Workshop Proposal: Cloud-Based Sharing of eHealth Data

CREDENTIAL – Secure Cloud Identity Wallet

Stephan Krenn[1] and Simone Fischer-Hübner[2] *

[1] AIT Austrian Institute of Technology GmbH, Austria
stephan.krenn@ait.ac.at
[2] Karlstad University, Sweden
simone.fischer-huebner@kau.se

1 Background

1.1 Data Sharing in the Cloud

Data sharing—and in particular sharing identity information—plays a vital role in many online systems, especially in high-security domains such as eGovernment, eBusiness, or eHealth. The EU H2020 project CREDENTIAL is therefore aiming at the development of a secure and privacy-preserving data sharing and identity management platform which gives stronger security guarantees than existing solutions on the market.

This will be achieved by using proxy re-encryption [1], a primitive that allows the cloud provider to convert a ciphertext encrypted under a key pk_A of party A into a ciphertext under pk_B of party B without the provider learning anything about the plaintext contained in the ciphertext. By doing so, the cloud provider no longer needs to be assumed to be trusted as it never learns the users' personal data.

To furthermore guarantee authenticity of the shared data, redactable signature schemes [2] will be deployed. Such schemes allow one to "black out" (redact) predefined parts of a signed message without affecting the validity of the signature. In particular in the case of identity management, the cloud provider can now redact unrequired parts of an electronic identity (eID) before forwarding it to a service provider requesting authentication of a user, while still guaranteeing, e.g., that the eID was issued by some public agency.

1.2 Secure Platform for Sharing eHealth Data

The results of CREDENTIAL will be showcased and evaluated through different pilots. One of those is concerned with a data sharing platform between patients, doctors, and further parties, in particular in the context of Type 2 Diabetes. Namely, the developed components will allow patients to record their health

* This work is being performed within the H2020 EU project CREDENTIAL.

data (blood sugar level, weight, blood pressure, etc.) using external mobile devices. The data measured on these devices will be collected by a CREDENTIAL eHealth mobile app, which remotely stores this data in the CREDENTIAL wallet. The user can then define who is allowed to access which parts of this medical data, to share specific parts of the measurements, e.g., with the family doctor, diabetologist, nutritionist, or personal trainer. Based on the data they see, they can then provide recommendations back to the user.

Because of the confidentiality of medical data, it is of prime importance that only legitimate users are able to access a user's data, therefore requiring strong means of (2-factor) authentication to the services.

At the same time, the trust assumptions that have to be made need to be minimized. For instance, a user's privacy should not rely, e.g., on the honest behavior of the service provider, or on the correct behavior of other users. However, such strong guarantees are often hard to realize, and the computational overhead would render the entire application inpracticable. In particular, the usage of constraint devices often puts hard limits on the (computational) complexity of the deployed primitives. Therefore, a balancing act between practicability and a strong adversary models becomes necessary.

Furthermore, also HCI (Human Computer Interaction) and trust related challenges need to be addressed by CREDENTIAL. First of all, users should be enabled to put the right scope of (dis-)trust into the CREDENTIAL system. Moreover, a usable design of the privacy-enhancing identity management functions will play a key role for a successful adoption and for enabling users to achieve the optimal levels of both privacy and security. In particular, functions for allowing users to define access rights, doing redactions and sharing different sub sets of data items ("partial identities") with different service providers need to be intuitive and easy to use (e.g., by providing suitable defaults that can easily be adapted) for allowing and motivating users to make well informed and reasonable choices. While too generous settings may contradict the privacy principle of data minimisation, too strictly defined settings may, on the other hand, impact the availability of services for the user or may, in case of the eHealth use case, even impact the patient's safety.

2 Workshop Plan

The objective of this workshop is not only the dissemination of the technology and use cases of CREDENTIAL, but also involving all participants in a critical discussion of technical and end user-related privacy and usability challenges for identifying of and creating awareness about obstacles, tradeoffs, requirements and possible solutions. The workshop is planned to consist of two parts: In the first part of the workshop, we will provide some introductory presentations on the cryptographic background and the project's eHealth use case. This will be followed by an open discussion of the general concept of the CREDENTIAL wallet, the intended eHealth use case as well as technical, application- and end user-related challenges and requirements.

More precisely, the following **two hour** workshop is proposed:

- 3 presentations à $20 - 25$ minutes (speakers are tentative):
  - Cryptographic background (introduction to redactable signature schemes and proxy re-encryption),
    Stephan Krenn (AIT, Austria)
  - Architecture of the CREDENTIAL wallet,
    N.N.
  - eHealth use-case plans and demonstration,
    Anna Schmaus-Klughammer (Klughammer GmbH, Germany)
- Open discussion lead by researchers from Karlstad University (depending on the number of participants, the discussion will either take place in the forum or in parallel groups).
- Summing up the main conclusions and how they may impact the project.

References

1. Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In: In EUROCRYPT, Springer-Verlag (1998) 127–144
2. Johnson, R., Molnar, D., Song, D., Wagner, D.: Homomorphic Signature Schemes. In: Topics in Cryptology - CT-RSA 2002. Volume 28913. (2002) 244–262