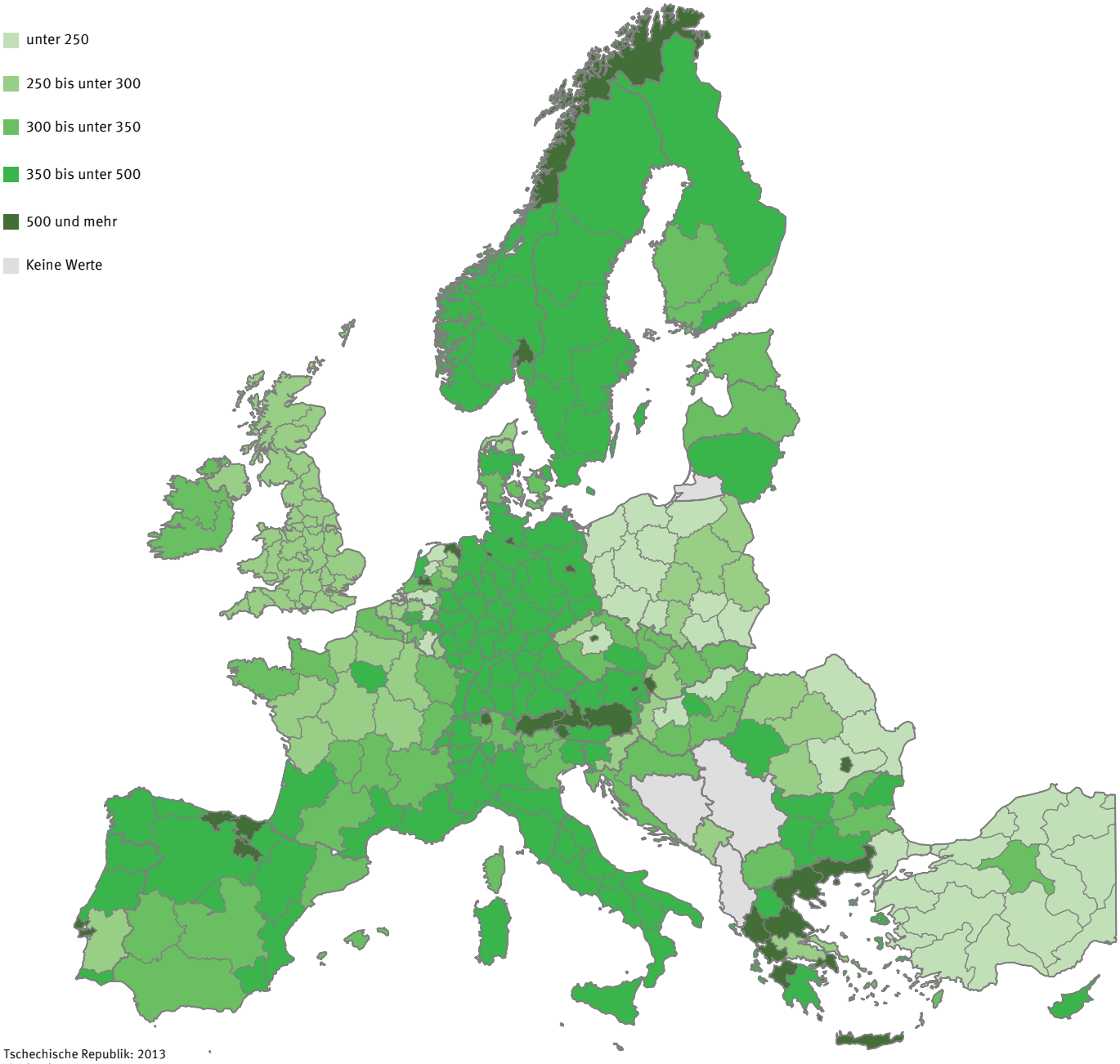


Kartengrundlage: © EuroGeographics bezüglich der Verwaltungsgrenzen
Quelle: Eurostat

2019 - 01 - 0310

A.4 Gesundheit

Praktizierende Ärztinnen und Ärzte nach Regionen (NUTS-2-Ebene) 2016
je 100 000 Einwohner/-innen



Tschechische Republik: 2013
Finnland: 2014
Dänemark und Schweden: 2015
Daten für Deutschland beziehen sich auf die NUTS-1-Ebene (Bundesländer).
Daten für Irland und das Vereinigte Königreich sind nicht regional aufschlüsselbar.

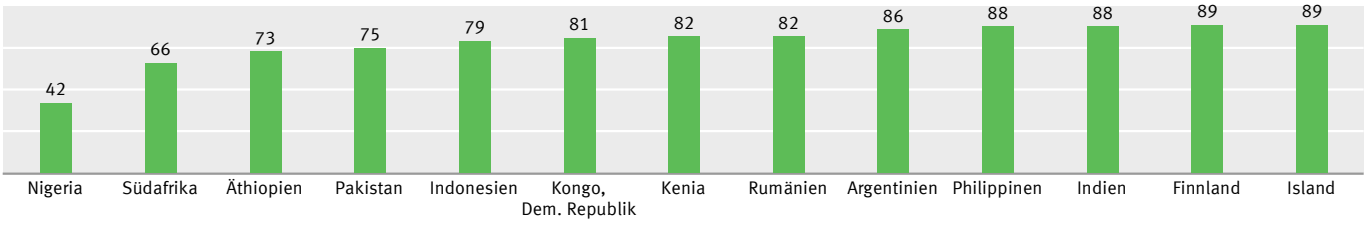
Quelle: Eurostat

2019 - 01 - 0311

A.4 Gesundheit

	Gesamtausgaben für Gesundheit [1]		Praktizierende Ärztinnen/ Ärzte [2]	Krankenhaus-betten [2]	Tuberkulose-neu-erkrankungen [2]	Sterbefälle von Kindern unter 5 Jahren [3]	Suizide [4]	Alkohol-konsum: Liter reiner Alkohol [5]	Anteil der Erwachsenen mit Adipositas (Body Mass Index > 30) [2]	Anteil der Erwachsenen mit erhöhtem Blutdruck [2]
	2015		2014 – 2018 [6]	2012 – 2015 [6]	2017		2016			2015
	% des BIP	US$ je Einwohner/-in	je 10 000 Einwohner/-innen		je 100 000 Einwohner/-innen	je 1 000 Lebend-geborene	je 100 000 Einwohner/-innen	je Einwohner/-in ab 15 Jahren	%	
Europa										
Europäische Union	.	.	.	.	.	.	.	.	.	.
Belgien	10,5	4 228	33	62	9	4	20,7	12,1	22,1	17,5
Bulgarien	8,2	572	40	68	25	8	11,5	12,7	25,0	28,4
Dänemark	10,3	5 497	45	25	5	4	12,8	10,4	19,7	20,6
Deutschland	**11,2**	**4 592**	**42**	**83**	**8**	**4**	**13,6**	**13,4**	**22,3**	**19,9**
Estland	6,5	1 112	35	50	15	3	17,8	11,6	21,2	27,4
Finnland	9,4	4 005	38	44	5	2	15,9	10,7	22,2	19,4
Frankreich	11,1	4 026	32	65	9	4	17,7	12,6	21,6	22,0
Griechenland	8,4	1 505	46	43	5	5	5,0	10,4	24,9	19,1
Irland	7,8	4 757	31	28	7	4	11,5	13,0	25,3	19,7
Island	8,6	4 375	40	32	5	2	14,0	9,1	21,9	19,7
Italien	9,0	2 700	41	34	7	3	8,2	7,5	19,9	21,2
Kroatien	7,4	852	30	56	10	5	16,5	8,9	24,4	32,4
Lettland	5,8	784	32	58	32	4	21,2	12,9	23,6	29,4
Litauen	6,5	923	43	73	50	4	31,9	15,0	26,3	29,3
Luxemburg	6,0	6 236	30	48	6	3	13,5	13,0	22,6	21,9
Malta	9,6	2 304	38	47	11	6	7,5	8,1	28,9	19,4
Niederlande	10,7	4 746	35	.	5	4	12,6	8,7	20,4	18,7
Norwegen	10,0	7 464	46	39	5	3	12,2	7,5	23,1	19,7
Österreich	10,3	4 536	51	76	7	4	15,6	11,6	20,1	21,0
Polen	6,3	797	24	65	17	5	16,2	11,6	23,1	28,7
Portugal	9,0	1 722	33	34	20	4	14,0	12,3	20,8	24,4
Rumänien	5,0	442	23	63	72	8	10,4	12,6	22,5	30,0
Russische Föderation	5,6	524	40	82	60	8	31,0	11,7	23,1	27,2
Schweden	11,0	5 600	54	26	6	3	14,8	9,2	20,6	19,3
Schweiz	12,1	9 818	42	47	7	4	17,2	11,5	19,5	18,0
Slowakei	6,9	1 108	25	58	5	6	12,8	11,5	20,5	28,5
Slowenien	8,5	1 772	30	46	6	2	18,6	12,6	20,2	30,5
Spanien	9,2	2 354	41	30	11	3	8,7	10,0	23,8	19,2
Tschechische Republik	7,3	1 284	43	65	5	3	13,1	14,4	26,0	27,9
Türkei	4,1	455	18	27	17	12	7,3	2,0	32,1	20,3
Ungarn	7,2	894	32	70	8	5	19,1	11,4	26,4	30,0
Vereinigtes Königreich	9,9	4 356	28	28	9	4	8,9	11,4	27,8	15,2
Zypern	6,8	1 563	20	34	5	3	5,3	10,8	21,8	19,8

Impfung gegen Diphtherie, Tetanus und Keuchhusten (DTP3) 2017
Impfrate von einjährigen Kindern in ausgewählten Ländern, in %



Quelle: Global Health Observatory (GHO), Weltgesundheitsorganisation (WHO)

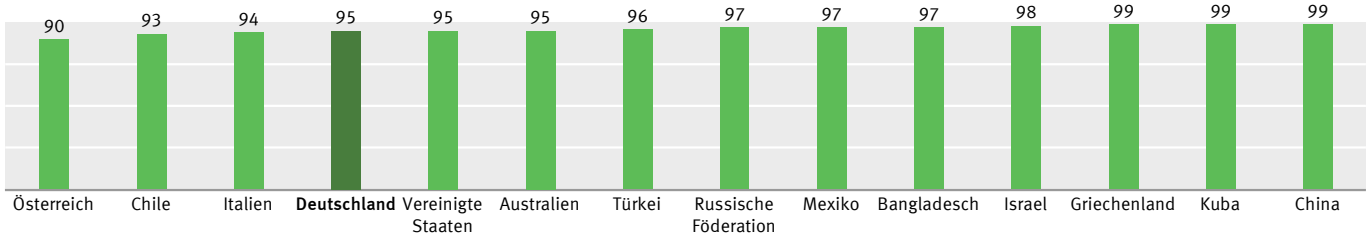
2019 - 01 - 0312

A.4 Gesundheit

	Gesamtausgaben für Gesundheit [1]		Praktizierende Ärztinnen/ Ärzte [2]	Krankenhaus-betten [2]	Tuberkulose-neu-erkrankungen [2]	Sterbefälle von Kindern unter 5 Jahren [3]	Suizide [4]	Alkohol-konsum: Liter reiner Alkohol [5]	Anteil der Erwachsenen mit Adipositas (Body Mass Index > 30) [2]	Anteil der Erwachsenen mit erhöhtem Blutdruck [2]
	2015		2014 – 2018 [6]	2012 – 2015 [6]	2017		2016			2015
	% des BIP	US$ je Einwohner/-in	je 10 000 Einwohner/-innen		je 100 000 Einwohner/-innen	je 1 000 Lebend-geborene	je 100 000 Einwohner/-innen	je Einwohner/-in ab 15 Jahren	%	
Afrika										
Ägypten	4,2	157	8	16	13	22	4,0	0,4	32,0	25,0
Äthiopien	4,0	24	1	3	164	59	7,2	2,8	4,5	30,3
Kenia	5,2	70	2	.	319	46	3,2	3,4	7,1	26,7
Kongo, Dem. Republik	4,3	20	.	.	322	91	5,9	7,8	6,7	28,5
Nigeria	3,6	97	.	.	219	100	9,5	13,4	8,9	23,9
Südafrika	8,2	471	9	.	567	37	11,6	9,3	28,3	26,9
Tansania, Ver. Republik	6,1	32	0	.	269	54	5,4	9,4	8,4	27,3
Amerika										
Argentinien	6,8	998	40	50	26	10	9,2	9,8	28,3	22,6
Brasilien	8,9	780	21	22	44	15	6,5	7,8	22,1	23,3
Chile	8,1	1 102	11	22	17	7	10,6	9,3	28,0	20,9
Kanada	10,4	4 508	26	27	6	5	12,5	8,9	29,4	13,2
Kolumbien	6,2	374	21	15	33	15	7,2	5,8	22,3	19,2
Mexiko	5,9	535	22	15	22	13	5,1	6,5	28,9	19,7
Vereinigte Staaten	16,8	9 536	26	29	3	7	15,3	9,8	36,2	12,9
Asien										
Bangladesch	2,6	32	5	8	221	32	5,9	0,0	3,6	24,7
China	5,3	426	18	42	63	9	9,7	7,2	6,2	19,2
Indien	3,9	63	8	.	204	39	16,3	5,7	3,9	25,8
Indonesien	3,3	112	4	12	319	25	3,4	0,8	6,9	23,8
Iran, Islamische Republik	7,6	366	11	15	14	15	4,1	1,0	25,8	19,7
Israel	7,4	2 756	32	31	3	4	5,4	3,8	26,1	16,6
Japan	10,9	3 733	24	134	15	3	18,5	8,0	4,3	17,6
Korea, Republik	7,4	2 013	24	115	70	3	26,9	10,2	4,7	11,0
Malaysia	4,0	386	15	19	93	8	5,5	0,9	15,6	22,9
Myanmar	4,9	59	9	9	358	49	7,8	4,8	5,8	24,6
Pakistan	2,7	38	10	6	267	75	2,9	0,3	8,6	30,5
Philippinen	4,4	127	.	.	554	28	3,2	6,6	6,4	22,6
Saudi-Arabien	5,8	1 194	24	27	10	7	3,2	0,2	35,4	23,3
Thailand	3,8	217	8	.	156	10	14,4	8,3	10,0	22,3
Ver. Arabische Emirate	3,5	1 402	24	12	1	9	2,8	3,8	31,7	21,1
Vietnam	5,7	117	8	26	129	21	7,3	8,3	2,1	23,4
Australien und Ozeanien										
Australien	9,4	4 934	36	38	7	4	13,2	10,6	29,0	15,2
Neuseeland	9,3	3 554	30	28	8	5	12,1	10,7	30,8	16,2

1 Quelle: Global Health Expenditure Database, Weltgesundheitsorganisation (WHO).
2 Quelle: Global Health Observatory (GHO), Weltgesundheitsorganisation (WHO).
3 Quelle: Inter-agency Group for Child Mortality Estimation (UN-IGME), Vereinte Nationen.
4 Quelle: Global Health Estimates, Weltgesundheitsorganisation (WHO).
5 Quelle: Global Information System on Alcohol and Health (GISAH), Weltgesundheits-organisation (WHO).
6 Aktuellster verfügbarer Wert innerhalb des angegebenen Berichtszeitraums.

Impfung gegen Diphtherie, Tetanus und Keuchhusten (DTP3) 2017
Impfrate von einjährigen Kindern in ausgewählten Ländern, in %



Quelle: Global Health Observatory (GHO), Weltgesundheitsorganisation (WHO)

2019 - 01 - 0312

A.5 Wohnen

	Durchschnittliche Zahl der Personen je Privathaushalt	In Mieterhaushalten lebende Personen	In Eigentümerhaushalten lebende Personen	In überbelegten Wohneinheiten lebende Personen	Durch Wohnkosten überbelastete Personen
	2017				
	Anzahl	% der Wohnbevölkerung insgesamt			
Europa					
Europäische Union	2,3	*30,7*	*69,3*	*16*	*10*
Belgien	2,3	*27,3*	*72,7*	*5*	*9*
Bulgarien	2,4	*17,1*	*82,9*	*42*	*19*
Dänemark	2,0	*37,8*	*62,2*	*9*	*16*
Deutschland	**2,0**	***48,6***	***51,4***	***7***	***15***
Estland	2,2	*18,2*	*81,8*	*14*	*5*
Finnland	2,0	*28,6*	*71,4*	*6*	*4*
Frankreich	2,2	*35,6*	*64,4*	*8*	*5*
Griechenland	2,6	*26,7*	*73,3*	*29*	*40*
Irland	2,7	*30,5*	*69,5*	*3*	*5*
Island	2,4 |1	*21,3* |1	*78,7* |1	*7* |1	*6* |1
Italien	2,3	*27,6*	*72,4*	*27*	*8*
Kroatien	2,8	*9,5*	*90,5*	*40*	*6*
Lettland	2,3	*18,5*	*81,5*	*42*	*7*
Litauen	2,2	*10,3*	*89,7*	*24*	*7*
Luxemburg	2,5	*25,3*	*74,7*	*8*	*10*
Malta	2,5	*18,7*	*81,3*	*3*	*1*
Niederlande	2,2	*30,6*	*69,4*	*4*	*9*
Norwegen	1,9	*18,5*	*81,5*	*5*	*9*
Österreich	2,2	*45,0*	*55,0*	*15*	*7*
Polen	2,8	*15,8*	*84,2*	*41*	*7*
Portugal	2,5	*25,3*	*74,7*	*9*	*7*
Rumänien	2,6	*3,2*	*96,8*	*47*	*12*
Russische Föderation	.	.	.	.	.
Schweden	2,1	*34,8*	*65,2*	*14*	*8*
Schweiz	2,2	*58,7*	*41,3*	*7*	*13*
Slowakei	2,8	*9,9*	*90,1*	*36*	*8*
Slowenien	2,5	*24,4*	*75,6*	*13*	*5*
Spanien	2,5	*22,9*	*77,1*	*5*	*10*
Tschechische Republik	2,4	*21,5*	*78,5*	*16*	*9*
Türkei |1	3,4	*40,9*	*59,1*	*44*	*10*
Ungarn	2,3	*14,8*	*85,2*	*41*	*11*
Vereinigtes Königreich	2,3	*35,0*	*65,0*	*3*	*12*
Zypern	2,7	*29,3*	*70,7*	*3*	*3*

1 2016.

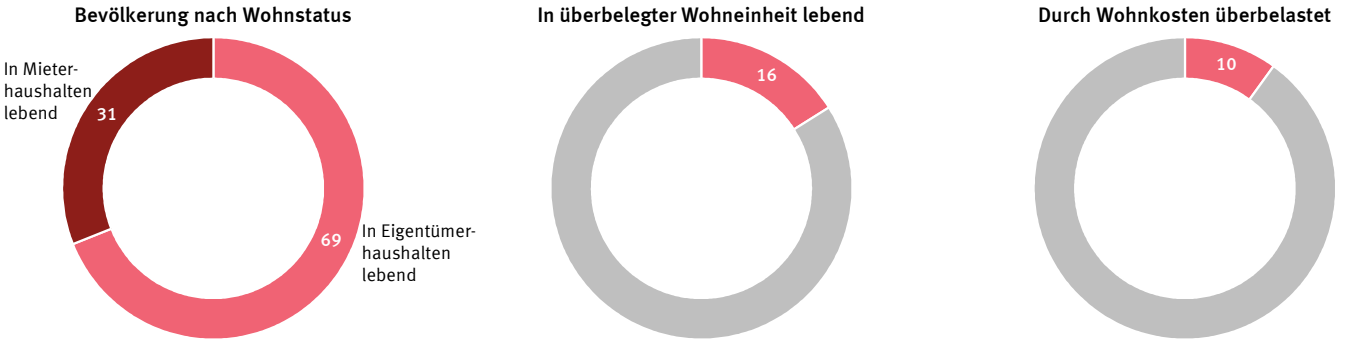
Quelle: LEBEN IN EUROPA (EU-SILC), Eurostat

Eine **Wohneinheit** gilt als **überbelegt**, wenn sie nicht mindestens folgende Kriterien erfüllt: ein Gemeinschaftszimmer, ein Zimmer je Paar im Haushalt, ein Zimmer für jede alleinstehende Person im Alter von 18 Jahren oder älter, ein Zimmer für bis zu zwei alleinstehende Personen desselben Geschlechts im Alter von 12 bis 17 Jahren, ein Zimmer je alleinstehende Person im Alter von 12 bis 17 Jahren (sofern nicht in der vorherigen Kategorie erfasst) sowie ein Zimmer für bis zu zwei Kinder unter 12 Jahren.

Personen gelten als **durch Wohnkosten überbelastet**, wenn sie in Haushalten leben, die mehr als 40 % ihres verfügbaren Einkommens für Wohnen aufwenden.

Wohnsituation in der Europäischen Union (EU-28) 2017

Anteil an der Wohnbevölkerung insgesamt, in %



Quelle: LEBEN IN EUROPA (EU-SILC), Eurostat

2019 - 01 - 0313

A.6 Einkommen, Konsum, Lebensbedingungen

	Median-äquivalenz-einkommen [1]	Armutsgefährdungs-grenze [1]		Armutsgefährdungsquote (nach Sozialtransfers) [1]			Konsum-ausgaben für Nahrungs-mittel und alkoholfreie Getränke [2]	Konsumaus-gaben für Wohnung, Wasser, Strom und Gas [2]
		Allein-lebende	Haushalte mit 2 Erwachse-nen und 2 Kindern unter 14 Jahren	insgesamt	Personen unter 18 Jahren	Personen ab 65 Jahren		
	2017							
	EUR			%			% der Konsumausgaben insgesamt	
Europa								
Europäische Union	16 909	.	.	*16,9*	*20,2*	*15,0*	*12,2*	*24,2*
Belgien	22 784	13 670	28 708	*15,9*	*18,6*	*16,0*	*13,4*	*24,2*
Bulgarien	3 590	2 154	4 524	*23,4*	*29,2*	*32,0*	*19,2*	*19,7*
Dänemark	29 383	17 630	37 023	*12,4*	*10,0*	*8,8*	*11,4*	*28,7*
Deutschland	**21 920**	**13 152**	**27 620**	***16,1***	***15,2***	***17,0***	***10,6***	***23,5***
Estland	9 384	5 631	11 824	*21,0*	*16,5*	*41,2*	*20,3*	*17,6*
Finnland	23 987	14 392	30 223	*11,5*	*10,2*	*12,3*	*11,6*	*28,8*
Frankreich	22 077	13 246	27 817	*13,3*	*19,1*	*7,8*	*13,3*	*26,2*
Griechenland	7 600	4 560	9 576	*20,2*	*24,5*	*12,4*	*16,9*	*19,8*
Irland	22 879	13 727	28 827	*15,6*	*17,0*	*14,8*	*9,2*	*23,9*
Island	28 393 [3]	17 036 [3]	35 776 [3]	*8,8* [3]	*10,4* [3]	*6,1* [3]	*12,7*	*22,1*
Italien	16 542	9 925	20 843	*20,3*	*26,4*	*15,6*	*14,2*	*23,3*
Kroatien	6 210	3 726	7 825	*20,0*	*21,4*	*28,6*	.	.
Lettland	6 607	3 964	8 325	*22,1*	*18,4*	*39,9*	*17,8*	*21,1*
Litauen	6 134	3 681	7 729	*22,9*	*25,7*	*33,4*	*21,6*	*14,8*
Luxemburg	36 076	21 645	45 455	*18,7*	*22,8*	*11,8*	*8,9*	*24,5*
Malta	14 522	8 713	18 298	*16,7*	*21,2*	*24,9*	*12,1*	*10,3*
Niederlande	23 561	14 137	29 687	*13,2*	*14,4*	*10,0*	*11,4*	*24,1*
Norwegen	38 471	23 083	48 474	*12,3*	*13,7*	*8,3*	*11,9*	*22,8*
Österreich	24 752	14 851	31 187	*14,4*	*19,1*	*12,9*	*9,9*	*22,6*
Polen	5 945	3 567	7 491	*15,0*	*14,0*	*13,8*	*16,8*	*20,8*
Portugal	9 071	5 443	11 429	*18,3*	*20,7*	*17,0*	*16,7*	*18,3*
Rumänien	2 742	1 645	3 455	*23,6*	*32,2*	*20,0*	*27,8*	*22,5*
Russische Föderation	.	.	.	.	.	.	.	.
Schweden	25 376	15 225	31 973	*15,8*	*18,6*	*15,8*	*12,4*	*26,1*
Schweiz	43 741	26 245	55 114	*15,5*	*18,0*	*25,9*	.	.
Slowakei	7 183	4 310	9 051	*12,4*	*19,9*	*6,9*	*18,1*	*23,7*
Slowenien	12 713	7 628	16 019	*13,3*	*12,8*	*16,4*	*14,6*	*19,3*
Spanien	14 203	8 522	17 896	*21,6*	*28,3*	*14,8*	*12,3*	*21,7*
Tschechische Republik	8 282	4 969	10 435	*9,1*	*11,6*	*10,7*	*16,3*	*25,4*
Türkei	3 866	2 320	4 871	*22,2*	*33,0*	*16,6*	*20,9*	*15,0*
Ungarn	4 988	2 993	6 285	*13,4*	*14,8*	*9,1*	*18,2*	*18,8*
Vereinigtes Königreich	20 995	12 597	26 454	*17,0*	*21,3*	*16,9*	*8,2*	*26,7*
Zypern	14 497	8 698	18 266	*15,7*	*16,5*	*21,6*	*13,7*	*15,4*

1 Quelle: LEBEN IN EUROPA (EU-SILC), Eurostat.
2 Quelle: Volkswirtschaftliche Gesamtrechnungen, Eurostat.
3 2016.

Das **Äquivalenzeinkommen** ist eine Rechengröße, um das Einkommen von Personen vergleichbar zu machen, die in Haushalten unterschiedlicher Größe und Zusammensetzung leben. Weitere Informationen hierzu siehe „Glossar" des Kapitels 6.

Das **Medianäquivalenzeinkommen** wird wie folgt ermittelt: Um das mittlere Einkommen zu bestimmen, wird der Median (Zentralwert) verwendet. Dabei werden Personen ihrem Äquivalenzeinkommen nach aufsteigend sortiert. Der Median ist der Einkommenswert derjenigen Person, die die Bevölkerung in genau zwei Hälften teilt. Das heißt, die eine Hälfte hat mehr Einkommen zur Verfügung, die andere weniger.

Die **Armutsgefährdungsgrenze** liegt bei 60 % des Medians der Äquivalenzeinkommen der Bevölkerung in Privathaushalten. Personen werden als (relativ) einkommensarm bezeichnet, wenn deren Äquivalenzeinkommen unter diesem Schwellenwert liegt. Weitere Informationen hierzu siehe „Glossar" des Kapitels 6.

Die **Armutsgefährdungsquote** ist definiert als der Anteil der Personen, deren Äquivalenzeinkommen unterhalb der Armutsgefährdungsschwelle liegt. Bei den hier aufgeführten Quoten wurden bei der Ermittlung des Einkommens auch Sozialtransfers (z. B. Wohngeld, Kindergeld, Rente, Pension, Pflegegeld) berücksichtigt.

