Cybersecurity – Identity Management
Prof. Dr. Anja Lehmann
Master Project | Winter Term 21/22

Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Privacy-Preserving & Copy-Resistant Immunity Certificates

In this project, we want to investigate how to use modern cryptography to realize immunity certificates that provide better privacy and are harder to copy than the current ones. Before we sketch how such certificates can be built and what the goal of the project is, we explain the currently deployed solution and its limitations in terms of security and privacy.

Immunity Certificates – Status Quo

Recently, digital immunity certificates have been rolled out as a digital version of the paper-based certificates of vaccination [1]. Their main purpose is to be a convenient solution for verifying that citizens have a valid Covid-19 vaccination, when this is made an access requirement, e.g., in public spaces or when crossing borders.

These certificates are issued by a trusted entity (in Germany the RKI) and contain the user's personal information such as name and date of birth, and the date and type of vaccination. This information is signed with a signature scheme under the secret key held by the trusted entity. Anyone receiving the user's data and signature – presented in form of a QR-Code – can verify its validity against the public key of the issuer. Security follows from unforgeability of the signature scheme, which guarantees that an adversary cannot create valid certificates for data that has not been signed by the issuer.

However, there are some security and privacy risks in the current solution: The QR-Code presented by the user contains her full information and certificate, i.e., a malicious verifier can store the certificate and create perfect copies that are valid under the issuer's key. This is obviously inherent in standard signatures and is not considered a real issue, as one is supposed to always show a valid ID-card along with the immunity certificate and the verifier must check that both belong to the right person. This renders illegitimate copies useless. Enabling this additional check is also the reason why the presentation of the digital immunity certificate must disclose the users' full personal data. The latter is obviously not ideal from a privacy perspective, as citizens are now required to present their personal data in machine-readable form on many occasions, and with the certificate serving as a unique fingerprint.

Security & Privacy Challenges in Reality ...

It is likely that the additional cross-verification with a valid ID card, that is crucial for security, will not be enforced by many venues, such as restaurants, cinemas, etc. That is, the verifier might simply check the digital certificate but does not verify that it is the real owner who shows it. That makes the cloning of certificates now a critical issue. It also makes the disclosure of personal information an unnecessary risk: if the user's identity isn't verified, then revealing her private information in every QR-Code serves no longer any purpose and is just a privacy risk.

Additional Security & Privacy Requirements

If one believes that the cross-verification of the immunity certificate with a valid ID card is **not** always enforced, this requires additional security and privacy properties from the immunity certificate:

Copy-Resistance: Presentation of the certificate towards a (malicious) verifier should not enable the verifier to obtain a copy of the user's certificate.

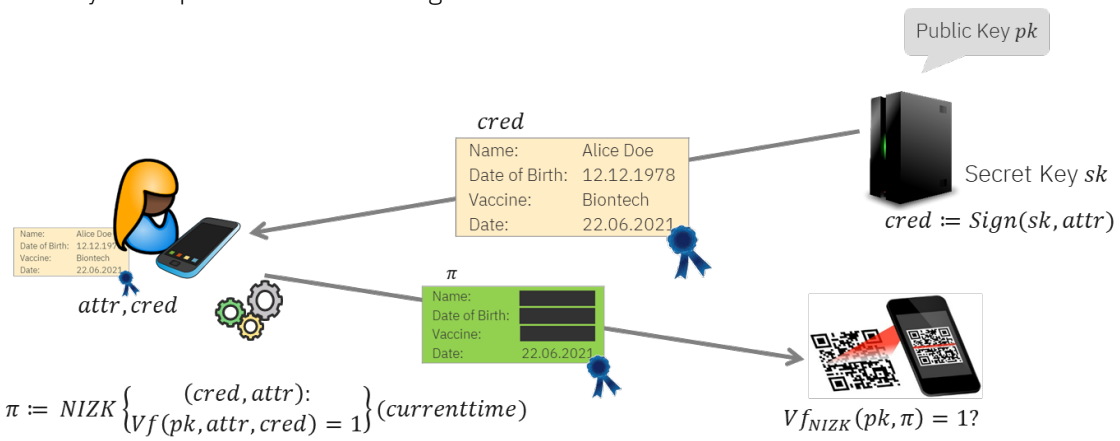
Privacy: In addition to the normal mode where the user is presenting her full details, there must be a privacy mode in which the presentation merely proves ownership of a valid certificate, but does not reveal the user's personal data. Further, to prevent tracking, every new presentation must be unlinkable to the previous ones.

