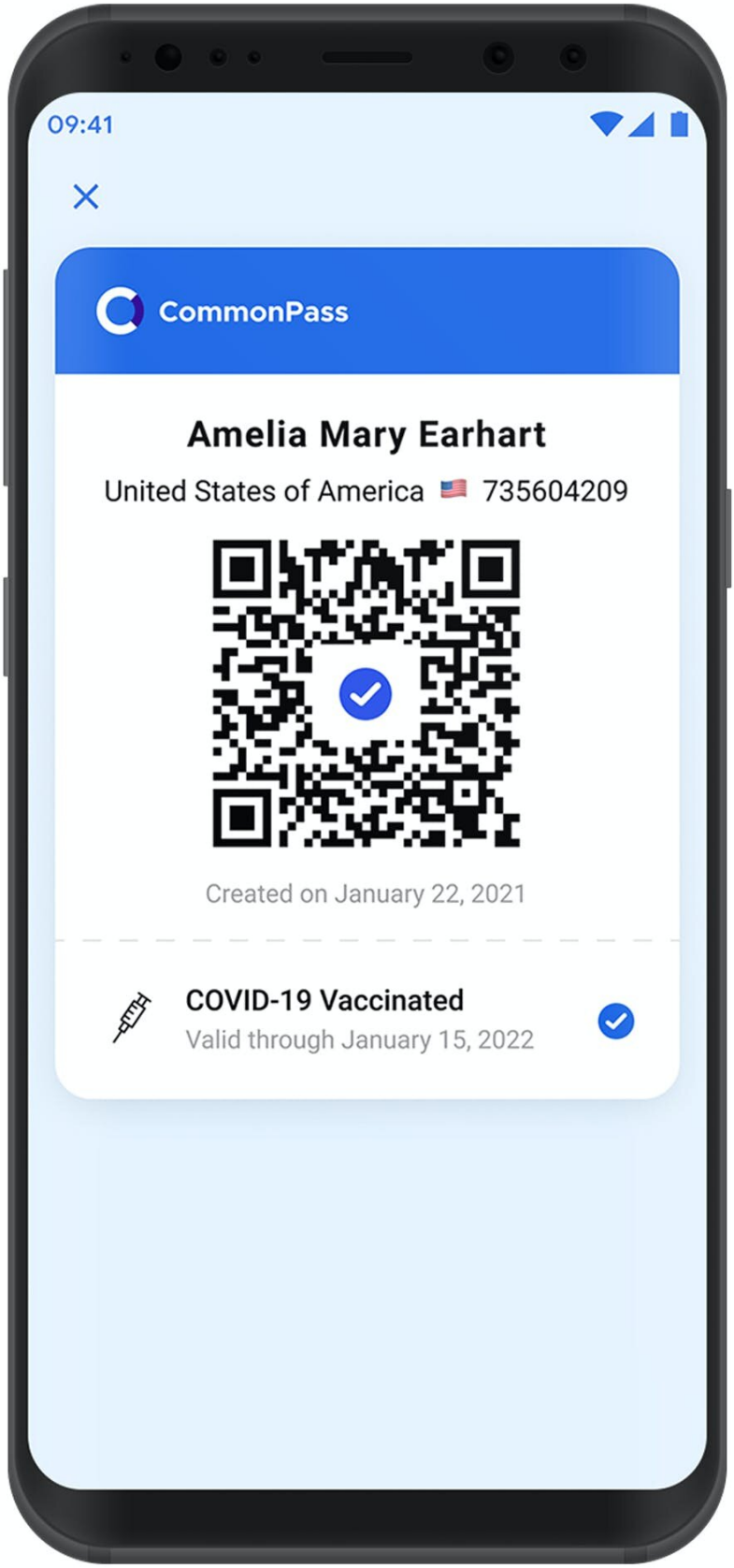
Vaccination passport apps could help society reopen—if they are secure, private and trusted

March 24 2021, by Laurin Weissinger


09:41
CommonPass
Amelia Mary Earhart
United States of America 735604209
Created on January 22, 2021
COVID-19 Vaccinated
Valid through January 15, 2022

The CommonPass vaccination passport app under development will include a scannable QR code. Credit: The Commons Project

You might soon have an additional app on your phone: a digital vaccination passport that allows people who have been vaccinated against COVID-19 to travel, enter business establishments and attend events. Not having the app could deny people access.

The theory goes that vaccination passport apps can help society reopen despite still-high infection risks, including from more infectious and deadly strains of the coronavirus, because they allow protected people to resume normal activities while keeping people vulnerable to infection out of high-risk environments.

