Remote Signing Service

Gabor Tanz, Patrick Hirt

29. Oktober 2019

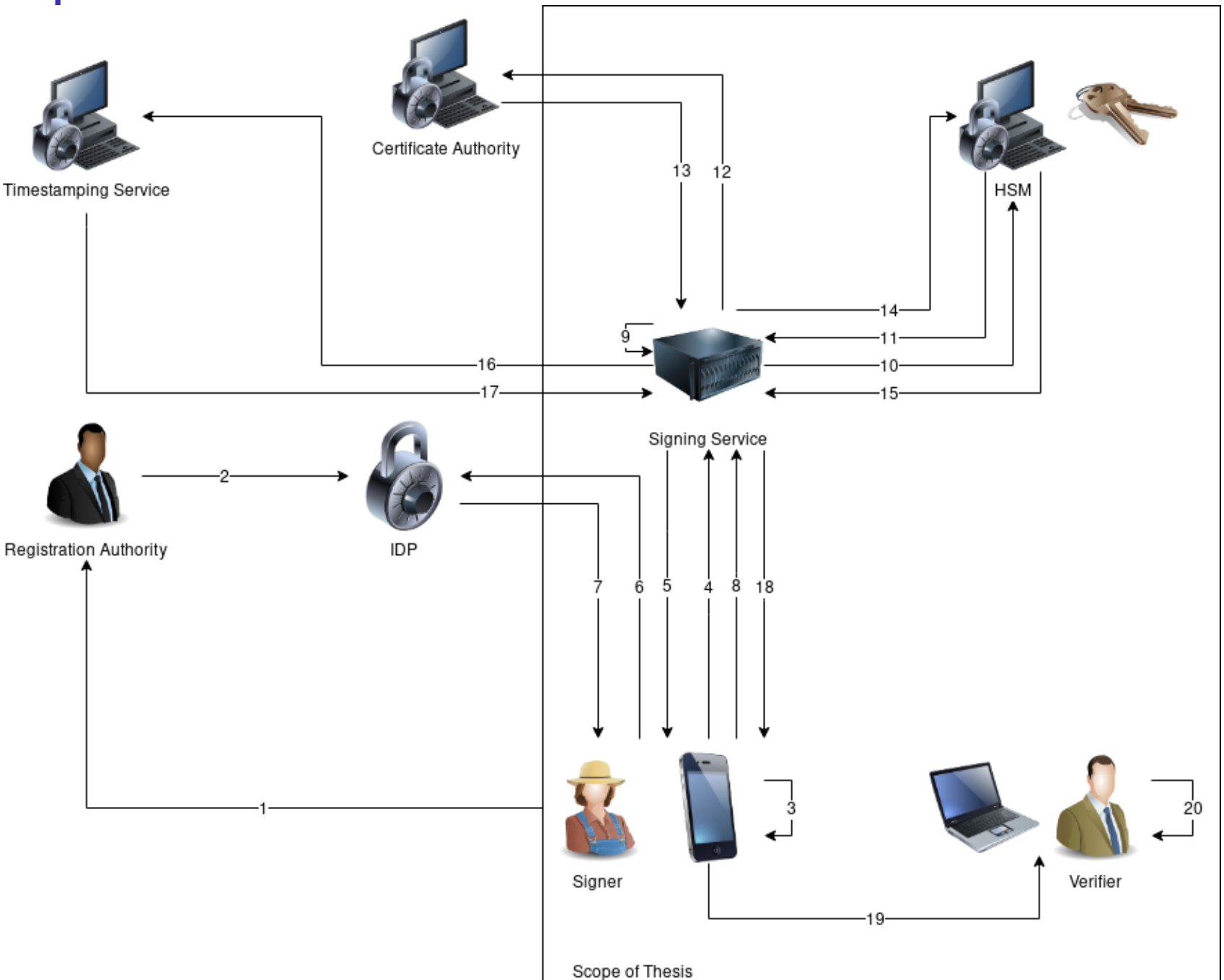
Inhalt

Problemstellung

Auftrag

- Spezifikation, Konzeption und Aufbau eines Remote Signing Services mit OIDC
- Aufbauend auf unserer Arbeit im Projekt 2
- Implementation bestehend aus:
  - Signing Server mit REST API
  - Integration mit CA, TSA, HSM
  - Plattformunabhängiges GUI für Desktop- sowie Mobilgeräte
  - Offline-Verifikation auf Desktop-Betriebssystemen

