Remote Signing Service

Gabor Tanz, Patrick Hirt

29. Oktober 2019

Inhalt

Problemstellung

Auftrag

- Spezifikation, Konzeption und Aufbau eines Remote Signing Services basierend auf OIDC
- Aufbauend auf unserer Arbeit im Projekt 2

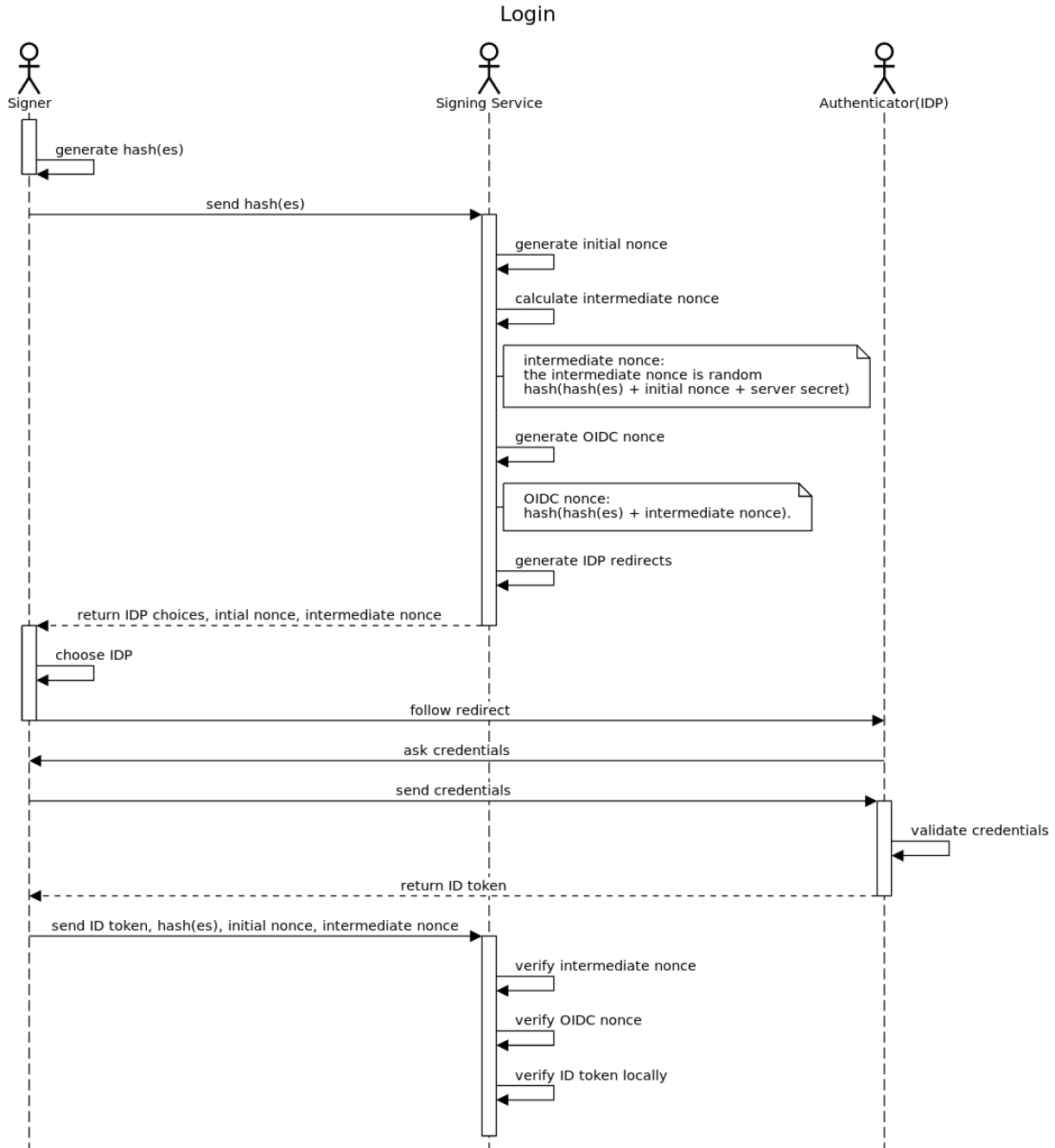
Technologien

- Protobuf
  - Serialisierungsformat
  - einfaches Schema
  - extrem kompakt
  - sehr schnell
- OIDC
  - Basierend auf OAuth 2
  - ID Token als JWT
  - Flows für verschiedene Anwendungszwecke

