Greenpass: genesi, opportunità e possibili problemi di privacy

Genesi:

- In origine era il “green certificate” o precisamente: EU Digital COVID Certificate.
- Un documento che certificava l’avvenuta immunizzazione.
- Appunto un certificato.

EU Digital COVID Certificate

- Ovvero quello che la stampa (e non solo) definì come green certificate e poi rinominò in green pass.
- Il link: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

Parte tecnica:

- Non informatica: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en
- Parte anche informatica: https://github.com/eu-digital-green-certificates

Nomen est omen

- https://en.wikipedia.org/wiki/EU_Digital_COVID_Certificate
- Ci mostra come in UE solo due paesi non si riferiscano a questo documento come un certificato.

Tecnicalità: ovvero facciamone uno

- dati testuali messi in formato json
- codificati cbor (https://cbor.io/spec.html)
- certificati cose (opzionali ?)
- compressi con zlib
- codificati base 45 (https://www.ietf.org/rfc/rfc9285.html)
- trasformati in qrcode

Crittografato o firmato ?

- Abbiamo visto un certificato nella generazione
- Ma nessuna operazione di cifratura dei dati.

La percezione

- Non provo a immaginare come possa essere stato percepito.
- Se su un motore di ricerca cerco “image green pass” ne saltano fuori ancora a bizzeffe. E alcuni contengono dati veri.
- Quindi...

Ma che cosa c’è dentro?

- Link: https://ec.europa.eu/commission/presscorner/api/files/attachment/868508/Digital%20Green%20Certificate_en.pdf.pdf
- Generalità (nome,cognome, data nascita)
- Dati dei vaccini
- “certificazione” o meglio firma di dati e generalità.

A ME PARE BEN FATTO.
ma...

- SE ABBIAMO UNA SERIE DI APP UFFICIALI, COME MAI I MOTORI DI RICERCA NE RIPORTANO MOLTE DI PIÙ?
- “app per verificare il green pass” … una bella lista.

Da cittadino

Sarei stato felice di trovare una lista ufficiale di app (lista magari firmata digitalmente) … in realtà almeno in Italia questa lista era almeno parzialmente disponibile.

Ora passiamo alla privacy

- Se il green/ue covid 19 certificate è un documento di che ci preoccupiamo ?
- Tecnicalmente di nulla.
- Di solito in ue un cittadino non mostra una id card per entrare in un esercizio commerciale.
- Di solito un agente di ps ha il potere di richiedere un id card.

Id card

- Generalità
- Indirizzo
- Foto
- Altro

Mostrare il certificate

- Al lavoro
- In certi esercizi commerciali
- In certe situazioni sui mezzi di trasporto
- Ricordo che deve esser letto tramite una app.
- Che potrebbe leggere anche la foto di un certificate.

Se la app fosse ‘rogue’ ?

- Immaginiamo che il ns salumiere non sia informaticamente capace e abbia scaricato la prima app che trova. Dandogli accesso a tutte le risorse del device.
- È evidente che pochi secondi dopo la ripresa la foto del ns. Certificato con allegati data, ora e posizione della ripresa potrebbe essere in mano a terzi, quarti e quinti.

Se la app non fosse rogue

- Mi domando solo perchè dover dare le ns generalità per entrare in un esercizio commerciale.

Ripasso di informatica

- PKI (vedere wikipedia)
- Chiave pubblica per crittografare e verificare firme
- Chiave privata per leggere e firmare
- Mi domando se questo approccio potesse consentire di far leggere le generalità a una platea più ridotta.
- Nota: le chiavi sono revocabili. (ovviamente si revocano pubblica e privata insieme)

Un appunto

- Quando ero militare di leva avevo un certificato (ovvero una id card ad hoc)
- Per allontanarmi avevo un pass (licenza o permesso) firmato singolarmente, E REVOCABILE SINGOLARMENTE.
- I pass di ogni cittadino son firmati con la stessa chiave ? E se fosse necessario revocarla ? E perche’ non usare la chiave di firma come possibile meccanismo di revoca del green-pass ?

Peggio.

- Se il certificate fosse esibito in un passaggio obbligato con telecamere:
- Avremmo un qrcode con generalità e altro associato a un volto. Su uno streaming video. O su un filmato video processabile a posteriori.

Conclusioni

- Buona (se non ottima)l’idea originale
- A me non piacciono gli adattamenti fatti di corsa.
- Ma non era il caso di affinarlo/rivederlo nel periodo del calo del covid ?

Bibliografia e altro

- La trovate su questo mio articolo su medium: https://medium.com/@GiovambattistaVieri/green-pass-genesi-descrizione-rischio-privacy-caf55ca415e2