

Grünschattierungen

Der Grüne Pass wird zum Schlüssel für einen deutlich unkomplizierteren Alltag. Die Einführung des Projekts verlief nicht ohne Schwierigkeiten. Hinter den EU-QR-Codes und der Check-App verstecken sich komplexe Abläufe.

Von Michaela Endemann

Urlauber und Touristiker atmeten auf. Der Grüne Pass kam gerade rechtzeitig, um die sommerlichen Pläne nicht obsolet werden zu lassen: Am 1. Juni startete auf EU-Ebene das Go-Live eines ganzen Bündels an technischen Systemen, um die grenzüberschreitende Überprüfung der Zertifikate zu ermöglichen.

Der Start des digitalen Impfpasses verlief holprig – nicht nur in Österreich. In Deutschland gründeten Datenschützer eine Fake-Apotheke, mit der gefälschte Impfpassse unbegrenzt ausstellbar gewesen wären.

Bulgarien, Tschechien, Dänemark, Deutschland, Griechenland, Kroatien und Polen hatten sich erfolgreich mit dem EU-Gateway verbunden und teilweise begonnen, die ersten EU-Zertifikate

auszustellen. Etwas später – am 10. Juni – war es in Österreich so weit: Die ersten Bescheinigungen für Genesene und Getestete wurden ausgestellt. Für Geimpfte hieß es, sich noch in Geduld zu üben: Es galt, die technischen und inhaltlichen Differenzen über den jeweiligen Impfstatus auszuräumen. Die Ungeduld in der Bevölkerung sorgte für die notwendige Einigung: Seit 20. Juni können die drei Gs – Getestete, Geimpfte und Gesundete – gültige Bestätigungen als PDF über die passwortgeschützte Website des österreichischen Gesundheitsportals anfordern und – wenn keine eigenen Geräte zur Verfügung stehen – bei Ärzten oder in Apotheken ausdrucken lassen.

Am 2. Juli ging schließlich eine iPhone-App online, die das vorher als PDF heruntergeladene Zertifikat darstellen konnte.

