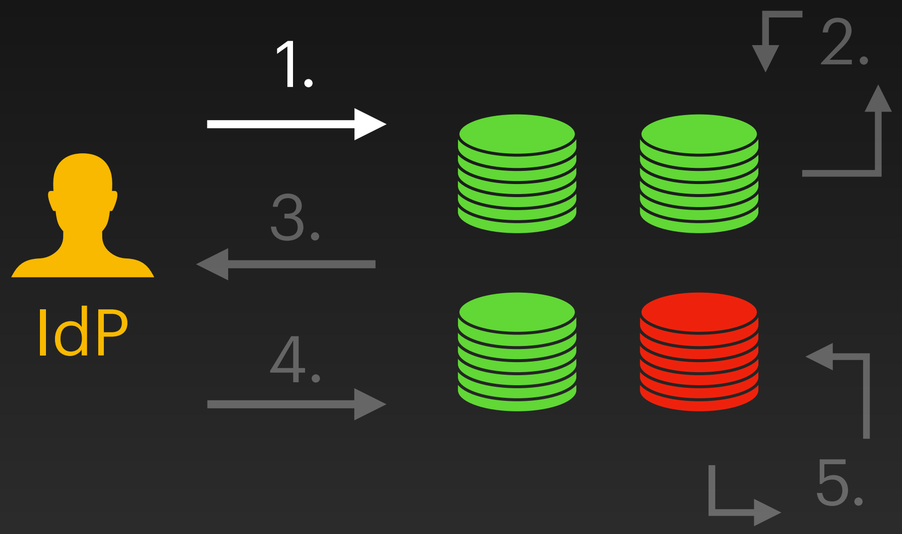
Key Transparency

HSM Protocol

Novi Research

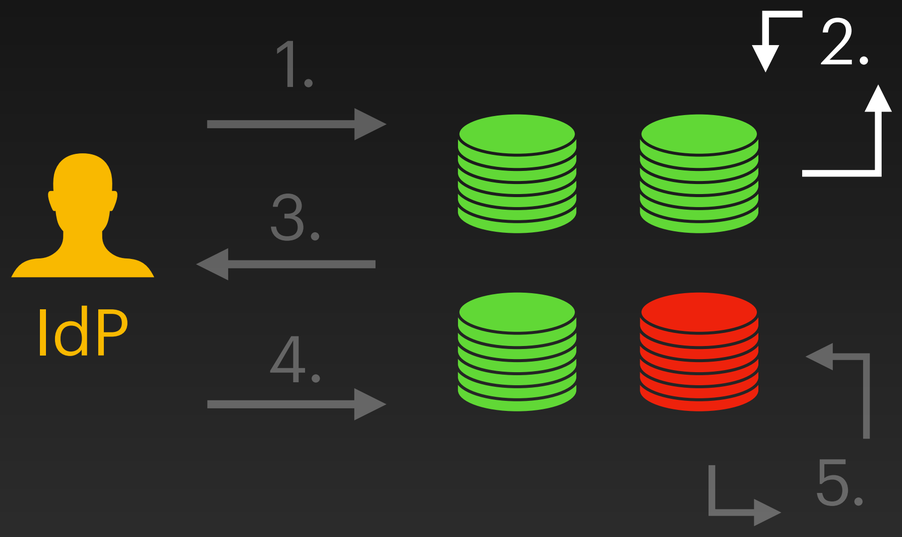
Publish
Protocol details



1. publish notification

- Sequence number
- Seemless proof
- IdP's signature

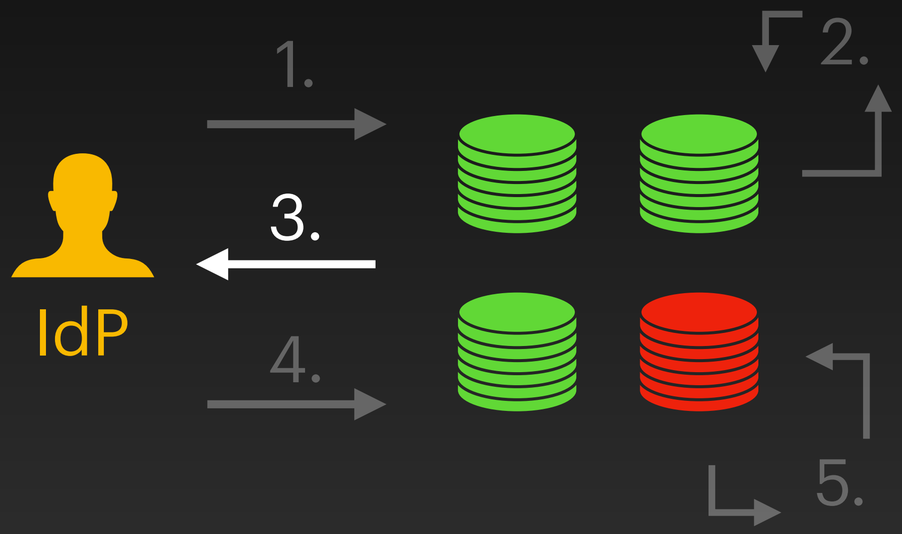
Publish
Protocol details



2. verify

- The IdP's signature
- Seemless proof
- No previous request is pending
- Sequence number is as expected

Publish
Protocol details



3. signed publish notification

- Each authority signed the publish notification received in step 1.

Publish
Protocol details

4. publish certificate

- Collect a quorum of signatures from the HSMs.