A.7 Kultur, Medien, Freizeit

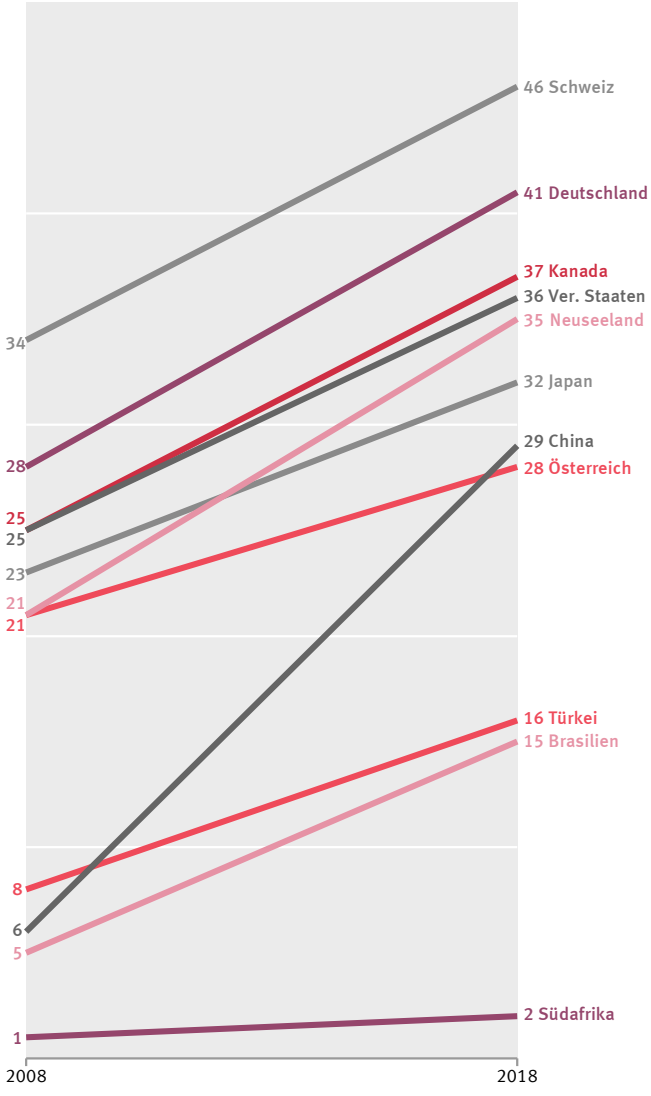
	Kultur und Freizeit			Medien: Telekommunikation und Internet [3]					
	Kinobesuche [1]	Live-Veranstaltungen (Theater, Konzerte) [2]	Sportveranstaltungen [2]	Haushalte mit eigenem Computer	Haushalte mit eigenem Internetanschluss	Festnetzanschlüsse	Mobilfunkverträge	festinstallierte Breitbandanschlüsse im Abonnement	aktive mobile Breitbandanschlüsse im Abonnement
		mindestens 4 Besuche in den letzten 12 Monaten							
	2017	2015		2017		2018			2017
	je Einwohner/-in	% der Personen ab 16 Jahren		%		je 100 Einwohner/-innen			
Europa									
Europäische Union	.	13,7	13,7	.	.	.	.	.	.
Belgien	1,85	20,3	19,6	85	86	36	103	39	66
Bulgarien	1,80	6,7	6,9	63	67	16	118	27	87
Dänemark	0,78	13,7	12,7	90	94	20	125	44	124
Deutschland	**1,61**	**14,9**	**17,1**	**88**	**88**	**52**	**129**	**41**	**77**
Estland	0,84	20,6	10,8	87	88	26	145	33	122
Finnland	1,48	24,1	21,5	87	88	6	132	31	152
Frankreich	1,47	17,8	11,5	78	71	59	108	45	82
Griechenland	2,28	4,6	4,9	72 [4]	69 [4]	47	116	38	53
Irland	2,19	14,3	25,8	84	89	38	103	30	101
Island	2,50	35,0	31,9	99 [4]	97 [4]	41	126	41	106
Italien	3,19	8,0	8,0	64	72	34	137	28	88
Kroatien	1,58	10,0	11,8	74	76	33	106	27	77
Lettland	0,93	17,5	11,8	77	79	14	107	27	76
Litauen	1,02	14,2	5,8	73	75	15	164	28	72
Luxemburg	1,49	26,9	21,7	95	97	45	132	37	84
Malta	1,85	10,8	11,5	84	86	58	140	44	76
Niederlande	3,34	20,6	32,2	91	96	38 [5]	121 [5]	42 [5]	88
Norwegen	4,27	23,4	31,2	95	97	11	107	41	94
Österreich	1,94	21,8	16,7	85	89	42	124	28	87
Polen	1,27	3,7	5,6	82	82	20 [5]	135	19	69
Portugal	1,28	17,3	13,8	71	77	49	116	37	63
Rumänien	2,52	6,7	6,3	73	76	19	116	26	80
Russische Föderation	2,01	.	.	74	76	22 [5]	157	22	74
Schweden	1,44	16,5	26,3	44 [4]	92 [4]	24	125	39	123
Schweiz	1,37	37,0	29,4	89 [4]	90	39	130	46	101
Slowakei	0,66	9,3	18,9	82	81	13	133	28	79
Slowenien	1,35	28,2	15,6	80	82	33	119	29	62
Spanien	1,80	12,3	14,3	78	84	42	116	32	90
Tschechische Republik	1,14	15,4	19,5	76	77	14	119	30	80
Türkei	1,04	.	.	57	81	14	97	16	65
Ungarn	0,74	9,5	9,7	76 [4]	82	31	103	32	45
Vereinigtes Königreich	2,57	17,9	13,9	90 [4]	91 [4]	48	118	40	89
Zypern	1,55	11,3	12,2	76	79	26	101	26	97

A.7 Kultur, Medien, Freizeit

	Medien: Telekommunikation und Internet [1]				
	Hauhalte mit eigenem Computer	Haushalte mit eigenem Internet-anschluss	Festnetz-anschlüsse	Mobilfunk-verträge	aktive mobile Breitband-anschlüsse im Abon-nement
	2017		2018		2017
	%		je 100 Einwohner/-innen		
Afrika					
Ägypten	58	49	8	95	47
Äthiopien	5 [4]	15 [4]	1 [5]	37 [5]	5
Kenia	7 [4]	30 [4]	.	96	26
Kongo, Dem. Republik	3 [4]	3 [4]	.	43	13
Nigeria	3	8	.	88	23
Südafrika	22	62	5	153	56
Tansania, Ver. Republik	4 [4]	8 [4]	.	77	9
Amerika					
Argentinien	64	76	22	132	78
Brasilien	46	61	18	99	89
Chile	60	88	16	134	72
Kanada	84 [4]	87 [4]	37	89	69
Kolumbien	44	50	14	130	47
Mexiko	45	51	17	93	59
Vereinigte Staaten	91	84	36	124	127
Asien					
Bangladesch	3	7	.	97	27
China	53 [4]	56 [4]	13	115	69
Indien	15 [4]	23 [4]	2	87	16
Indonesien	19	57	4	120	34
Iran, Islamische Republik	66	70	37	108	34
Israel	78	74	38	128	92
Japan	77	96	50	139	131
Korea, Republik	80	100	51	130	110
Malaysia	74	86	20	135	92
Myanmar	3	24 [4]	1	114	56
Pakistan	16 [4]	22 [4]	1	73	20
Philippinen	23 [4]	39 [4]	4 [5]	110 [5]	55
Saudi-Arabien	73	91	9	123	74
Thailand	25	64	4	180	93
Ver. Arabische Emirate	93	97	24	209	165
Vietnam	24 [4]	26 [4]	15	147	46
Australien und Ozeanien					
Australien	82	86	32	114	131
Neuseeland	87 [4]	86 [4]	37	135	101

1 Quelle: MEDIA Salles.
2 Quelle: Eurostat.
3 Quelle: Internationale Fernmeldeunion (ITU), Vereinte Nationen.
4 2016.
5 2017.

Festinstallierte Internet-Breitbandanschlüsse
im Abonnement, je 100 Einwohner/-in



Quelle: Internationale Fernmeldeunion (ITU), Vereinte Nationen

2019 - 01 - 0314

A.8 Soziales

	Ausgaben für Sozialschutzleistungen									Zahl der Rentenbezieher/-innen [1]	Lohnersatzquote der Rentenbezieher/-innen [2]
	Sozialschutzleistungen			Leistungen nach Funktion							
				Alter, Hinterbliebene	Gesundheitsversorgung	Invalidität, Gebrechen	Familie, Kinder	Arbeitslosigkeit	Wohnen und Sonstiges		
	2016										2017
	Mill. EUR	% des BIP	EUR je Einwohner/-in	% aller Sozialschutzleistungen						je 100 Einwohner/-innen	%
Europa											
Europäische Union	4 051 410	*27,1*	*7 932*	*45,6*	*29,5*	*7,4*	*8,7*	*4,7*	*4,2*	.	*58*
Belgien	119 298	*28,1*	*10 528*	*44,9*	*26,6*	*8,6*	*7,5*	*9,1*	*3,3*	*25*	*50*
Bulgarien	8 192	*17,0*	*1 149*	*50,0*	*27,5*	*7,4*	*10,4*	*3,2*	*1,6*	*31*	*37*
Dänemark	84 150	*29,8*	*14 691*	*42,8*	*20,7*	*13,1*	*11,4*	*4,7*	*7,4*	*26*	*48*
Deutschland	***890 498***	***28,2***	***10 814***	***38,7***	***34,9***	***8,1***	***11,4***	***3,5***	***3,4***	***28***	***46***
Estland	3 556	*16,4*	*2 703*	*41,8*	*29,8*	*11,4*	*13,0*	*2,9*	*1,1*	*32*	*45*
Finnland	67 680	*31,3*	*12 316*	*43,4*	*22,7*	*9,9*	*9,9*	*8,3*	*5,9*	*28*	*53*
Frankreich	714 501	*32,1*	*10 709*	*45,5*	*28,6*	*6,4*	*7,6*	*6,2*	*5,6*	*29*	*68*
Griechenland	45 697	*25,9*	*4 241*	*65,1*	*20,5*	*5,9*	*4,0*	*3,7*	*0,9*	*24*	*62*
Irland	41 441	*15,2*	*8 715*	*33,7*	*38,1*	*5,4*	*8,6*	*10,1*	*4,2*	*20*	*33*
Island	.	.	.	.	.	.	.	.	.	*20*	.
Italien	480 550	*28,4*	*7 926*	*57,8*	*23,1*	*5,8*	*6,2*	*6,1*	*1,0*	*26*	*71*
Kroatien	9 747	*20,9*	*2 336*	*43,3*	*33,4*	*10,9*	*8,6*	*2,4*	*1,5*	*30*	*41*
Lettland	3 731	*14,9*	*1 904*	*49,0*	*25,0*	*9,1*	*11,1*	*4,7*	*1,2*	*30*	*43*
Litauen	5 648	*14,5*	*1 969*	*45,9*	*31,4*	*9,3*	*7,8*	*3,3*	*2,3*	*33*	*43*
Luxemburg	11 471	*21,5*	*19 709*	*39,5*	*24,6*	*10,8*	*15,4*	*5,8*	*3,9*	*31*	*86*
Malta	1 680	*16,2*	*3 689*	*52,5*	*33,0*	*3,6*	*5,9*	*2,7*	*2,3*	*19*	*56*
Niederlande	198 458	*28,0*	*11 653*	*42,6*	*32,9*	*9,4*	*4,0*	*4,7*	*6,4*	*21*	*52*
Norwegen	95 609	*28,5*	*18 265*	*36,2*	*29,3*	*16,4*	*11,7*	*2,6*	*3,8*	*26*	*58*
Österreich	103 638	*29,1*	*11 862*	*50,0*	*25,3*	*6,4*	*9,6*	*5,8*	*3,0*	*28*	*64*
Polen	84 892	*19,9*	*2 236*	*55,6*	*23,2*	*6,7*	*12,8*	*0,9*	*0,8*	*25*	*62*
Portugal	44 712	*24,0*	*4 330*	*57,9*	*25,2*	*7,2*	*4,9*	*3,8*	*1,0*	*29*	*67*
Rumänien	24 509	*14,4*	*1 244*	*54,6*	*27,1*	*6,9*	*9,6*	*0,6*	*1,2*	*27*	*61*
Russische Föderation	.	.	.	.	.	.	.	.	.	.	.
Schweden	134 534	*29,0*	*13 558*	*43,2*	*25,9*	*10,9*	*10,3*	*3,5*	*6,2*	*27*	*57*
Schweiz	155 958	*25,7*	*18 626*	*46,9*	*31,2*	*8,8*	*5,9*	*3,8*	*3,5*	*36*	*48*
Slowakei	14 499	*17,9*	*2 670*	*45,0*	*32,5*	*8,8*	*9,0*	*3,0*	*1,7*	*26*	*62*
Slowenien	9 247	*22,9*	*4 478*	*48,1*	*33,3*	*5,4*	*7,5*	*2,6*	*3,2*	*31*	*46*
Spanien	267 258	*23,9*	*5 750*	*50,4*	*27,6*	*7,1*	*5,4*	*8,1*	*1,5*	*21*	*69*
Tschechische Republik	32 326	*18,3*	*3 059*	*47,0*	*32,4*	*6,4*	*8,9*	*2,6*	*2,8*	*28*	*51*
Türkei	98 937	*12,7*	*1 248*	*61,0*	*27,6*	*3,6*	*3,7*	*2,5*	*1,6*	*16*	*96*
Ungarn	21 479	*18,9*	*2 189*	*50,0*	*27,6*	*6,3*	*11,9*	*1,7*	*2,4*	*22*	*64*
Vereinigtes Königreich	624 559	*26,0*	*9 519*	*42,3*	*32,6*	*6,6*	*9,9*	*1,4*	*7,2*	*24*	*54*
Zypern	3 456	*18,7*	*4 058*	*56,2*	*18,6*	*4,2*	*7,1*	*5,5*	*8,4*	*17*	*43*

1 Eigene Berechnungen basierend auf Eurostat Daten.
2 Die Lohnersatzquote ist definiert als das Verhältnis vom Median-Renteneinkommen der Altersklasse 65 bis 74 Jahre zum Median-Bruttoeinkommen der Altersklasse 50 bis 59 Jahre ohne Berücksichtigung von Sozialleistungen.

Quelle: Eurostat, zum Teil vorläufige Werte

A.9 Finanzen und Steuern

Finanzierungssaldo und Bruttoschuldenstand des Staates 2018

im Rahmen des EU-Defizitverfahrens, EU-Staaten, in % des BIP

Der **Finanzierungssaldo des Staates** ergibt sich aus der Differenz zwischen Staatseinnahmen und Staatsausgaben.
Sind die Ausgaben in einer Periode höher als die Einnahmen, spricht man von einem Finanzierungsdefizit. Ein positiver Saldo wird als Finanzierungsüberschuss bezeichnet.

Der **Bruttoschuldenstand des Staates** ist im Vertrag von Maastricht definiert als Brutto-Gesamtschuldenstand des gesamten Staatssektors zum Nominalwert am Jahresende nach Konsolidierung. Der Staatssektor umfasst Zentralstaat, Länder, Gemeinden und Sozialversicherung. Konsolidierung ist ein Verfahren, bei dem statistische Daten für eine Gruppe von Einheiten wie institutionelle Sektoren so dargestellt werden, als wäre diese Gruppe eine einzige Einheit. Die Zahlen für den Staatssektor sind zwischen den Teilsektoren auf Ebene des Gesamtstaates konsolidiert.

Das **Defizitverfahren** wird von der Europäischen Kommission eingeleitet, wenn ein EU-Mitgliedstaat mit seinem Haushalt die im Stabilitäts- und Wachstumspakt festgelegte Defizitgrenze überschreitet. Entsprechend dem Protokoll über das Verfahren bei einem übermäßigen Defizit, im Anhang zum Vertrag von Maastricht über die Wirtschafts- und Währungsunion, sollen die Mitgliedstaaten der Eurozone folgende Konvergenzkriterien einhalten: Das **jährliche Haushaltsdefizit** des Staates soll 3 % des Bruttoinlandsprodukts (BIP) nicht übersteigen und der **konsolidierte Bruttoschuldenstand** nicht mehr als 60 % des BIP betragen.

Quelle: Finanzstatistik des Sektors Staat (Government Finance Statistics), Eurostat

2019 - 01 - 0315

A.9 Finanzen und Steuern

	Gesamteinnahmen des Staates			Gesamtausgaben des Staates		Finanzierungssaldo des Staates [1]	Finanzierungssaldo des Staates [3]	Bruttoschuldenstand des Staates (konsolidiert) [3]	Finanzierungssaldo des Staates [3]	Bruttoschuldenstand des Staates (konsolidiert) [3]
	insgesamt [1]	darunter [2]		insgesamt [1]	darunter Sozialausgaben [2]					
		Steuern	Sozialbeiträge							
	2017								2018	
	Mrd. US$	%		Mrd. US$	%	Mrd. US$	% des BIP			
Europa										
Europäische Union	.	.	.	.	.	.	*– 1,0*	*81,7*	*– 0,6*	*80,0*
Belgien	254,3	*59,8*	*30,9*	258,7	*48,1*	*– 4,4*	*– 0,8*	*103,4*	*– 0,7*	*102,0*
Bulgarien	19,4	*58,1*	*23,1*	19,0	*38,0*	*0,5*	*1,2*	*25,6*	*2,0*	*22,6*
Dänemark	172,6	*87,7*	*1,7*	168,8	*34,8*	3,9	*1,4*	*35,5*	*0,5*	*34,1*
Deutschland	**1 665,0**	***52,4***	***37,2***	**1 626,6**	***54,5***	***38,4***	***1,0***	***64,5***	***1,7***	***60,9***
Estland	10,4	*55,1*	*29,4*	10,4	*35,9*	*– 0,1*	*– 0,4*	*9,2*	*– 0,6*	*8,4*
Finnland	134,8	*58,3*	*22,8*	136,5	*40,8*	*– 1,7*	*– 0,8*	*61,3*	*– 0,7*	*58,9*
Frankreich	1 392,6	*55,4*	*35,0*	1 462,0	*45,7*	*– 69,5*	*– 2,8*	*98,4*	*– 2,5*	*98,4*
Griechenland	98,3	*56,0*	*30,0*	96,2	*44,2*	*2,1*	*0,7*	*176,2*	*1,1*	*181,1*
Irland	86,5	*73,1*	*16,5*	87,3	*38,3*	*– 0,8*	*– 0,3*	*68,5*	*0,0*	*64,8*
Island	10,7	.	.	10,6	.	*0,1*	*0,5* [1]	*43,1* [1]	*1,1* [1]	*35,4* [1]
Italien	904,6	*62,4*	*28,1*	951,5	*45,3*	*– 46,9*	*– 2,4*	*131,4*	*– 2,1*	*132,2*
Kroatien	25,8	.	.	25,3	.	*0,5*	*0,8*	*77,8*	*0,2*	*74,6*
Lettland	10,9	*60,3*	*23,4*	11,1	*31,4*	*– 0,3*	*– 0,6*	*40,0*	*– 1,0*	*35,9*
Litauen	15,6	*51,9*	*37,4*	15,4	*38,9*	*0,2*	*0,5*	*39,4*	*0,7*	*34,2*
Luxemburg	27,8	*62,0*	*28,2*	26,9	*49,3*	*0,9*	*1,4*	*23,0*	*2,4*	*21,4*
Malta	5,0	*67,5*	*15,9*	4,6	*28,5*	*0,4*	*3,4*	*50,2*	*2,0*	*46,0*
Niederlande	363,9	*56,0*	*32,8*	354,3	*49,7*	*9,6*	*1,2*	*57,0*	*1,5*	*52,4*
Norwegen	216,5	*51,8*	*18,8*	196,3	*35,6*	*20,2*	*5,1* [1]	*36,8* [1]	*7,5* [1]	*36,8* [1]
Österreich	201,8	*56,0*	*31,3*	204,7	*45,5*	*– 2,9*	*– 0,8*	*78,2*	*0,1*	*73,8*
Polen	208,9	*53,2*	*34,9*	216,3	*42,7*	– 7,4	*– 1,5*	*50,6*	*– 0,4*	*48,9*
Portugal	93,9	*58,7*	*27,3*	100,4	*39,3*	*– 6,5*	*– 3,0*	*124,8*	*– 0,5*	*121,5*
Rumänien	59,2	*52,9*	*30,3*	65,2	*35,3*	– 6,0	*– 2,7*	*35,2*	*– 3,0*	*35,0*
Russische Föderation	525,2	.	.	548,3	.	*– 23,1*	*– 1,5* [1]	*15,5* [1]	*2,8* [1]	*14,0* [1]
Schweden	267,2	*81,5*	*6,6*	259,2	*34,6*	*8,0*	*1,4*	*40,8*	*0,9*	*38,8*
Schweiz	226,3	.	.	223,8	.	*2,5*	*0,4* [1]	*41,8* [1]	*0,3* [1]	*40,5* [1]
Slowakei	37,8	*46,3*	*37,5*	38,5	*45,4*	*– 0,7*	*– 0,8*	*50,9*	*– 0,7*	*48,9*
Slowenien	19,0	*50,4*	*34,3*	19,3	*40,0*	*– 0,3*	*0,0*	*74,1*	*0,7*	*70,1*
Spanien	499,6	*58,7*	*32,3*	540,1	*43,0*	*– 40,6*	*– 3,1*	*98,1*	*– 2,5*	*97,1*
Tschechische Republik	87,5	*49,8*	*37,2*	84,1	*37,4*	*3,3*	*1,6*	*34,7*	*0,9*	*32,7*
Türkei	268,0	*58,7*	*23,7*	288,0	*35,2*	*– 19,9*	*– 2,3* [1]	*28,3* [1]	*– 3,6* [1]	*29,1* [1]
Ungarn	62,5	*56,8*	*28,6*	65,5	*30,1*	*– 3,1*	*– 2,2*	*73,4*	*– 2,2*	*70,8*
Vereinigtes Königreich	964,4	*70,1*	*20,0*	1 013,2	*38,5*	*– 48,8*	*– 1,9*	*87,1*	*– 1,5*	*86,8*
Zypern	8,6	*63,6*	*22,2*	8,2	*36,3*	*0,4*	*1,8*	*95,8*	*– 4,8*	*102,5*

A.9 Finanzen und Steuern

	Gesamteinnahmen des Staates [1]	Gesamtausgaben des Staates [1]	Finanzierungssaldo des Staates [1]		Bruttoschuldenstand des Staates (konsolidiert) [1]	Finanzierungssaldo des Staates [1]	Bruttoschuldenstand des Staates (konsolidiert) [1]
	2017					2018	
	Mrd. US$		% des BIP				
Afrika							
Ägypten	42,5	62,8	– 20,4	*– 10,4*	*103,2*	*– 9,5*	*92,6*
Äthiopien	11,3	13,8	– 2,5	*– 3,3*	*59,0*	*– 3,0*	*61,1*
Kenia	14,2	20,4	– 6,2	*– 7,8*	*54,8*	*– 7,3*	*57,2*
Kongo, Dem. Republik	4,1	4,7	– 0,6	*– 1,5*	*18,1*	*– 0,5*	*15,7*
Nigeria	23,2	43,5	– 20,3	*– 5,4*	*25,3*	*– 4,5*	*28,4*
Südafrika	98,6	113,9	– 15,3	*– 4,4*	*53,0*	*– 4,4*	*56,7*
Tansania, Ver. Republik	8,2	8,8	– 0,6	*– 1,2*	*36,6*	*– 1,8*	*36,0*
Amerika							
Argentinien	221,6	264,6	– 43,0	*– 6,7*	*57,1*	*– 5,2*	*86,3*
Brasilien	631,7	793,8	– 162,1	*– 7,9*	*84,1*	*– 6,8*	*87,9*
Chile	63,2	70,4	– 7,3	*– 2,6*	*23,5*	*– 1,5*	*25,6*
Kanada	659,0	664,1	– 5,1	*– 0,3*	*90,1*	*– 0,4*	*90,6*
Kolumbien	79,2	87,4	– 8,2	*– 2,6*	*49,8*	*– 2,2*	*50,5*
Mexiko	285,6	297,9	– 12,3	*– 1,1*	*54,0*	*– 2,3*	*53,6*
Vereinigte Staaten	6 028,6	6 778,1	– 749,5	*– 3,8*	*106,2*	*– 4,3*	*105,8*
Asien							
Bangladesch	25,1	33,3	– 8,2	*– 3,3*	*32,5*	*– 4,1*	*34,8*
China	.	.	.	*– 3,9*	*46,8*	*– 4,8*	*50,5*
Indien	520,2	704,4	– 184,1	*– 7,0*	*69,8*	*– 6,7*	*69,8*
Indonesien	142,7	168,2	– 25,5	*– 2,5*	*28,9*	*– 1,8*	*29,2*
Iran, Islamische Republik	78,1	86,2	– 8,1	*– 1,8*	*39,5*	*– 3,9*	*33,2*
Israel	133,6	136,9	– 3,4	*– 1,0*	*60,4*	*– 2,2*	*59,6*
Japan	1 664,5	1 818,4	– 153,9	*– 3,2*	*235,0*	*– 3,2*	*237,1*
Korea, Republik	354,4	318,9	35,5	*2,3*	*39,8*	*2,8*	*40,7*
Malaysia	61,2	68,8	– 7,7	*– 2,4*	*55,2*	*– 3,6*	*56,2*
Myanmar	11,3	13,1	– 1,8	*– 2,7*	*47,3*	*– 2,5*	*49,4*
Pakistan	47,1	64,5	– 17,4	*– 5,8*	*67,0*	*– 6,5*	*72,1*
Philippinen	61,3	62,4	– 1,1	*– 0,4*	*39,9*	*– 1,0*	*39,6*
Saudi-Arabien	165,7	229,3	– 63,6	*– 9,2*	*17,2*	*– 4,6*	*19,1*
Thailand	94,3	98,6	– 4,2	*– 0,9*	*41,9*	*– 0,3*	*42,1*
Ver. Arabische Emirate	110,1	116,4	– 6,2	*– 1,6*	*19,7*	*– 1,8*	*18,7*
Vietnam	52,7	63,5	– 10,8	*– 4,8*	*58,2*	*– 4,6*	*57,5*
Australien und Ozeanien							
Australien	484,1	504,8	– 20,6	*– 1,5*	*40,7*	*– 1,2*	*40,7*
Neuseeland	74,8	72,5	2,3	*1,1*	*31,6*	*0,4*	*29,4*

1 Quelle: Eigene Berechnungen basierend auf World Economic Outlook, Internationaler Währungsfonds (IMF). Zum Teil vorläufige Werte.
2 Quelle: International Financial Statistics, Internationaler Währungsfonds (IMF).
3 Quelle: Finanzstatistik des Sektors Staat (Government Finance Statistics), Eurostat.

A.10 Wahlen zum Europaparlament

	Wahlbeteiligung		Mandate	Davon								Frauenanteil an den Mandaten
				EVP	S&D	Renew Europe	Grüne/ EFA	ID	EKR	GUE/ NGL	Fraktionslose/ Sonstige	
	2014	2019										
	%		Anzahl									%
Europäische Union	*42,6*	*50,6*	751	182	154	108	74	73	62	41	57	*41*
Belgien	*89,6*	*88,5*	21	4	3	4	3	3	3	1	–	*38*
Bulgarien	*35,8*	*32,6*	17	7	5	3	–	–	2	–	–	*29*
Dänemark	*56,3*	*66,0*	13	1	3	5	2	1	–	1	–	*46*
Deutschland	***48,1***	***61,4***	**96**	**29**	**16**	**7**	**25**	**11**	**1**	**6**	**1**	***36***
Estland	*36,5*	*37,6*	6	–	2	3	–	1	–	–	–	*33*
Finnland	*39,1*	*40,7*	13	3	2	3	2	2	–	1	–	*54*
Frankreich	*42,4*	*50,1*	74	8	5	21	12	22	–	6	–	*50*
Griechenland	*60,0*	*58,8*	21	8	2	–	–	–	1	6	4	*24*
Irland	*52,4*	*49,7*	11	4	–	1	2	–	–	4	–	*45*
Italien	*57,2*	*54,5*	73	7	19	–	–	28	5	–	14	*41*
Kroatien	*25,2*	*29,9*	11	4	3	1	–	–	1	–	2	*36*
Lettland	*30,2*	*33,5*	8	2	2	1	1	–	2	–	–	*50*
Litauen	*47,4*	*53,5*	11	4	2	2	2	–	1	–	–	*27*
Luxemburg	*85,6*	*84,2*	6	2	1	2	1	–	–	–	–	*50*
Malta	*74,8*	*72,7*	6	2	4	–	–	–	–	–	–	*50*
Niederlande	*37,3*	*41,9*	26	6	6	6	3	–	4	1	–	*50*
Österreich	*45,4*	*59,8*	18	7	5	1	2	3	–	–	–	*50*
Polen	*23,8*	*45,7*	51	17	8	–	–	–	26	–	–	*35*
Portugal	*33,7*	*30,8*	21	7	9	–	1	–	–	4	–	*43*
Rumänien	*32,4*	*51,1*	32	14	10	8	–	–	–	–	–	*22*
Schweden	*51,1*	*55,3*	20	6	5	3	2	–	3	1	–	*55*
Slowakei	*13,1*	*22,7*	13	4	3	2	–	–	2	–	2	*15*
Slowenien	*24,6*	*28,9*	8	4	2	2	–	–	–	–	–	*50*
Spanien	*43,8*	*60,7*	54	12	20	8	2	–	3	6	3	*47*
Tschechische Republik	*18,2*	*28,7*	21	5	–	6	3	2	4	1	–	*33*
Ungarn	*29,0*	*43,4*	21	13	5	2	–	–	–	–	1	*38*
Vereinigtes Königreich	*35,6*	*36,9*	73	–	10	17	11	–	4	1	30	*47*
Zypern	*44,0*	*45,0*	6	2	2	–	–	–	–	2	–	*0*

Weitere Informationen zu den Europawahlen siehe Kapitel 10.

Quelle: Europäisches Parlament

EVP: Fraktion der Europäischen Volkspartei (Christdemokraten), **S&D**: Fraktion der Progressiven Allianz der Sozialdemokraten im Europäischen Parlament, **Renew Europe**: Renew Europe group, **Grüne/EFA**: Fraktion der Grünen/Freie Europäische Allianz, **ID**: Identität und Demokratie, **EKR**: Fraktion der Europäischen Konservativen und Reformer, **GUE/NGL**: Konföderale Fraktion der Vereinigten Europäischen Linken/Nordische Grüne Linke.

Zuordnung der deutschen Parteien zu den europäischen Fraktionen: CDU/CSU (EVP-Fraktion), SPD (S&D), FDP und FREIE WÄHLER (Renew Europe), GRÜNE, PIRATEN, ÖDP, Die PARTEI und VOLT (Grüne/EFA), AfD (ID), FAMILIEN-Partei Deutschlands (EKR), DIE LINKE und Tierschutzpartei (GUE/NGL), Die PARTEI (fraktionslos).

