Many vaccine passports have security flaws – here's how to make them safer

December 2 2021, by Matthew Comb

EU DIGITAL COVID CERTIFICATE

Certificat COVID numérique UE

Nom(s) de famille et prénom(s)

Date de naissance

Par souci de confidentialité de vos données de santé, nous vous recommandons de ne présenter que le seul QR code de preuve en pliant cette attestation.

CERTIFICAT DE VACCINATION

VACCINATION CERTIFICATE

Maladie ou agent ciblé

COVID-19

SARS-CoV-2 mRNA vaccine

COVID-19 Vaccine

The European Union’s paper digital COVID vaccination certificate. Credit: Nataliya Vaitkevich / Pexels, CC BY-SA 4.0

COVID vaccination passports have proved extremely divisive during the coronavirus pandemic, due to issues relating to civil liberties or their potential to discriminate against the more vaccine-hesitant groups within society.

But as many governments around the world push forward with their implementation in an attempt to curb the spread of COVID-19, the security of our data has become a major cause for concern.

Many COVID passes work by producing a QR code or 2D barcode for each user that can be scanned as proof of vaccination. The barcodes used in some of these passports are not that secure because they are not generated with encrypted data. However, they could be made secure if national governments, international organizations and global tech companies work together to make the most of the exciting possibilities this technology presents.

Embedded within the barcode is a verifiable credential which proves vaccination status, and a number of personal details depending on the barcode's format. These are likely to include the user's full name and date of birth. To ensure authenticity and prevent fraud, the barcode also contains a unique digital signature which is generated based on its contents.

A number of vaccine passport programs have already come under fire for a lack of security, including those in New York and Quebec, which have been criticized for allowing people to obtain other people's barcodes by entering their details. To mitigate some concerns, the EU has established its own open standard for vaccine passports—the EU Digital COVID Certificate (EUDCC). It has been adopted by the 27 EU states and 18 other countries.

However, this hasn't addressed the fact that the contents of the certificate are not encrypted, so anyone with access to the barcode (and the necessary skills) can decode it and retrieve the personal information contained within. This applies to COVID passports in the EU, Canada, UK, California and New Zealand. There are only slight differences in how the data is encoded—but in all these cases it is not encrypted.

To encrypt the COVID certificate's contents, there must be what's known as an encryption key associated with the certificate and the owner's digital identity. Currently, most COVID barcodes do not encrypt their contents due to the lack of digital identity infrastructure as well as the requirement to operate offline. This puts a user's personal information at risk.

There is also another problem with the current COVID certificates. They are signed by the issuer (for example the NHS) using a region- or country-specific key, or code. If someone should attain the key, they could create a false certificate. The authorities would have to respond to the fraudulent COVID passports by revoking the compromised key, which would mean that all preexisting COVID certificates would become invalid.

Why use barcodes

Up until recently, digital identity management for a computer user has consisted of a simple username and password credential. It's a system that has worked, in the main, for more than 60 years. But the current explosion in online content, cybersecurity challenges and privacy concerns are driving the need for a user to have more control of their own digital identity.

Our identity is essentially made up of millions of small truths about ourselves. Verifiable credentials in a barcode could enable us to share just a single truth rather than our whole identity, to suit the particular situation if the data is adequately encrypted.

To its credit, the COVID certificate does just that. It is a simple proof of an individual truth, in theory enabling you to demonstrate you have been vaccinated without giving any other details away. The fact that the certificate is not entirely secure indicates the absence of a more robust digital identity infrastructure.

Potential risks

The absence of this piece of the digital identity puzzle must be rectified at some point in the future. Until then, the current COVID passports could be open to abuse.

The personal information involved in the vaccination certificate is not particularly sensitive at face value, because it is often easily found in other places such as a driver's license, school records or passport. But in the future, when this technology is more widespread, we will probably be using similar certificates which contain verifiable credentials in pretty much every aspect of our lives—such as to access a building or services, or to approve purchases (both instore and online).

This has positive and negative consequences for users. On the plus side, we will only need to provide the minimum amount of personal information in a very user friendly way. For example we will be able to sign up to websites without even entering a name.

But if we present non-secure barcodes in many places, each containing small single truths about ourselves, then eventually these can potentially be combined together and the identity of the individual to whom they relate may be compromised.

This is how many cybercriminals currently work, combining data from different sources of information, which allow a person's digital identity to be constructed over time. This could lead to an increased risk of identity theft, and potentially be used as a basis for a variety of cybercrimes.

However for all these concerns about digital passports, we should remember that if it can be made secure on an international scale, this kind of digital identity technology has significant potential upside for citizens—and not just for vaccination certificates.

Provided by The Conversation

Citation: Many vaccine passports have security flaws – here's how to make them safer (2021, December 2) retrieved 3 May 2024 from https://techxplore.com/news/2021-12-vaccine-passports-flaws-safer.html