Publish
Protocol details

5. settle

- Verify the certificate's signatures
- Increase the sequence number
- Set the pending order to None
- (Persist the certificate)

Byzantine Consistent Broadcast

Validity: A certificate only requires a quorum

No duplication: Sequence numbers prevent replays

Integrity: Notifications are signed

Consistency: Pending field prevents split-views

Publish
Core API

IdP core

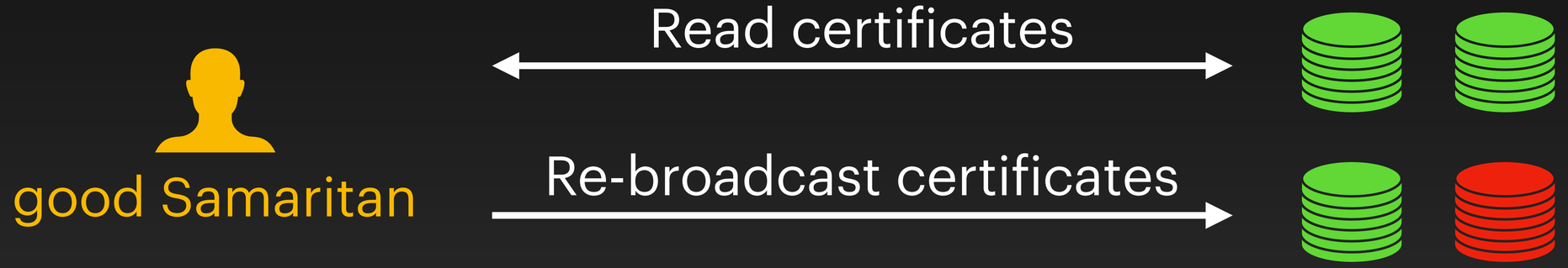
- makeNotification(updates) -> Notification
- handleVote(v) -> Option<Certificate>

Witness core

- handleNotification(n) -> Vote
- handleCertificate(c)

