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

Thesis B.Sc.

Thesis M.Sc.

Role Based Qualified Electronic Signatures

Motivation

There are several proposals for architectures for qualified electronic signatures (QESs). QESs enable users to create legally binding signatures on digital documents, e. g., when signing a contract. The current schemes enable individual persons to create a signature for themselves. There are other use cases in which persons create signatures when executing a role, e. g., when acting as a representative for a company. In particular, a role-based signature needs to be verifiable afterward by outside parties. The realization of such scenarios requires an extension to existing schemes or new architectures.

Topic

The goal of this thesis is to research an architecture that enables role-based QES. To elicit the requirements of such an architecture, you need to analyze existing QES methods and compare them. Afterward, you need to research the special properties of role-based signatures to identify their challenges. A focus should in particular, lie on identification schemes and how the relationship between persons and roles can be transparently established. Based on the insights, your task is to design a new procedure or extend an existing QES scheme to support transparent role-based QESs. You should then implement a proof of concept of your role-based QES scheme. This should then be evaluated regarding its security properties and verifiability to outsiders.

Your Task

- Analyze existing QES methods
- Analyze challenges of role-based QES
- Develop a new procedure or extend an existing QES method to support role-based QES
- Identify potential pitfalls of role-based signature schemes
- Implement a proof of concept
- Evaluate the security guarantees of your proposed approach

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/TechnischeRichtlin
03130.html

Contact

Lars Wüstrich wuestrich@net.in.tum.de

http://go.tum.de/080755