Vaccination passports, however, can have unintended, negative consequences. And beyond ethical issues, building vaccination passport apps is far from straightforward. As a cybersecurity researcher, I see several challenges, including how best to ensure security and privacy, and to get people to trust the verification systems.

Fuzzy on the details

Like nationality, vaccine status is not visible to others. Passports and government IDs have long been used to prove identity, citizenship and birth dates, and the World Health Organization's carte jaune, or yellow card, has served this role to prove vaccinations for international travel. These rely on governments as trusted third parties.

A lot is still up in the air when it comes to vaccination passport apps.

This month, the EU announced its vaccination passport plans. Judging from initial documentation, the system is meant to be decentralized, relying on health authorities to issue certificates that store only necessary information. Notably, it allows for paper and app-based certificates.

In either case, verification would be based on digital signatures, and all health data would remain with the issuing authority or member state. However, while the concept document is promising, what gets rolled out and whether anyone breaks the rules by storing or tracking data remain to be seen.

The CommonPass app being built by an international nonprofit organization appears to be the most developed vaccination passport app. It currently documents test results. However, while its makers claim that records will be stored only locally on users' devices, the app is closed source, and the only documentation is a superficial FAQ.

Israel has rolled out its "green pass" app, which verifies that a person has been vaccinated or has recovered from COVID-19, but the system has raised privacy and security concerns. Several other countries have also launched vaccination passport apps for internal use, including China and Saudi Arabia.

How an ideal app works

App designers are faced with a difficult task: They need to create a system that is secure, privacy preserving, easy to use, compatible with as many devices as possible, highly scalable and able to operate across borders. The system will have to track institutions providing the vaccination records and the chains of trust – the digital handshakes that prove each part of the system is what it claims to be—linking those records to the app.

It's preferable for users and the organizations that have to verify records to deal with fewer apps, which means that each app would have many users. Security vulnerabilities in these key applications would thus have widespread impact. The large number of users also increases the incentive for attackers who would benefit from abusing a trusted, health-related, government-backed app.

Therefore, it's important for vaccine passport apps to maximize privacy by collecting and retaining only needed data, similar to what the EU is proposing. This would include identity, type of vaccine and date of vaccination. Not only does this reduce internal misuse of data, but it also reduces risk in case of breaches.

A matter of trust

Who could be trusted to build and maintain this app? Some people worry about government and private-sector surveillance. Indeed, there is reason for concern: Vaccine passport apps might become required or quasi required, link identity to personal health information, and, depending on implementation, could be used to establish detailed personal profiles, including movement patterns.

Private companies exist to make money and would thus have incentive to monetize passport apps, usually through data mining or sale. Government-backed apps might raise concerns about surveillance and citizens' rights.

Therefore, to build trust, it's important to clarify concepts and designs beforehand, documenting what data will be collected and processed, and how. As practiced by the German contact-tracing app, any passport application's back end and front end need to be fully open source and penetration-tested by security experts to build public trust.

There are many challenges, but the technology to build a trusted, secure

and privacy-respecting vaccination passport app is available. Technology, however, is just part of the picture. It's also important to consider a vaccine passport system in the context of COVID-19 and society as a whole.

Thorny issues

Governments will need to consider in more depth the consequences of requiring a vaccination passport app to access restaurants or gyms in places where vaccine doses are not easily and cheaply available to everyone, which is most of the world.

Passport apps create inequality between vaccinated and unvaccinated individuals. Those selected by governments to be vaccinated first would enjoy considerable privileges. In the U.S., these have tended to be disproportionately older, wealthier and white. Younger people and communities of color—both groups have been hit particularly hard by the effects of the pandemic—are more likely to be left out. Thus, these apps might increase social tensions.

The perceived safety gains may also have various unintended consequences. For example, premature opening could increase transmission from vaccinated but infected individuals or through increased patronage requiring more unvaccinated staff on site.

Last but not least, requiring passporting apps may encourage the unvaccinated to misrepresent their status, whether to make ends meet, to hold on to a job, or simply to avoid being left out, further increasing infection risks.

Therefore, in places like the U.S., where all willing individuals will soon be vaccinated, it would make sense to wait to roll out vaccine passports until everyone has had the chance to be vaccinated. Second, there need

to be clear, open and public discussions about what these apps are supposed to provide and how they should work.

A more analog approach that does not need a smartphone or app to work would be more accessible, cheaper and more privacy preserving. The EU's approach, as it currently stands, allows the use of paper records, verifiable by QR code. A similar system is also being developed by an MIT nonprofit. These semi-digital approaches could be hacked, but so can apps

Provided by The Conversation