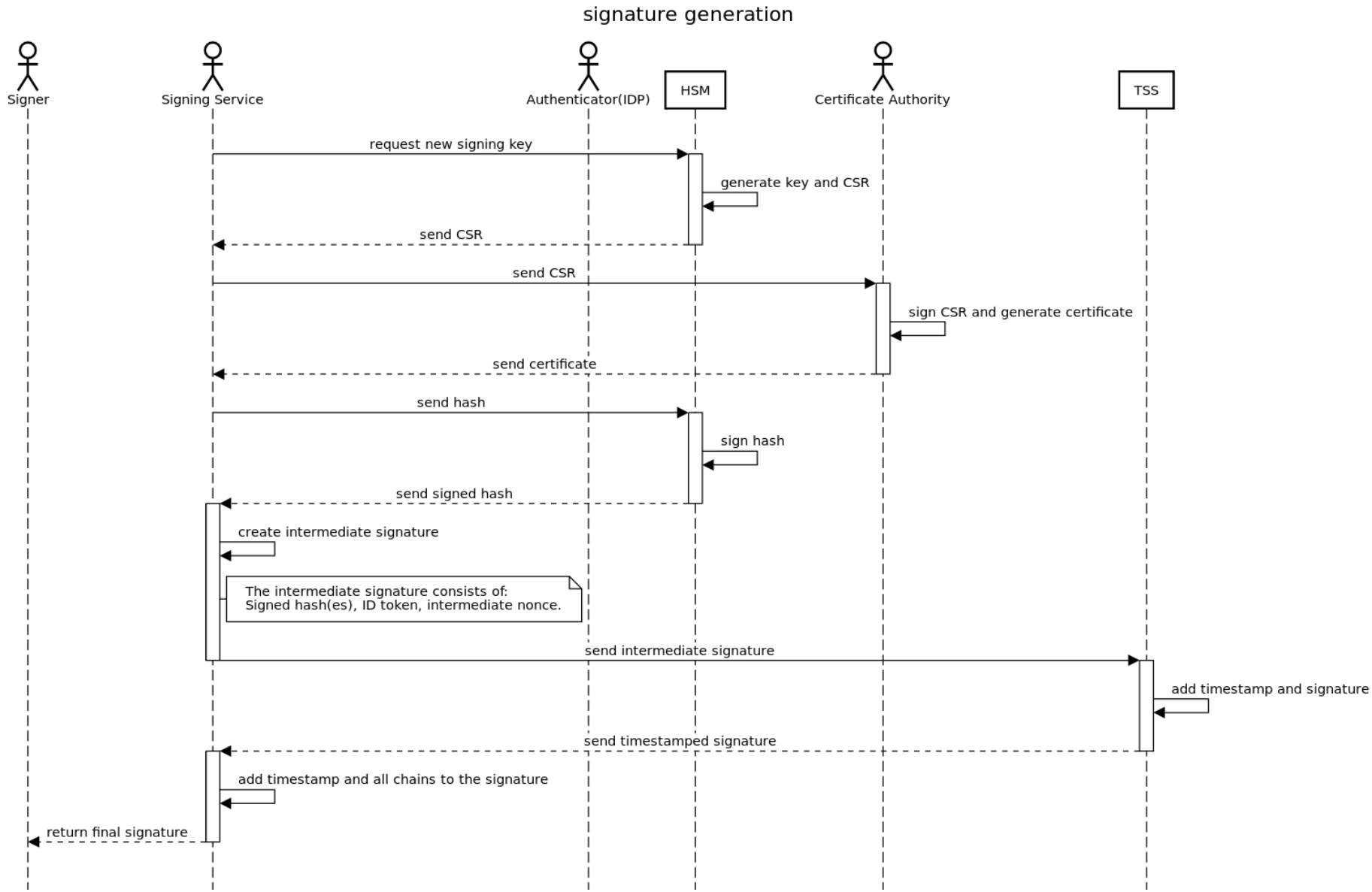
Grobkonzept

- 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!