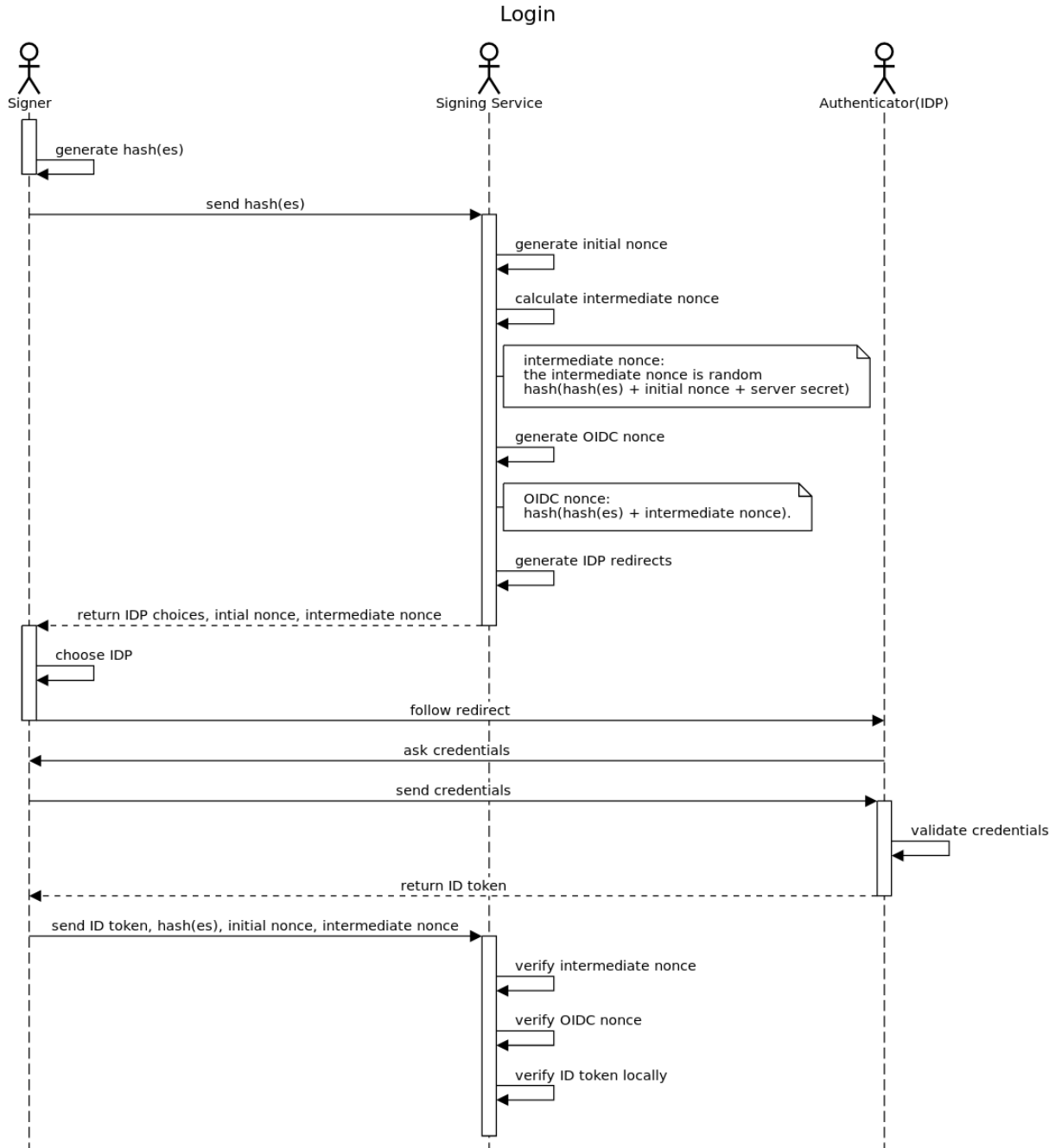
Komponenten



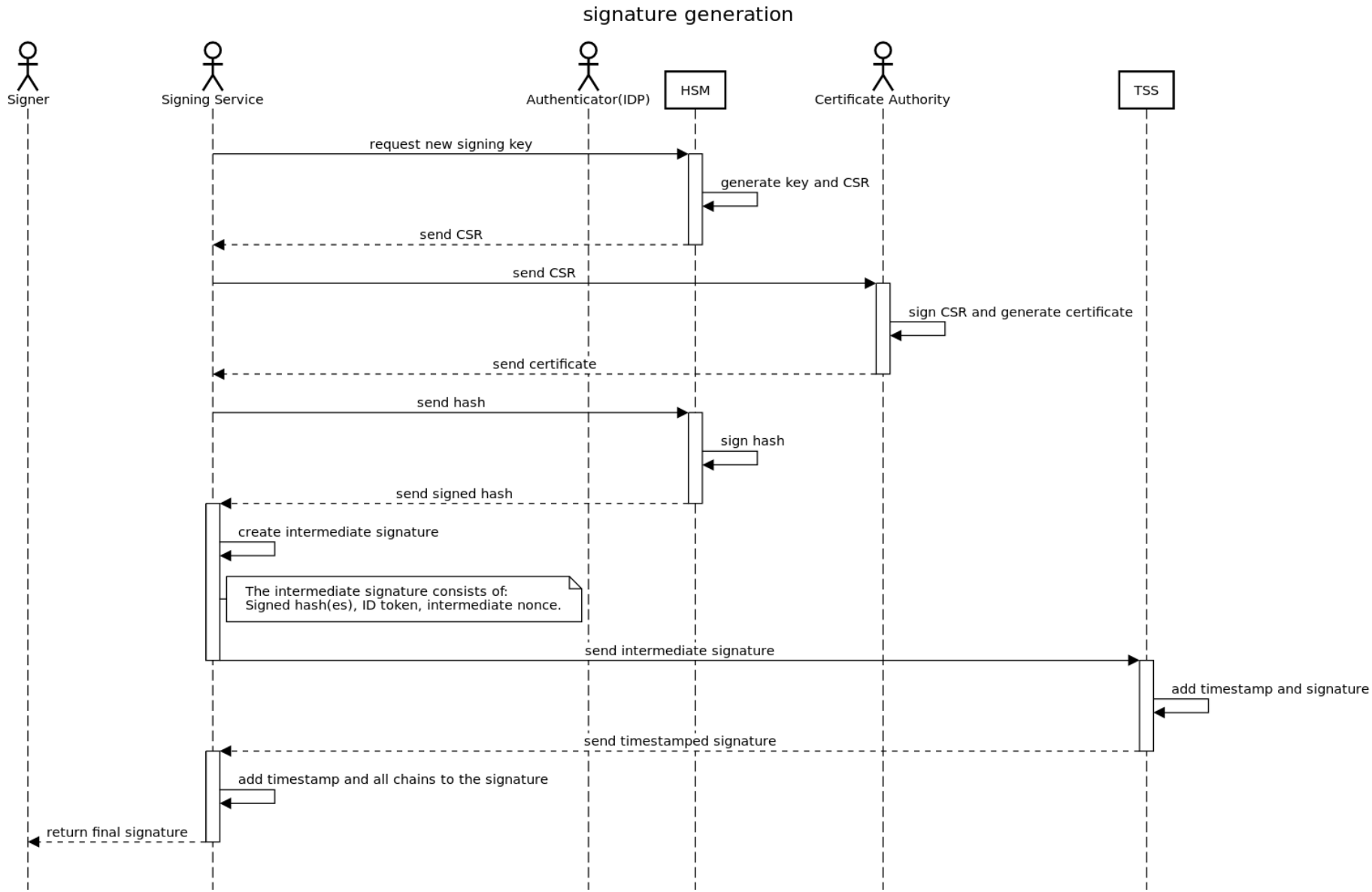
Grobkonzept

- Separate Signaturdatei, um formatsunabhängig signieren zu können
- Hash-Wert mit Identität verknüpfen
- Timestamps und Gültigkeit
- Signing Service generiert Zertifikate im Namen des Users

Prozess für qualifizierte Signaturen (1/2)



Prozess für qualifizierte Signaturen (2/2)



Vielen Dank!