Crash-Recovery

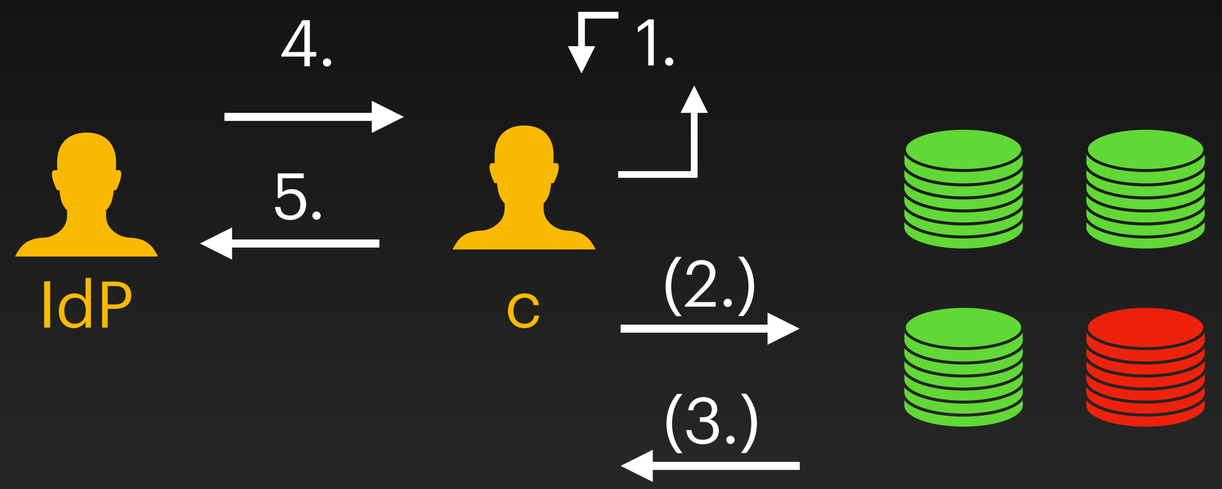
Idempotent core & Totality



EXTRA

Freshness

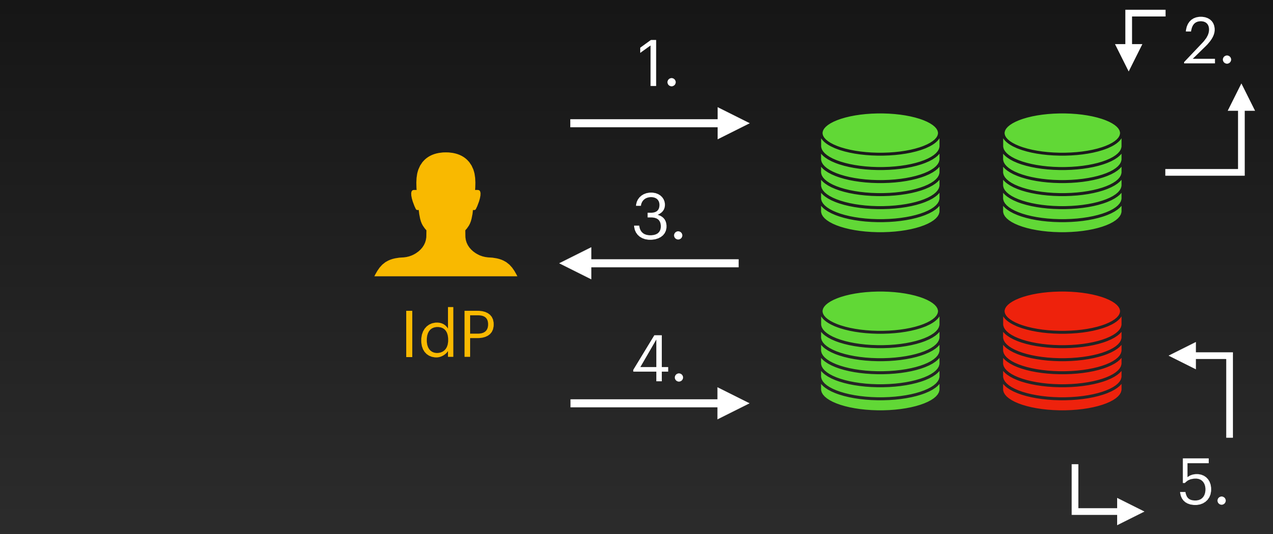
(Clients-Authorities communication)



Censorship Resistance

(Sacrifice privacy)

Committee Rotation



Committee Rotation