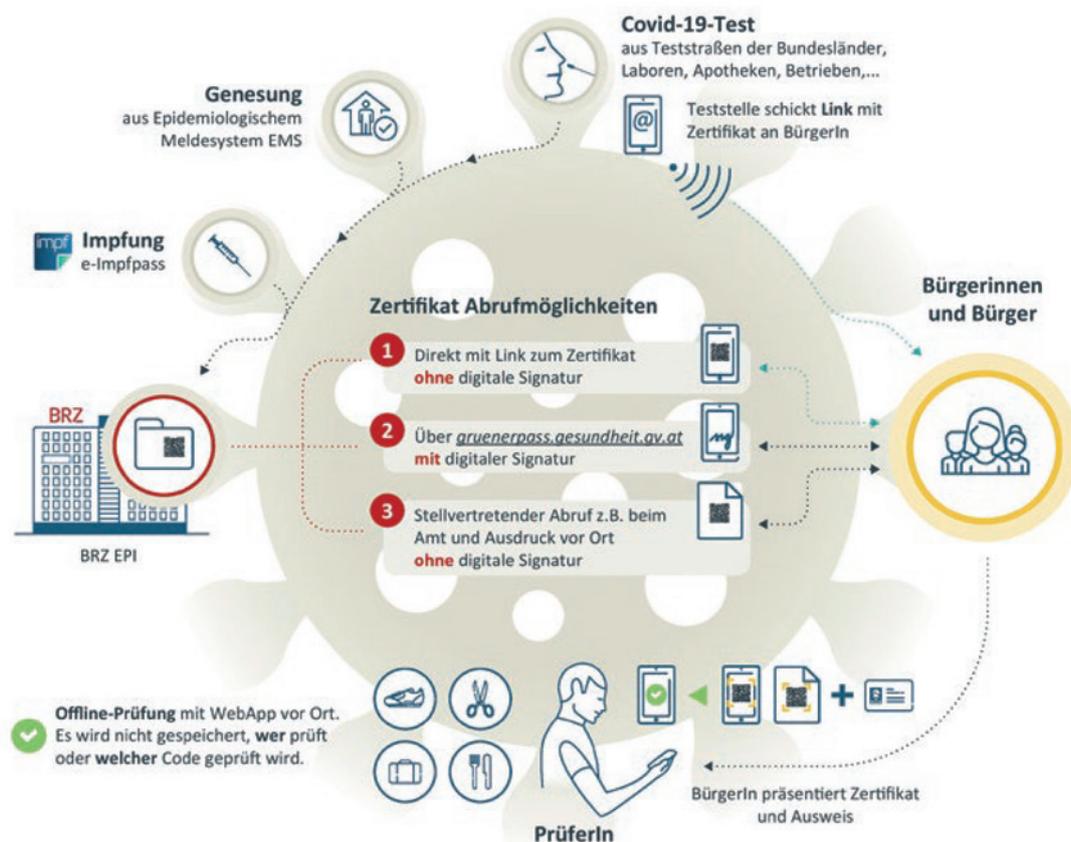


Foto: Bodo Marks / dpa / picturedesk.com

DER WEG ZUM GRÜNEN PASS

Zertifikat mit QR-Code
lt. EU-Standard

APA-Auftragsgrafik
Auftraggeber:
Bundesrechenzentrum



Eine Android-Version war ein paar Tage später verfügbar. Ebenfalls online ging die Prüfanwendung GreenCheck (www.greencheck.gv.at), mit der Gastronomen und andere Kontrollorgane mithilfe eines Smartphones die Gültigkeit des QR-Codes überprüfen können.

Wie wird ein Zertifikat erstellt?

Je nach Datenherkunft werden die vorhandenen Daten, also „Geimpft, Getestet oder Genesen“, aus den vorhandenen Datenquellen abgerufen und ein Zertifikat mit QR Code und mit Sicherheitsschlüssel zur Verifikation erstellt. Da dieser Prozess der Zusammenführung der Ursprungsdaten je nach Datenhaltung in den Ländern sehr unterschiedlich ist, konnte die EU keine Empfehlungen für die Implementierung aussprechen. In Österreich wurde vom Bundesrechenzentrum (BRZ) ein Epidemiologisches Informationssystem (EPI) ins Leben gerufen, das vom Gesundheitsministerium verwaltet wird. Dieses fungiert als Sammelstelle für alle Datenquellen und erzeugt die digitale Signatur am Zertifikat.

Bei einer Anfrage nach einem Impfzertifikat, werden die Daten aus dem eImpfpass geholt. Zertifikate für Genesene werden aus dem epidemiologischen Melderegister des Bundesministeriums geholt (EMS – die ÖKZ berichtete), das für die Erfassung meldepflichtiger Infektionskrankheiten zuständig ist. Um auch negative Testzertifikate erstellen zu können, ist es nach einer Gesetzesänderung möglich, dass auch negative Tests an das EPI-Service als zuständige Gesundheitsbehörde gemeldet werden. Zusätzlich wurde mit einer Novelle (BGBl. II Nr. 323/2020) eine Verpflichtung geschaffen, im Falle der „Pandemie mit COVID-19“ auch alle

negativen und ungültigen Ergebnisse an die Bezirksverwaltungsbehörde als Gesundheitsbehörde zu übermitteln.