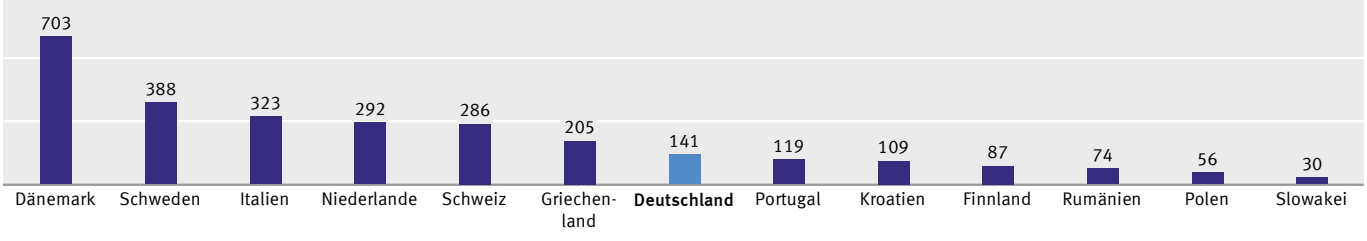
A.11 Justiz

	Tötungsdelikte	Raubdelikte	Wohnungs-einbrüche	Diebstahl	Darunter Kfz-Diebstahl	Polizisten/ Polizistinnen [1]	Strafgefangene
	2017						
	je 100 000 Einwohner/-innen						
Europa							
Europäische Union	.	.	.	.	.	.	.
Belgien [2]	2,0	197	591	1 660	132	342	98
Bulgarien	1,3	22	62 [2]	452	33	398	98
Dänemark	1,1	36	703	3 721	4	188	59
Deutschland	**0,9**	**47**	**141**	**1 401**	**66**	**299**	**80**
Estland	2,2	15	73	580	26	296	207
Finnland	1,3	30	87	2 003	111	137	56
Frankreich	1,4	150	361 [3]	2 069 [3]	242 [3]	321	103
Griechenland	0,7	40	205	1 019	316	497	93
Irland	0,9	46	.	1 455	102	278 [4]	77
Island	0,9	14	113	1 130	138	192	39
Italien	0,6	51	323	1 766	241	453 [3]	97
Kroatien	1,1	21	109	299	21	493	75
Lettland	5,6	31	73	745	55	461 [3]	193
Litauen	4,0	38	91	598	35	289	232
Luxemburg	0,3	77	368 [3]	1 743 [3]	296 [3]	337	116
Malta	2,0	44	185	1 793	72	493	128
Niederlande	17,1	47	292	1 518	149	357	64
Norwegen	0,5	15	99 [4]	1 791	77	168 [4]	80 [3]
Österreich [3]	0,6	36	149	1 652	104	333	99
Polen	0,7	21	56	282	33	260	196
Portugal	0,7	115	119	759	99	449	132
Rumänien	1,5	16	74	489	15	243	119
Russische Föderation	.	.	.	.	.	.	.
Schweden	1,1	87	388	3 525	248	198	57
Schweiz	0,5	21	286	1 648	79	220	78
Slowakei	1,5	9	30	287	28	405	185
Slowenien	0,9	12	141	994	26	347	63 [3]
Spanien	0,7	144	226	349	71	360	126
Tschechische Republik	0,6	15	68	632	202	381	209
Türkei [3]	22,3	34	.	216	.	.	255
Ungarn	1,6	9	206 [2]	820	32 [2]	406	177
Vereinigtes Königreich [5]	1,2	120	34 [3]	2 555	180	225 [3]	142 [3]
Zypern	0,8	14	108	110	112	585	69

1 Ohne Kommissarinnen und Kommissare.
2 2015.
3 2016.
4 2014.
5 Eigene Berechnungen basierend auf Eurostat Daten.

Quelle: Kriminalitätsstatistik, Eurostat

Wohnungseinbrüche 2017
je 100 000 Einwohner/-innen



Quelle: Kriminalitätsstatistik, Eurostat

2019 - 01 - 0316

A.12 Volkswirtschaftliche Gesamtrechnungen

	Bruttoinlandsprodukt (BIP) [1]			Bruttowertschöpfung [2]			Bruttoinlandsprodukt nach Verwendung [3]			
	nominal	je Einwohner/-in		Land- und Forstwirtschaft, Fischerei	Produzierendes Gewerbe	Dienstleistungsbereich	Konsumausgaben der privaten Haushalte	Konsumausgaben des Staates	Bruttoinvestitionen	Außenbeitrag
	2018			2017						
	Mill. US$	US$	Internat. US$ [4]	% des BIP						
Europa										
Europäische Union	18 750 050	.	*43 148*	.	.	.	*55,8*	*20,3*	*20,5*	*3,4*
Belgien	533 153	*46 724*	*48 245*	*0,7*	*22,0*	*77,3*	*51,0*	*23,2*	*24,6*	*1,2*
Bulgarien	64 963	*9 267*	*23 156*	*4,7*	*28,4*	*66,9*	*60,6*	*15,6*	*20,1*	*3,7*
Dänemark	350 874	*60 692*	*52 121*	*1,6*	*23,1*	*75,2*	*46,7*	*24,6*	*21,6*	*7,1*
Deutschland	**4 000 390**	***48 264***	***52 559***	***0,9***	***31,0***	***68,1***	***52,9***	***19,5***	***20,1***	***7,6***
Estland	30 312	*22 990*	*34 096*	*2,8*	*27,2*	*69,9*	*50,1*	*19,9*	*26,1*	*4,6*
Finnland	275 321	*49 845*	*46 430*	*2,7*	*28,2*	*69,1*	*54,3*	*23,0*	*22,6*	*0,3*
Frankreich	2 775 250	*42 878*	*45 775*	*1,7*	*19,5*	*78,8*	*54,0*	*23,7*	*23,4*	*– 1,1*
Griechenland	219 097	*20 408*	*29 123*	*4,2*	*17,2*	*78,6*	*68,7*	*19,8*	*12,5*	*– 1,0*
Irland	372 695	*76 099*	*78 785*	*1,2*	*38,6*	*60,2*	*31,9*	*12,1*	*24,7*	*30,4*
Island	25 882	*74 278*	*55 917*	*5,7*	*22,4*	*71,9*	*50,4*	*23,5*	*22,1*	*4,1*
Italien	2 072 200	*34 260*	*39 637*	*2,1*	*24,1*	*73,8*	*60,8*	*18,7*	*17,6*	*2,9*
Kroatien	60 688	*14 816*	*26 221*	*3,7*	*26,2*	*70,1*	*57,3*	*19,5*	*20,9*	*2,2*
Lettland	34 881	*18 032*	*29 901*	*3,7*	*22,6*	*73,8*	*59,7*	*18,0*	*22,2*	*0,1*
Litauen	53 323	*19 143*	*34 826*	*3,5*	*29,0*	*67,6*	*63,0*	*16,4*	*17,9*	*2,8*
Luxemburg	68 770	*114 234*	*106 705*	*0,3*	*12,1*	*87,7*	*30,7*	*17,0*	*19,0*	*33,3*
Malta	14 505	*31 058*	*45 606*	*1,1*	*12,9*	*86,0*	*44,2*	*15,3*	*19,1*	*21,3*
Niederlande	912 899	*53 106*	*56 383*	*2,1*	*19,4*	*78,5*	*44,4*	*24,2*	*20,7*	*10,7*
Norwegen	434 937	*81 695*	*74 356*	*2,3*	*33,7*	*64,0*	*44,5*	*24,1*	*28,2*	*3,2*
Österreich	457 637	*51 509*	*52 137*	*1,3*	*28,3*	*70,3*	*52,0*	*19,6*	*25,1*	*3,1*
Polen	586 015	*15 431*	*31 939*	*3,2*	*32,9*	*63,9*	*58,3*	*17,7*	*19,8*	*4,2*
Portugal	238 510	*23 186*	*32 006*	*2,3*	*22,4*	*75,3*	*64,8*	*17,5*	*16,9*	*0,8*
Rumänien	239 851	*12 285*	*26 447*	*5,2*	*35,9*	*58,9*	*63,1*	*15,7*	*23,4*	*– 2,1*
Russische Föderation	1 630 660	*11 327*	*29 267*	*4,4*	*33,3*	*62,3*	*52,7*	*18,1*	*24,1*	*5,3*
Schweden	551 135	*53 873*	*52 984*	*1,2*	*25,1*	*73,7*	*44,6*	*26,1*	*25,6*	*3,7*
Schweiz	703 750	*82 950*	*64 649*	*0,7*	*25,5*	*73,8*	*53,8*	*12,0*	*23,5*	*10,7*
Slowakei	106 585	*19 582*	*35 130*	*3,4*	*34,9*	*61,7*	*54,9*	*19,5*	*22,5*	*3,1*
Slowenien	54 242	*26 234*	*36 746*	*2,0*	*32,8*	*65,2*	*51,9*	*18,2*	*20,2*	*9,7*
Spanien	1 425 870	*30 697*	*40 139*	*3,0*	*24,1*	*72,9*	*57,5*	*18,5*	*21,1*	*2,9*
Tschechische Republik	242 052	*22 850*	*37 371*	*2,3*	*37,0*	*60,7*	*47,4*	*19,2*	*25,9*	*7,5*
Türkei	766 428	*9 346*	*27 956*	*6,9*	*32,9*	*60,2*	*59,0*	*14,5*	*31,0*	*– 4,5*
Ungarn	155 703	*15 924*	*31 903*	*4,4*	*30,3*	*65,3*	*49,5*	*20,2*	*22,7*	*7,6*
Vereinigtes Königreich	2 828 640	*42 558*	*45 705*	*0,7*	*20,2*	*79,2*	*65,7*	*18,3*	*17,2*	*– 1,2*
Zypern	24 492	*28 340*	*39 973*	*2,1*	*13,1*	*84,7*	*67,8*	*15,1*	*20,6*	*– 3,5*

Daten zum **Wirtschaftswachstum** bzw. zur jährlichen Veränderungsrate des **Bruttoinlandsprodukts (BIP)** sind der Tabelle A.0 auf den Seiten 652 und 653 zu entnehmen.

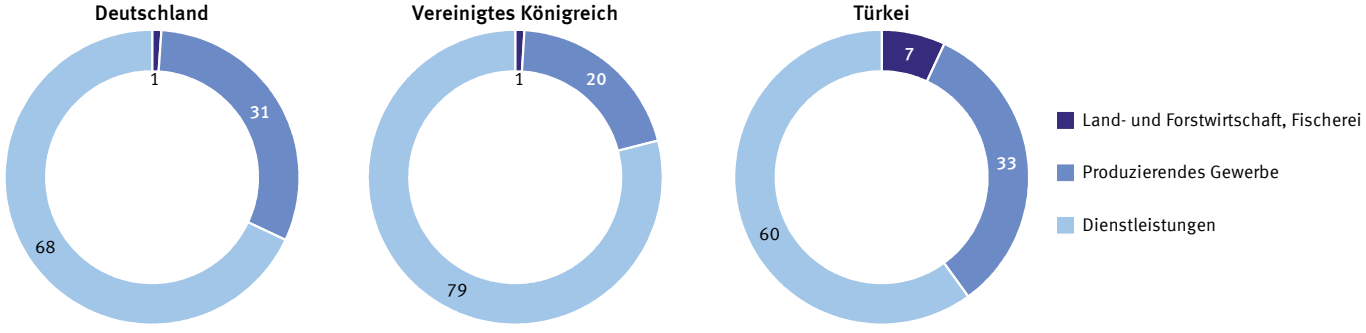
Der **internationale US-Dollar** – auch US$ purchasing power parity (US$ PPP) genannt – ist eine künstliche Währung, mit deren Hilfe Preisniveau-Unterschiede zwischen den Ländern weltweit ausgeglichen werden. Die Kaufkraft eines internationalen Dollars entspricht dabei der Kaufkraft von 1 US$ in den Vereinigten Staaten. Die Angaben in dieser Währung ermöglichen einen kaufkraftbereinigten Vergleich des Wohlstandsniveaus weltweit.

Die **Bruttoinvestitionen** setzen sich aus den Bruttoanlageinvestitionen und den Vorratsveränderungen zusammen. Als Bruttoanlageinvestitionen gelten Käufe neuer Anlagen sowie Käufe abzüglich Verkäufe von gebrauchten Anlagen und Land. Die Vorratsveränderungen ergeben sich aus der Differenz zwischen dem Anfangs- und Endbestand von Vorräten, die von Buchwerten auf eine konstante Preisbasis umgerechnet werden.

Der **Außenbeitrag** entspricht dem Saldo zwischen der Ausfuhr und der Einfuhr von Waren und Dienstleistungen. Staaten, die einen Exportüberschuss erzielen, weisen demnach einen positiven Außenbeitrag aus.

Weitere Erläuterungen zu diesen und anderen Begriffen aus dem Bereich der Volkswirtschaftlichen Gesamtrechnungen siehe „Glossar“/„Methodik“ des Kapitels 12.

Bruttowertschöpfung nach Sektoren 2017
in % des BIP



Quelle: Eigene Berechnungen basierend auf UNdata, Vereinte Nationen

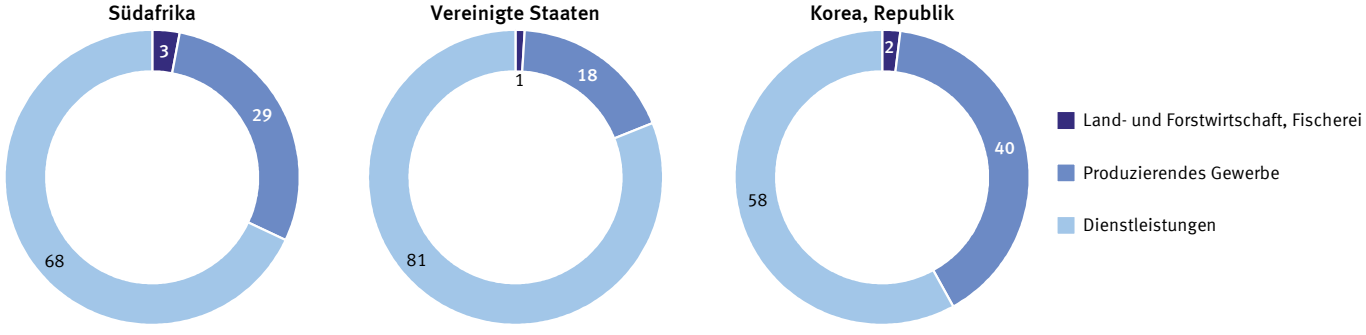
2019 - 01 - 0317

A.12 Volkswirtschaftliche Gesamtrechnungen

	Bruttoinlandsprodukt (BIP) [1]			Bruttowertschöpfung [2]			Bruttoinlandsprodukt nach Verwendung [3]			
	nominal	je Einwohner/-in		Land- und Forstwirtschaft, Fischerei	Produzierendes Gewerbe	Dienstleistungsbereich	Konsumausgaben der privaten Haushalte	Konsumausgaben des Staates	Bruttoinvestitionen	Außenbeitrag
	2018			2017						
	Mill. US$	US$	Internat. US$ [4]	% des BIP						
Afrika										
Ägypten	249 559	2 573	13 366	11,7	34,3	54,0	88,1	10,1	15,3	– 13,5
Äthiopien	80 279	853	2 332	36,2	24,4	39,4	66,5	11,1	38,4	– 15,8
Kenia	89 205	1 857	3 691	33,4	18,5	48,1	81,6	12,7	18,8	– 11,0
Kongo, Dem. Republik	42 644	449	767	.	.	.	72,7	6,1	25,0	– 3,8
Nigeria	397 270	2 049	6 027	21,1	22,6	56,4	79,9	4,6	15,5	.
Südafrika	368 135	6 377	13 675	2,6	28,9	68,6	59,4	20,9	18,6	1,4
Tansania, Ver. Republik	57 862	1 134	3 444	.	.	.	59,4	8,5	34,0	– 2,0
Amerika										
Argentinien	518 092	11 627	20 537	6,7	25,8	67,5	66,3	17,7	18,8	– 2,7
Brasilien	1 868 180	8 968	16 154	5,2	22,6	72,2	64,0	20,0	15,0	1,0
Chile	298 172	16 079	25 978	4,2	32,8	63,0	63,0	14,0	21,6	1,4
Kanada	1 711 390	46 261	49 651	1,7	27,4	70,9	58,2	20,7	23,6	– 2,3
Kolumbien	333 114	6 684	14 943	7,1	32,0	60,9	68,6	14,9	21,6	– 5,1
Mexiko	1 223 360	9 807	20 602	3,6	32,5	63,9	65,3	11,7	23,0	– 1,8
Vereinigte Staaten	20 494 050	62 606	62 606	0,9	18,5	80,7	68,4	14,0	20,6	– 3,0
Asien										
Bangladesch	287 630	1 745	4 620	14,2	29,3	56,5	68,7	6,0	30,5	– 5,2
China	13 407 400	9 608	18 110	8,4	41,3	50,4	38,7	14,5	44,3	1,8
Indien	2 716 750	2 036	7 874	17,1	29,1	53,9	59,0	11,0	30,9	– 3,2
Indonesien	1 022 450	3 871	13 230	13,7	41,0	45,4	57,3	9,1	33,7	1,0
Iran, Islamische Republik	452 275	5 491	19 557	9,6	35,3	55,0	47,6	13,4	34,7	1,1
Israel	369 843	41 644	37 972	1,3	21,7	76,9	54,9	22,6	20,8	1,7
Japan	4 971 930	39 306	44 227	1,1	28,1	70,8	55,5	19,7	23,9	0,9
Korea, Republik	1 619 420	31 346	41 351	2,2	39,6	58,3	48,1	15,3	31,1	5,4
Malaysia	354 348	10 942	30 860	8,9	39,3	51,7	55,3	12,2	25,6	6,9
Myanmar	68 559	1 298	6 511	23,7	36,2	40,1	.	.	32,8	– 8,0
Pakistan	312 570	1 555	5 680	24,7	19,1	56,3	82,0	11,3	16,1	– 9,3
Philippinen	330 846	3 104	8 936	9,7	30,5	59,9	73,5	11,2	25,1	– 9,8
Saudi-Arabien	782 483	23 566	55 944	2,5	45,1	52,4	41,2	24,4	28,9	5,5
Thailand	487 239	7 187	19 476	8,7	35,1	56,3	48,7	16,4	22,8	13,8
Ver. Arabische Emirate	424 635	40 711	69 382	0,8	43,6	55,6	34,9	12,3	24,8	28,0
Vietnam	241 272	2 551	7 511	17,0	37,1	45,8	68,0	6,5	26,6	2,8
Australien und Ozeanien										
Australien	1 418 280	56 352	52 373	2,7	24,7	72,6	56,7	18,6	24,1	0,6
Neuseeland	203 404	41 267	40 135	5,4	22,9	71,7	57,5	18,0	23,5	0,9

1 Quelle: World Economic Outlook, Internationaler Währungsfonds (IMF). Zum Teil vorläufige Werte.
2 Quelle: Eigene Berechnungen basierend auf UNdata, Vereinte Nationen.
3 Quelle: World Development Indicators, Weltbank.
4 Weitere Informationen zu dieser Währungseinheit siehe Erläuterungen auf Seite 674.

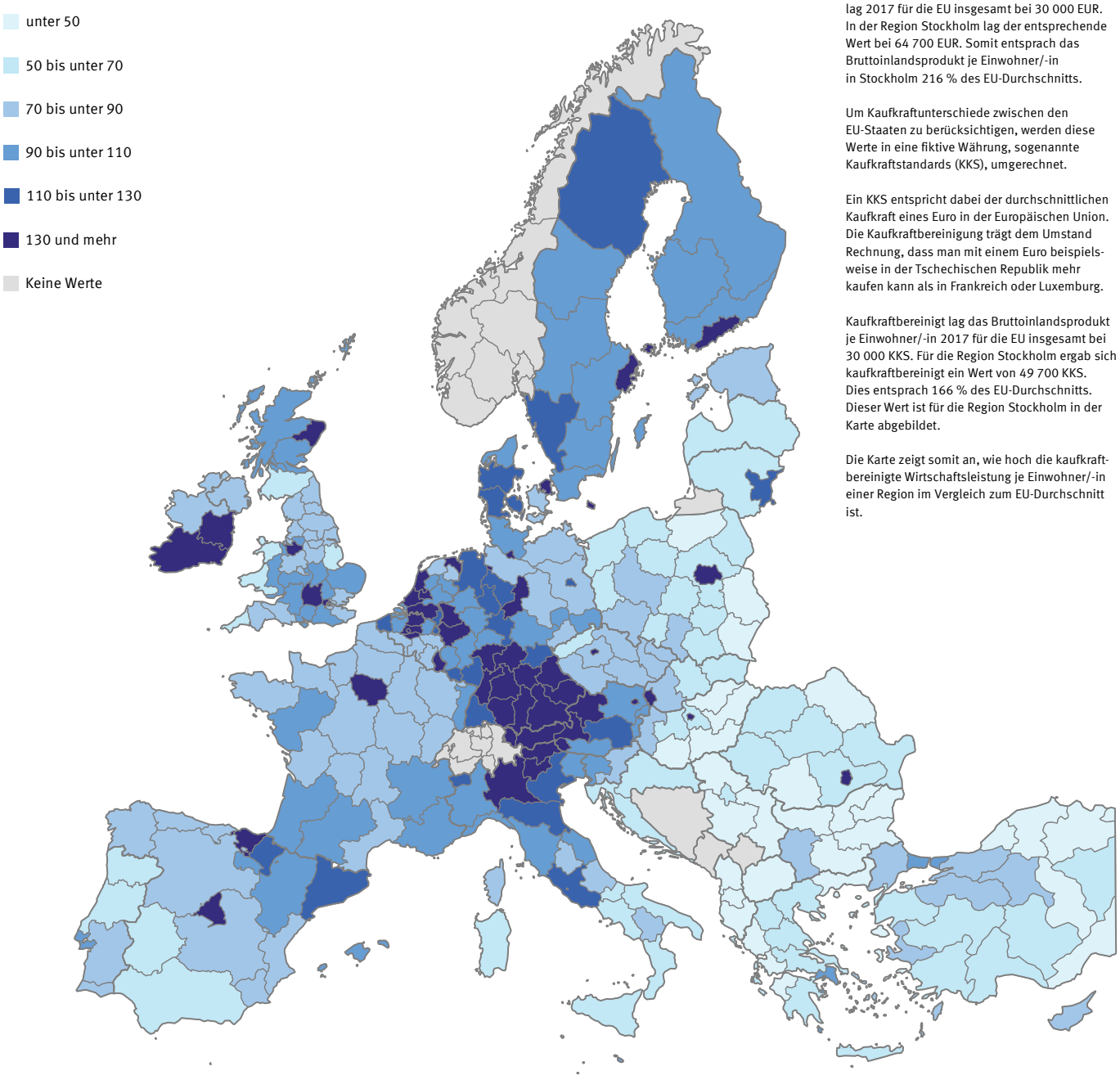
Bruttowertschöpfung nach Sektoren 2017
in % des BIP



Quelle: Eigene Berechnungen basierend auf UNdata, Vereinte Nationen

2019 - 01 - 0318

Bruttoinlandsprodukt je Einwohner/-in nach Regionen (NUTS-2-Ebene) 2017
Kaufkraftbereinigt, in % des EU-Durchschnitts (EU = 100)



Beispiel zur Interpretation der Karte:
Das **Bruttoinlandsprodukt (BIP) je Einwohner/-in** lag 2017 für die EU insgesamt bei 30 000 EUR. In der Region Stockholm lag der entsprechende Wert bei 64 700 EUR. Somit entsprach das Bruttoinlandsprodukt je Einwohner/-in in Stockholm 216 % des EU-Durchschnitts.

Um Kaufkraftunterschiede zwischen den EU-Staaten zu berücksichtigen, werden diese Werte in eine fiktive Währung, sogenannte Kaufkraftstandards (KKS), umgerechnet.

Ein KKS entspricht dabei der durchschnittlichen Kaufkraft eines Euro in der Europäischen Union. Die Kaufkraftbereinigung trägt dem Umstand Rechnung, dass man mit einem Euro beispielsweise in der Tschechischen Republik mehr kaufen kann als in Frankreich oder Luxemburg.

Kaufkraftbereinigt lag das Bruttoinlandsprodukt je Einwohner/-in 2017 für die EU insgesamt bei 30 000 KKS. Für die Region Stockholm ergab sich kaufkraftbereinigt ein Wert von 49 700 KKS. Dies entsprach 166 % des EU-Durchschnitts. Dieser Wert ist für die Region Stockholm in der Karte abgebildet.

Die Karte zeigt somit an, wie hoch die kaufkraftbereinigte Wirtschaftsleistung je Einwohner/-in einer Region im Vergleich zum EU-Durchschnitt ist.

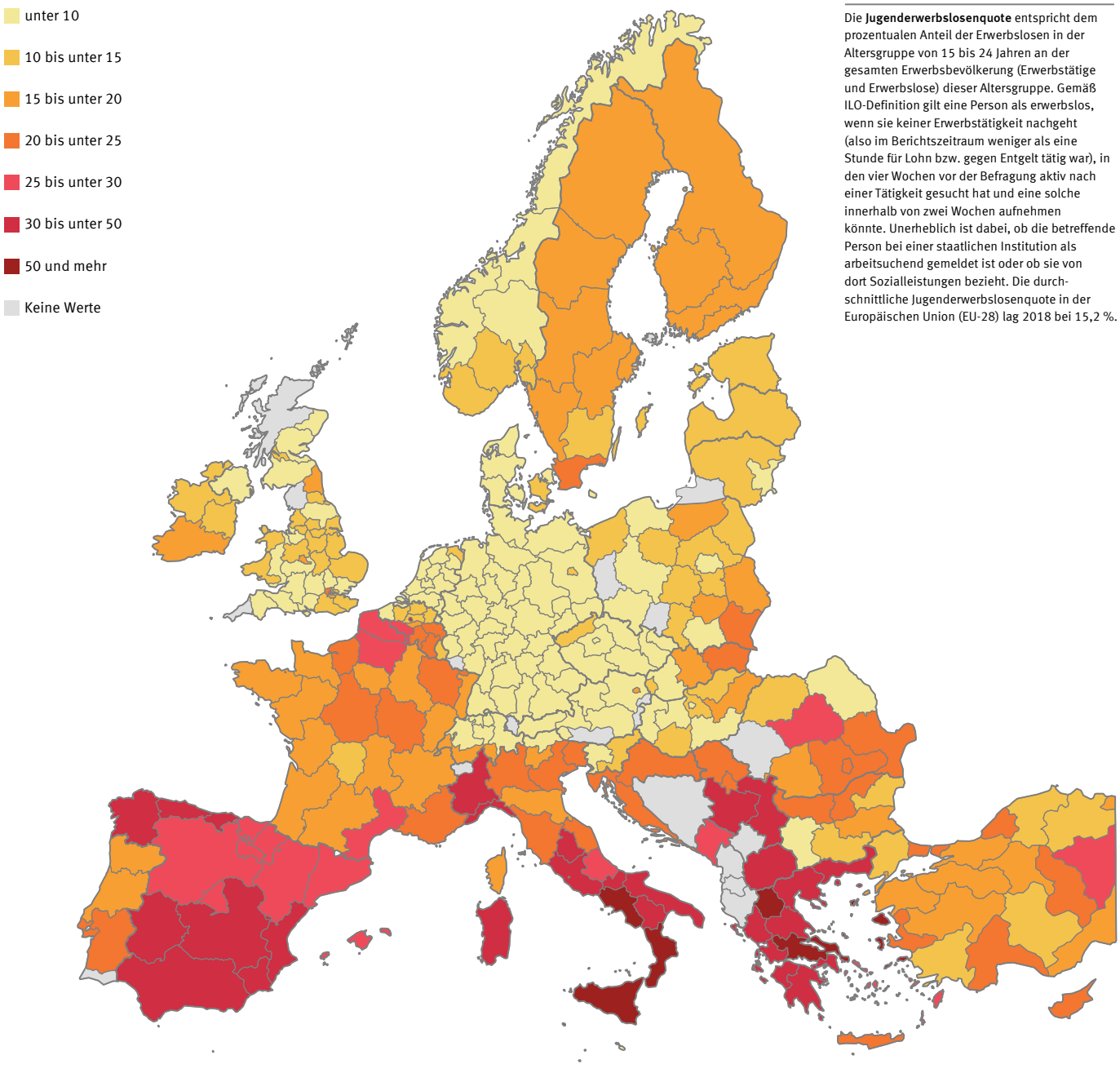
Kartengrundlage: © EuroGeographics bezüglich der Verwaltungsgrenzen
Quelle: Volkswirtschaftliche Gesamtrechnungen, Eurostat

2019 - 01 - 0319

A.13 Arbeitsmarkt

Jugenderwerbslosenquote nach Regionen (NUTS-2-Ebene) 2018

in % der Erwerbsbevölkerung im Alter von 15 bis 24 Jahren



Die **Jugenderwerbslosenquote** entspricht dem prozentualen Anteil der Erwerbslosen in der Altersgruppe von 15 bis 24 Jahren an der gesamten Erwerbsbevölkerung (Erwerbstätige und Erwerbslose) dieser Altersgruppe. Gemäß ILO-Definition gilt eine Person als erwerbslos, wenn sie keiner Erwerbstätigkeit nachgeht (also im Berichtszeitraum weniger als eine Stunde für Lohn bzw. gegen Entgelt tätig war), in den vier Wochen vor der Befragung aktiv nach einer Tätigkeit gesucht hat und eine solche innerhalb von zwei Wochen aufnehmen könnte. Unerheblich ist dabei, ob die betreffende Person bei einer staatlichen Institution als arbeitsuchend gemeldet ist oder ob sie von dort Sozialleistungen bezieht. Die durchschnittliche Jugenderwerbslosenquote in der Europäischen Union (EU-28) lag 2018 bei 15,2 %.

Kartengrundlage: © EuroGeographics bezüglich der Verwaltungsgrenzen

Quelle: Arbeitskräfteerhebung, Eurostat

2019 - 01 - 0320

A.13 Arbeitsmarkt

	Erwerbspersonen [1]	Erwerbstätigenquote [1]		Teilzeitquote [2]		Selbstständige [1]	Erwerbstätige [1]			Erwerbslosenquote [1]	
		Männer	Frauen	Männer	Frauen		Land- und Forstwirtschaft, Fischerei	Produzierendes Gewerbe	Dienstleistungsbereich	15 – 64 Jahre	15 – 24 Jahre
	15 – 64 Jahre										
	2017										
	1 000	%		% der erwerbstätigen Männer bzw. Frauen im Alter 15 – 64 Jahre		% der Erwerbstätigen	%			% der Erwerbspersonen der jeweiligen Altersgruppe	
Europa											
Europäische Union	243 039	72,9	62,4	7,3	26,3	15,6	4,3	24,0	71,8	7,8	16,8
Belgien	5 004	67,5	58,7	6,2	27,7	14,3	1,3	21,3	77,4	7,2	19,3
Bulgarien	3 290	70,6	63,1	1,3	2,0	11,9	6,3	29,3	64,5	6,2	12,9
Dänemark	2 886	76,9	71,5	14,4	24,6	8,2	2,6	18,8	78,6	5,9	11,0
Deutschland	**42 061**	**78,9**	**71,5**	**7,9**	**36,0**	**10,2**	**1,3**	**27,3**	**71,5**	**3,8**	**6,8**
Estland	663	77,4	70,9	4,3	9,6	10,2	3,9	29,9	66,2	5,9	12,1
Finnland	2 640	71,4	68,5	9,2	16,3	13,2	3,9	22,3	73,8	8,8	20,1
Frankreich	29 857	68,4	61,2	6,5	21,7	11,6	2,9	20,4	76,8	9,5	22,3
Griechenland	5 004	62,7	44,4	7,0	16,4	34,1	12,1	15,3	72,6	21,7	43,6
Irland	2 237	73,0	62,4	10,6	32,8	15,4	5,4	19,2	75,5	6,9	14,4
Island	194	88,6	83,5	9,9	23,3	11,8	3,6	16,6	79,8	2,9	7,9
Italien	24 613	67,1	48,9	7,9	32,4	23,2	3,9	26,3	69,8	11,4	34,7
Kroatien	1 832	63,8	54,0	3,0	4,8	12,4	7,5	27,0	65,4	11,3	27,4
Lettland	976	71,9	68,4	4,0	8,2	12,7	7,5	24,0	68,5	8,9	17,0
Litauen	1 450	70,6	70,2	4,4	8,5	12,0	7,8	25,0	67,2	7,3	13,3
Luxemburg	282	69,9	62,5	4,4	26,0	9,9	1,0	11,9	87,1	5,5	15,4
Malta	199	80,1	57,6	4,1	16,9	14,6	1,3	19,4	79,3	4,1	10,6
Niederlande	8 809	80,4	71,3	17,3	58,3	16,7	2,2	16,5	81,3	4,9	8,9
Norwegen	2 680	75,6	72,4	10,9	26,7	6,5	2,1	19,5	78,5	4,3	10,4
Österreich	4 449	76,2	68,2	7,7	34,2	12,4	4,3	25,6	70,1	5,6	9,8
Polen	18 222	72,8	59,5	2,9	8,9	20,4	10,6	31,3	58,1	5,0	14,8
Portugal	5 018	71,1	64,8	3,5	9,5	17,0	6,8	24,8	68,3	9,2	23,9
Rumänien	8 839	71,8	55,8	2,3	4,2	26,3	22,9	29,1	48,0	5,1	18,3
Russische Föderation	72 839	75,6	65,5	2,3	4,5	6,6	6,7	26,9	66,4	5,2	16,3
Schweden	5 123	78,3	75,4	8,3	16,0	9,9	1,9	18,1	80,0	6,9	17,9
Schweiz	4 746	84,3	75,2	9,2	43,4	14,9	3,5	20,7	75,8	5,0	8,1
Slowakei	2 736	72,0	60,3	3,8	7,5	15,2	2,9	36,3	60,8	8,2	18,9
Slowenien	1 018	72,5	65,8	5,6	11,5	14,6	4,9	32,6	62,5	6,7	11,2
Spanien	22 620	66,5	55,7	6,6	22,0	16,5	4,1	19,5	76,4	17,3	38,6
Tschechische Republik	5 303	80,9	66,2	1,8	7,6	17,1	2,9	37,9	59,3	2,9	8,0
Türkei	31 085	70,7	32,2	5,4	17,5	32,7	19,4	26,8	53,8	11,1	20,5
Ungarn	4 637	75,2	61,3	2,0	4,6	10,3	5,0	30,2	64,8	4,2	10,7
Vereinigtes Königreich	32 673	78,6	69,7	10,0	35,9	15,4	1,1	18,4	80,5	4,4	12,1
Zypern	599	70,0	61,4	7,0	13,0	13,2	3,5	17,0	79,4	11,3	24,7

Zu den **Erwerbspersonen** zählen alle Personen einer bestimmten Altersgruppe, die Arbeit haben (Erwerbstätige) oder suchen (Erwerbslose).

