# Right to erase

Non-repudiation protocol

# Definitions

- P - prover, the party which shares the data and may request for execution of RTE in the future
- V - verifier, the party which receives and stores the data from the prover
- N - notary
- L - ledger
- Flag RTE - the indicator of RTE supported by verifier
- PRQ - proof request, template of attributes required by V

# Definitions

| | |
|---|---|
| $\{data\}_{key}$ | data signed by some key |
| $\{data\}^{key}$ | data encrypted by some key |
| $[data]$ | optional data |
| $PK_{party}$ | public key of the party |
| RK | temporary recipient key |
| H(data) | hash of the data |
| $time_x$ | timeframe for the next step in the protocol |

# Prerequisites

- V and N have their public keys published on trusted L

- P , V  and N use an encrypted protocol to communicate

# The initiation

- P generates random SID - session ID
- P sends to V: $\{SID, time_1, PK_v\}_{PK_p}$
- V responds: $\{SID, time_2, PRQ, Flag_{rte}, [contract]\}$
- P agrees, generates PROOF, RK
- P chooses notary N

# The signature exchange

P sends to V

$$ProverSignature = \{SID, time_3, PK_v, PK_n, PRQ, H(RK), H(Proof)\}_{PK_p}$$

$$\{RK\}^{PK_n}$$

$$\{Proof\}^{RK}$$

V sends to N

$$VerifierSignature = \{SID, time_4, PK_n, H(Proof)\}_{PK_v}^{PK_n}$$

$$ProverSignature$$

$$\{RK\}^{PK_n}$$

# The notary

- N verifies both signatures [and possibly makes a record of the session for legal purposes]

- N publishes the tuple to a store

$$\{SID, \{RK\}^{PK_v}, PK_v, PK_n\}$$

- N sends to both P and V

$$\{SID, timestamp, PK_v, PK_p, H(ProverSignature), H(VerifierSignature)\}_{PK_n}$$

# The verifier

- V reads from store. The store publishes proof-of-sharing to the ledger:

$$\{SID, Flag_{consumed}, PK_v\}$$