Der QR-Code

QR steht für „quick response“. QR-Codes – 1994 von einem japanischen Unternehmen entwickelt – sorgen weltweit für schnellen Check und Re-Check von Informationen. Die darin enthaltenen Daten sind nach dem Prinzip der Datensparsamkeit und nach den EU-Leitlinien der technischen Standards erstellt. Im QR-Code ist nur ein „Minimum Dataset“ aus Personenidentifikation, eine der 3G-Informationen und Metadaten zur Überprüfung der Echtheit hinterlegt. Die Herausforderung: Der EU-konforme QR-Code kann aus Sicherheitsgründen nicht von einem gewöhnlichen QR-Code-Reader gelesen werden. „Daher ist die Überprüfung nur mittels eigens programmierter Anwendung möglich“, betont das Gesundheitsministerium in einer Pressemeldung. In Österreich sorgt die webbasierte Prüf-App „GreenCheck“ für die notwendige Kontrollfunktion bei Grenzübertritt oder im Restaurant. Über einen simplen Scan kann festgestellt werden, ob das Zertifikat echt und ob die 3Gs auch gültig sind.

Private und Public Key

„Es ist ein gängiges und etabliertes asymmetrisches kryptographisches Verfahren und wird auch Public-Key-Verschlüsselung genannt“, erklärt Jakob Stadlhuber von der FH Hagenberg. „Wir benutzen dieses Verfahren im Alltag oft, ohne es zu wissen, z.B. eben digital signierte PDFs oder verschlüsselte Emails. Aber auch Websites sind mit HTTPS, das ebenfalls eine Public-Key-Verschlüsselung ist, sicherer geworden.“ Die Entwicklung die-

ser Verschlüsselungstechnik reicht bis in die 1970er-Jahre zurück. Das Prinzip: ein Schlüsselpaar, das aus einem öffentlichen Schlüssel (public key) und einem geheimen privaten Schlüssel (private key) besteht. Bei der digitalen Signatur werden die Daten mit bestimmten Kennzeichen versehen. „Mit dem öffentlichen Schlüssel kann mit geeigneter Überprüfungssoftware festgestellt werden, ob das Zertifikat echt und die Daten korrekt sind“, so Stadlhuber.

EU-Gateway und Trustliste

Würde nun jedes Land seinen eigenen öffentlichen Schlüssel zur Überprüfung verwalten, wäre das System zwar innerstaatlich ebenfalls funktional, jedoch bei Grenzübertritt nicht mehr abrufbar. Da kommt nun das EU-Gateway und die Trustliste ins Spiel. Diese Liste ist ein Verzeichnis innerhalb des EU-Gateways, das Informationen über von einem Land veröffentlichte öffentliche Schlüssel enthält. Jedes Land, das die technischen Voraussetzungen für die Verbindung zum EU-Gateway und zur Trustliste aufgebaut hat und über entsprechende Prüfsoftware verfügt, kann so alle in der EU erstellten Zertifikate mit den jeweiligen Länder-Public-Key(s) überprüfen. Wieviele Public Keys dort pro Land hinterlegt werden, ist Ländersache, da abhängig von der IT-Infrastruktur.

Wie lange sind die 3G gültig?

Nach erfolgter Echtheitsüberprüfung untersucht „GreenCheck“ die Gültigkeit des Grünen Passes. Ziel des EU-Zertifikats war und ist es, Grenzübertritte zu erleichtern. Die Voraussetzungen

zogenen Daten zu speichern“, heißt es in einem Blogbeitrag der Datenschutzorganisation epicenter.works. Dies sei „das Maximum, das die europäische Gesetzgebung zur Lösung des Problems beitragen könne“. „Mitgliedstaaten, die über die Verordnung hinausgehen und dieses System nutzen, um den Zugang zu Geschäften und Restaurants im Inland zu kontrollieren, müssten nationale Gesetze mit gleichwertigen Sicherheitsvorkehrungen erlassen“, unterstreicht epicenter.works, eine Nachfolgeorganisation des „Arbeitskreises Vorratsdaten Österreich“, der 2014 federführend die Abschaffung der Vorratsdatenspeicherung erwirkte.