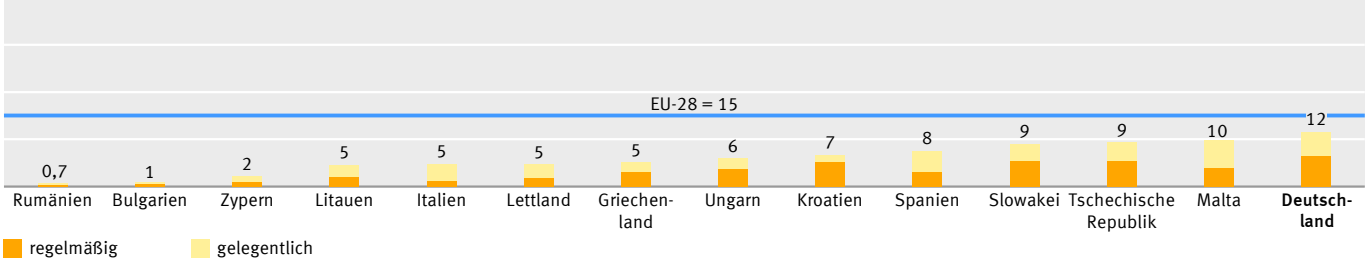
Die **Erwerbstätigenquote** beschreibt den Anteil der Erwerbstätigen einer Altersgruppe an der Gesamtbevölkerung derselben Altersgruppe.

Die **Teilzeitquote** der OECD entspricht dem Anteil der erwerbstätigen Männer bzw. Frauen, deren reguläre Wochenarbeitszeit weniger als 30 Stunden beträgt.

Alle hier aufgeführten Indikatoren entsprechen dem **Erwerbskonzept der Internationalen Arbeitsorganisation (ILO)**. Nähere Informationen hierzu sowie weitere Begriffserläuterungen zum Thema Arbeitsmarkt siehe „Glossar“/„Methodik“ des Kapitels 13.

Arbeiten im Home-Office 2018

Anteil der Erwerbstätigen im Alter von 15 bis 64 Jahren, der zuhause arbeitet, in %



Quelle: Arbeitskräfteerhebung, Eurostat

2019 - 01 - 0321

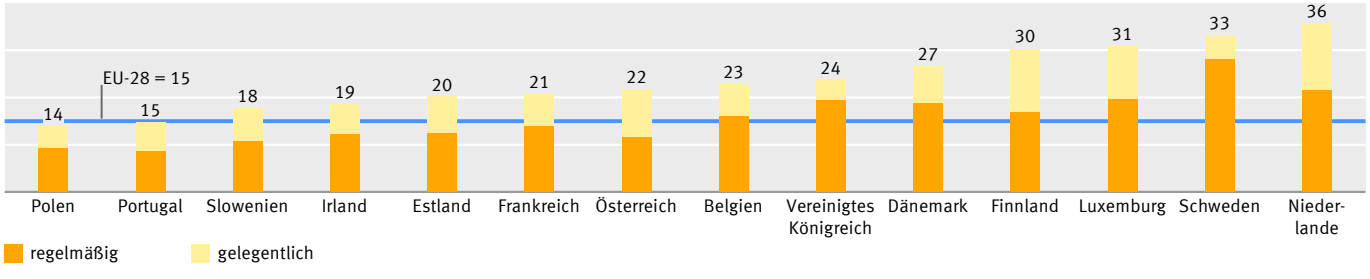
A.13 Arbeitsmarkt

	Erwerbspersonen [1]	Erwerbstätigenquote [1]		Teilzeitquote [2]		Selbstständige [1]	Erwerbstätige [1]			Erwerbslosenquote [1]	
		Männer	Frauen	Männer	Frauen		Land- und Forstwirtschaft, Fischerei	Produzierendes Gewerbe	Dienstleistungsbereich	15 – 64 Jahre	15 – 24 Jahre
	15 – 64 Jahre										
	2017										
	1 000	%		% der erwerbstätigen Männer bzw. Frauen im Alter 15 – 64 Jahre		% der Erwerbstätigen	%			% der Erwerbspersonen der jeweiligen Altersgruppe	
Afrika											
Ägypten	30 565	63,7	17,7	.	.	31,9	24,8	25,5	49,6	11,9	29,6
Äthiopien	48 293	.	.	.	.	86,8	68,2	9,4	22,4	17,9 [3]	7,4
Kenia	18 889	75,7 [4]	69,8 [4]	.	.	61,9	38,0	14,3	47,8	2,9 [4]	26,2
Kongo, Dem. Republik	26 537	.	.	.	.	81,8	81,9	11,1	7,0	.	7,3
Nigeria	56 151	54,3 [4]	45,9 [4]	.	.	81,6	36,6	11,6	51,8	6,6 [4]	13,8
Südafrika	22 190	49,1	37,6	5,8	12,6	15,2	5,6	23,4	71,1	27,3	53,3
Tansania, Ver. Republik	25 205	87,9 [3]	79,8 [3]	.	.	85,8	66,7	6,0	27,3	2,2 [3]	3,9
Amerika											
Argentinien	19 372	72,9	51,1	.	.	25,3	0,5	23,3	76,1	8,5	22,6
Brasilien	102 393	70,1	51,0	10,0	21,7	32,3	10,3	20,9	68,8	13,1	29,2
Chile	8 486	72,5	52,8	11,1	23,6	28,7	9,6	22,8	67,6	7,3	17,2
Kanada	19 249	76,3	70,6	11,5	25,2	15,2	2,0	19,6	78,4	6,4	11,6
Kolumbien	25 175	79,0	55,6	7,8	25,0	51,1	16,1	19,4	64,5	9,2	17,8
Mexiko	55 451	79,0	44,9	10,7	25,5	31,5	13,1	25,8	61,1	3,6	6,9
Vereinigte Staaten	154 222 [5]	75,4 [5]	65,0 [5]	.	.	6,3	1,7	18,9	79,5	4,4 [5]	9,2 [6]
Asien											
Bangladesch	66 908	80,9	35,5	.	.	60,5	39,1	21,1	39,9	4,6	12,8
China	771 318	.	.	.	.	47,5	17,5	26,6	55,9	.	10,8
Indien	481 660	.	.	.	.	78,8	42,7	23,8	33,5	.	10,5
Indonesien	123 046	80,0	52,1	19,2	33,8	51,2	31,2	21,7	47,1	4,4	15,6
Iran, Islamische Republik	26 849	67,4	15,0	.	.	45,3	17,1	32,4	50,5	12,3	28,4
Israel	3 642	72,5	65,7	7,8	20,8	12,4	1,1	17,3	81,6	4,3	7,3
Japan	59 537	82,9	67,4	7,7	34,1	10,4	3,5	25,6	70,9	3,0	4,6
Korea, Republik	25 512	76,1	56,9	5,6	14,3	25,4	4,9	24,8	70,3	3,8	10,4
Malaysia	14 931	77,7 [4]	52,2 [4]	.	.	25,4	11,0	27,4	61,6	3,4 [4]	10,9
Myanmar	23 883	80,7	50,9	.	.	63,2	49,9	16,6	33,5	1,6	4,0
Pakistan	66 196	80,0 [7]	23,5 [7]	.	.	61,0	42,0	23,7	34,3	3,4 [7]	7,7
Philippinen	41 210	73,6	45,6	.	.	37,8	26,0	17,7	56,3	2,7	7,5
Saudi-Arabien	13 701	77,5 [7]	17,6 [7]	.	.	4,8	6,3	22,6	71,2	5,7 [4]	25,0
Thailand	36 749	81,3	65,9	.	.	50,6	32,8	22,6	44,7	0,9	4,4
Ver. Arabische Emirate	6 717	92,1	49,9	.	.	3,5	0,4	38,9	60,7	2,5	7,7
Vietnam	55 092	84,1	77,0	.	.	57,2	40,9	25,1	34,1	2,1	7,5
Australien und Ozeanien											
Australien	12 406	77,9	68,2	13,8	37,1	16,9	2,6	19,1	78,3	5,8	12,6
Neuseeland	2 471	81,9	72,0	9,7	30,3	18,6	6,6	20,2	73,1	4,9	12,7

1 Quelle: ILOSTAT, Internationale Arbeitsorganisation (ILO).
2 Quelle: Eigene Berechnungen basierend auf Daten der OECD.
3 2014.
4 2016.
5 Altersklasse 16 bis 64 Jahre.
6 Altersklasse 16 bis 24 Jahre.
7 2015.

Arbeiten im Home-Office 2018

Anteil der Erwerbstätigen im Alter von 15 bis 64 Jahren, der zuhause arbeitet, in %



Quelle: Arbeitskräfteerhebung, Eurostat

2019 - 01 - 0321

A.14 Verdienste und Arbeitskosten

	Durchschnittlicher Bruttostundenverdienst		Lohnnebenkosten	Arbeitskosten			Gesetzlicher, branchenübergreifender monatlicher Mindestlohn	Gender Pay Gap: Unterschied zwischen Bruttostundenverdienst von Frauen und Männern
	Produzierendes Gewerbe und marktbestimmte Dienstleistungen (NACE B-N)					Verarbeitendes Gewerbe		
	Vollbeschäftigte in Unternehmen mit 10 oder mehr Beschäftigten		je 100 EUR Bruttoverdienst [1]	je geleistete Stunde	Veränderung zum Vorjahr [1]	je geleistete Stunde		
	2014		2018				2019	2017
	EUR	KKS [2]	EUR		%	EUR	EUR/Monat	%
Europa								
Europäische Union	15,23	14,61	*30*	*26,60*	*2,4*	*27,00*	–	*16*
Belgien	19,90	18,31	*37*	*40,00*	*1,7*	*42,60*	1 594	*6*
Bulgarien	2,34	4,90	*19*	*5,30*	*6,5*	*4,70*	286	*14*
Dänemark	27,61	19,85	*16*	*44,70*	*2,1*	*45,20*	–	*15*
Deutschland	**17,78**	**17,52**	***27***	***35,00***	***2,3***	***40,00***	**1 557**	***21***
Estland	5,78	7,64	*35*	*12,60*	*5,6*	*11,70*	540	*26*
Finnland	19,61	16,03	*25*	*34,50*	*1,4*	*36,80*	–	*17*
Frankreich	17,40	16,16	*45*	*36,50*	*2,8*	*37,60*	1 521	*15*
Griechenland	9,48	11,09	*33*	*16,10*	*2,4*	*15,60*	758	.
Irland	24,22	19,81	*18*	*30,50*	*3,2*	*32,10*	1 656	.
Island	16,06	13,61	.	.	.	.	.	*16*
Italien	15,42	14,98	*40*	*27,20*	*1,6*	*27,50*	–	*5*
Kroatien	5,73	8,67	*19*	*10,90*	*8,9*	*9,90*	506	*12*
Lettland	4,41	6,29	*29*	*9,70*	*12,1*	*8,80*	430	*16*
Litauen	3,91	6,23	*43*	*9,20*	*10,0*	*8,80*	555	*15*
Luxemburg	22,94	19,05	*13*	*40,30*	*1,5*	*33,80*	2 071	*5*
Malta	9,89	12,23	*8*	*14,10*	*0,1*	*13,70*	762	*12*
Niederlande	17,89	16,29	*30*	*34,70*	*2,2*	*38,50*	1 636	*15*
Norwegen	30,80	21,03	.	.	.	.	–	*14*
Österreich	15,93	15,06	*38*	*34,90*	*2,9*	*37,50*	–	*20*
Polen	5,66	10,13	*22*	*9,90*	*6,9*	*9,10*	523	*7*
Portugal	7,45	9,15	*26*	*13,30*	*1,8*	*11,40*	700	*16*
Rumänien	2,79	5,26	.	*6,50*	*8,5*	*5,90*	446	*4*
Russische Föderation	.	.	.	.	.	.	.	.
Schweden	20,64	16,44	*48*	*39,30*	*– 4,5*	*40,70*	–	*13*
Schweiz	33,72	22,65	.	.	.	.	–	*17*
Slowakei	5,33	7,86	*37*	*11,80*	*6,7*	*12,10*	520	*20*
Slowenien	8,84	10,82	*19*	*18,30*	*3,4*	*18,10*	887	*8*
Spanien	11,85	12,84	*35*	*21,30*	*1,8*	*23,00*	1 050	*15*
Tschechische Republik	5,38	8,45	*37*	*12,70*	*10,7*	*12,60*	519	*21*
Türkei	3,84	6,41	.	.	.	.	422	.
Ungarn	4,64	8,07	*25*	*9,90*	*5,6*	*9,70*	464	*14*
Vereinigtes Königreich	18,76	15,44	*20*	*26,30*	*2,3*	*26,30*	1 525	*21*
Zypern	11,09	12,31	*16*	*14,40*	*2,9*	*12,20*	–	*14*

1 Eigene Berechnungen basierend auf Eurostat Daten.
2 Weitere Informationen zur Einheit KKS (Kaufkraftstandard) siehe Erläuterungstext neben der Tabelle.

Quelle: Eurostat

Der **Bruttostundenverdienst** enthält alle Zahlungen an Arbeitnehmerinnen und Arbeitnehmer, einschließlich aller Zuschläge. Enthalten sind Arbeitnehmeranteile, jedoch nicht Arbeitgeberanteile zur Sozialversicherung.

Hauptbestandteil der **Lohnnebenkosten** sind die Sozialbeiträge der Arbeitgeber, also vor allem die gesetzlichen Arbeitgeberbeiträge zu den Sozialversicherungen, die Aufwendungen für die betriebliche Altersversorgung sowie die Aufwendungen für die Lohn- und Gehaltsfortzahlungen im Krankheitsfall.

Die **Arbeitskosten** umfassen die Gesamtheit aller Aufwendungen, die Arbeitgeberinnen und Arbeitgeber durch die Beschäftigung von Arbeitskräften tragen. Zu den Arbeitskosten gehören das Arbeitnehmerentgelt mit Bruttoverdiensten, die Sozialbeiträge der Arbeitgeberinnen und Arbeitgeber, die Kosten der beruflichen Aus- und Weiterbildung, sonstige Aufwendungen sowie Steuern auf die Lohnsumme oder Beschäftigtenzahl.

Vollbeschäftigte sind Vollzeitbeschäftigte und Teilzeitbeschäftigte, wobei der Verdienst der Teilzeitbeschäftigten so hochgerechnet wird, als würden sie Vollzeit arbeiten.

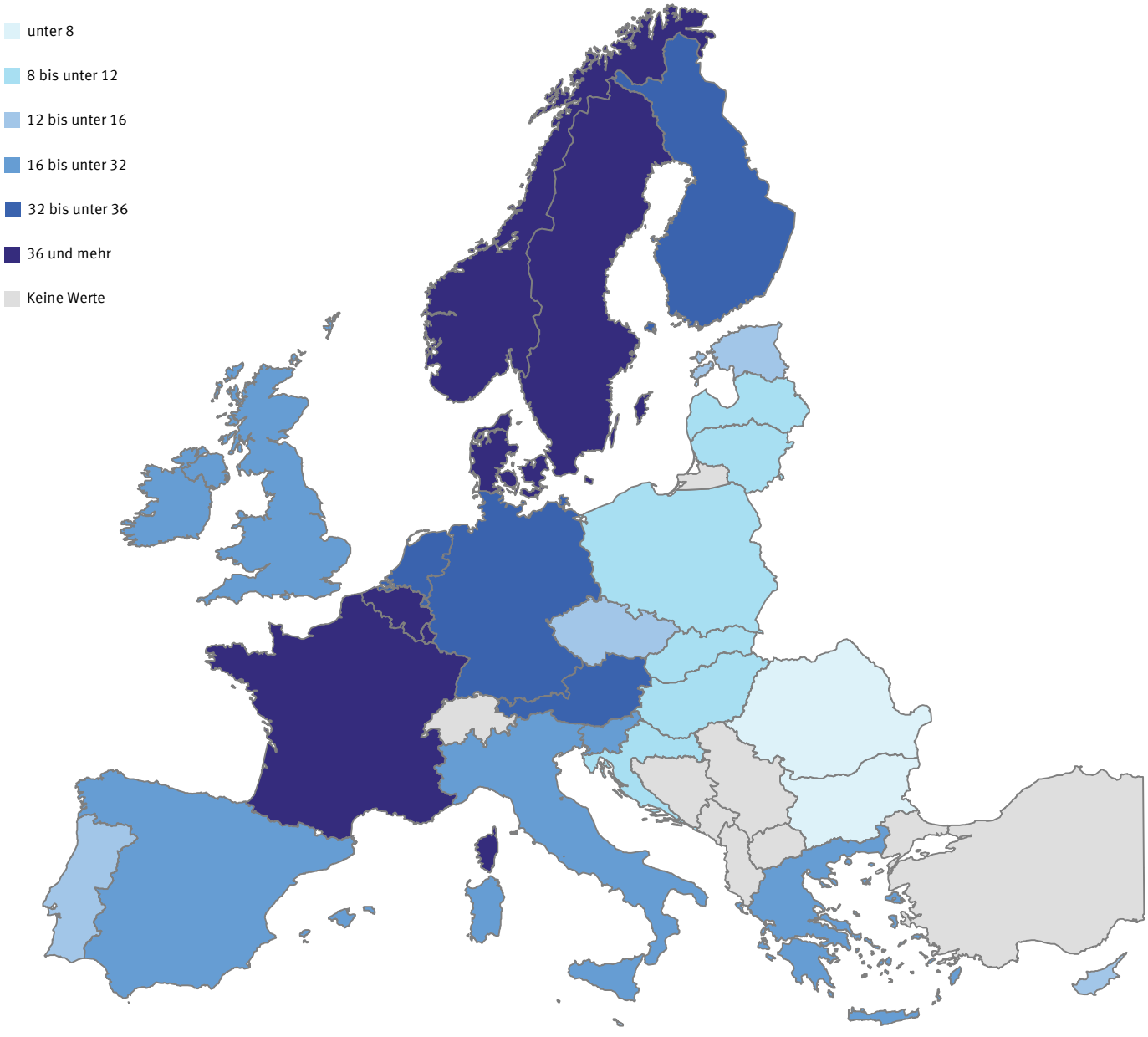
Die Einteilung der **Wirtschaftsbereiche** entspricht der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2). Abschnitt C: Verarbeitendes Gewerbe/Herstellung von Waren, Abschnitte B bis N: Produzierendes Gewerbe und marktbestimmte Dienstleistungen.

Der hier aufgeführte **Verdienstunterschied zwischen Frauen und Männern** entspricht dem unbereinigten Gender Pay Gap. Während der unbereinigte Wert die vorhandenen Einkommensunterschiede von Frauen und Männern misst ohne mögliche Einflussfaktoren zu berücksichtigen, werden beim bereinigten Gender Pay Gap Verzerrungseffekte (z.B. geschlechtsspezifische Unterschiede hinsichtlich Qualifikation oder Berufswahl) herausgerechnet. Der Verdienstunterschied wird angegeben in Prozent des durchschnittlichen Bruttostundenverdienstes von Männern. Ein Wert von 5% bedeutet, dass Frauen durchschnittlich pro Stunde brutto 5% weniger verdienen als Männer.

KKS oder **Kaufkraftstandard** ist eine künstliche Währung, mit deren Hilfe Unterschiede im Preisniveau zwischen den EU-Staaten ausgeglichen werden. Ein KKS entspricht dabei der durchschnittlichen Kaufkraft eines Euro in der Europäischen Union. Die Angaben in Kaufkraftstandards ermöglichen einen kaufkraftbereinigten Vergleich der Verdienste in Europa.

A.14 Verdienste und Arbeitskosten

Arbeitskosten je Stunde 2018
Produzierendes Gewerbe und marktbestimmte Dienstleistungen (NACE B-N), in Euro



Kartengrundlage: © EuroGeographics bezüglich der Verwaltungsgrenzen
Quelle: Eurostat

2019- 01 - 0322

A.15 Preise

	Verbraucherpreise			Erzeugerpreise gewerblicher Produkte [1]		Preisniveauvergleich [2]
	insgesamt [3]		Nahrungsmittel und alkoholfreie Getränke [4]	insgesamt		Index
	2018	2017		2018	2017	2018
	Veränderung gegenüber Vorjahr in %					Deutschland = 100
Europa						
Europäische Union	*1,9*	*1,7*	.	.	.	96
Belgien	*2,1*	*2,1*	*1,4*	*4,5*	*8,1*	108
Bulgarien	*2,8*	*2,1*	*4,5*	*3,9*	*5,0*	44
Dänemark	*0,8*	*1,1*	*3,0*	*4,3*	*2,5*	133
Deutschland	***1,7***	***1,5***	***3,2***	***2,6***	***2,7***	**100**
Estland	*3,4*	*3,4*	*7,1*	*2,6*	*3,6*	73
Finnland	*1,1*	*0,8*	*– 1,1*	*8,2*	*4,0*	119
Frankreich	*1,9*	*1,0*	*1,0*	*2,4*	*2,3*	103
Griechenland	*0,6*	*1,1*	*0,4*	*3,2*	*4,2*	79
Irland	*0,5*	*0,3*	*– 2,0*	*– 2,4*	*0,8*	124
Island	*2,7*	*1,8*	*– 2,9*	*6,8*	*– 4,6*	157
Italien	*1,1*	*1,2*	*2,1*	*3,3*	*2,3*	97
Kroatien	*1,5*	*1,1*	*3,2*	*2,4*	*2,1*	61
Lettland	*2,5*	*2,9*	*6,2*	*4,5*	*2,6*	67
Litauen	*2,7*	*3,7*	*4,1*	*5,5*	*6,0*	59
Luxemburg	*1,5*	*1,7*	*3,1*	*5,8*	*4,8*	136
Malta	*1,2*	*1,4*	*3,3*	*4,7*	*1,6*	80
Niederlande	*1,7*	*1,4*	*2,9*	*3,0*	*4,8*	110
Norwegen	*2,8*	*1,9*	*0,0*	.	*9,3*	149
Österreich	*2,0*	*2,1*	*2,8*	*2,4*	*2,0*	109
Polen	*1,8*	*2,1*	*4,6*	*2,1*	*2,8*	52
Portugal	*1,0*	*1,4*	*1,6*	*3,1*	*3,3*	81
Rumänien	*4,6*	*1,3*	*2,4*	.	*3,6*	47
Russische Föderation	*2,9*	*3,7*	*4,6*	*12,2*	*7,6*	.
Schweden	*2,0*	*1,8*	*2,4*	*6,6*	*5,2*	122
Schweiz	*0,9*	*0,5*	*0,4*	*1,3*	*0,0*	153
Slowakei	*2,5*	*1,3*	*4,4*	.	*2,8*	63
Slowenien	*1,7*	*1,4*	*2,6*	*1,9*	*1,3*	80
Spanien	*1,7*	*2,0*	*1,4*	*3,0*	*4,4*	90
Tschechische Republik	*2,1*	*2,5*	*6,1*	*2,0*	*1,8*	62
Türkei	*16,3*	*11,1*	*21,1*	*27,0*	*15,8*	36
Ungarn	*2,9*	*2,3*	*3,2*	*5,5*	*3,3*	57
Vereinigtes Königreich	*2,3*	*2,6*	*2,3*	*2,9*	*7,1*	113
Zypern	*0,8*	*0,5*	*– 0,4*	*2,2*	*3,4*	87

Der **Verbraucherpreisindex** misst die Preisentwicklung aller Waren und Dienstleistungen, die private Haushalte für Konsumzwecke kaufen (z. B. die Preisentwicklung bei Nahrungsmitteln, Mieten, Strom, Kraftstoffen oder Reparaturen). Die hier angezeigte Veränderung des Verbraucherpreisindex gegenüber dem Vorjahr wird auch als **Inflationsrate** bezeichnet.

Der **Erzeugerpreisindex gewerblicher Produkte** misst die durchschnittliche Entwicklung der Verkaufspreise für Produkte einzelner Wirtschaftszweige auf der Wirtschaftsstufe der Erzeugerinnen und Erzeuger.

Die aufgeführten Verbraucher- und Erzeugerpreisdaten sind **nationale Indizes**. Um einen direkten Vergleich der EU-Staaten zu ermöglichen, veröffentlicht Eurostat auch **harmonisierte Preisindizes**, die zum Teil leicht von den nationalen Indizes abweichen. Mehr zu diesem Thema auf der Eurostat Website unter *ec.europa.eu/eurostat/product?code=teicp000*

Preisniveauindizes liefern eine Messgröße für die Preisniveauunterschiede zwischen Staaten. Liegt beispielsweise der Index in Österreich im Vergleich zu Deutschland (Bezugsgröße = 100) bei 109, so sind die Lebenshaltungskosten in Österreich 9 % höher als in Deutschland.

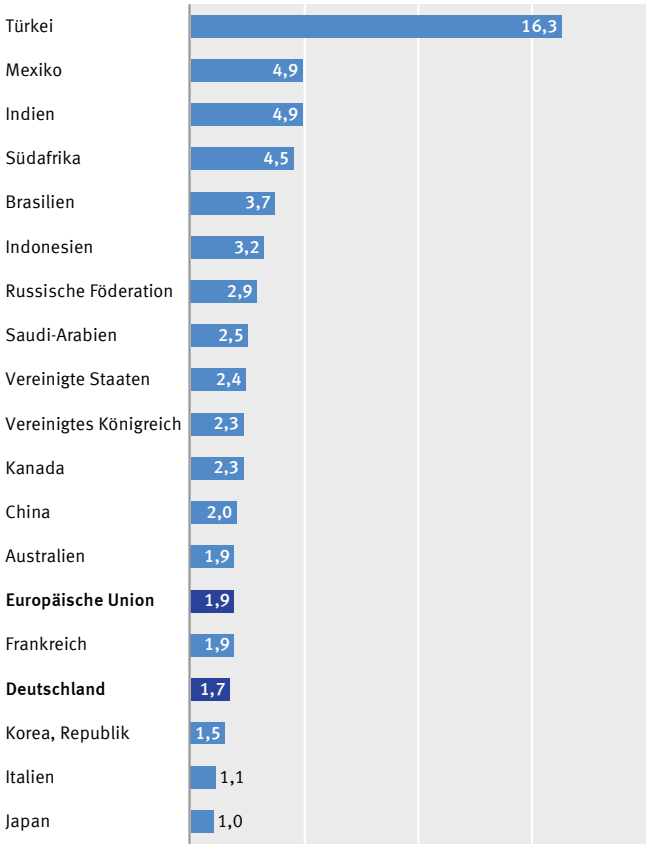
A.15 Preise

	Verbraucherpreise			Erzeugerpreise gewerblicher Produkte [1]	
	insgesamt [3]		Nahrungsmittel und alkoholfreie Getränke [4]	insgesamt	
	2018	2017		2018	2017
	Veränderung gegenüber Vorjahr in %				
Afrika					
Ägypten	.	29,5	87,5	.	.
Äthiopien	.	9,8	29,6	.	.
Kenia	4,7	8,0	25,3	.	.
Kongo, Dem. Republik	.	.	.	.	.
Nigeria	12,1	16,5	36,1	.	.
Südafrika	4,5	5,2	10,5	5,5	4,9
Tansania, Ver. Republik	3,5	5,3	.	.	.
Amerika					
Argentinien	.	.	.	.	.
Brasilien	3,7	3,4	1,7	6,9	– 0,7
Chile	2,4	2,2	2,4	4,9	10,5
Kanada	2,3	1,6	0,0	3,9	3,1
Kolumbien	3,2	4,3	0,9	.	0,5
Mexiko	4,9	6,0	9,2	3,9	6,9
Vereinigte Staaten	2,4	2,1	– 0,3	2,9	2,3
Asien					
Bangladesch	5,5	5,7	.	.	.
China	.	1,6	– 1,6	.	.
Indien	4,9	2,5	2,4	.	.
Indonesien	3,2	3,8	2,6	.	.
Iran, Islamische Republik	.	10,0	12,2	.	9,7
Israel	0,8	0,2	0,2	3,4	1,5
Japan	1,0	0,5	2,2	2,5	2,3
Korea, Republik	1,5	1,9	4,0	2,0	3,5
Malaysia	0,9	3,9	5,2	– 1,1	6,7
Myanmar	6,9	4,6	6,2	.	.
Pakistan	5,1	4,1	4,8	.	.
Philippinen	5,2	2,9	3,4	0,7	– 0,9
Saudi-Arabien	2,5	– 0,8	– 0,9	.	.
Thailand	1,1	0,7	0,0	0,4	0,7
Ver. Arabische Emirate	3,1	2,0	1,5	.	.
Vietnam	3,5	3,5	– 1,1	.	.
Australien und Ozeanien					
Australien	1,9	1,9	0,8	1,8	1,6
Neuseeland	1,6	1,9	2,4	4,2	4,5

1 Eigene Berechnungen basierend auf Daten des Internationalen Währungsfonds (IMF).
2 Quelle: Eigene Berechnungen basierend auf Eurostat Daten.
3 Quelle: Internationaler Währungsfonds (IMF).
4 Quelle: Eigene Berechnungen basierend auf Daten des Monthly Bulletin of Statistics (MBS), Vereinte Nationen.

