Technical University of Munich

Thesis B.Sc.

Thesis M.Sc.

IDP

Threshold Cryptography enabled QES

Motivation

Qualified Electronic Signatures (QESs) enable users to create legally binding signatures. In contrary to their analog counterparts, QES can be done on digital documents, e. g., when signing a contract, and remotely. Current implementations of QES schemes rely on centralized trusted third parties to create the signature. This introduces a single point of failure and attack. To further increase the trust of users in signature schemes, information about issued signatures should be verifiable by third parties. One solution for this is the use of transparency logs. However, transparency logs also rely a single point of trust (and failure). This thesis should explore distributed cryptographic mechanisms such as threshold signing that allow for collaborative signature creation without a need to trust a single party.

Topic

The goal of this thesis is to research and develop an distributed architecture for QESs. To identify the requirements of such an QES architectures you need to analyze exitsting QES schemes and identify shortcomings due to their centralized nature. Based on the requirements, identify suitable threshold signing scheme and analyze its impact on the system. Based on the insights, you should design a new QES architecture that combines the threshold signing to solve the identified shortcomings. You should then implement a proof of concept and evaluate the security guarantees of the proposed architecture.

Your Task

- Analyze existing QES schemes
- Analyze methods for threshold signing and transparent storage of information
- Design a new distributed QES scheme
- Implement a proof of concept of the proposed scheme
- Evaluate the proposed concept

Requirements

- Knowledge in a common programming language
- Ability to write easy maintainable code

Sources

- [1] BSI - Technische Richtlinie TR-03130, https://www.bsi.bund.de/DE/Publikationen/TechnischeRicht
03130.html

Contact

Filip Rezabek frezabek@net.tum.de
Lars Wüstrich wuestrich@net.in.tum.de

http://go.tum.de/080755