Eine Schweizer App als Vorbild

Die österreichische App „Grüner Pass“ nutzt die technische Basis der Open-Source-App des Schweizer Bundesamts für Informatik und Telekommunikation (BIT), mit dem das Bundesrechenzentrum (BRZ) u.a. in der EURITAS vernetzt ist. Verantwortlich für die Entwicklung der österreichischen Lösung ist das Bundesrechenzentrum (BRZ). „Das BIT pflegt bereits seit Jahren einen freundschaftlichen, engen Austausch mit dem österreichischen Bundesrechenzentrum. Daher haben wir eine entsprechende Anfrage sehr gerne positiv beantwortet – auch wenn die Anfrage nur formeller Natur war, denn im Rahmen der Freigabe der Open-Source-Software wäre das nicht notwendig gewesen.“ Der Quellcode ist verfügbar auf Github, einer öffentlich zugänglichen Programmier-Bibliothek. „Es freut uns, dass wir unterstützen konnten und so auch andere von unseren Arbeiten profitieren können“, heißt es aus dem BIT.

Vom Stolpern ins Laufen

Jeder große Software-Roll out kämpft in seinen Anfängen mit Schwierigkeiten. Die Applikation für den österreichischen Impfpass macht dabei keine Ausnahme. „Wir haben festgestellt, dass man jedes beliebige, gut gefälschte Zertifikat einbinden kann, denn in der App selbst wird keine Echtheitsüberprüfung durchgeführt“, so Stadlhuber. Anders sei es in der ursprünglich in der Schweiz entwickelten App. „Mit den notwendigen Anpassungen an österreichische Regelungen scheinen Fehler passiert zu sein,

die wir dem BRZ mitgeteilt hatten. Nachdem uns erklärt wurde, das sei bekannt und nicht wichtig, sind wir an die Medien gegangen.“ Doch auch wenn ein Update kommen sollte: „Es gibt keine Verpflichtung, die App upzudaten. Wer das nicht macht, kann auch in Zukunft x-beliebige gefälschte Zertifikate einbinden“, so Stadlhuber.

Grenzöffner Grüner Pass:

Eine webbasierte Kontroll-App sorgt per Handy-Scan dafür, dass Echtheit und Gültigkeit jederzeit geprüft werden können.

dafür sind aber europaweit unterschiedlich: Die Gültigkeit von Impfung und Tests oder die Bestätigung der Genesung sind bei Grenzübertritt in den jeweiligen Prüfstellen in der länderspezifischen Prüfanwendung abzurufen. Die fehlende EU-Regelung treibt die Kosten für die Umsetzung in den Ländern hoch. Stadlhuber: „Jedes Land muss nun seine jeweils gültigen Bedingungen in die Überprüfungssoftware einarbeiten.“

Keine Überwachung möglich

Die Verifizierung eines Zertifikats erfolgt laut EU-Regel offline und ohne Benachrichtigung der ausstellenden Behörde bzw. weiterer dritter Parteien. „Darüber hinaus wird es den Prüfstellen untersagt sein, die aus dem Zertifikat gewonnenen personenbe-

ber. Unter Experten ist man sich über diesen „Fehler“ uneinig, wie Diskussionen auf Github zeigen. „Eine Signaturüberprüfung würde die App unnötig aufblähen“, heißt es dort in einschlägigen Kommentaren. Auch Thomas Lohninger vom epicenter.works meint dazu, es sei nicht Teil des Sicherheitskonzeptes des Grünen Passes, dass die Zertifikate geprüft werden. „Für die Überprüfung sollte der QR-Code gescannt werden, was in der Praxis meist nicht durchgeführt wird.“ Das hat vermutlich auch das Ministerium bewogen, in einer Kampagne nochmals darauf hinzuweisen, die QR-Codes beim Eintritt in die Gastronomie oder bei anderen Dienstleistern doch zu scannen. Nur so könne man sicher sein, dass das Zertifikat auch echt und mit realen Daten ausgestellt wurde.



Foto: Pixabay