Anonymous Electronic Petition Signing

Josep Balasch

K.U.Leuven ESAT/COSIC
Anonymous Credentials

- Cryptographic tokens
- Authenticate and prove certified attributes
  - Example: “Age > 18” and “Nationality = Belgian”
- Improve privacy w.r.t. PKI certificates
  - Data minimization
  - Unlinkability of transactions
Anonymous Credentials. Model

- Master secret in smart card → Tamper-resistance
- Expensive computations → Outsource to Host
- Two protocols: issue, verify
  - Unlinkability of transactions
Protocols

- Issuing Protocol

1. Blind master secret
2. Forward it to issuer
3. Sign request
4. Send credential parameters
5. Store part of credential
6. Compute and store credential secrets

- Verification Protocol

1. Send fresh nonce
2. Create proof of possession
3. Send proof
4. Verify authenticity of proof
   = Accept / Reject
Use Case. Petition Signing

- Formal request addressed to an authority and signed by numerous individuals
Use Case. Petition Signing

- Formal request addressed to an authority and signed by numerous individuals.

![Image of petition signing page on Number10.gov.uk](image-url)
Use Case. Petition Signing

- Formal request addressed to an authority and signed by numerous individuals.
Use Case. Petition Signing

- Formal request addressed to an authority and signed by numerous individuals
- Electronic Petitions
  - Insecure: easy to impersonate
Use Case. Petition Signing

- Formal request addressed to an authority and signed by numerous individuals
- Electronic Petitions
  - Insecure: easy to impersonate
- Alternative approach
  - Sign (and authenticate) with e-ID
  - Privacy issues
Proof–of–concept demonstrator

- Anonymous credentials on a Java Card
Conclusions

- Using PKI certificates introduces privacy issues
  - No data minimization
  - Linkability of transactions
- Anonymous credentials satisfy authentication and privacy requirements simultaneously
- Master secret safely stored in smart card
- Outsourcing of non-critical operations to untrusted host
Questions?