Identity chain management for banks: law 7.8.2009/617

"Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista"
17 §: "Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen"

Tero Keski-Valkama

CYBERCOM
GROUP

2017-11-22

- The law for electronic identification includes the 17 § which allows banks to perform the first identification of a new customer using an electronic strong identification method. In practice this means identification through electronic identification performed by another bank.

- The text of the relevant part of the law: "Olemassa olevan vahvan sähköisen tunnistusvälineen avulla on voitava hakea vastaavan tasoista sähköistä tunnistusvälinettä. Aiempaan tunnistukseen luottava vahvan sähköisen tunnistuspalvelun tarjoaja vastaa mahdollisesta tunnistuksen virheellisyydestä suhteessa vahingon kärsineeseen."

- So, what happens if a criminal uses a stolen strong authentication of user X in bank A to create an account in another bank B?

- The consumer reports the credentials as stolen to bank A, and bank A revokes the credentials. What happens to the new credentials in bank B?

- Cybercom and blockchain to the rescue! Let's store all the identity related actions in an unmodifiable, shared log.

- Guardtime KSI offers a convenient service component for establishing specific kinds of guarantees regarding trust.
- In practice KSI can be used to prove that a specific document has existed at a specific point of time, by storing the hash digest of the document in an unmodifiable hash calendar (merkle tree).
- Guardtime only receives the hash digest of the document, never the whole document.
- In Cybercom Identity Chain proposal Guardtime KSI is used to offer additional guarantees that the shared identity event log is unmodifiable.

- In addition to hash digests, we will also need to store the master data in a manner that is robustly available to all cooperating banks.
- IBM Hyperledger Fabric is a platform for implementing consortium blockchains.
- As opposed to public blockchains like Ethereum, consortium blockchains do not require an associated cryptocurrency and they require a trusted party that manages consortium memberships.
- Storing a shared registry of identity events in a consortium blockchain makes it unmodifiable after once written, and available to all cooperating parties.
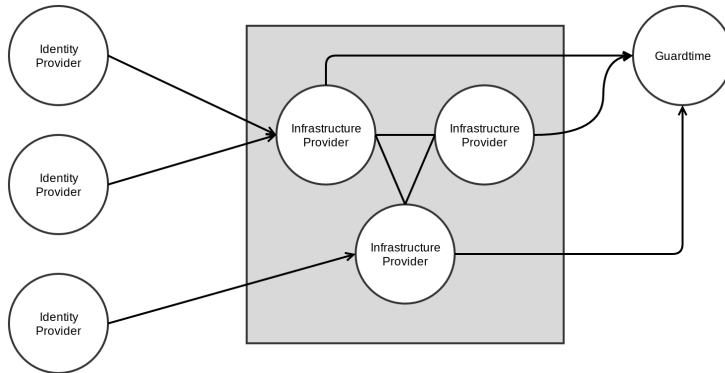
- Banks can work as infrastructure providers and/or identity providers in the architecture.
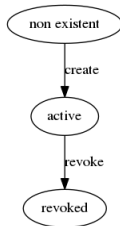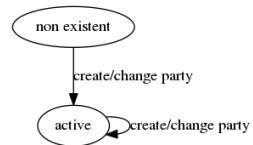
Figure: Identity state machine

Figure: Identity provider (party) state machine