Privacy preserving credentials on mobile devices

Jonas Lindstrøm Jensen, Alexandra Institute
Use case: eID
Solutions with online issuer

- e.g. OpenID, Facebook Connect, SAML:

  1. Age > 18?
  2. Age = 30
  3. Authenticate
  4. Age = 30

- BigBrother issuer knows where you are shopping.
- Usually linkability across shops.
Solutions with offline issuer

- e.g. X.509 v3 certificates:
  - Always reveal full identity.
  - Linkable across shops.
Privacy ABCs.

- Privacy-preserving Attribute-based-credentials (Privacy ABCs):
  - Minimal disclosure of information
  - Unlinkable across verifiers and issuers
Advanced features

• Predicates on attributes
  – Can prove “Age > 18” instead of “Age = 30”.

• Pseudonyms
  – Limited linkability (account creation), e.g. if you want to collect bonus points at a shop.

• Revocation
  – Revoke ID if it is no longer valid or has been stolen.

• Inspection
  – Reveal information in certain circumstances – e.g. if a stolen credit card has been used.
ABC4Trust

• Create a common framework for existing Privacy ABC technologies
  – Microsoft’s U-Prove.
  – IBM’s Identity Mixer.

• … and put it in use!
ABC4Trust pilot projects

• Söderhamn, Sweden
  – Online chat forum at an elementary school.
  – Some forums are only accessible for pupils of a certain age or pupils following a certain course.
  – Inspection if teachers find that a pupil violates the forums policy.

• Patras, Greece
  – Anonymous course evaluation system at a university.
  – The Users were given smart cards which they should present every time they attended a course.
  – Evaluation only possible if attendance was high enough.
The framework developed by the ABC4Trust project is created to be easily integrated in applications.

The cryptography behind Privacy ABCs is complicated, but developers should not have to deal with these details.
Device

- Since the User is in full control, he needs a device…
  - …for storing credentials.
  - …to perform cryptographic calculations during presentation.

- In the pilot projects this was a combination of…
  - … laptops (for running the software)
  - … and smart card (for storage of the User’s credentials)
Mobile devices

• Using an electronic ID in a physical shop doesn’t make sense on a laptop.
• On mobile devices, the memory and computational capabilities are limited.
• But it's even possible to run on smart cards (IRMA) and possibly on other small embedded systems.
Conclusion

- User’s will leave traces online – but it should be kept at a minimum.
- This issue is even more present in a future where a User has many online devices.
- Privacy ABCs puts the User in control of what information is left behind.
- The framework created by ABC4Trust is easily integrated in applications.
- It works – please use it!
Thank you!