Inflationsraten der G20-Mitglieder 2018

Veränderung des Verbraucherpreisindex gegenüber Vorjahr, in %



Für Argentinien liegen keine verlässlichen Daten vor.
Quelle: Internationaler Währungsfonds (IMF)

2019 - 01 - 0323

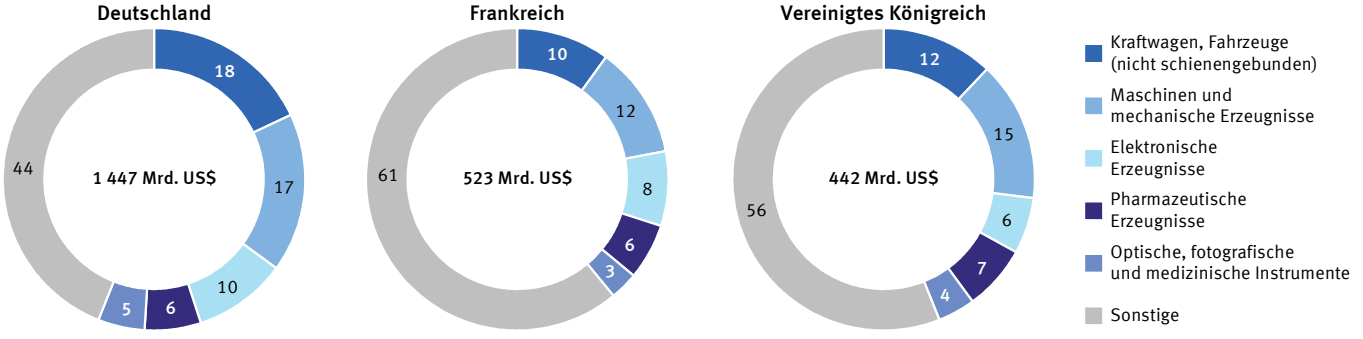
A.16 Außenhandel

	Exporte von Waren [1]	Importe von Waren [1]	Außenhandelsbilanz [1]	Wertindex der Warenexporte [2]	Wertindex der Warenimporte [2]	Warenexporte je Einwohner/-in [3]	Anteil der Warenexporte nach Deutschland [4]	Anteil der Warenimporte aus Deutschland [4]
	2017							
	Mill. US$			2000 = 100		US$	%	
Europa								
Europäische Union [5]	2 120 912	2 095 737	25 175	*241*	*231*	*4 139*	X	X
Belgien	429 980	406 412	23 568	*229*	*230*	*37 810*	*16,6*	*13,8*
Bulgarien	31 588	34 264	– 2 675	*620*	*522*	*4 464*	*12,9*	*12,2*
Dänemark	101 443	92 121	9 322	*200*	*205*	*17 582*	*14,2*	*21,3*
Deutschland	**1 446 642**	**1 167 753**	**278 889**	***263***	***235***	***17 494***	**X**	**X**
Estland	15 384	17 358	– 1 974	*380*	*329*	*11 694*	*6,9*	*10,3*
Finnland	67 281	70 100	– 2 820	*148*	*205*	*12 208*	*14,0*	*15,2*
Frankreich	523 385	613 133	– 89 748	*164*	*185*	*7 798*	*14,8*	*15,8*
Griechenland	32 155	55 301	– 23 146	*278*	*170*	*2 988*	*7,1*	*10,2*
Irland	138 072	88 828	49 244	*177*	*174*	*28 684*	*8,2*	*8,7*
Island	4 883	6 971	– 2 088	*256*	*269*	*14 307*	*7,6*	*10,6*
Italien	503 054	451 416	51 638	*211*	*189*	*8 308*	*12,5*	*16,3*
Kroatien	15 732	24 513	– 8 780	*363*	*315*	*3 813*	*12,3*	*15,8*
Lettland	13 030	15 897	– 2 867	*748*	*526*	*6 714*	*7,3*	*11,3*
Litauen	29 350	30 979	– 1 629	*785*	*591*	*10 379*	*7,2*	*12,1*
Luxemburg	13 959	21 071	– 7 112	*188*	*201*	*23 286*	*26,9*	*24,1*
Malta	4 039 [6]	7 182 [6]	– 3 143 [6]	*103*	*170*	*8 869* [6]	*10,7* [6]	*5,7* [6]
Niederlande	505 941	450 076	55 866	*280*	*264*	*29 530*	*21,9*	*18,5*
Norwegen	101 976	85 526	16 450	*173*	*241*	*19 306*	*15,5*	*11,1*
Österreich	159 971	166 475	– 6 505	*249*	*243*	*18 159*	*29,7*	*36,5*
Polen	221 308	217 979	3 329	*727*	*470*	*5 828*	*27,2*	*22,7*
Portugal	62 170	77 834	– 15 664	*256*	*196*	*6 040*	*11,3*	*13,7*
Rumänien	70 627	85 318	– 14 691	*680*	*650*	*3 606*	*23,0*	*20,1*
Russische Föderation	359 152	228 213	130 939	*337*	*531*	*2 486*	*4,3*	*10,0*
Schweden	153 106	153 856	– 751	*176*	*212*	*15 208*	*10,7*	*18,7*
Schweiz	299 309	267 501	31 807	*376* [6]	*327* [6]	*35 354*	*15,1*	*20,7*
Slowakei	84 487	82 977	1 510	*714*	*653*	*15 531*	*20,6*	*17,0*
Slowenien	28 773	28 192	581	*438*	*356*	*13 922*	*20,3*	*17,1*
Spanien	319 622	350 922	– 31 300	*278*	*226*	*6 863*	*10,9*	*12,5*
Tschechische Republik	182 231	162 899	19 332	*619*	*507*	*17 206*	*32,6*	*25,8*
Türkei	156 993	233 800	– 76 807	*565*	*429*	*1 944*	*9,6*	*9,1*
Ungarn	113 382	104 284	9 098	*403*	*334*	*11 592*	*27,3*	*26,5*
Vereinigtes Königreich	442 066	641 332	– 199 267	*155*	*186*	*6 696*	*10,6*	*14,0*
Zypern	3 360	9 308	– 5 948	*345*	*237*	*2 849*	*4,1*	*6,9*

Der **Wertindex der Warenexporte bzw. -importe** setzt den Wert der Warenexporte bzw. -importe im Jahr 2017 ins Verhältnis zum entsprechenden Wert im Basisjahr 2000. Beträgt der Index der Warenexporte beispielsweise 241 repräsentiert dies einen Wertanstieg der gehandelten Waren von 141 % im Zeitraum 2000 bis 2017. Diese Indexwerte orientieren sich ausschließlich am Wert der gehandelten Waren und nicht an der Menge.

Export ausgewählter Warengruppen 2017

Anteil an den Warenexporten insgesamt, in %



Quelle: UN Comtrade, Vereinte Nationen

2019 - 01 - 0324

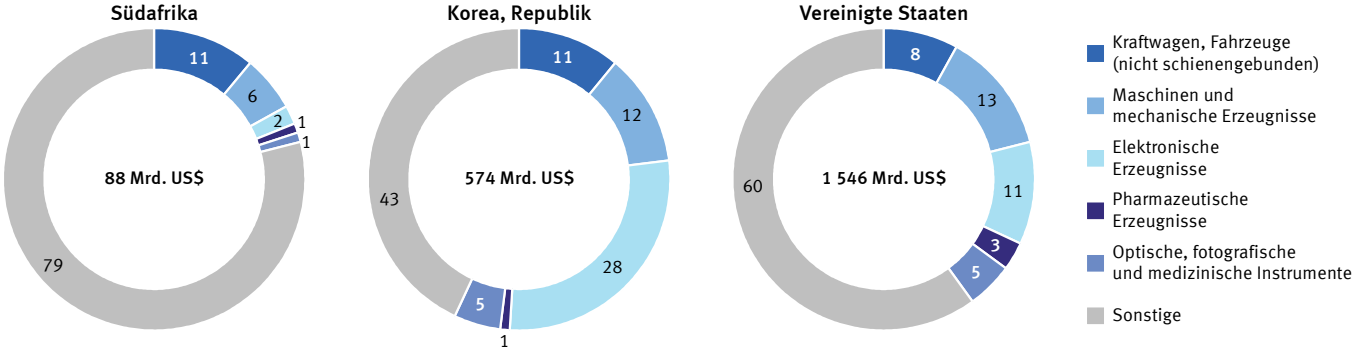
A.16 Außenhandel

	Exporte von Waren [1]	Importe von Waren [1]	Außenhandelsbilanz [2]	Wertindex der Warenexporte [3]	Wertindex der Warenimporte [3]	Warenexporte je Einwohner/-in [4]	Anteil der Warenexporte nach Deutschland [2]	Anteil der Warenimporte aus Deutschland [2]
	2017							
	Mill. US$			2000 = 100		US$	%	
Afrika								
Ägypten	25 943	66 339	– 40 396	*485*	*423*	*266*	*2,2*	*6,8*
Äthiopien	1 724 [6]	19 121 [6]	– 17 397 [6]	*651*	*1 265*	*17* [6]	*8,6* [6]	*2,1* [6]
Kenia	5 747	16 690	– 10 943	*331*	*537*	*116*	*2,0*	*2,5*
Kongo, Dem. Republik	.	.	.	*963*	*764*	.	.	.
Nigeria	44 466	31 270	13 196	*224*	*516*	*233*	*1,5*	*4,0*
Südafrika	88 268	83 031	5 237	*296*	*341*	*1 556*	*6,6*	*11,5*
Tansania, Ver. Republik	4 178	7 765	– 3 587	*592*	*658*	*73*	*1,2*	*3,0*
Amerika								
Argentinien	58 384	66 899	– 8 515	*222*	*266*	*1 319*	*2,0*	*4,8*
Brasilien	217 739	150 749	66 990	*395*	*269*	*1 040*	*2,3*	*6,1*
Chile	69 229	65 062	4 168	*360*	*352*	*3 834*	*1,6*	*4,1*
Kanada	420 632	432 405	– 11 773	*152*	*181*	*11 459*	*0,7*	*3,2*
Kolumbien	37 766	46 050	– 8 284	*290*	*399*	*770*	*1,3*	*4,1*
Mexiko	409 451	420 369	– 10 918	*246*	*241*	*3 170*	*1,7*	*3,9*
Vereinigte Staaten	1 545 609	2 407 390	– 861 781	*198*	*191*	*4 745*	*3,5*	*5,0*
Asien								
Bangladesch	31 734 [7]	48 059 [7]	– 16 325 [7]	*561*	*595*	*197* [7]	*14,7* [7]	*1,8* [7]
China	2 263 371	1 843 793	419 578	*908*	*819*	*1 633*	*3,1*	*5,3*
Indien	294 364	444 052	– 149 688	*706*	*868*	*220*	*2,8*	*2,9*
Indonesien	168 810	157 388	11 422	*258*	*360*	*639*	*1,6*	*2,1*
Iran, Islamische Republik	.	.	.	*317*	*353*	.	.	.
Israel	61 150	69 116	– 7 966	*195*	*191*	*7 019*	*2,7*	*6,8*
Japan	698 097	671 474	26 623	*146*	*177*	*5 506*	*2,7*	*3,5*
Korea, Republik	573 627	478 469	95 158	*333*	*298*	*11 146*	*1,5*	*4,1*
Malaysia	216 428	193 856	22 572	*222*	*238*	*6 844*	*2,9*	*3,1*
Myanmar	13 879	19 253	– 5 375	*857*	*812*	*260*	*2,6*	*1,1*
Pakistan	21 878	57 440	– 35 562	*241*	*532*	*111*	*5,9*	*1,9*
Philippinen	68 713	101 889	– 33 177	*180*	*275*	*655*	*3,9*	*2,1*
Saudi-Arabien	221 835	134 519	87 316	*281*	*445*	*6 702*	*0,1*	*5,8*
Thailand	213 593 [6]	195 714 [6]	17 879 [6]	*343*	*358*	*3 102* [6]	*2,1* [6]	*3,0* [6]
Ver. Arabische Emirate	313 504	270 955	42 549	*629*	*782*	*33 045*	*0,5*	*4,4*
Vietnam	215 119	213 215	1 903	*1 480*	*1 353*	*2 274*	*3,0*	*1,5*
Australien und Ozeanien								
Australien	230 163	228 442	1 721	*362*	*320*	*9 357*	*0,7*	*4,7*
Neuseeland	38 050	40 128	– 2 078	*286*	*289*	*7 937*	*1,3*	*5,3*

1 Quelle: UN Comtrade, Vereinte Nationen.
2 Quelle: UNCTAD, Vereinte Nationen.
3 Quelle: Eigene Berechnungen basierend auf Daten von UN Comtrade und Weltbank.
4 Quelle: Eigene Berechnungen basierend auf UN Comtrade Daten.
5 Extra-EU-Handel (Gesamthandel mit allen Staaten, die nicht Mitglied der Europäischen Union sind).
6 2016.
7 2015.

Export ausgewählter Warengruppen 2017

Anteil an den Warenexporten insgesamt, in %



Quelle: UN Comtrade, Vereinte Nationen

2019 - 01 - 0325

A.17 Zahlungsbilanz

	Leistungsbilanz					Saldo der Vermögensänderungsbilanz	Saldo der Kapitalbilanz	Saldo der statistisch nicht aufgliederbaren Transaktionen
	Saldo insgesamt		Saldo des Waren- u. Dienstleistungsverkehrs	Primäreinkommen	Sekundäreinkommen			
	2018							
	% des BIP	Mill. US$						
Europa								
Europäische Union	.	.	.	.	.	.	.	.
Belgien	*– 1,3*	– 6 819	– 4 843	7 289	– 9 263	– 85	– 6 326	578
Bulgarien	*4,5*	2 959	1 301	– 653	2 311	696	2 374	– 1 281
Dänemark	*5,8*	20 406	17 684	8 455	– 5 732	40	11 109	– 9 337
Deutschland	***7,3***	**291 440**	**239 750**	**107 813**	**– 56 123**	**2 319**	**267 112**	**– 26 646**
Estland	*1,7*	524	1 045	– 594	73	359	986	103
Finnland	*– 1,9*	– 5 190	– 1 522	– 877	– 2 791	193	– 10 397	– 5 399
Frankreich	*– 0,3*	– 9 247	– 21 436	66 240	– 54 051	2 443	– 49 062	– 42 258
Griechenland	*– 2,9*	– 6 370	– 3 932	– 1 917	– 520	419	– 4 624	1 327
Irland	*9,2*	34 638	117 724	– 77 072	– 6 014	– 25 590	32 324	23 276
Island	*2,9*	756	810	148	– 202	– 15	1 623	882
Italien	*2,4*	50 559	51 213	20 120	– 20 774	– 741	34 697	– 15 121
Kroatien	*2,4*	1 459	530	– 1 103	2 031	888	1 600	– 746
Lettland [1]	*– 0,8*	– 246	– 408	– 219	380	240	202	208
Litauen	*1,5*	817	1 610	– 1 760	968	781	1 321	– 277
Luxemburg	*4,9*	3 426	23 268	– 19 323	– 519	798	4 238	14
Malta	*11,2*	1 628	3 113	– 1 338	– 147	81	765	– 943
Niederlande	*10,8*	98 507	95 720	9 501	– 6 715	– 978	100 584	3 056
Norwegen	*8,1*	35 182	24 122	17 862	– 6 803	– 106	33 094	– 1 985
Österreich	*2,4*	10 801	17 691	– 2 444	– 4 446	– 355	9 242	– 1 204
Polen	*– 0,7*	– 3 929	20 090	– 22 330	– 1 689	11 802	6 386	– 1 487
Portugal	*– 0,6*	– 1 508	2 339	– 6 738	2 891	2 498	1 634	645
Rumänien	*– 4,5*	– 10 757	– 7 609	– 5 933	2 785	2 843	– 6 823	1 090
Russische Föderation	*6,9*	113 811	164 507	– 41 397	– 9 300	– 1 114	115 261	2 565
Schweden	*1,9*	10 643	11 508	8 455	– 9 320	– 70	1 331	– 9 242
Schweiz	*10,2*	72 186	78 855	2 724	– 9 393	4 608	75 420	– 1 375
Slowakei [1]	*– 2,0*	– 1 939	1 751	– 2 255	– 1 435	900	– 2 559	– 1 520
Slowenien	*7,0*	3 785	5 075	– 871	– 420	– 245	2 501	– 1 039
Spanien	*0,9*	12 924	27 694	– 625	– 14 147	7 407	25 640	5 307
Tschechische Republik	*0,4*	860	15 707	– 12 956	– 1 891	625	768	– 717
Türkei	*– 3,5*	– 27 115	– 16 260	– 11 720	865	58	– 9 852	17 205
Ungarn	*0,5*	806	7 428	– 5 952	– 669	2 762	– 131	– 3 699
Vereinigtes Königreich	*– 3,8*	– 108 745	– 41 146	– 35 521	– 32 078	– 3 254	– 83 846	28 153
Zypern	*– 6,9*	– 1 685	– 493	– 693	– 498	172	– 1 009	504

A.17 Zahlungsbilanz

	Leistungsbilanz					Saldo der Vermögensänderungsbilanz	Saldo der Kapitalbilanz	Saldo der statistisch nicht aufgliederbaren Transaktionen
	Saldo insgesamt		Saldo des Waren- u. Dienstleistungsverkehrs	Primäreinkommen	Sekundäreinkommen			
	2018							
	% des BIP	Mill. US$						
Afrika								
Ägypten [1]	*– 3,4*	– 7 940	– 27 349	– 5 365	24 774	– 156	– 11 730	– 3 634
Äthiopien [1]	*– 6,8*	– 5 566	– 12 513	– 456	7 404	.	– 9 173	– 3 607
Kenia [1]	*– 6,4*	– 5 018	– 8 646	– 820	4 448	184	– 4 768	66
Kongo, Dem. Republik [1]	*– 3,2*	– 1 213	– 1 440	– 1 232	1 458	465	– 895	– 147
Nigeria [1]	*2,8*	10 381	– 86	– 11 492	21 959	.	4 321	– 6 061
Südafrika	*– 3,7*	– 13 381	1 156	– 11 800	– 2 737	18	– 11 079	2 284
Tansania, Ver. Republik [1]	*– 3,1*	– 1 634	– 822	– 1 214	402	351	– 708	574
Amerika								
Argentinien	*– 5,4*	– 28 003	– 10 575	– 18 723	1 295	86	– 28 385	– 468
Brasilien	*– 0,8*	– 14 509	19 637	– 36 668	2 522	440	– 7 742	6 328
Chile	*– 3,1*	– 9 157	673	– 12 241	2 411	42	– 8 076	1 040
Kanada	*– 2,7*	– 45 461	– 36 488	– 7 133	– 1 840	– 61	– 37 992	7 530
Kolumbien	*– 3,8*	– 12 661	– 9 125	– 11 141	7 605	.	– 11 981	679
Mexiko	*– 1,8*	– 22 186	– 22 587	– 32 277	32 678	– 65	– 35 909	– 13 658
Vereinigte Staaten	*– 2,4*	– 488 480	– 622 115	244 299	– 110 664	9 408	– 519 559	– 40 487
Asien								
Bangladesch [1]	*– 2,5*	– 6 365	– 17 659	– 2 718	14 013	298	– 7 520	– 1 452
China	*0,4*	49 092	102 921	– 51 420	– 2 410	– 569	– 111 680	– 160 203
Indien [1]	*– 1,4*	– 38 168	– 72 212	– 26 423	60 467	37	– 38 980	– 850
Indonesien	*– 3,0*	– 31 060	– 7 533	– 30 420	6 892	93	– 32 239	– 1 272
Iran, Islamische Republik	.	.	.	.	.	.	.	.
Israel	*2,9*	10 797	2 680	102	8 015	370	– 908	– 12 074
Japan	*3,5*	174 719	3 981	189 108	– 18 370	– 1 942	182 222	9 445
Korea, Republik	*4,7*	76 409	82 130	2 778	– 8 499	189	70 489	– 6 108
Malaysia [1]	*3,0*	9 450	21 935	– 8 448	– 4 037	– 6	2 871	– 6 572
Myanmar [1]	*– 6,8*	– 4 504	– 4 803	– 1 980	2 280	1	– 4 784	– 281
Pakistan	*– 5,8*	– 18 250	– 36 787	– 5 547	24 084	347	– 18 351	– 448
Philippinen	*– 2,4*	– 7 879	– 38 543	3 844	26 820	65	– 10 138	– 2 324
Saudi-Arabien	*9,2*	72 337	102 111	7 522	– 37 296	– 1 469	66 007	– 4 860
Thailand	*7,0*	35 159	51 188	– 24 030	8 001	– 611	29 181	– 5 367
Ver. Arabische Emirate	.	.	.	.	.	.	.	.
Vietnam [1]	*2,7*	6 124	7 624	– 9 900	8 400	.	– 7 659	– 13 783
Australien und Ozeanien								
Australien	*– 2,1*	– 30 508	16 433	– 46 090	– 851	– 384	– 33 743	– 2 852
Neuseeland	*– 3,6*	– 7 396	5	– 7 178	– 223	– 29	– 466	6 958

1 2017.

Quelle: World Development Indicators, Weltbank

A.18 Umwelt

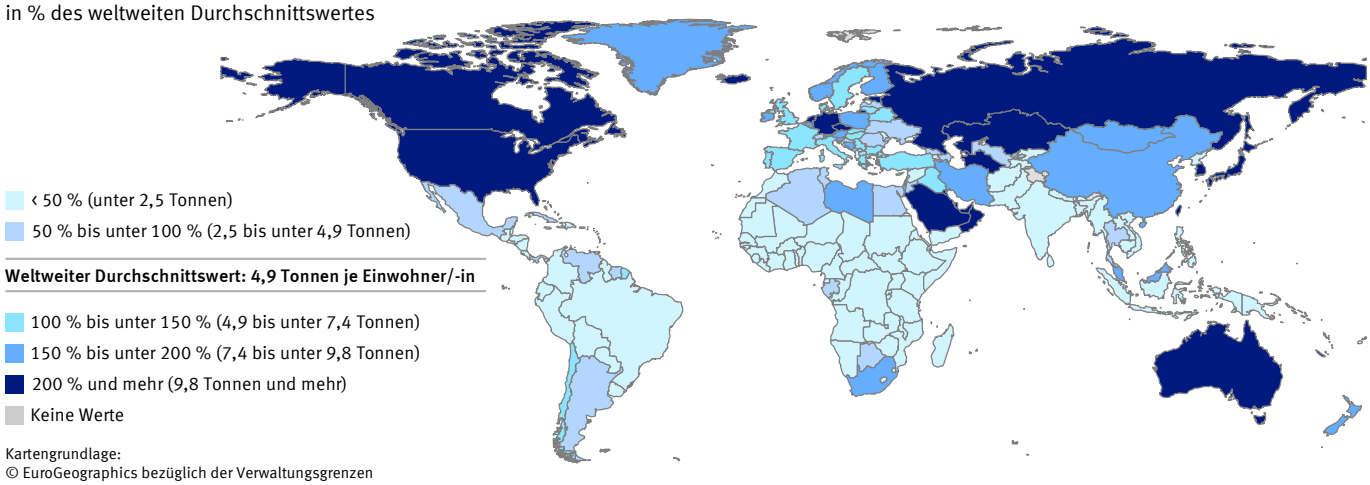
	Kohlendioxidemissionen durch fossile Brennstoffe und Zementproduktion [1]			Treibhausgas-emissionen [2]	Erneuerbare Wasser-ressourcen [3]	Siedlungs-abfälle [4]	Schutz-gebiete [5]
	insgesamt	Veränderung gegenüber 1990	je Einwohner/-in				Anteil an der Landfläche
	2017						
	Mill. t	%	t	t CO_2-Äquivalente	m^3	kg	%
Europa							
Europäische Union	3 548,0	– 19,5	7,0	8,4	.	486	26
Belgien	104,2	– 10,1	9,1	10,1	1 601	410	23
Bulgarien	49,6	– 39,8	7,0	8,7	3 006	435	35
Dänemark	33,6	– 37,5	5,9	8,5	1 046	781	18
Deutschland	**796,5**	**– 21,8**	**9,7**	**11,0**	**1 875**	**633**	**38**
Estland	17,9	– 53,5	13,7	15,8	9 779	390	20
Finnland	46,8	– 18,2	8,5	10,0	19 917	510	15
Frankreich	338,2	– 12,4	5,2	7,0	3 247	514	26
Griechenland	72,1	– 8,9	6,5	8,9	6 129	504	35
Irland	38,9	+ 18,5	8,2	12,6	10 920	.	14
Island	4,1	+ 74,6	12,2	13,8	507 463	656	18
Italien	361,2	– 16,2	6,1	7,1	3 223	489	22
Kroatien	17,5	– 30,6	4,2	6,1	25 185	416	38
Lettland	8,0	– 60,0	4,1	5,8	17 918	438	18
Litauen	15,3	– 56,6	5,3	7,2	8 478	455	17
Luxemburg	9,5	– 18,8	16,4	17,2	5 998	607	41
Malta	1,9	– 20,2	4,4	4,6	117	604	30
Niederlande	174,8	+ 8,3	10,3	11,3	5 342	513	11
Norwegen	46,9	+ 28,7	8,8	10,0	74 081	748	17
Österreich	72,2	+ 14,8	8,3	9,4	8 895	570	28
Polen	319,0	– 14,0	8,4	10,9	1 585	315	40
Portugal	56,8	+ 30,0	5,5	6,8	7 493	487	23
Rumänien	81,1	– 56,6	4,1	5,8	10 773	272	24
Russische Föderation	1 764,9	– 25,8	12,3	14,9	31 426	.	10
Schweden	50,9	– 12,5	5,1	5,2	17 556	452	15
Schweiz	39,7	– 11,6	4,7	5,6	6 312	706	10
Slowakei	37,9	– 37,5	6,9	8,0	9 196	378	38
Slowenien	15,2	– 8,5	7,3	8,4	15 322	471	54
Spanien	282,4	+ 22,8	6,1	7,3	2 405	462	28
Tschechische Republik	109,8	– 32,6	10,3	12,1	1 238	344	22
Türkei	429,6	+ 186,6	5,3	6,5	2 621	425	.
Ungarn	50,9	– 29,3	5,2	6,5	10 697	385	23
Vereinigtes Königreich	379,2	– 35,6	5,7	7,2	2 221	468	29
Zypern	7,0	+ 55,0	6,0	7,6	661	637	19

Kohlendioxid (CO_2) ist das bekannteste **Treibhausgas**. Es gibt jedoch auch andere, wie zum Beispiel Methan und Lachgas. Um die Klimawirksamkeit der unterschiedlichen Treibhausgase hinsichtlich ihres Potenzials zur Erwärmung der Atmosphäre miteinander vergleichbar zu machen, werden diese in **Kohlendioxidäquivalente (CO_2-Äquivalente)** umgerechnet. Methan ist etwa 21-mal so klimawirksam wie Kohlendioxid; eine Tonne (t) Methan entspricht somit 21 t CO_2-Äquivalente.

Zu den **erneuerbaren Wasserressourcen** zählen insbesondere Oberflächengewässer (Flüsse, Seen) sowie das Grundwasser.

In dem von den Vereinten Nationen (UN) initiierten Übereinkommen über die biologische Vielfalt ist ein **Schutzgebiet** definiert als ein geografisch festgelegtes Gebiet, das im Hinblick auf die Verwirklichung bestimmter Erhaltungsziele ausgewiesen ist oder geregelt und verwaltet wird. Hierzu zählen Naturreservate, Nationalparks, Naturmonumente, Biotope, geschützte Landschaften bzw. marine Gebiete sowie Ressourcenschutzgebiete.

Kohlendioxidemissionen je Einwohner/-in 2017
in % des weltweiten Durchschnittswertes



Kartengrundlage:
© EuroGeographics bezüglich der Verwaltungsgrenzen

Quelle: Europäische Kommission: Joint Research Centre (JRC)/PBL, EDGAR

2019 - 01 - 0327

A.18 Umwelt

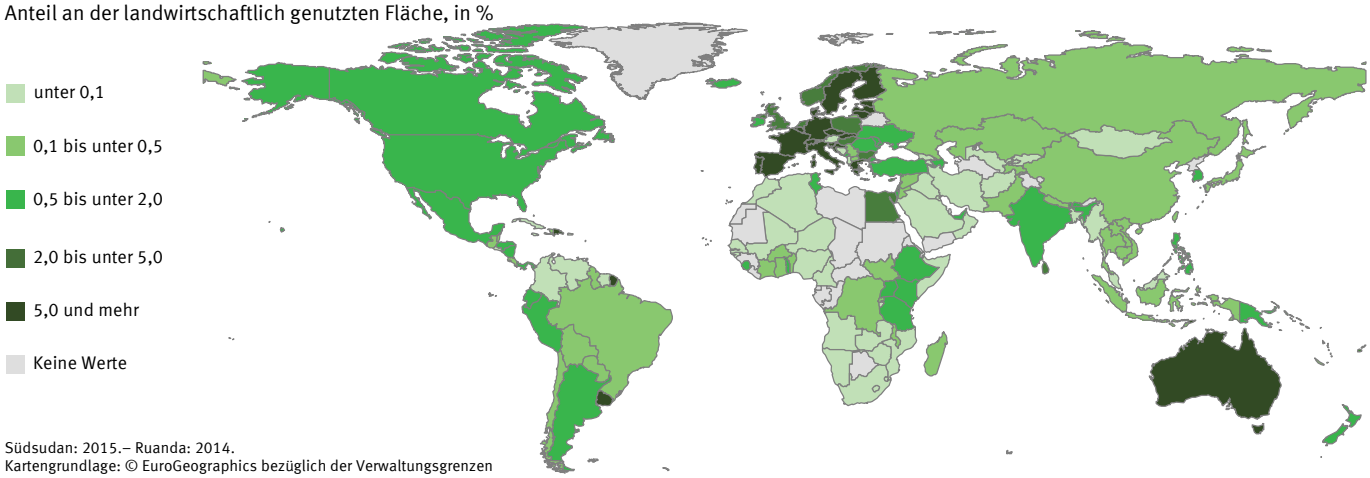
	Kohlendioxidemissionen durch fossile Brennstoffe und Zementproduktion [1]			Treibhausgas-emissionen [2]	Erneuerbare Wasser-ressourcen [3]	Schutz-gebiete [5]
	insgesamt	Veränderung gegenüber 1990	je Einwohner/-in			Anteil an der Landfläche
	2017					
	Mill. t	%	t	t CO_2-Äquivalente	m^3	%
Afrika						
Ägypten	258,7	+ 184,9	2,7	.	589	13
Äthiopien	14,9	+ 523,4	0,1	.	1 162	18
Kenia	18,6	+ 187,5	0,4	.	618	12
Kongo, Dem. Republik	3,5	+ 1,6	.	.	15 773	14
Nigeria	94,8	+ 38,3	0,5	.	1 499	14
Südafrika	467,7	+ 49,7	8,2	.	905	8
Tansania, Ver. Republik	14,7	+ 598,9	0,3	.	1 680	38
Amerika						
Argentinien	210,0	+ 86,7	4,7	.	19 792	9
Brasilien	492,8	+ 115,6	2,4	.	41 316	29
Chile	90,3	+ 176,6	5,0	.	51 127	18
Kanada	617,3	+ 35,4	16,9	19,6	79 238	10
Kolumbien	75,0	+ 44,4	1,5	.	48 098	15
Mexiko	507,2	+ 74,7	3,9	.	3 576	15
Vereinigte Staaten	5 107,4	+ 0,4	15,7	19,9	9 459	13
Asien						
Bangladesch	84,5	+ 509,6	0,5	.	7 451	5
China	10 877,2	+ 353,8	7,7	.	1 971	15
Indien	2 454,8	+ 305,1	1,8	.	1 427	6
Indonesien	511,3	+ 215,6	1,9	.	7 648	12
Iran, Islamische Republik	671,5	+ 224,7	8,3	.	1 688	9
Israel	66,9	+ 89,6	8,0	.	214	20
Japan	1 320,8	+ 14,9	10,4	10,2	3 373	29
Korea, Republik	673,3	+ 149,3	13,2	.	1 367	12
Malaysia	258,8	+ 336,9	8,2	.	18 341	19
Myanmar	28,5	+ 546,7	0,5	.	21 885	6
Pakistan	197,3	+ 197,7	1,0	.	1 253	12
Philippinen	137,2	+ 214,4	1,3	.	4 565	15
Saudi-Arabien	638,8	+ 284,4	19,4	.	73	5
Thailand	279,3	+ 200,3	4,0	.	6 353	19
Ver. Arabische Emirate	202,8	+ 256,3	21,6	.	16	18
Vietnam	218,7	+ 983,8	2,3	.	9 254	8
Australien und Ozeanien						
Australien	402,3	+ 46,1	16,5	22,5	20 123	19
Neuseeland	36,8	+ 53,3	7,8	16,9	69 486	33

1 Quelle: Europäische Kommission: Joint Research Centre (JRC)/PBL, EDGAR. Bei diesen Werten werden Landnutzungsänderungen und forstwirtschaftliche Maßnahmen (z. B. Wiederaufforstung) nicht berücksichtigt.
2 Quelle: Eigene Berechnungen basierend auf Daten der Klimarahmenkonvention (UNFCCC), Vereinte Nationen.
3 Quelle: Aquastat, Welternährungsorganisation (FAO), Vereinte Nationen.
4 Quelle: Abfallstatistik, Eurostat. Teilweise Schätzungen.
5 Quelle: World Development Indicators, Weltbank.

