Med

CellPress

Correspondence

The privacy challenge in the race for digital vaccination certificates

Alexander Rieger,[1,*] Tamara Roth,[1] Johannes Sedlmeir,[2,3] and Gilbert Fridgen[1]

In the wake of COVID vaccination campaigns, companies and governments make haste in launching digital vaccination certificates. These digital certificates often differ in design and structure but are typically stored in mobile apps. However, using these apps comes with two significant challenges: interoperability and privacy. Interoperability is important for broad and easy usability of digital vaccination certificates. Yet, it is difficult to establish because poor coordination and a rat race for innovation have complicated the adoption of common technical standards.[1] Data privacy is important for user trust and legal compliance. It is, in fact, an even bigger challenge than interoperability.

Privacy concerns are driving decentralization

Information on a person's vaccination status is highly sensitive, and storing such information involves significant privacy requirements. For instance, it is cumbersome to reconcile mobile apps that store vaccination information in a central database with data privacy regulations. In particular, a central database makes it difficult for users to prevent unintended use of their vaccination information or linking to related personal data.[2] Moreover, such "honey pots" of sensitive personal data are widely discouraged as they present prime targets for cyberattacks.

Many initiatives have, therefore, opted to issue digital vaccination certificates and store them in special mobile apps of individual users, so-called digital wallets. In this "decentralized" approach, only users have access to their digital vaccination certificates and can decide on a case-by-case basis which particular information they want to disclose. The authenticity of their certificates can be checked via digital signatures—a unique, mathematical code—without having to contact the physician or vaccination center that issued the certificate. This decentralized approach is effective in preventing unintended links between vaccination status and other personal data—even if stored in the same digital wallet app—which is especially important in countries, like the United States, where such links are all too common.[3]

Organizations and initiatives that follow the decentralized approach, such as IATA,[4] the COVID-19 Credential Initiative,[5] and the Vaccination Credential Initiative[6] predominantly use the W3C Verifiable Credentials (VC) standard. This VC standard offers a flexible, privacy-oriented alternative to the digital certificates typically used to identify internet servers. The VC standard also offers essential guidelines on the design and structure of digital certificates, which limits the risk of major "format wars"[1].

Why blockchain should be used with care

A blockchain is a decentralized database that securely stores data in multiple places at the same time. Once stored, the data on a blockchain cannot be tampered with or erased without such a change being noticed by other actors in the blockchain network.[7] Some companies and governments try to use these security features for digital vaccination certificates.

However, it can be very difficult to ensure compliance with data privacy regulation when using a blockchain. The GDPR, among others, requires that personal data can be erased or at least fully anonymized, which can pose significant challenges for the use of blockchain.[8] Privacy rules are particularly strict when it comes to medical data. Thus, storing vaccination records on a blockchain,[9] even in encrypted form, is not recommended.

Moreover, blockchain's capability to prevent data from being tampered with or erased does not automatically protect against fraudulent certificates. Instead, legitimate vaccination certificates require a trusted and authorized issuer who guarantees their authenticity. They further require a strong bond between the vaccination certificate and the digital wallet app of the vaccinated person. Such a bond also obviates the presentation of additional personal information, for instance an ID card, to prove the validity of a vaccination certificate.

For all of the above reasons, many initiatives focus on digital wallet apps and use blockchain only to store information on authorized issuers of vaccination certificates. This information is essential to establish that a certificate was issued by a registered physician or vaccination center. When used in such a way, blockchain can indeed be a promising technological alternative or supplement, albeit one that still poses certain additional challenges,

[1]Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg City, Luxembourg

[2]Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Bayreuth, Germany

[3]FIM Research Center, University of Bayreuth, Bayreuth, Germany

*Correspondence: alexander.rieger@uni.lu

https://doi.org/10.1016/j.medj.2021.04.018

such as limited experience with deployment and performance at scale.

The caveat of limited technical maturity and capabilities

While the decentralized approach is gaining momentum, the required software components are not yet fully mature and interoperable. For instance, the first marketable version of the Hyperledger Aries software, which is commonly used to issue and exchange digital certificates, was only released in February 2021. Some digital wallets have already been successfully tested for interoperability, but the rapid pace of development frequently introduces new incompatibilities.

The lack of technical capabilities is another substantial challenge. Few physicians or vaccination centers will manage to be quick enough in establishing the required capacities to issue digital vaccination certificates. Similar concerns apply to those who need to verify the certificates, such as immigration authorities. Moreover, many elderly and technologically challenged people may be unable to use digital wallet apps. Some may also lack the resources to afford smartphones, while others may instead refrain from using them for personal reasons. As a result, companies and governments will have to offer a choice between digital and paper-based vaccination certificates. This choice is also important for another reason: to avoid further ethical and equality concerns. Such concerns have already been raised, for instance, with regard to limited access to public buildings and restaurants as well as travel bans for people without vaccination certificates.[10]

Concluding remarks

Since many initiatives for vaccination certificates build on the same privacy-oriented standards, they help to ensure privacy and further interoperability. Of course, their limited technical maturity carries a certain risk, but the associated challenges can be overcome and addressed in due course. Thus, we recommend a level-headed approach that does not sacrifice inclusion, privacy, security, and, ultimately, trust in digital vaccination certificates for the sake of a rushed implementation.

Instead, we propose a gradual transition from paper-based to digital vaccination certificates that gives the initiatives time to address the maturity challenges and converge their efforts accordingly. In the short term, physicians and vaccination centers could begin by issuing paper-based vaccination certificates with QR codes and preliminary digital equivalents. Once the identified challenges have been addressed, these QR codes could be used to re-issue privacy-oriented vaccination certificates bound to interoperable digital wallet apps. For those who cannot or do not wish to use digital wallet apps, paper-based certificates should remain available. In parallel, governments are called upon address the relevant ethical concerns[1,10] and establish the required regulatory frameworks. After all, digital vaccination certificates depend on a solid legal basis for effective use.

DECLARATION OF INTERESTS

The authors declare no competing interests.

1. Marhold, K., and Fell, J. (2021). Electronic vaccination certificates: avoiding a repeat of the contact-tracing 'format wars'. Nat. Med. Published online March 4, 2021. https://doi.org/10.1038/s41591-021-01286-w.

2. Politou, E., Alepis, E., and Patsakis, C. (2018). Forgetting personal data and revolking consent under the GDPR: Challenges and proposed solutions. J Cybersecurity. *4*, tyy001.

3. Blumenthal, D. (2019). Why Google's Move into Patient Information Is a Big Deal. Havard Business Review, November 26, 2019. https://hbr.org/2019/11/why-googles-move-into-patient-information-is-a-big-deal.

4. International Air Transport Association (2021). https://www.iata.org/en/programs/passenger/travel-pass/.

5. Covid-19 Credentials Initiative (2021). https://www.covidcreds.org.

6. Vaccination Credential Initiative (2021). https://vaccinationcertificate.org/.

7. Tapscott, D., and Tapscott, A. (2020). What Blockchain Could Mean For Your Health Data. Havard Business Review, June 12, 2020. https://hbr.org/2020/06/what-blockchain-could-mean-for-your-health-data.

8. Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., and Fridgen, G. (2019). Building a Blockchain Application that Complies with the EU General Data Protection Regulation. MIS Q. Exec. *18*, 263–279.

9. Cheung, J.C.-S. (2021). Vaccination: keep records secure with blockchain. Nature *590*, 389.

10. Baylis, F., and Kofler, N. (2021). Vaccination certificates could entrench inequality. Nature *591*, 529.