Obviously, these requirements come on top of the standard unforgeability, i.e., an adversary must not be able to create valid presentations or certificates that verify under the issuer's key but have not been obtained legitimately.

Outline of Privacy-Preserving & Copy-Resistant Immunity Certificates

In this master project, we want to realize immunity certificates with the aforementioned properties by using anonymous credentials [2,3]. The high-level idea we want to pursue is as follows.

Roughly, the immunity certificate will be realized by a so-called anonymous credential. This can be seen as a more advanced signature of the trusted issuer on the users' attributes, which allows for more flexibility in the presentation of the signature.



When asked to prove her vaccination status, the user – instead of revealing the original credential in the QR-Code – now derives a short-lived presentation token from the credential (valid for a few minutes, or hours) that will be shown as QR-Code to the verifier. The token can still be verified against the issuer's public key but copying it is rather useless, as it can only be used for a short time, and cannot be used to derive other tokens for a different time.

In the privacy mode, the presentation token will not contain the user's personal data but only be a proof of a valid credential. As these presentation tokens are non-interactive zero-knowledge proofs of the original credential, they do not reveal any information of the user's identity and are fully unlinkable.

A more detailed description of this approach can be found in the lecture notes of the current "Advanced Cryptography" course [4].

Goal of the Master Project

The goal of this master project is to work out a full cryptographic specification and prototypical realization of such a privacy-friendly and copy-resistant immunity certificate. The exact scope will depend on the interests and size of the group, and contain a subset of the following:

- Define the desired security and privacy properties through a formal model
- Investigate further desirable properties, e.g., privacy-friendly issuance or misuse detection
- Propose a (generic) construction that provably satisfies these requirements
- Select (& possibly) adapt concrete instantiations of the required building blocks (i.e., the exact signature scheme, e.g., [5] and zero-knowledge proofs)
- Implement of a simple prototype

Requirements

We expect a solid understanding and interest in cryptography and provably-secure constructions. You should have attended & enjoyed the "Introduction to Cryptography", and ideally also the "Advanced Cryptography" course, but we will also give enough time to read up on the cryptographic building blocks in the beginning, if you haven't attended the latter. In any case, you should bring the willingness and curiosity to delve into the (mathematical) details of the constructions of anonymous credentials and zero-knowledge proofs.

Contact

Prof. Anja Lehmann: anja.lehmann@hpi.de

In the "Advanced Cryptography" lecture on July 6th '21, 13:30-15:00 we will discuss the idea of the cryptographic construction in a bit more detail. Feel free to join:

https://zoom.us/j/99355141240?pwd=TkFFV0VGYXMrdVNvMFBST1Rjb0Z6QT09

References

[1] https://digitaler-impfnachweis-app.de/

[2] Design and Implementation of the idemix Anonymous Credential System. Jan Camenisch, Els Van Herreweghen. CCS 2002.

[3] Formal Treatment of Privacy-Enhancing Credential Systems. Jan Camenisch, Stephan Krenn, Anja Lehmann,Gert Læssøe Mikkelsen, Gregory Neven, Michael Østergaard Pedersen. https://eprint.iacr.org/2014/708.pdf (No need to understand it all. We will not need such a complex security model or construction, just a small subset.)

[4] Advanced Cryptography Lectures 7-9 (ZKP & Anonymous Credentials), 10: Case Study: Immunity Certificates. See https://moodle.hpi.de/course/view.php?id=156

[5] Reassessing Security of Randomizable Signatures. David Pointcheval and Olivier Sanders. https://eprint.iacr.org/2017/1197.pdf