Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis M.Sc.

An fault-proof and tamper-resistant certificate issuance process

Motivation

Various scenarios exist where a certificate authority (CA) issues a certificate to the owner of a public keys to bind her identity to this key. The web PKI, which is used to authenticate domain names in the WWW, is maybe the most prominent example. Further examples include identity management systems (IDMS) for organizations that issue S/MIME certificates for secure emails to employees.
The issuance process of certificates always follow a similar pattern (simplified): The future certificate holder must prove that she possesses the identity stated in the certificate to a *registration authority (RA)* of the CA using a personal identity card. If the identity could be confirmed, the RA authorizes the certificate issuance.
This process is error prone do to organizational and technical issues: **1)** the RA might be careless and issue a valid certificate without checking the identity document properly, **2)** the RA might be deceptive and issue a valid certificate for a partner in crime, **3)** the RA/CA might be compromized by attackers who can now simply issue certificates at their discretion. The result is that certificates are not as trustworthy as actually required.

Approach

In previous work, we investigated how Distributed Ledger Technology (DLT) can help in this context. DLT is able to manage data in a community effort of numerous peers, which can even belong to different, competing organizations. Whenever changes need to be applied to a data asset (create new asset, change an asset's value, etc.), the changes can only be applied when the network reaches a consensus that authorizes the change.
We implemented a basic DLT-based certificate issuance process that involves not just one but several RAs. After a policy-defined set of RAs has verified the claimed identity, the DLT-based IDMS authorizes the issuance of the certificate. However, the problem is still that the CA's private signing key could be compromized and abused. The goal of this thesis is to investigate on appropriate cryptographic technology able to share a private signing key between n peers. Once the DLT-based IDMS authorized the certificate issuance, the certificate shall be issued as a community effort of $m < n$ peers.

Your Tasks

1) Understand requirements and goals of this application scenario. **2)** Investigate on related work. **3)** Study on cryptographic mechanisms, e.g. secret sharing, suitable to implement a sharing concept for private signing keys across different nodes. **4)** Implement a protoype of the collaborative signing solution. **5)** Merge your solution with the DLT-based IDMS code.

Contact

Dr. Holger Kinkelin, Stefan Liebald, Heiko Niedermayer (lastname@net.in.tum.de)