A.19 Land- und Forstwirtschaft

	Landfläche [1]					Anteil der landw. genutzten Fläche (LF), der ökologisch bewirtschaftet wird [2]	Produktion tierischer Erzeugnisse [1]		Ernte pflanzlicher Erzeugnisse [1]	
	insgesamt	darunter [2]					Rind- und Büffelfleisch	Schweinefleisch	Kartoffeln	Getreide
		Waldfläche	landw. genutzte Fläche (LF)	davon						
				Ackerland und Dauerkulturen	Dauergrünland					
	2016						2017			
	km²	% der Landfläche				%	1 000 t			
Europa										
Europäische Union	4 238 694	*38*	*43*	*28*	*15*	.	7 867	23 686	61 320	307 062
Belgien	30 280	*23*	*45*	*29*	*16*	*5,8*	282	1 045	4 417	2 764
Bulgarien	108 560	*35*	*46*	*34*	*13*	*3,2*	17	75	228	9 476
Dänemark	41 990	*15*	*62*	*57*	*5*	*7,7*	124	1 532	2 171	10 027
Deutschland	**349 360**	***33***	***48***	***34***	***13***	***6,8***	**1 137**	**5 506**	**11 720**	**45 557**
Estland	43 470	*51*	*23*	*16*	*7*	*18,0*	12	42	91	1 312
Finnland	303 910	*73*	*7*	*7*	.	*10,5*	86	182	612	3 422
Frankreich	547 557	*31*	*52*	*35*	*17*	*5,4*	1 423	2 136	7 342	64 496
Griechenland	128 900	*32*	*48*	*25*	*22*	*5,6*	44	81	536	3 149
Irland	68 890	*11*	*65*	*6*	*58*	*1,7*	617	294	412	2 395
Island	100 250	*1*	*19*	*1*	*17*	*0,5*	5	6	9	7
Italien	294 140	*32*	*43*	*31*	*12*	*14,1*	756	1 467	1 347	16 241
Kroatien	55 960	*34*	*28*	*17*	*11*	*6,1*	44	97	156	2 657
Lettland	62 180	*54*	*31*	*21*	*10*	*13,4*	18	38	408	2 693
Litauen	62 642	*35*	*47*	*35*	*12*	*7,5*	42	71	237	5 074
Luxemburg	2 430	*36*	*54*	*26*	*28*	*3,5*	10	13	21	149
Malta	320	*1*	*32*	*32*	.	*0,3*	1	5	9	15
Niederlande	33 690	*11*	*53*	*32*	*22*	*2,9*	441	1 456	7 392	1 394
Norwegen	365 123	*33*	*3*	*2*	.	*4,8*	85	137	315	1 285
Österreich	82 523	*47*	*32*	*17*	*15*	*21,4*	227	508	653	4 875
Polen	306 190	*31*	*47*	*37*	*10*	*3,7*	572	2 048	9 172	31 925
Portugal	91 606	*35*	*39*	*19*	*20*	*6,8*	91	378	515	1 119
Rumänien	230 080	*30*	*59*	*39*	*20*	*1,7*	96	452	3 117	27 139
Russische Föderation	16 376 870	*50*	*13*	*8*	*6*	*0,1*	1 614	3 530	29 590	131 144
Schweden	407 310	*69*	*7*	*6*	*1*	*18,2*	132	241	853	5 950
Schweiz	39 516	*32*	*38*	*11*	*28*	*9,3*	140	239	459	977
Slowakei	48 080	*40*	*39*	*28*	*11*	*9,9*	11	58	150	3 484
Slowenien	20 142	*62*	*31*	*12*	*19*	*7,1*	36	30	77	552
Spanien	499 564	*37*	*53*	*34*	*18*	*7,7*	644	4 299	2 239	16 660
Tschechische Republik	77 220	*35*	*45*	*33*	*12*	*14,1*	68	220	689	7 461
Türkei	769 630	*15*	*50*	*31*	*19*	*1,4*	989	.	4 800	36 126
Ungarn	90 530	*23*	*58*	*50*	*9*	*3,5*	28	470	403	14 029
Vereinigtes Königreich	241 930	*13*	*72*	*25*	*47*	*2,8*	902	901	6 218	23 000
Zypern	9 240	*19*	*12*	*12*	.	*5,0*	5	42	135	49

Ökologische Anbaufläche 2016
Anteil an der landwirtschaftlich genutzten Fläche, in %



Südsudan: 2015.– Ruanda: 2014.
Kartengrundlage: © EuroGeographics bezüglich der Verwaltungsgrenzen
Quelle: Eigene Berechnungen basierend auf Daten der Welternährungsorganisation (FAO)

2019 - 01 - 0327

A.19 Land- und Forstwirtschaft

	Landfläche [1]					Anteil der landw. genutzten Fläche (LF), der ökologisch bewirtschaftet wird [2]	Produktion tierischer Erzeugnisse [1]		Ernte pflanzlicher Erzeugnisse [1]	
	insgesamt	darunter [2]								
		Waldfläche	landw. genutzte Fläche (LF)	davon			Rind- und Büffelfleisch	Schweinefleisch	Kartoffeln	Getreide
				Ackerland und Dauerkulturen	Dauergrünland					
	2016						2017			
	km²	% der Landfläche				%	1 000 t			
Afrika										
Ägypten	995 450	.	4	4	.	2,8	816	.	4 325	23 217
Äthiopien	1 000 000	13	36	16	20	0,5	393	2	933	26 277
Kenia	569 140	8	49	11	37	0,6	589	13	1 520	3 711
Kongo, Dem. Republik	2 267 050	67	12	4	8	0,4	14	24	103	2 988
Nigeria	910 770	7	78	44	33	0,1	373	278	1 284	28 873
Südafrika	1 213 090	8	80	11	69	.	1 014	235	2 451	18 906
Tansania, Ver. Republik	885 800	52	45	18	27	0,7	314	15	1 749	10 093
Amerika										
Argentinien	2 736 690	10	54	15	40	1,9	2 842	566	2 454	76 397
Brasilien	8 358 140	59	34	10	23	0,3	9 550	3 825	3 657	117 784
Chile	743 532	24	21	2	19	0,1	200	489	1 426	3 471
Kanada	9 093 510	38	7	5	2	1,8	880	2 142	4 411	56 311
Kolumbien	1 109 500	53	40	3	37	0,1	753	355	2 819	4 329
Mexiko	1 943 950	34	55	13	42	0,6	1 927	1 442	1 715	37 487
Vereinigte Staaten	9 147 420	34	44	17	27	0,5	11 907	11 611	20 017	440 117
Asien										
Bangladesch	130 170	11	71	66	5	0,1	197	.	10 216	53 332
China	9 424 700	22	56	14	42	0,4	7 275	55 449	99 206	619 857
Indien	2 973 190	24	60	57	3	0,8	2 524	305	48 605	313 610
Indonesien	1 811 570	50	31	25	6	0,2	564	344	1 165	109 334
Iran, Islamische Republik	1 628 760	7	28	10	18	.	485	.	5 102	20 981
Israel	21 640	8	25	18	6	0,8	141	15	522	221
Japan	364 560	68	12	12	.	0,2	469	1 272	2 151	10 906
Korea, Republik	97 489	63	17	17	1	1,2	281	1 280	614	5 468
Malaysia	328 550	68	26	25	1	.	50	194	.	2 974
Myanmar	653 080	44	20	19	.	.	475	961	500	28 119
Pakistan	770 880	2	48	41	6	0,1	1 877	.	4 142	44 097
Philippinen	298 170	28	42	37	5	1,6	312	1 837	118	27 192
Saudi-Arabien	2 149 690	.	81	2	79	.	42	.	476	1 429
Thailand	510 890	32	43	42	2	0,3	154	902	127	38 717
Ver. Arabische Emirate	71 020	5	5	1	4	1,2	18	.	5	7
Vietnam	310 070	48	39	37	2	0,4	410	3 733	304	47 877
Australien und Ozeanien										
Australien	7 692 020	16	48	6	42	7,3	2 049	397	1 105	50 049
Neuseeland	263 310	39	40	2	38	0,7	642	47	466	937

1 Quelle: Welternährungsorganisation (FAO), Vereinte Nationen. Teilweise Schätzungen der FAO.
2 Quelle: Eigene Berechnungen basierend auf FAO Daten.

A.20 Produzierendes Gewerbe und Dienstleistungen im Überblick

	Unternehmen nach ausgewählten Wirtschaftsbereichen [1]				Bruttowertschöpfung zu Faktorkosten nach ausgewählten Wirtschaftsbereichen [1]			
	Produzierendes Gewerbe [2]	Handel [3]	Gastgewerbe	Verkehr und Lagerei	Produzierendes Gewerbe [2]	Handel [3]	Gastgewerbe	Verkehr und Lagerei
	2016							
	Anzahl				Mill. EUR			
Europa								
Europäische Union	2 330 219	6 316 410	1 998 320	1 246 259	2 291 361 [4]	1 352 939	264 371	550 000 [4]
Belgien	36 319	127 781	49 261	18 095	64 708	42 803	5 236	16 014
Bulgarien	34 204	140 524	27 032	22 711	9 845	5 287	817	2 182
Dänemark	19 610	41 772	14 087	10 945	42 354	27 201	3 382	12 215
Deutschland	**211 079**	**588 705**	**230 040**	**106 559**	**638 519**	**304 319**	**44 505**	**103 634**
Estland	7 921	16 351	2 799	5 244	3 850	2 253	309	1 110
Finnland	23 485	42 661	12 042	20 538	32 480	15 282	2 365	8 062
Frankreich	260 245	760 007	270 760	115 627	256 093	178 553	38 475	84 791
Griechenland	71 580	255 503	118 052	62 878	15 757	10 388	3 000	5 634
Irland	17 555	46 595	18 377	24 614	91 740	22 226	5 058	8 595
Island [5]	2 276	4 024	1 817	1 745	2 611	1 610	624	1 137
Italien	410 791	1 105 396	323 563	123 442	267 088	133 308	31 165	60 161
Kroatien	21 210	36 620	19 913	8 372	7 651	4 440	1 786	2 000
Lettland	12 284	28 991	4 092	7 654	3 223	2 534	274	1 586
Litauen	21 960	59 639	5 985	13 603	5 249	4 009	345	2 269
Luxemburg	926	7 570	2 808	972	3 721	5 208	743	1 638
Malta	2 450	9 298	2 437	1 430	.	1 040	392	.
Niederlande	68 723	250 117	58 088	42 081	83 388	78 928	10 560	29 515
Norwegen	19 947	50 239	11 806	20 831 [6]	72 491	23 263	3 596	17 110 [6]
Österreich	29 985	77 808	47 474	14 141	62 821	35 647	9 415	14 145
Polen	209 175	502 029	54 833	153 586	86 467	39 043	2 726	14 384
Portugal	73 204	220 359	97 562	21 799	26 317	16 417	4 718	6 640
Rumänien	53 743	169 712	25 612	44 504	22 933	14 178	1 356	4 888
Russische Föderation	.	.	.	.	.	.	.	.
Schweden	61 927	127 965	32 694	29 652	64 936	41 638	6 928	15 142
Schweiz	21 784	32 856	16 864	4 798	107 410	90 832	10 642	25 212
Slowakei	70 561	113 274	18 048	19 020	15 762	6 149	487	2 604
Slowenien	21 091	26 382	11 130	8 574	8 888	3 884	705	1 948
Spanien	189 789	796 049	306 851	196 166	136 197	104 023	28 825	44 757
Tschechische Republik	193 274	240 599	60 120	38 439	44 906	15 047	1 782	6 491
Türkei	.	.	.	.	.	.	.	.
Ungarn	52 861	135 197	29 976	27 668	24 929	9 482	1 104	5 145
Vereinigtes Königreich	148 998	373 175	149 009	104 957	268 960	227 924	56 784	95 939
Zypern	5 269	16 331	5 675	2 988	1 422	1 730	1 129	734

1 Die Einteilung der Wirtschaftsbereiche entspricht der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2).
2 Verarbeitendes Gewerbe, Bergbau, Energie- und Wasserversorgung.
3 Einschl. Instandhaltung und Reparatur von Kraftfahrzeugen.
4 Abweichende Definition, Eurostat Schätzung.
5 Vorläufige Werte.
6 Abweichende Definition.

Quelle: Strukturelle Unternehmensstatistik, Eurostat

Die **Bruttowertschöpfung zu Faktorkosten** ist ein Maß zur Beurteilung der wirtschaftlichen Leistung und umfasst die Bruttoerträge durch betriebliche Aktivitäten nach Abzug der Waren- und Dienstleistungskäufe und nach Anpassung bezüglich der betrieblichen Subventionen und indirekten Steuern. Nähere Angaben zur Berechnung siehe „Glossar"/„Methodik" des Kapitels 20.

Der **Produktionsindex** ist ein Maß für die Leistung eines bestimmten Wirtschaftsbereichs. Er misst Veränderungen in der Leistung (Outputvolumen, Aktivität) des jeweiligen Wirtschaftssektors. Er ist aufgrund seiner Periodizität und seiner schnellen Verfügbarkeit ein zentraler und aktueller Indikator für die konjunkturelle Entwicklung.

Der **Umsatzindex** berücksichtigt den Wert aller im Berichtszeitraum von Betrieben des jeweiligen Wirtschaftsbereichs über die an Dritte gelieferten eigenen Erzeugnisse und industriellen/handwerklichen Dienstleistungen (Summe der Rechnungsendbeträge ohne Umsatzsteuer). Auch dieser Indexwert zählt zu den wichtigsten Indikatoren für die Beobachtung und Analyse der Konjunkturentwicklung.

A.21 Verarbeitendes Gewerbe

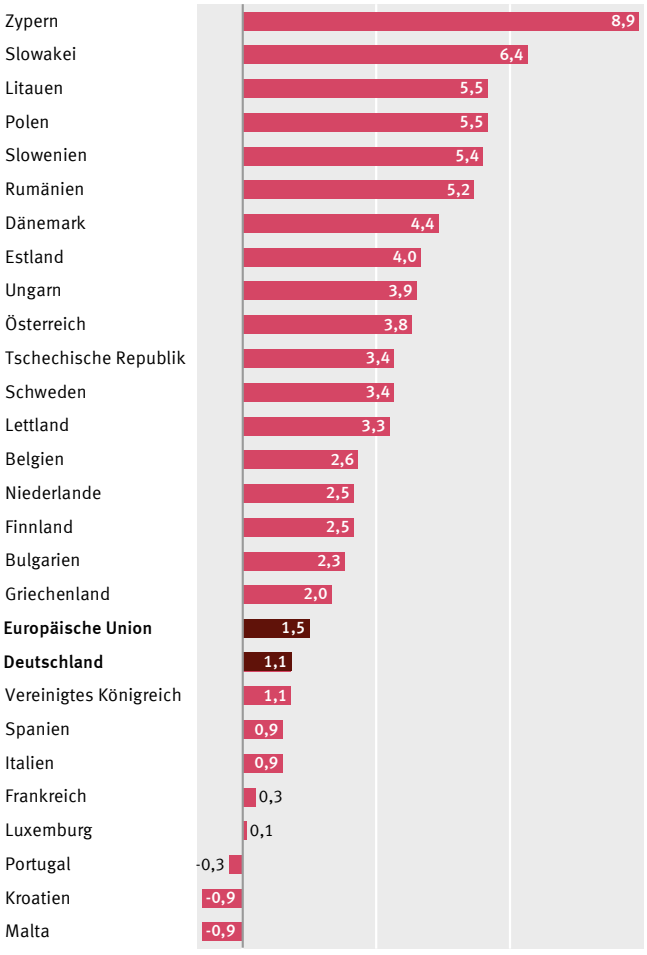
	Wirtschaftsbereich Verarbeitendes Gewerbe				
	Unternehmen	Tätige Personen	Bruttowertschöpfung zu Faktorkosten	Produktionsindex [1]	Umsatzindex [1]
	2016			2018	
	Anzahl		Mill. EUR	2015 = 100	
Europa					
Europäische Union	2 120 592	30 472 486	1 912 371	*107*	*111*
Belgien	34 132	494 618	55 192	*109*	*112*
Bulgarien	31 323	548 990	7 135	*113*	*120*
Dänemark	15 244	305 386	33 722	*113*	*109*
Deutschland	**201 826**	**7 360 959**	**569 864**	***106***	***108***
Estland	7 259	108 920	2 863	*111*	*117*
Finnland	20 264	332 334	26 984	*111*	*115*
Frankreich	216 049	2 905 577	213 732	*104*	*110*
Griechenland	61 862	311 369	10 426	*110*	*118*
Irland	15 583	213 117	86 629	.	.
Island	2 089 [2]	22 685 [2]	1 912 [2]	.	.
Italien	387 866	3 662 318	224 995	*107*	*109*
Kroatien	19 475	264 183	5 768	*107*	*107*
Lettland	11 090	119 537	2 156	*117*	*122*
Litauen	19 969	214 557	4 213	*116*	*122*
Luxemburg	767	33 612	3 118	*103*	*110*
Malta	2 230	22 585	707	*98*	*105*
Niederlande	65 243	686 186	67 208	*109*	*111*
Norwegen	17 143	224 995	21 075	*97*	*102*
Österreich	25 037	629 053	54 390	*112*	*114*
Polen	196 067	2 584 381	64 220	*118*	*124*
Portugal	66 953	686 651	20 136	*103*	*113*
Rumänien	48 349	1 209 753	16 944	*122*	*130*
Russische Föderation	.	.	.	.	.
Schweden	53 795	595 261	53 528	*110*	*120*
Schweiz	20 367	653 727 [3]	97 668	*113*	*112*
Slowakei	68 413	478 893	12 901	*115*	*115*
Slowenien	19 074	197 012	7 652	*124*	*124*
Spanien	166 984	1 854 926	105 310	*107*	*113*
Tschechische Republik	175 425	1 293 677	37 469	*115*	*113*
Türkei	.	.	.	*114*	*184*
Ungarn	49 951	739 145	21 785	*111*	*110*
Vereinigtes Königreich	135 396	2 589 745	202 362	*105*	*111*
Zypern	4 966	29 741	963	*130*	*129*

Weitere Erläuterungen zu den Indikatoren siehe Tabelle A.20.

1 Arbeitstäglich bereinigte Daten. Zum Teil vorläufige Werte oder Eurostat Schätzungen.
2 Vorläufige Werte.
3 Abweichende Definition.

Quelle: Strukturelle Unternehmensstatistik und Konjunkturstatistik, Eurostat

Produktionsindex des Verarbeitenden Gewerbes 2018
Veränderung des Produktionsvolumens gegenüber Vorjahr, in %



Daten liegen für alle EU-Staaten außer Irland vor. Zum Teil vorläufige Werte.
Quelle: Konjunkturstatistik, Eurostat

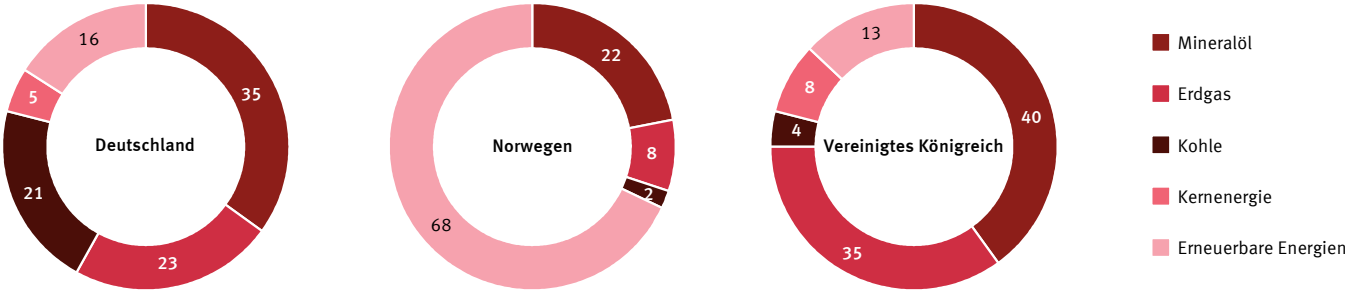
2019 - 01 - 0328

A.22 Energie

	Wirtschaftsbereich Energieversorgung [1]			Primärenergieverbrauch		Anteil am Primärenergieverbrauch insgesamt [4]					Bruttostrom-verbrauch [5]
	Unternehmen	Tätige Personen	Bruttowertschöpfung zu Faktorkosten	insgesamt [2]	je Einwohner/-in [3]	Mineralöl	Erdgas	Kohle	Kernenergie	Erneuerbare Energien	je Einwohner/-in
	2016			2018							2016
	Anzahl		Mill. EUR	Mill. t RÖE	t RÖE	%					kWh
Europa											
Europäische Union	110 065	1230 000	223 000 [6]	1 688,2	3,3	38,3	23,4	13,2	11,1	14,1	6 010
Belgien	727	18 394	5 884	62,2	5,4	54,8	23,3	5,3	10,4	6,2	7 778
Bulgarien	1 704	32 137	1 744	18,6	2,6	24,9 [7]	14,8 [7]	31,7 [7]	19,7 [7]	8,8 [7]	4 956
Dänemark	1 600	11 373	4 452	17,0	2,9	47,0 [7]	16,9 [7]	12,3 [7]	.	23,8 [7]	5 882
Deutschland	**1 974**	**227 843**	**39 815**	**323,9**	**3,9**	**34,9**	**23,4**	**20,5**	**5,3**	**15,8**	**6 956**
Estland	235	4 930	672	6,9	5,2	.	.	.	.	.	7 155
Finnland	934	13 847	3 654	29,3	5,3	36,7	6,0	14,6	17,8	24,9	15 468
Frankreich	29 687	189 412	30 241	242,6	3,6	32,5	15,1	3,5	38,5	10,4	7 148
Griechenland	6 920	30 677	4 159	28,3	2,6	56,3	14,4	16,5	–	12,9	5 501
Irland	551	9 206	3 886	16,1	3,3	46,4 [7]	28,3 [7]	14,3 [7]	.	10,9 [7]	5 887
Island	92 [8]	1 571 [8]	597 [8]	5,6	15,8	.	.	.	.	.	53 913
Italien	11 523	88 287	24 461	154,5	2,6	39,3	38,5	5,7	–	16,4	5 081
Kroatien	670	15 076	1 204	8,6	2,1	.	.	.	.	.	3 967
Lettland	567	11 320	822	3,7	1,9	.	.	.	.	.	3 564
Litauen	1 441	12 692	672	5,8	2,1	54,5 [7]	33,6 [7]	3,5 [7]	.	8,5 [7]	4 051
Luxemburg	83	1 611	448	4,0	6,6	.	.	.	.	.	14 274
Malta	14	10 [8]	.	.	.	.	.	.	.	.	4 954
Niederlande	1 201	27 721	7 310	84,8	4,9	48,2	36,2	9,7	0,9	5,0	6 734
Norwegen	482	13 698	5 999	47,4	8,9	22,0	8,1	1,8	–	68,1	23 692
Österreich	2 430	29 340	5 582	35,0	4,0	38,3	21,3	8,2	–	32,2	8 258
Polen	3 670	125 805	11 668	105,2	2,8	31,2	16,1	48,0	–	4,6	4 141
Portugal	3 977	12 343	4 303	26,0	2,5	44,5	19,4	10,5	–	25,7	4 873
Rumänien	1 350	70 559	3 052	33,4	1,7	30,7	28,0	15,9	7,7	17,7	2 688
Russische Föderation	.	.	.	720,7	5,0	21,1	54,2	12,2	6,4	6,0	6 715
Schweden	5 910	31 788	7 657	53,6	5,3	27,7	1,3	3,7	29,0	38,4	13 756
Schweiz	465	29 255	6 683	27,8	3,3	37,8	9,3	0,4	20,9	31,6	7 481
Slowakei	551	17 525	2 091	16,3	3,0	25,1 [7]	24,8 [7]	19,6 [7]	21,0 [7]	9,5 [7]	5 226
Slowenien	1 503	8 861	813	7,0	3,4	.	.	.	.	.	6 997
Spanien	14 077	41 022	19 830	141,4	3,0	47,1	19,1	7,9	8,9	17,0	5 505
Tschechische Republik	11 026	34 799	5 114	42,1	4,0	25,2	16,3	37,4	16,1	5,0	6 460
Türkei	1 513 [9]	86 303 [9]	5 652 [9]	153,5	1,9	31,6	26,5	27,6	–	14,3	3 114
Ungarn	678	24 712	2 156	23,7	2,4	37,3	34,8	9,2	15,0	3,6	4 178
Vereinigtes Königreich	5 001	134 716	30 881	192,3	2,9	40,1	35,3	3,9	7,7	13,1	5 033
Zypern	61	2 102	299	2,8	2,4	.	.	.	.	.	5 453

Primärenergieverbrauch nach Energieträgern 2018

in %



Quelle: Eigene Berechnungen basierend auf Statistical Review of World Energy 2019, BP

2019 - 01 - 0329

A.22 Energie

	Primärenergieverbrauch		Anteil am Primärenergieverbrauch insgesamt [4]					Bruttostrom-verbrauch [5]
	insgesamt [2]	je Einwohner/-in [3]	Mineralöl	Erdgas	Kohle	Kernenergie	Erneuerbare Energien	je Einwohner/-in
	2018							2016
	Mill. t RÖE	t RÖE	%					kWh
Afrika								
Ägypten	94,5	1,0	38,8	54,2	2,9	–	4,1	1 783
Äthiopien	.	.	.	.	.	.	.	89
Kenia	.	.	.	.	.	.	.	165
Kongo, Dem. Republik	.	.	.	.	.	.	.	95
Nigeria	.	.	.	.	.	.	.	141
Südafrika	121,5	2,1	21,6	3,1	70,8	2,1	2,5	4 031
Tansania, Ver. Republik	.	.	.	.	.	.	.	108
Amerika								
Argentinien	85,1	1,9	35,4	49,2	1,4	1,8	12,1	3 109
Brasilien	297,6	1,4	45,7	10,4	5,3	1,2	37,4	2 504
Chile	40,1	2,1	45,3	13,8	19,2	–	21,8	4 182
Kanada	344,4	9,3	31,9	28,9	4,2	6,6	28,4	14 844
Kolumbien	46,9	0,9	35,3	23,9	12,5	–	28,3	1 444
Mexiko	186,9	1,5	44,3	41,2	6,4	1,6	6,5	2 295
Vereinigte Staaten	2 300,6	7,0	40,0	30,5	13,8	8,4	7,3	12 825
Asien								
Bangladesch	35,8	0,2	25,1	68,1	6,0	–	0,8	353
China	3 273,5	2,4	19,6	7,4	58,2	2,0	12,7	4 279
Indien	809,2	0,6	29,5	6,2	55,9	1,1	7,3	918
Indonesien	185,5	0,7	45,0	18,1	33,2	–	3,8	865
Iran, Islamische Republik	285,7	3,5	30,2	67,9	0,5	0,6	0,9	3 153
Israel	25,6	2,9	44,7	35,3	18,2	–	1,8	6 893
Japan	454,1	3,6	40,2	21,9	25,9	2,4	9,6	7 974
Korea, Republik	301,0	5,8	42,8	16,0	29,3	10,0	1,9	10 618
Malaysia	99,3	3,1	37,1	35,7	21,3	–	5,8	4 656
Myanmar	.	.	.	.	.	.	.	293
Pakistan	85,0	0,4	28,6	44,1	13,6	2,6	11,0	500
Philippinen	47,0	0,4	46,7	7,5	34,6	–	11,2	799
Saudi-Arabien	259,2	7,7	62,8	37,2	.	.	.	9 818
Thailand	133,0	1,9	49,5	32,3	13,9	–	4,3	2 868
Ver. Arabische Emirate	112,2	11,6	40,2	58,7	0,9	–	0,2	13 045
Vietnam	85,8	0,9	29,0	9,7	40,0	–	21,4	1 616
Australien und Ozeanien								
Australien	144,3	5,8	37,0	24,7	30,7	–	7,7	9 911
Neuseeland	21,7	4,4	38,7	17,2	5,8	–	38,3	8 474

1 Quelle: Strukturelle Unternehmensstatistik, Eurostat.
2 Quelle: Statistical Review of World Energy 2019, BP.
3 Quelle: Eigene Berechnungen basierend auf Statistical Review of World Energy 2019, BP und World Development Indicators, Weltbank.
4 Quelle: Eigene Berechnungen basierend auf Statistical Review of World Energy 2019, BP.
5 Quelle: Internationale Energieagentur (IEA).
6 Abweichende Definition.
7 2016.
8 2015.
9 2014.

Erläuterungen zur **Bruttowertschöpfung zu Faktorkosten** finden Sie bei Tabelle A.20.

Primärenergieträger sind Energieträger, die in der Natur vorkommen und technisch noch nicht umgewandelt sind.

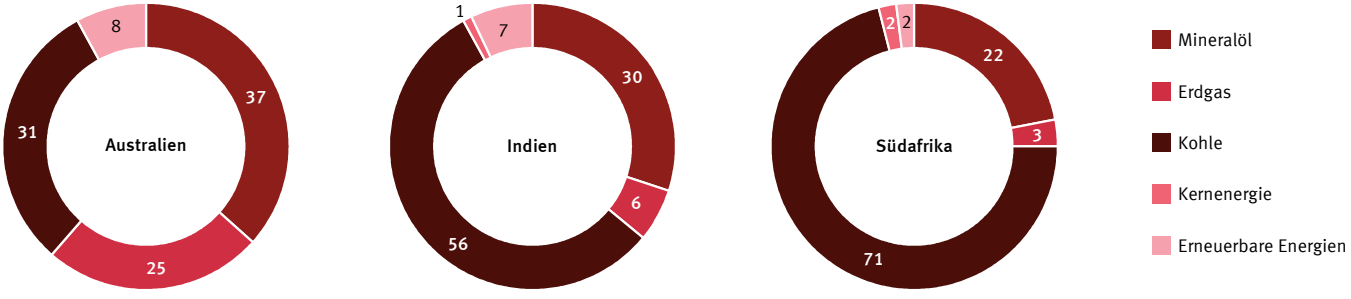
Der **Primärenergieverbrauch** bezeichnet den Verbrauch von Primärenergie vor der Umwandlung in andere, für den Endverbrauch geeignete Brennstoffe. Dies entspricht der inländischen Produktion von Primärenergieträgern zuzüglich der Einfuhren und Bestandsveränderungen, abzüglich der Ausfuhren und der Brennstoffe für den internationalen Luft- und Schiffsverkehr.

