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

Why?

- 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.

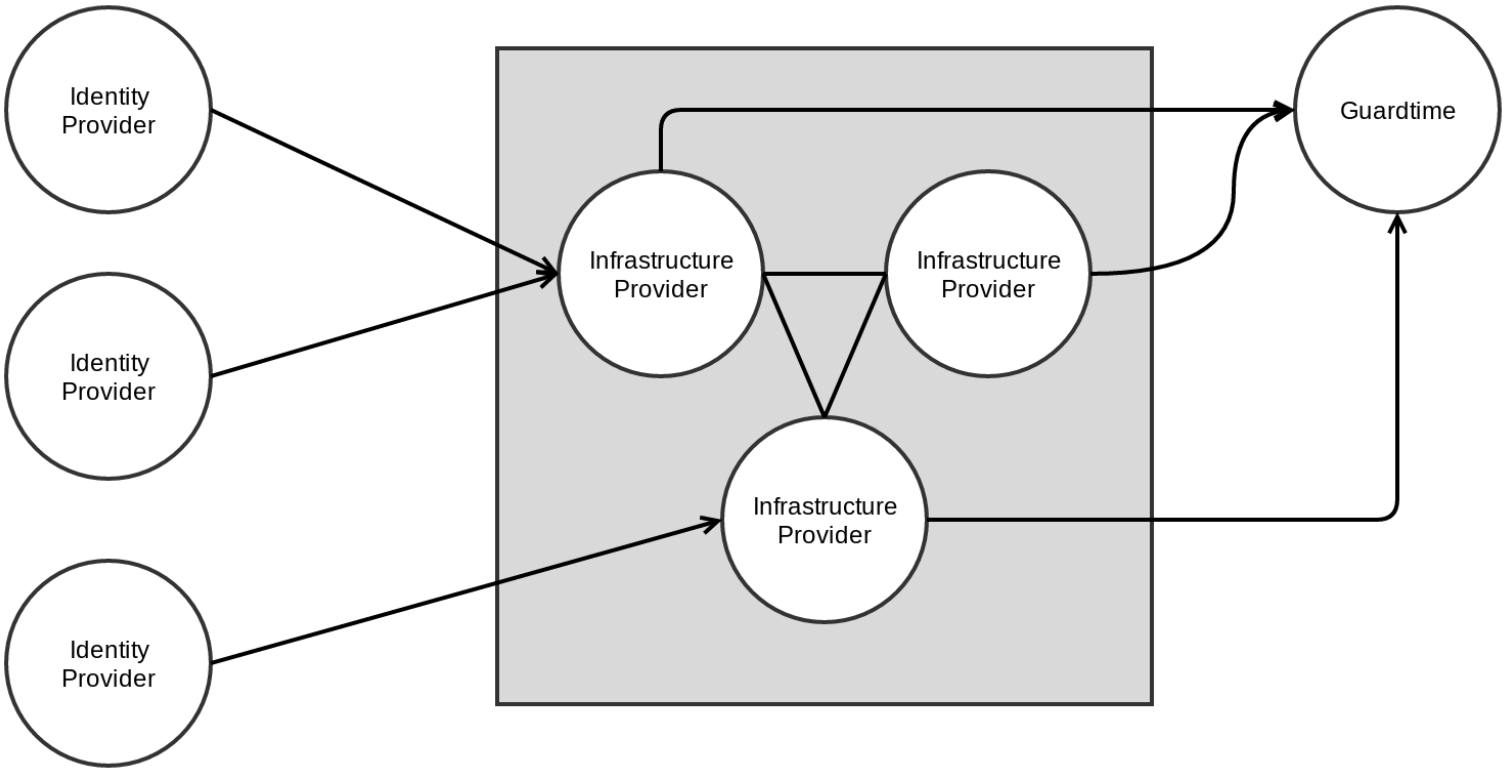
Background – Guardtime Keyless Signature Infrastructure

- 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.

Background – IBM Hyperledger Fabric

- 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.

Architecture



- Banks can work as infrastructure providers and/or identity providers in the architecture.

Operation

1. Person A has their identity for Bank X stolen
2. Stolen identity (X) used to create a new account in Bank Y
3. Person A retroactively revokes their identity at Bank X
4. Fake identity (Y) used to create a new account in Bank Z
5. Fake identity (Z) used in criminal activity

- If Bank Z did not check the identity chain state in blockchain at (4), then Bank Z is liable for damages.
- If Bank Z did check, but Bank X did not correctly mark this revocation in time to the blockchain to prevent (4), then Bank X is liable.
- If Bank X marked the revocation and Bank Z checked the chain status, then (4) failed and (5) did not happen.
- Liability is based on consortium membership contract. Blockchain provides an indisputable log of events to determine liability.