Neues zur Corona-Warn-App und Luca-App

Sylvia Lange

Cryptoparty Tübingen 12.6.2021

Inhalt

Digitaler Impfpass

- QR-Code
- Enthält Daten zur Impfung, z.B. Datum, Impfstoff, Name des Geimpften
- Fälschungssicher durch Signatur des Robert-Koch-Instituts (Daten nach Signatur wieder gelöscht)
- Signatur beruht auf Public-Key-Verfahren
- Sicherheit beruht auf Geheimhaltung des geheimen Schlüssels des RKI
- KEINE zentrale Speicherung von Daten ✔

Digitaler Impfpass

- Staat beauftragt Entwicklung der App CovPass, obwohl es in die CWA integriert ist
- 😠 Chance die CWA weiter zu verbreiten wird unterwandert!
- QR-Code kann beliebig oft eingescannt werden

  `https://www.coronawarn.app/de/faq/#vac_cert_multiple_scan_possible`
- Bei Kontrolle muss also mit Lichtbildausweis abgeglichen werden
- Es gibt EU-Verordnung für Impfzertifikat → Einheitlichkeit in EU

CWA vs. Luca

Vgl.	**CWA**	**Luca**
anonym	✔ `https://media.ccc.de/c/rc3`	✘ #LucaTrack `https://media.ccc.de/v/cccs`
CheckIn-Fkt.	✔	✔
Schnelle autom. Warnung ohne GA	✔	✘ GA lädt Excel-Listen herunter, telefoniert
erfüllt Pflicht der Kontaktdaten-erfassung	✘ zusätzl. Papier!	✔
entlastet GA	✔	✘
gutes Marketing	✘	✔

„Sicherheit“ bei Luca

- Kein Sicherheitskonzept zu Beginn, das alle Funktionalitäten erfasst
- Nachträgliches Anflanschen von Funktionalitäten → Kompromittierung des Sicherheitskonzepts

  https://media.ccc.de/v/cccs-202105-lucatrack-und-andere-gefahren
- #LucaTrack Bewegungsprofile von NutzerInnen der Schlüsselanhänger erhackbar
- Marcus Mengs zeigt, dass Bewegungsprofilen von allen NutzerInnen erhackbar https://youtu.be/UVcsY4xAjUE und

  https://github.com/mame82/misc/blob/master/luca_traceIds.md
- Gesundheitsämter kompromittierbar durch CSV-Injection
  https://logbuch-netzpolitik.de/lnp396-hochsicherheit-kommt-vor-dem-fall

Entlastung der Gesundheitsämter durch Luca?

- NutzerInnen, die die Sicherheitslücken kennen, werden bei LucaApp-Zwang falsche Daten angeben
- Viele unrelevante Daten
  - Z.B. Tischnummer in Restaurant wird nicht erfasst.
  - #LucaFail und Osnabrücker Zoo
- Schlimmstenfalls wird Arbeit der GA durch Ransomware unterbunden (CSV-Injection)

Quellen

Impfpass

- https://www.coronawarn.app/de/faq/#vac_cert_multiple_scan_possible
- https://netzpolitik.org/2021/corona-krise-eu-system-fuer-digitales-impfzertifikat-gestartet/
- https://netzpolitik.org/2021/gruener-pass-eu-einigung-ueber-einheitlichen-nachweis-fuer-impfungen-und-tests/

LucaApp

- https://github.com/mame82/misc/blob/master/luca_traceIds.md
- TheMame82 auf Youtube https://www.youtube.com/user/TheMame82/videos
- https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse
- https://logbuch-netzpolitik.de/lnp396-hochsicherheit-kommt-vor-dem-fall
- https://media.ccc.de/v/cccs-202105-lucatrack-und-andere-gefahren

Download dieser Folien

- https://raw.githubusercontent.com/sylvialange/vortraege/main/cwa2106.pdf