Die **Rohöleinheit (RÖE)** ist eine Maßeinheit für den Energiegehalt von Stoffen. 1 **Tonne Rohöleinheit (t RÖE)** entspricht 11 630 **Kilowattstunden (kWh)**.

Zu den **erneuerbaren Energien** zählen Wasser- und Windkraft, geothermische Energie, Solarenergie sowie Biomasse.

Der **Bruttostromverbrauch** ist die inländische Bruttostromerzeugung (einschl. Eigenerzeugung) zuzüglich Einfuhren, abzüglich Ausfuhren.

Primärenergieverbrauch nach Energieträgern 2018
in %



Quelle: Eigene Berechnungen basierend auf Statistical Review of World Energy 2019, BP

2019 - 01 - 0330

A.23 Baugewerbe

	Wirtschaftsbereich Baugewerbe				
	Unternehmen	Tätige Personen	Bruttowertschöpfung zu Faktorkosten	Produktionsindex [1]	Baugenehmigungen von Wohnungen in Wohngebäuden [1]
	2016			2018	
	Anzahl		Mill. EUR	2015 = 100	
Europa					
Europäische Union	3 512 568	12 690 460	540 000 [2]	*109*	*125*
Belgien	106 444	318 302	16 723	*103*	*136*
Bulgarien	19 526	142 663	1 385	*89*	*206*
Dänemark	31 973	168 959	11 178	*114*	*133* [2]
Deutschland	**358 919**	**2 272 627**	**101 464**	***109***	***115***
Estland	10 167	46 239	1 027	*149*	*125*
Finnland	40 891	192 361	10 587	*113* [2]	*132*
Frankreich	507 048	1 651 096 [2]	83 354	*102*	*113*
Griechenland	77 229	145 060	2 033	*106*	*176*
Irland	51 568	120 341	6 922	*147*	*224*
Island [1]	5 023	12 480	875	.	.
Italien	508 696	1 324 178	48 009	*102*	.
Kroatien	17 598	98 850	1 706	*111*	*169*
Lettland	11 752	63 450	740	*121*	*168*
Litauen	31 151	105 014	1 404	*113*	*123*
Luxemburg	3 760	43 750	2 624	*109*	*137*
Malta	3 949	10 851	.	*126*	*327*
Niederlande	167 022	435 174	26 907	*123*	*129*
Norwegen	57 377	234 624	17 677	*112*	*118*
Österreich	35 078	292 359	16 779	*117*	*107* [2]
Polen	264 440	889 264	13 349	*117*	*138*
Portugal	78 866	301 862	5 234	*101*	*246*
Rumänien	49 717	373 779	4 212	*88*	*109*
Russische Föderation	.	.	.	.	.
Schweden	101 868	394 421	22 486	*109*	*111*
Schweiz	21 364	322 321 [3]	29 454	*102*	.
Slowakei	87 665	152 398	1 930	*100*	*117*
Slowenien	18 706	61 113	1 252	*116*	*136*
Spanien	367 601	1 095 710	36 951	*106*	*192*
Tschechische Republik	174 910	367 291	5 971	*106*	*127*
Türkei	.	.	.	.	*73*
Ungarn	63 871	206 521	2 549	*129*	*302*
Vereinigtes Königreich	314 823	1 395 463	111 851	*112*	*106*
Zypern	7 330	21 364	617	*180*	*194*

Als **Baugenehmigung** gilt die Erteilung einer bauamtlichen Genehmigung zur Bauausführung. Der Baugenehmigungsindex zählt zu den wichtigsten Indikatoren zur Einschätzung der konjunkturellen Lage und gibt Aufschluss über die zu erwartende Auftragslage im Baugewerbe. Die Bestimmungen und Verfahren für die Erteilung einer Genehmigung sind in den einzelnen Mitgliedstaaten der Europäischen Union unterschiedlich.

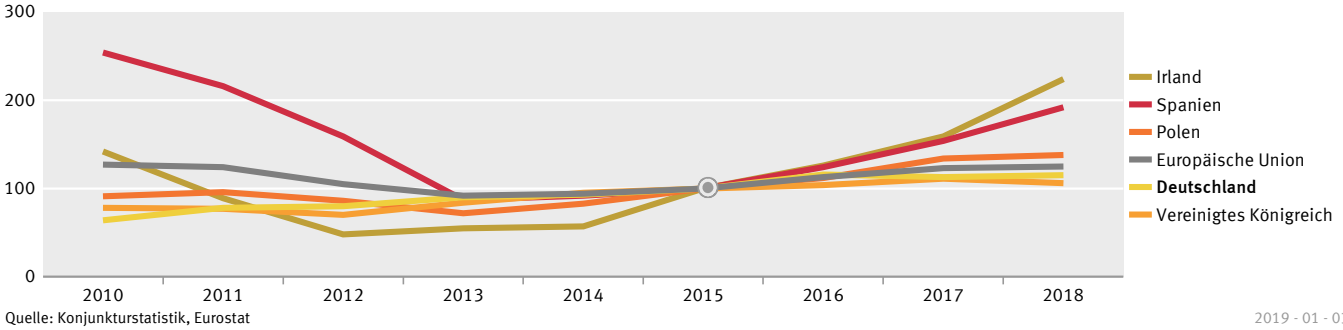
Weitere Erläuterungen zu den Indikatoren siehe Tabelle A.20.

1 Zum Teil vorläufige Werte.
2 Eurostat Schätzung.
3 Abweichende Definitionen.

Quelle: Strukturelle Unternehmensstatistik und Konjunkturstatistik, Eurostat

Baugenehmigungen von Wohnungen in Wohngebäuden

Indexwert, Basisjahr 2015 = 100



Quelle: Konjunkturstatistik, Eurostat

2019 - 01 - 0331

A.24 Binnenhandel

	Unternehmen nach Wirtschaftsbereichen			Tätige Personen nach Wirtschaftsbereichen			Bruttowertschöpfung zu Faktorkosten nach Wirtschaftsbereichen		
	Einzelhandel [1]	Großhandel [1]	Handel mit Kraftfahrzeugen	Einzelhandel [1]	Großhandel [1]	Handel mit Kraftfahrzeugen	Einzelhandel [1]	Großhandel [1]	Handel mit Kraftfahrzeugen
	2016								
	Anzahl						Mill. EUR		
Europa									
Europäische Union	3 629 519	1 818 221	868 670	18 869 334	10 488 191	3 931 997	519 383	660 123	173 433
Belgien	70 109	39 060	18 612	321 356	218 876	78 571	13 155	23 387	6 261
Bulgarien	97 514	28 853	14 157	302 406	157 778	48 971	1 803	3 017	467
Dänemark	18 784	15 240	7 748	245 196	158 599	50 296	7 681	16 280	3 241
Deutschland	**333 294**	**144 145**	**111 266**	**3 566 038**	**1 866 944**	**862 809**	**108 012**	**152 179**	**44 127**
Estland	6 166	6 999	3 186	50 785	30 412	12 143	807	1 130	315
Finnland	19 444	13 826	9 391	158 504	87 269	43 798	6 158	6 798	2 326
Frankreich	506 635	155 595	97 777	1 963 367 [2]	1 099 428 [2]	414 699 [2]	75 360	82 952	20 241
Griechenland	163 633	64 904	26 966	426 411	217 992	64 026	3 471	6 269	648
Irland	24 160	13 608	8 827	219 713	100 543	35 801	8 539	12 098	1 590
Island [3]	1 514	1 757	753	13 512	8 511	3 468	622	729	260
Italien	606 224	383 304	115 868	1 862 465	1 139 069	370 099	52 157	67 291	13 860
Kroatien	16 502	15 091	5 027	133 832	73 271	21 129	2 069	1 974	397
Lettland	14 497	9 331	5 163	93 489	46 685	19 318	1 037	1 255	242
Litauen	36 492	10 891	12 256	138 021	80 212	37 660	1 408	2 129	473
Luxemburg	3 186	3 579	805	25 242	18 280	7 411	1 483	3 267	457
Malta	5 793	2 253	1 252	19 816	11 582	2 954	420	552	69
Niederlande	128 711	87 450	33 956	838 176	513 041	138 682	21 720	49 771	7 438
Norwegen	24 596	16 959	8 684	229 308	105 371	49 958	9 060	10 372	3 830
Österreich	41 785	25 353	10 670	368 505	207 636	81 011	13 343	17 419	4 885
Polen	283 420	126 070	92 539	1 270 958	765 824	261 567	15 036	20 034	3 973
Portugal	133 267	58 332	28 760	431 314	224 032	93 824	7 080	7 405	1 932
Rumänien	100 064	51 566	18 082	487 279	322 425	97 311	5 687	7 092	1 400
Russische Föderation	.	.	.	.	.	.	.	.	.
Schweden	60 345	45 579	22 041	333 226	253 093	89 078	14 491	21 613	5 535
Schweiz	15 328	10 626	6 902	307 589 [4]	201 966 [4]	74 402 [4]	21 699	62 772	6 360
Slowakei	59 131	44 679	9 464	189 439	124 192	29 247	2 793	2 785	571
Slowenien	7 940	13 740	4 702	56 797	42 298	15 072	1 614	1 705	565
Spanien	486 684	229 956	79 409	1 739 721	1 069 748	298 023	42 959	50 902	10 163
Tschechische Republik	119 189	89 508	31 902	349 173	272 570	86 570	5 351	7 894	1 802
Türkei	.	.	.	.	.	.	.	.	.
Ungarn	82 021	31 891	21 285	324 483	175 098	74 320	3 605	4 827	1 049
Vereinigtes Königreich	195 247	103 297	74 631	2 917 553	1 190 508	589 838	101 315	87 361	39 247
Zypern	9 282	4 121	2 928	36 069	20 786	7 769	829	738	163

Weitere Erläuterungen zu den Indikatoren siehe Tabelle A.20.

1 Ohne Handel mit Kraftfahrzeugen.
2 Eurostat Schätzung.
3 Vorläufige Werte.
4 Abweichende Definition.

Quelle: Strukturelle Unternehmensstatistik, Eurostat

A.25 Transport und Verkehr

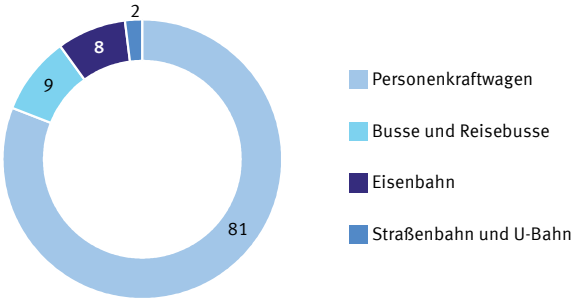
	Wirtschaftsbereich Verkehr und Lagerei [1]			Personenkraftwagen (Pkw) [2]	Getötete im Straßenverkehr [2]	Güterverkehr nach Verkehrsträgern (ohne Pipelines, Luftverkehr) [3]			Personenverkehr nach Verkehrsträgern (ohne Luft- und Seeverkehr) [2]		
	Unternehmen	Tätige Personen	Bruttowertschöpfung zu Faktorkosten			Eisenbahn	Straße	Binnenschifffahrt	Pkw	Busse, Reisebusse, Straßenbahn und U-Bahn	Eisenbahn
	2016										
	Anzahl		Mill. EUR	je 1 000 Einwohner/-innen	je 1 Mill. Einwohner/-innen	Anteil der Tonnenkilometer in %			Anteil der Personenkilometer in %		
Europa											
Europäische Union	1 246 259	11 328 250	550 000 [4]	*507*	*50,2*	*17,6* [4]	*76,2* [4]	*6,3* [4]	*81,3*	*11,1*	*7,6*
Belgien	18 095	211 429	16 014	*505*	*56,2*	*11,0* [4]	*74,4* [4]	*14,6* [4]	*81,0*	*11,3*	*7,7*
Bulgarien	22 711	169 272	2 182	*443*	*99,3*	*17,1*	*55,7*	*27,2*	*79,6*	*18,3*	*2,0*
Dänemark	10 945	146 776	12 215	*429*	*36,8*	*11,3*	*88,7*	*0,0*	*81,1*	*10,2*	*8,7*
Deutschland	**106 559**	**2 341 914**	**103 634**	***555***	***38,9***	***18,8***	***72,4***	***8,8***	***84,3***	***7,2***	***8,5***
Estland	5 244	38 222	1 110	*534*	*54,0*	*42,9*	*57,1*	*0,0*	*79,5*	*18,5*	*2,0*
Finnland	20 538	142 995	8 062	*608*	*46,9*	*26,8*	*72,9*	*0,3*	*81,8*	*12,6*	*5,6*
Frankreich	115 627	1 382 231	84 791	*479*	*52,0*	*10,9*	*86,4*	*2,8*	*80,0*	*10,5*	*9,5*
Griechenland	62 878	184 151	5 634	*486*	*76,5*	*1,3*	*98,7*	*0,0*	*80,8*	*18,2*	*1,0*
Irland	24 614	97 662	8 595	*428*	*39,1*	*0,9*	*99,1*	*0,0*	*79,6*	*17,5*	*2,9*
Island	1 745 [5]	12 676 [5]	1 137 [5]	*711*	.	.	.	.	*88,6*	*11,4*	*0,0*
Italien	123 442	1 117 011	60 161	*625*	*54,2*	*14,7*	*85,3*	*0,0*	*81,3*	*12,7*	*6,0*
Kroatien	8 372	83 153	2 000	*374*	*73,6*	*16,4* [4]	*76,3* [4]	*7,3* [4]	*83,3*	*14,0*	*2,6*
Lettland	7 654	78 606	1 586	*341*	*80,6*	*76,6*	*23,4*	*0,0*	*82,8*	*13,8*	*3,5*
Litauen	13 603	120 336	2 269	*456*	*66,9*	*65,0*	*35,0*	*0,0*	*89,9*	*9,1*	*1,0*
Luxemburg	972	20 655	1 638	*662*	*54,8*	*6,2*	*87,9*	*5,9*	*83,1*	*12,3*	*4,6*
Malta	1 430	11 846	.	*615*	*50,5*	*0,0*	*100,0*	*0,0*	*82,6*	*17,4*	*0,0*
Niederlande	42 081	401 050	29 515	*481*	*31,3*	*6,0*	*49,7*	*44,2*	*85,5*	*3,6*	*10,9*
Norwegen	20 831 [6]	154 335 [6]	17 110 [6]	*506*	.	*13,0*	*87,0*	*0,0*	*87,9*	*7,1*	*5,0*
Österreich	14 141	199 140	14 145	*550*	*49,4*	*32,0*	*65,1*	*2,9*	*72,6*	*16,1*	*11,4*
Polen	153 586	789 208	14 384	*571*	*79,7*	*24,7*	*75,2*	*0,1*	*77,2*	*15,6*	*7,3*
Portugal	21 799	159 888	6 640	*470*	*54,5*	*14,5*	*85,5*	*0,0*	*88,2*	*7,6*	*4,2*
Rumänien	44 504	365 814	4 888	*279*	*97,2*	*30,3*	*40,3*	*29,4*	*75,0*	*21,1*	*3,9*
Russische Föderation	.	.	.	.	.	.	.	.	.	.	.
Schweden	29 652	273 856	15 142	*477*	*27,2*	*29,5*	*70,5*	*0,0*	*81,9*	*8,9*	*9,2*
Schweiz	4 798	211 335 [6]	25 212	*537*	.	*37,4*	*62,5*	*0,1*	*77,0*	*6,0*	*17,0*
Slowakei	19 020	105 157	2 604	*390*	*50,6*	*34,5*	*61,7*	*3,7*	*74,2*	*16,5*	*9,3*
Slowenien	8 574	46 856	1 948	*531*	*63,0*	*33,3*	*66,7*	*0,0*	*86,3*	*11,8*	*2,0*
Spanien	196 166	854 350	44 757	*492*	*38,9*	*5,3*	*94,7*	*0,0*	*80,1*	*13,4*	*6,5*
Tschechische Republik	38 439	279 750	6 491	*502*	*57,8*	*26,4*	*73,5*	*0,1*	*66,5*	*25,4*	*8,0*
Türkei	.	.	.	*142*	.	.	.	.	.	.	.
Ungarn	27 668	247 103	5 145	*338*	*61,9*	*28,5*	*66,2*	*5,3*	*66,5*	*24,5*	*9,0*
Vereinigtes Königreich	104 957	1 442 412	95 939	*484*	*28,4*	*9,4*	*90,5*	*0,1*	*85,0*	*6,3*	*8,7*
Zypern	2 988	17 407	734	*595*	*54,0*	*0,0*	*100,0*	*0,0*	*81,4*	*18,6*	*0,0*

1 Quelle: Strukturelle Unternehmensstatistik, Eurostat. Weitere Erläuterungen zu den Indikatoren siehe Tabelle A.20.
2 Quelle: Transport in Figures 2018, Europäische Kommission.
3 Quelle: Verkehrsstatistik, Eurostat.
4 Eurostat Schätzungen.
5 Vorläufige Werte.
6 Abweichende Definition.

A.25 Transport und Verkehr

Personen- und Güterbeförderung nach Verkehrsträgern in der EU
in %

Personenbeförderung 2016

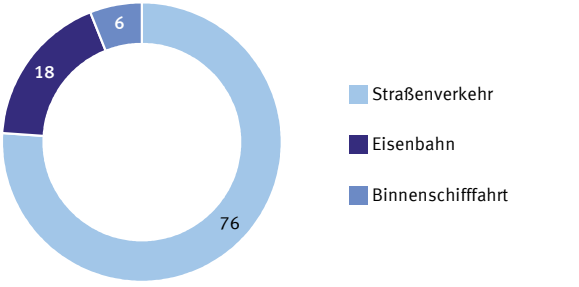


Nicht berücksichtigt sind im Luftverkehr und zu Fuß oder mit dem Fahrrad zurückgelegte Wege.
Quelle: GD Mobilität und Verkehr der Europäischen Kommission

Die **Beförderungsleistung im Personenverkehr** wird in der Maßeinheit **Personenkilometer (Pkm)** gemessen. Sie berechnet sich durch Multiplikation der Zahl der beförderten Personen mit den von ihnen zurückgelegten Kilometern. Fahren beispielsweise 30 Personen in einem Bus eine Entfernung von 20 km zwischen den Orten A und B, so wird eine Beförderungsleistung von 600 Pkm nachgewiesen.

Die **Beförderungsleistung im Güterverkehr** ist das Produkt aus dem Gewicht der beförderten Gütermenge mit der zurückgelegten Transportstrecke. Die so ermittelte Beförderungsleistung wird in der Maßeinheit **Tonnenkilometer (tkm)** gemessen. Werden in einem Lkw beispielsweise 15 Tonnen (t) Güter über eine Entfernung von 200 km zwischen den Orten A und B befördert, so ergibt dies eine Beförderungsleistung von 3 000 tkm.

Güterbeförderung 2016



Nicht berücksichtigt sind im Luftverkehr oder über eine Pipeline transportierte Güter.
Quelle: Verkehrsstatistik, Eurostat

2019 - 01 - 0332

A.26 Gastgewerbe, Tourismus

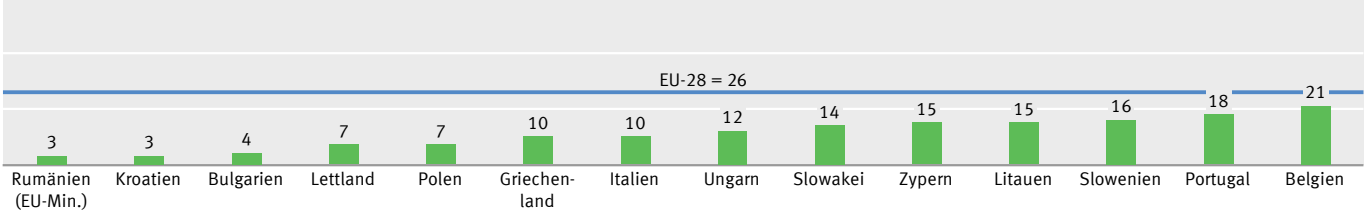
	Wirtschaftsbereich Gastgewerbe (Beherbergung und Gastronomie) [1]			Hotels, Gasthöfe und Pensionen [2]		
	Unternehmen	Tätige Personen	Bruttowertschöpfung zu Faktorkosten	Beherbergungsbetriebe	Betten	Übernachtungen
	2016			2017		
	Anzahl		Mill. EUR	Anzahl	1 000	
Europa						
Europäische Union	1 998 320	11 900 000 [3]	264 371	201 489	13 925	1 952 255
Belgien	49 261	175 436	5 236	1 517	129	18 945
Bulgarien	27 032	142 785	817	2 110	293	24 071
Dänemark	14 087	127 731	3 382	559	93	15 547
Deutschland	**230 040**	**2 300 813**	**44 505**	**32 749**	**1 812**	**288 759**
Estland	2 799	24 806	309	422	34	5 267
Finnland	12 042	72 780	2 365	787	140	17 780
Frankreich	270 760	1 057 696 [3]	38 475	18 391	1 320	214 275
Griechenland	118 052	488 149	3 000	9 772	795	87 628
Irland	18 377	179 827	5 058	2 348 [4]	150 [4]	26 265 [4]
Island	1 817 [5]	16 149 [5]	624 [5]	405	31	5 169 [4]
Italien	323 563	1 379 644	31 165	32 988	2 239	275 134
Kroatien	19 913	100 269	1 786	1 037	166	24 537
Lettland	4 092	35 635	274	349	27	3 845
Litauen	5 985	44 697	345	411	29	4 081
Luxemburg	2 808	20 268	743	225	16	1 694
Malta	2 437	.	392	183	43	9 310
Niederlande	58 088	447 559	10 560	3 636	270	48 873
Norwegen	11 806	116 595	3 596	1 058	188	22 484 [4]
Österreich	47 474	302 905	9 415	12 153	609	91 612
Polen	54 833	259 677	2 726	4 064	336	47 138
Portugal	97 562	317 808	4 718	2 538	363	59 534
Rumänien	25 612	176 177	1 356	2 766	220	22 242
Russische Föderation	.	.	.	.	.	.
Schweden	32 694	207 463	6 928	2 025	246	36 554
Schweiz	16 864	201 444 [6]	10 642	4 949 [4]	272 [4]	35 533 [4]
Slowakei	18 048	60 624	487	1 471	97	10 118
Slowenien	11 130	36 790	705	698	47	7 751
Spanien	306 851	1 401 056	28 825	19 630	1 917	340 578
Tschechische Republik	60 120	170 580	1 782	5 967	317	39 590
Türkei	.	.	.	3 763	933	112 190 [4]
Ungarn	29 976	138 371	1 104	2 184	181	24 307
Vereinigtes Königreich	149 009	2 155 468	56 784	39 715 [4]	1 950 [4]	190 046 [4]
Zypern	5 675	42 980	1 129	794	85	16 776

Weitere Erläuterungen zu den Indikatoren siehe Tabelle A.20.

1 Quelle: Strukturelle Unternehmensstatistik, Eurostat. Daten beziehen sich auf alle Unternehmen der Wirtschaftsgliederung „Gastgewerbe/Beherbergung und Gastronomie".
2 Quelle: Tourismusstatistik, Eurostat. Teilweise Schätzungen.
3 Eurostat Schätzung.
4 2016.
5 Vorläufige Werte.
6 Abweichende Definition.

Online-Buchungen von Urlaubsunterkünften 2018

16- bis 74-Jährige, die in den letzten 12 Monaten eine Urlaubsunterkunft online gebucht haben, in %



Quelle: Erhebung zur IKT-Nutzung, Eurostat

2019 - 01 - 0333

A.27 Weitere Dienstleistungen

	Unternehmen nach ausgewählten Dienstleistungsbereichen [1]			Tätige Personen nach ausgewählten Dienstleistungsbereichen [1]			Bruttowertschöpfung zu Faktorkosten nach ausgewählten Dienstleistungsbereichen [1]		
	Information und Kommunikation	Grundstücks- und Wohnungswesen	Freiberufliche, wissenschaftliche u. technische Dienstleistungen	Information und Kommunikation	Grundstücks- und Wohnungswesen	Freiberufliche, wissenschaftliche u. technische Dienstleistungen	Information und Kommunikation	Grundstücks- und Wohnungswesen	Freiberufliche, wissenschaftliche u. technische Dienstleistungen
	2016								
	Anzahl						Mill. EUR		
Europa									
Europäische Union	1 189 388	1 436 433	4 589 039	6 780 000 [2]	2 911 538	13 544 746	597 647	287 868	743 659
Belgien	32 079	47 370	150 094	128 423	75 700	319 362	14 772	7 193	24 450
Bulgarien	12 646	21 767	43 082	94 783	36 766	106 239	2 333	643	1 434
Dänemark	17 126	28 446	35 104	112 527	60 455	164 057	11 052	12 067	14 894
Deutschland	**123 523**	**151 322**	**485 448**	**1 240 715**	**486 368**	**2 733 362**	**117 174**	**76 742**	**160 939**
Estland	4 802	5 939	12 564	21 910	11 529	27 632	847	805	660
Finnland	10 156	27 420	35 840	94 304	24 224	122 655	9 108	4 588	7 172
Frankreich	133 824	275 371	481 900	869 310 [2]	345 887 [2]	1 409 837 [2]	82 624	42 247	95 726
Griechenland	19 069	8 813	152 320	79 568	15 677	249 317	3 367	468	2 805
Irland	14 570	13 249	40 452	95 220	25 744	135 887	24 210	1 707	10 187
Island [3]	2 356	3 211	4 785	8 705	1 684	9 360	780	488	663
Italien	101 269	243 883	734 520	557 589	304 673	1 254 856	47 651	18 745	56 708
Kroatien	6 642	4 585	24 170	39 936	11 611	73 552	1 599	527	1 513
Lettland	6 871	14 459	20 107	32 330	32 371	48 140	875	717	667
Litauen	6 887	13 369	29 096	33 726	25 455	65 336	975	753	1 023
Luxemburg	2 365	3 317	8 260	17 899	4 212	36 445	2 804	875	3 489
Malta	1 264	1 933	4 232	.	2 060	13 867	604	264	816
Niederlande	92 838	27 559	345 527	295 949	74 099	660 124	28 961	17 289	40 947
Norwegen	16 666	51 238	47 298 [4]	95 022	32 478	134 760 [4]	11 366	10 006	11 924 [4]
Österreich	18 510	17 966	66 079	110 564	49 134	245 215	9 909	9 409	15 684
Polen	94 054	54 893	268 255	357 902	196 110	645 241	12 943	5 072	11 709
Portugal	16 453	35 787	120 198	94 132	56 778	240 536	5 303	1 752	5 325
Rumänien	22 012	15 349	60 324	178 879	47 229	212 174	5 194	1 386	3 368
Russische Föderation	.	.	.	.	.	.	.	.	.
Schweden	60 399	64 233	180 842	236 057	87 842	328 563	21 303	18 792	23 394
Schweiz	6 425	4 494	23 837	141 017 [4]	38 662 [4]	281 838 [4]	24 833	6 980	38 115
Slowakei	20 190	13 852	70 452	64 219	29 702	137 946	2 596	1 261	2 901
Slowenien	9 092	2 885	32 527	25 747	5 141	57 004	1 209	283	1 669
Spanien	67 437	169 031	394 359	460 593	238 428	1 018 950	33 137	13 900	41 055
Tschechische Republik	41 382	46 480	183 979	130 642	59 891	274 887	6 219	3 370	6 304
Türkei	.	.	.	.	.	.	.	.	.
Ungarn	39 149	32 831	124 004	127 761	70 925	248 318	4 162	1 963	4 072
Vereinigtes Königreich	213 430	93 444	478 251	1 265 460	531 505	2 689 971	145 904	44 970	203 704
Zypern	1 349	880	7 053	9 979	2 022	25 273	812	81	1 044

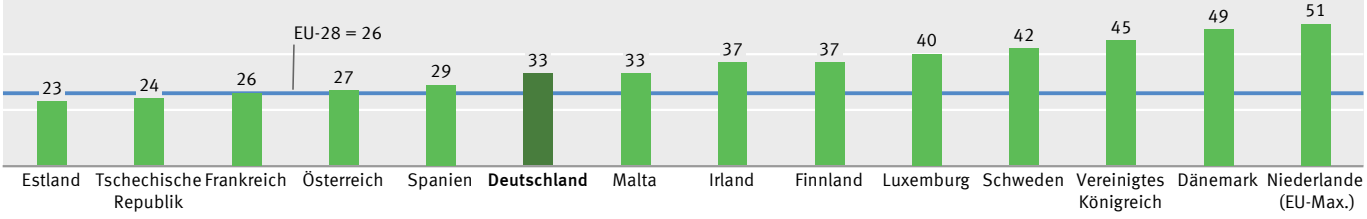
Weitere Erläuterungen zu den Indikatoren siehe Tabelle A.20.

1 Die Einteilung der Wirtschaftsbereiche entspricht der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2).
2 Eurostat Schätzung.
3 Vorläufige Werte.
4 Abweichende Definition.

Quelle: Strukturelle Unternehmensstatistik, Eurostat

Online-Buchungen von Urlaubsunterkünften 2018

16- bis 74-Jährige, die in den letzten 12 Monaten eine Urlaubsunterkunft online gebucht haben, in %



Quelle: Erhebung zur IKT-Nutzung, Eurostat

2019 - 01 - 0334

Methodik

Datenquellen

Die im Kapitel „Internationales“ aufgeführten Statistiken stammen aus zahlreichen amtlichen internationalen Quellen.

Um das Datenspektrum zu erweitern, wurden im Einzelfall auch nicht amtliche Quellen (z. B. BP) verwendet.

In vielen Fällen finden sich methodische Hinweise zu den Daten in den Erläuterungstexten direkt neben der jeweiligen Tabelle. Weitere methodische Hinweise zu den jeweiligen Indikatoren sind den folgenden Originalquellen zu entnehmen:

BP p.l.c.
› *bp.com/statisticalreview*

DWD – Deutscher Wetterdienst
› *dwd.de*

EuroGeographics
› *eurogeographics.org*

Europäisches Parlament
› *europarl.europa.eu*

Eurostat – Statistisches Amt der Europäischen Union
› *ec.europa.eu/eurostat*

FAO – Welternährungsorganisation der Vereinten Nationen
› *faostat.fao.org*

IEA – Internationale Energieagentur
› *iea.org*

ILO – Internationale Arbeitsorganisation der Vereinten Nationen
› *ilo.org/ilostat*

IMF – Internationaler Währungsfonds
› *imf.org/external/data.htm*
› *data.imf.org*

ITU – Internationale Fernmeldeunion, Vereinte Nationen
› *itu.int/ITU-D/ict*

JRC – Europäische Kommission: Joint Research Centre – EDGAR Datenbank
› *edgar.jrc.ec.europa.eu*

OECD – Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
› *stats.oecd.org*

UN Comtrade – Außenhandelsdatenbank der Vereinten Nationen
› *comtrade.un.org*

UNCTAD – Konferenz für Handel und Entwicklung, Vereinte Nationen
› *unctadstat.unctad.org*

UNdata – Datenportal der Vereinten Nationen
› *data.un.org*

UNESCO – Organisation der Vereinten Nationen für Bildung, Wissenschaft und Kultur
› *data.uis.unesco.org*

UNFCCC – Klimarahmenkonvention der Vereinten Nationen
› *di.unfccc.int*

UN-IGME – Inter-agency Group for Child Mortality, Vereinte Nationen
› *childmortality.org*

UN MBS – Monthly Business Statistics, Vereinte Nationen
› *unstats.un.org/unsd/mbs*

UN DESA – Hauptabteilung Wirtschaftliche und Soziale Angelegenheiten (DESA): Abteilung Bevölkerung, Vereinte Nationen
› *un.org/esa/population*

Weltbank – World Development Indicators
› *databank.worldbank.org/wdi*

WHO – Weltgesundheitsorganisation
› *who.int/gho/en*
› *who.int/gho/gisah*
› *who.int/nha*

Hinweise zur Auswahl der Staaten und zur territorialen Abgrenzung im Kapitel „Internationales“

Einseitige Tabellen | Diese enthalten ausschließlich Daten zu europäischen Staaten. Aufgelistet sind alle EU- und EFTA-Staaten (außer Liechtenstein) sowie einige weitere bevölkerungsreiche europäische Staaten.

Zweiseitige Tabellen | Diese umfassen sämtliche EU-, G20- und OECD-Staaten, die sogenannten BRICS- und Next Eleven-Staaten, alle NAFTA- und EFTA-Staaten (außer Liechtenstein) sowie die weltweit 30 bevölkerungsreichsten und 30 wirtschaftlich stärksten Staaten (gemessen am Bruttoinlandsprodukt).

Daten zu allen 193 Mitgliedstaaten der Vereinten Nationen finden Sie in der Übersichtstabelle „Auf einen Blick“ (A.0). In dieser Tabelle nicht berücksichtigt sind die zwei Staaten mit UN-Beobachterstatus – der Vatikan und die Palästinensischen Gebiete.

Hinsichtlich der territorialen Abgrenzung der Staaten gilt in der Regel: China ohne Hongkong, Macau und Taiwan. Dänemark ohne Färöer und Grönland. Frankreich einschl. Überseegebiete. Israel ohne Palästinensische Gebiete. Niederlande ohne Überseegebiete. Portugal einschl. Azoren und Madeira. Spanien einschl. Balearen und Kanarische Inseln sowie einschl. Ceuta und Melilla. Zypern nur Republik Zypern (griechischer Teil der Insel). Detaillierte Erläuterungen zur jeweiligen territorialen Abgrenzung sind den entsprechenden Quellen zu entnehmen.

Mitgliedstaaten internationaler Organisationen

Europäische Union | Die Europäische Union umfasst derzeit 28 Mitgliedstaaten (EU-28). Zuletzt trat im Jahr 2013 Kroatien der EU bei. In Klammern angegeben ist das Beitrittsjahr zur Europäischen Union bzw. zu einer der Vorgängerorganisationen. Fünf Staaten haben derzeit offiziell den Status eines EU-Beitrittskandidaten: Albanien, Nordmazedonien, Montenegro, Serbien und die Türkei.

Belgien (1957)
Bulgarien (2007)
Dänemark (1973)
Deutschland (1957)
Estland (2004)
Finnland (1995)
Frankreich (1957)
Griechenland (1981)
Irland (1973)
Italien (1957)
Kroatien (2013)
Lettland (2004)
Litauen (2004)
Luxemburg (1957)
Malta (2004)
Niederlande (1957)
Österreich (1995)
Polen (2004)
Portugal (1986)
Rumänien (2007)
Schweden (1995)
Slowakei (2004)
Slowenien (2004)
Spanien (1986)
Tschechische Republik (2004)
Ungarn (2004)
Vereinigtes Königreich (1973)
Zypern (2004)

Eurozone | Die Eurozone (auch Euroraum genannt) umfasst alle Mitgliedstaaten der EU, die den Euro als Landeswährung eingeführt haben. Derzeit besteht die Eurozone aus 19 Mitgliedstaaten. Jüngstes Beitrittsland ist Litauen, das am 1.1.2015 den Euro einführte. Im Folgenden sind sämtliche Mitgliedstaaten der Eurozone aufgelistet. In Klammern angegeben ist jeweils das Jahr der Einführung des Euro-Buchgelds. Die Bargeldeinführung erfolgte bei den Gründungsstaaten erst mit Zeitverzug. Bei den späteren Erweiterungen erfolgte die Buch- und Bargeldeinführung stets zeitgleich.

Belgien (1999)
Deutschland (1999)
Estland (2011)
Finnland (1999)
Frankreich (1999)
Griechenland (2001)
Irland (1999)
Italien (1999)
Lettland (2014)
Litauen (2015)
Luxemburg (1999)
Malta (2008)
Niederlande (1999)
Österreich (1999)
Portugal (1999)
Slowakei (2009)
Slowenien (2007)
Spanien (1999)
Zypern (2008)

Europäische Freihandelsassoziation (EFTA) | Die Europäische Freihandelsassoziation wurde 1960 gegründet. Zielsetzung war die Förderung von Wachstum und Wohlstand ihrer Mitgliedstaaten sowie die Vertiefung des Handels mit anderen westeuropäischen Staaten. Viele ehemalige EFTA-Staaten sind später der Europäischen Union beigetreten. Derzeit umfasst die EFTA vier Staaten. In Klammern angegeben ist das Beitrittsjahr.

Island (1970)
Liechtenstein (1991)
Norwegen (1960)
Schweiz (1960)

Mitgliedstaaten der Vereinten Nationen | Derzeit umfassen die Vereinten Nationen insgesamt 193 Staaten. Eine Auflistung dieser Staaten finden Sie nach Kontinenten gegliedert in der Tabelle A.0.

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) | Die OECD ist ein Zusammenschluss von Industrienationen, der die Förderung von Wohlstand und wirtschaftlichem Wachstum zum Ziel hat. Die Organisation entstand 1961 aus der Organisation für Europäische Wirtschaftliche Zusammenarbeit. Die 36 Mitgliedstaaten sind den Prinzipien der Demokratie und der Marktwirtschaft verpflichtet. Am 5. Juli 2018 ist zuletzt Litauen der OECD beigetreten. Mit Costa Rica und Kolumbien werden derzeit Beitrittsgespräche geführt. Aufgelistet sind die derzeitigen Mitgliedstaaten unter Angabe des jeweiligen Beitrittsjahres.

Australien (1971)
Belgien (1961)
Chile (2010)
Dänemark (1961)
Deutschland (1961)
Estland (2010)
Finnland (1969)
Frankreich (1961)
Griechenland (1961)
Irland (1961)
Island (1961)
Israel (2010)
Italien (1962)
Japan (1964)
Kanada (1961)
Korea, Republik (1996)
Lettland (2016)
Litauen (2018)
Luxemburg (1961)
Mexiko (1994)
Neuseeland (1973)
Niederlande (1961)
Norwegen (1961)
Österreich (1961)
Polen (1996)
Portugal (1961)
Schweden (1961)
Schweiz (1961)
Slowakei (2000)
Slowenien (2010)
Spanien (1961)
Tschechische Republik (1995)
Türkei (1961)
Ungarn (1996)
Vereinigtes Königreich (1961)
Vereinigte Staaten (1961)

G20-Staaten | Die G20 ist ein seit 1999 bestehender Zusammenschluss von 19 Staaten und der Europäischen Union und gilt als Gruppe der führenden Industrie- und Schwellenländer. Bei den jährlichen Gipfeltreffen wird über wirtschaftliche Zusammenarbeit, Finanzmarktregulierung und wirtschaftliche Reformen diskutiert.

Argentinien
Australien
Brasilien
China
Deutschland
Europäische Union
Frankreich
Indien
Indonesien
Italien
Japan
Kanada
Korea, Republik
Mexiko
Russische Föderation
Saudi-Arabien
Südafrika
Türkei
Vereinigtes Königreich
Vereinigte Staaten

BRICS, Next Eleven | Zu den BRICS-Staaten, einer Vereinigung von fünf aufstrebenden Volkswirtschaften, zählen Brasilien, die Russische Föderation, Indien, China und Südafrika. Der Begriff BRICS setzt sich aus den Anfangsbuchstaben der Ländernamen zusammen und geht auf eine Abhandlung des Volkswirts Jim O'Neill zurück. 2005 identifizierte O'Neill eine weitere Gruppe aufstrebender Staaten und bezeichnete diese als Next Eleven (N11). Die N11-Staaten umfassen Ägypten, Bangladesch, Indonesien, Iran, Korea (Republik), Mexiko, Nigeria, Pakistan, Philippinen, Türkei und Vietnam.

Mehr zum Thema

Liebe Leserin, lieber Leser,
ein Thema in diesem Kapitel spricht Sie besonders an oder Sie benötigen weitere Informationen? Auf dieser Seite nennen wir Ihnen weitere Veröffentlichungen unseres Hauses zum Thema „Internationales“. Ausführliche Informationen zu den Produktkategorien sowie dem Informationsangebot des Statistischen Bundesamtes finden Sie auf Seite 8 dieser Ausgabe.

Web-Angebote

www.destatis.de ist Ihre erste Adresse in Sachen Statistik. Hier finden Sie alle Informationen, die das Statistische Bundesamt veröffentlicht, tagesaktuell. Unsere Veröffentlichungen können Sie direkt über unsere Website *www.destatis.de* › Themen downloaden.

Unter *www.destatis.de/international* gelangen Sie direkt zum Angebot der internationalen Statistik.

Unter *www.destatis.de/europa* finden Sie statistische Informationen zu den Mitgliedstaaten der Europäischen Union.

GENESIS-Online – die zentrale Datenbank

Unter *www.destatis.de* › GENESIS-Online Datenbank bietet das Statistische Bundesamt eine Auswahl an internationalen Schlüsselindikatoren in Form von Zeitreihen an. Diese Indikatoren stammen aus unterschiedlichen Quellen der internationalen amtlichen Statistik (z. B. Weltbank, Internationaler Währungsfonds, Weltgesundheitsorganisation). Daten zur *Internationalen Statistik* finden Sie unter dem Menüpunkt › Themen, Code 9 (Nationale und internationale Indikatorensysteme) und dort unter dem Code *999*

Weitere Veröffentlichungen

Auf einen Blick

G20 in Zahlen – Gipfel der G20-Staaten in Europa (2017)
Arbeitsmarkt auf einen Blick – Deutschland und Europa (2018)
Tierhaltung weltweit – Zahlen Fakten (2018)

Statistische Länderprofile

Statistische Länderprofile zu allen UN-Staaten

Government launches Green Pass for vaccinated, warns fraudsters will be jailed

By TOI staff 18 February 2021, 5:13 pm Edit

The Health Ministry on Thursday launched the long-awaited "Green Pass" certificate which will enable those vaccinated or recovered from the coronavirus to take part in various activities. At the same time, the ministry warned of serious legal penalties for those who falsify the passes.

Health Minister Yuli Edelstein, Ministry Director-General Chezy Levy, and other health officials presented the new certification and demonstrated the methods of issuing the QR-code-secured pass, which has been the target of skepticism following reports demonstrating how easy it is to falsify.

Cabinet ministers on Monday approved the reopening of stores, gyms, hotels, and other venues starting Sunday, in a major easing of sweeping lockdown measures meant to slow the spread of COVID-19.

Street-front shops, malls, markets, museums, and libraries will be open to all Israelis. But only those who have been vaccinated or have recovered from COVID-19 will be able to use gyms and pools, attend sporting and culture events, and stay at hotels.

To be allowed to open Sunday, relevant businesses must undertake to scan for the pass and only accept those carrying it.

In a further easing of restrictions, the Health Ministry and the Prime Minister's Office said Tuesday that the government will allow outdoor gatherings of up to 20 people, and indoor gatherings of up to 10, starting Friday morning. The previous rules restricted outdoor gatherings to 10 people and indoors to five.

Those eligible will be able to get the Green Pass using three methods starting Sunday, February 21:

1. Downloading the Traffic Light (Ramzor) app on Google Play or the Apple App Store, entering personal details and getting the pass on one's phone.
2. Signing up on the Health Ministry website and downloading a printable personal document.
3. Calling the Health Ministry's hotline at *5400 and having the pass sent by email or fax.

"The vaccinated and recovered will be able to enter gyms, events, hotels, and synagogues that are registered under the Green Pass certificate from Sunday," Edelstein said. "This is how the first stage will look in the return to your almost normal lives."

Still, he stressed the importance of continuing to wear masks — even those who've received both vaccine doses.

The pass has already been criticized as easy to counterfeit. A black market for fake certificates is thriving on Telegram, where more than 100,000 users have joined groups that offer the forgeries at a price, Channel 12 News reported.

In response, Edelstein stated, "Those who think this a game and print a vaccination certificate without being vaccinated will be caught and their activities may end with them in jail."

Israelis sit in Dizengoff Square in Tel Aviv on February 15, 2021. (Miriam Alster/Flash90)

At the same time, Edelstein said, "There will be no forced vaccination in Israel; those who choose not to be vaccinated — it is their choice." He added that there "won't be any personal sanctions against those who do not vaccinate."

Deputy Attorney General Raz Nizri said Thursday that under certain circumstances, employers can legally demand their workers get vaccinated, but stressed that the demand must be "justified."

Nizri, writing a legal opinion on the issue, said he opposes any sort of blanket ban on employers conditioning their workers' continued employment on their immunization from the coronavirus.

"It is not possible to establish a blanket ban on employers in these contexts (of the obligation to vaccinate), and at the same time it is not possible to establish a general requirement to be vaccinated without examining and establishing the justification of the requirement, and examining its proportionality, meaning of refusal, etc.," Nizri wrote.

He instructed employers to examine each decision according to the specific circumstances of the workplace and its nature, and also suggested employing other alternatives which can "fulfill the important purpose of preventing infection in the workplace and protecting the public."

Health Ministry Director-General Chezy Levy, speaking after Edelstein, called upon citizens to get vaccinated in order to "exit where we are now, and renew activities and return to normalcy.

Health Ministry Director-General Chezy Levy during the announcement of the "Green Pass" certification on February 18, 2021 (Health Ministry)

"We should remember that the main benefit from vaccinating is the health of everyone," Levy said.

On the subject of forgeries, Levy said: "Today we conducted a meeting with police officials on the subject of enforcing and issuing an uncompromising punishment against counterfeit Green Pass producers.

Ran Bar-Zik, an expert on cybersecurity, wrote in a Facebook post Tuesday that it is "easy, with a graphics program, to change the text on the pass, but the QR code is what looks scary and hard to forge, no? Actually, this is very easy,"

Bar-Zik explained that the QR code on the pass has no encryption, and corresponds directly to a string of text with the holder's personal information, including name, ID number, and date of vaccination, identical to the text printed on the pass itself.

"Whoever scans the false pass will see the exact same details as are printed on the pass, and there are already tens of thousands of people forging it," Bar-Zik said.

A sign reads 'The False Passport' as Israelis protest against the COVID-19 vaccine outside the Knesset in Jerusalem, January 4, 2021. (Yonatan Sindel/Flash90)

The concerns regarding forged vaccination certificates come amid widespread government efforts to provide incentives, both positive and negative, to Israelis who are leery of receiving the shots.

A Tuesday survey of Israelis who have not vaccinated found that 41 percent said they fear possible side effects, 30% are not sure the vaccine is effective, 27% will vaccinate soon, 10% cited information on social media and 4% said the incentives are insufficient. Respondents were allowed to give more than one answer.

About 25% of those who haven't been vaccinated yet said they had no intention of getting the shot.

A young woman receives a COVID-19 vaccine, at Clalit vaccination center in Jerusalem, on February 08, 2021. (Olivier Fitoussi/Flash9)

Another Tuesday poll found that, despite a sharp increase in infections among children, only 41% of Israeli parents said they intend to vaccinate their kids once inoculations become available for those under 16. The poll, conducted by the Rushinek research institute, found that 29% of parents don't plan on vaccinating their 6- to 15-year-olds, 30% are unsure, and 41% plan to do so, Channel 13 reported.

Vaccine hesitancy and skepticism have become a growing concern in recent weeks as Israel's world-leading inoculation campaign has slowed. However, rates have ticked up again this week as ministers approved measures to reopen certain venues and events only to those who have been vaccinated or previously contracted the virus.

Over four million Israelis, or some 45 percent of the country's total population and two-thirds of those eligible, have now received the first dose of the coronavirus vaccine, ministry data showed Thursday. About 2.7 million Israelis have received both doses. Fewer than 2 million eligible Israelis have yet to receive either dose.

Israeli Prime Minister Benjamin Netanyahu and Health Minister Yuli Edelstein seen during a visit at a COVID-19 vaccination center in Zarzir, northern Israel, February 9, 2021. (David Cohen/Flash90)

“If we continue at this high vaccination rate and keep to the guidelines — we won’t need a fourth lockdown,” Edelstein said.

Around 3 million Israelis are not eligible to be vaccinated, including those younger than 16 and those who have recovered from COVID-19, among other reasons.

U.S. Department of Commerce
U.S. Census Bureau

Table 1. APPORTIONMENT POPULATION AND NUMBER OF REPRESENTATIVES BY STATE: 2020 CENSUS

STATE	APPORTIONMENT POPULATION (APRIL 1, 2020)	NUMBER OF APPORTIONED REPRESENTATIVES BASED ON 2020 CENSUS[2]	CHANGE FROM 2010 CENSUS APPORTIONMENT
Alabama	5,030,053	7	0
Alaska	736,081	1	0
Arizona	7,158,923	9	0
Arkansas	3,013,756	4	0
California	39,576,757	52	-1
Colorado	5,782,171	8	1
Connecticut	3,608,298	5	0
Delaware	990,837	1	0
Florida	21,570,527	28	1
Georgia	10,725,274	14	0
Hawaii	1,460,137	2	0
Idaho	1,841,377	2	0
Illinois	12,822,739	17	-1
Indiana	6,790,280	9	0
Iowa	3,192,406	4	0
Kansas	2,940,865	4	0
Kentucky	4,509,342	6	0
Louisiana	4,661,468	6	0
Maine	1,363,582	2	0
Maryland	6,185,278	8	0
Massachusetts	7,033,469	9	0
Michigan	10,084,442	13	-1
Minnesota	5,709,752	8	0
Mississippi	2,963,914	4	0
Missouri	6,160,281	8	0
Montana	1,085,407	2	1
Nebraska	1,963,333	3	0
Nevada	3,108,462	4	0
New Hampshire	1,379,089	2	0
New Jersey	9,294,493	12	0
New Mexico	2,120,220	3	0
New York	20,215,751	26	-1
North Carolina	10,453,948	14	1
North Dakota	779,702	1	0
Ohio	11,808,848	15	-1
Oklahoma	3,963,516	5	0
Oregon	4,241,500	6	1
Pennsylvania	13,011,844	17	-1
Rhode Island	1,098,163	2	0
South Carolina	5,124,712	7	0
South Dakota	887,770	1	0
Tennessee	6,916,897	9	0
Texas	29,183,290	38	2
Utah	3,275,252	4	0
Vermont	643,503	1	0
Virginia	8,654,542	11	0
Washington	7,715,946	10	0
West Virginia	1,795,045	2	-1
Wisconsin	5,897,473	8	0
Wyoming	577,719	1	0
TOTAL APPORTIONMENT POPULATION[1]	331,108,434	435	

[1] Includes the resident population for the 50 states, as ascertained by the Twenty-Fourth Decennial Census under Title 13, United States Code, and counts of U.S. military and federal civilian employees living overseas (and their dependents living with them overseas) allocated to their home state, as reported by the employing federal agencies. The apportionment population excludes the population of the District of Columbia. The counts of overseas personnel (and dependents) are used for apportionment purposes only.

[2] The U.S. Census Bureau prepared these calculations using the existing size of the U.S. House of Representatives (435 members) and the Method of Equal Proportions, as provided for in Title 2, United States Code, Sections 2a and 2b.

VIEWPOINT

Incentivizing Vaccination Uptake
The "Green Pass" Proposal in Israel

Rachel Wilf-Miron, MD, MPH
Tel Aviv University, Tel Aviv, Israel; and The Gertner Institute for Epidemiology and Health Policy Research, Ramat Gan, Israel.

Vicki Myers, PhD
The Gertner Institute for Epidemiology and Health Policy Research, Ramat Gan, Israel.

Mor Saban, PhD
The Gertner Institute for Epidemiology and Health Policy Research, Ramat Gan, Israel.

Supplemental content

Corresponding Author: Mor Saban, PhD, The Gertner Institute for Epidemiology and Health Policy Research, Ramat Gan 3498838, Israel (morsab1608@gmail.com).

Vaccine hesitancy, identified in 2019 by the World Health Organization as one of the major threats to global health, has become a potentially more important issue during the COVID-19 pandemic. After a year of worldwide morbidity, mortality, social distancing, and lockdowns, and despite the development of several clinically tested and efficacious vaccines, not everyone is willing to be vaccinated. In light of the devastating health, economic, and social effects of the pandemic, the availability of effective vaccines represents an important component of the hope to return society to normalcy.

However, some have expressed concerns regarding the fast-tracked new technology involved with the development of COVID-19 vaccines, and these, along with the well-established concerns of vaccine opponents, have contributed to substantial hesitance regarding the willingness to seek and receive these vaccines. For instance, a nationally representative survey conducted in March-April 2020, with sample sizes ranging from 1041 (Ireland) to 2025 (UK), reported rates of potential acceptance of COVID-19 vaccines of 65% in Ireland and 69% in the UK.[1] A more recent 32-country study conducted before vaccine approval (October-December 2020; n = 26 758), with sample sizes between 500 and 1500, found various levels of potential acceptance regarding COVID-19 vaccines. Results ranged from 91% of individuals who reported likely vaccine acceptance in China and India to 81% in the UK, 66% in the US, and 44% in France.[2]

In Israel, a country with a population of 9.3 million, a sufficient supply of the Pfizer-BioNTech vaccine was obtained in late 2020 and vaccination began on December 20, 2020. The vaccination program began with health care staff, people aged 60 years and older, and those with other risks (eg, immunodeficiency, chronic lung disease, diabetes). Vaccination of younger groups followed within 1 month. By February 20, 2021, 40% of eligible citizens aged 16 years and older and more than 80% of those aged 60 years and older had received 2 vaccine doses.[3] This high vaccine uptake resulted from a well-organized vaccination drive that was conducted by the 4 national health maintenance organizations, which provide insurance for all citizens, and offered easy access throughout the country.

However, large sectors of the population were initially slow to receive the vaccine. Organized antivaccination groups with a strong social media presence have contributed to mounting anxieties concerning vaccination both in Israel and worldwide.[4] In an attempt to increase vaccination rates toward achieving herd immunity, reduce the strain on the health care system, and remove societal restrictions, the government considered various incentives and penalties. Incentives have been used previously to encourage vaccination; for example, Australia's "no jab no pay" child benefit scheme,[5] various financial or nonfinancial benefits such as food vouchers or infant products, or the requirement in many US states for children to be fully immunized before starting school. Some proposals in the US have suggested considering financial incentives for COVID vaccination.[6]

The Israeli Ministry of Health has developed a different model of incentives intended to compensate for the months of social restrictions that have characterized the pandemic. This proposed model, termed the "green pass," would allow access (currently limited to 6 months) to social, cultural, and sports events, as well as to gyms, hotels, and restaurants, for individuals with immunity, whether based on having recovered from COVID-19 or being fully vaccinated (1 week after the second dose). The green pass would also give exemption from quarantine (ie, the need to isolate for 10-14 days after contact with a confirmed COVID-19 case or upon returning from international travel).[7] The aim of the pass is to encourage citizens, including those at lower risk of severe COVID-19 disease, to receive vaccination in a national attempt to achieve 95% immunization rate, presumably a sufficient percentage to reach herd immunity.

As opposed to traditional incentives, the green pass allows entry to certain places for individuals who have been vaccinated while penalizing those who have not. Individuals who have been vaccinated can download the pass from the Israeli Ministry of Health app or website, or use a printed document with a QR code. They will be required to show this permit to purchase tickets for events or on entry to certain venues. Pass forgery is regarded as a criminal act punishable by fine or incarceration. Media campaigns have been promoting the green pass, transmitting messages of mutual social responsibility associated with getting vaccinated and using celebrities to influence social norms surrounding vaccination. This proposal has been met with both enthusiasm and some opposition, given the ethical and legal issues it raises, potentially creating a basis for discrimination based on vaccination status.

Fluctuations in COVID-19 vaccination rates in Israel have coincided to some extent with various actions and statements regarding incentives and penalties associated with vaccination (eFigure in the Supplement).[8] Exemptions from quarantine and the promise of lifted restrictions and freer movement may have encouraged some individuals who were uncertain about vaccination to receive it. However, although incentives may increase vaccination rates somewhat, they may not be sufficient to overcome

health concerns or doubts regarding efficacy and safety of these novel vaccines. In addition, it is clear that access to vaccines varies widely within and between countries. In a recent survey conducted in 2021, among 503 Israelis, 21% reported not intending to be vaccinated soon. Of these individuals (n = 106), 31% said the offer of a green pass and the associated benefits would possibly or definitely persuade them to get vaccinated, whereas 46% said that incentives would not persuade them.[9]

Israel has considered compulsory vaccination. The mere suggestion of a law that would make COVID-19 vaccination obligatory, and reports of incidents in which employees in the health care or education systems have been forbidden from entering the workplace for not being vaccinated, have resulted in antagonism and increased distrust among individuals who were already concerned about infringement on citizens' rights. It seems that an approach of mandatory vaccination and penalties for failure to comply will be abandoned and replaced by the incentives promised by the green pass (which came into effect on February 21, 2021). In light of this incentive-based approach, and to increase accessibility, vaccination has been made increasingly available in areas with low rates, including minority areas; for example, mobile vaccination units have been brought to Bnei-Brak, an ultraorthodox Jewish city; to central nightlife areas in Tel Aviv; and to geographically remote Arab villages, accompanied by experts who can answer questions, along with free food or drink to attract those who are hesitant or undecided about vaccination.

The early rollout of the COVID-19 vaccine in Israel, and the relatively high vaccination rate per population, can provide helpful information for other countries that may wish to develop incentive schemes to achieve higher vaccination rates. Issues of equity, with groups of low socioeconomic status initially demonstrating lower vaccination rates despite higher disease burden, should be addressed with outreach actions. Other countries, including Chile, Germany, and the UK, have discussed the use of "immunity passports." It has been suggested that these be considered alternatives to enforcing strict public health measures, or allowing unlimited infection spread, both of which would exacerbate inequalities; thus, the "least restrictive alternative" should be favored.[10]

Creative use of incentives is likely to boost vaccination rates in some groups, whereas other groups will need more to allay their concerns, which should not be dismissed. To build trust, authorities need to understand these concerns and provide appropriate, transparent, and easily accessible information, including empirical data on vaccine effectiveness in the population, on adverse effects of COVID-19 in different population groups, and on the relative health risks from contracting COVID-19 vs from receiving the vaccine.

In parallel, the Israeli parliament passed a bill on February 24, 2021, allowing the Israeli Ministry of Health to transfer personal identification of people who have not yet received their first vaccine dose to the local authorities and to the Ministry of Education (to improve the low vaccination rates among educational staff). This bill, which raises concerns about citizens' right to autonomy over their body and free choice about whether to receive the COVID-19 vaccine, might detract from the effect of the green pass on vaccination acceptance.

The effectiveness of the green pass may be observed in changing vaccination rates in the coming weeks in different age groups. Surveys could evaluate individuals' motivation for vaccination and the role of the green pass in that decision. Although the proposed green pass model provides little more than freer movement, once adopted, after months of restrictions it certainly could be perceived as an incentive. If this model is to be implemented, all barriers to vaccination must be removed for individuals who want to receive the vaccine, including obstacles related to access, logistics, and health literacy, as well as provision of reliable information to help people make an informed and free choice.

ARTICLE INFORMATION

Published Online: March 15, 2021. doi:10.1001/jama.2021.4300

Conflict of Interest Disclosures: None reported.

REFERENCES

1. Murphy J, Vallières F, Bentall RP, et al. Psychological characteristics associated with COVID-19 vaccine hesitancy and resistance in Ireland and the United Kingdom. *Nat Commun*. 2021;12(1):29. doi:10.1038/s41467-020-20226-9

2. Wouters OJ, Shadlen KC, Salcher-Konrad M, et al. Challenges in ensuring global access to COVID-19 vaccines. *Lancet*. Published online February 12, 2021. doi:10.1016/S0140-6736(21)00306-8

3. Israel Ministry of Health. Status report. Accessed February 26, 2021. https://datadashboard.health.gov.il/COVID-19/general

4. Puri N, Coomes EA, Haghbayan H, Gunaratne K. Social media and vaccine hesitancy: new updates for the era of COVID-19 and globalized infectious diseases. *Hum Vaccin Immunother*. 2020;16(11):2586-2593. doi:10.1080/21645515.2020.1780846

5. Parliament of Australia. "No Jab No Pay" and other immunisation measures. Published May 2015. Accessed February 21, 2021. https://www.aph.gov.au/about_parliament/parliamentary_departments/parliamentary_library/pubs/rp/budgetreview201516/vaccination

6. Largent EA, Miller FG. Problems with paying people to be vaccinated against COVID-19. *JAMA*. 2021;325(6):534-535. doi:10.1001/jama.2020.27121

7. Ministry of Health. What is the green pass? Accessed February 27, 2021. https://corona.health.gov.il/en/directives/green-pass-info/

8. Our World in Data. Statistics and research: coronavirus (COVID-19) vaccinations. Accessed February 26, 2021. https://ourworldindata.org/covid-vaccinations

9. N12 News and Midgam Company. Coronavirus disease 2019 vaccine hesitancy in Israel. Accessed February 27, 2021. https://www.mako.co.il/news-lifestyle/2021_q1/Article-68e8d4dff2ca771026.htm

10. Persad G, Emanuel EJ. The ethics of COVID-19 immunity-based licenses ("immunity passports"). *JAMA*. 2020;323(22):2241-2242. doi:10.1001/jama.2020.8102