A Movie Streaming Application & ABC4Trust as Services in the Cloud

Dr. Anja Lehmann
IBM Research – Zurich

A research project funded by the European Commission’s 7th Framework Programme.
Lessons learned from the pilots ...

- Privacy-ABCs hard to deploy
- Demos are “private” – hard to try out
- Smart card integration somewhat slow

New demo

- Public demo
- Verifier and Issuer as cloud services
- New smart card prototyp and optimized integration
Alice wants to watch a movie

I wish to see Alice in Wonderland

Alice

Movie Streaming Service
Alice wants to watch a movie

Sure, if you have
  - subscription &
  - are older than 12
Watching the movie with the traditional solution

OK, here's
- my eID
- my subscription
Watching the movie with the traditional solution

Aha, you are
- Alice Doe
- born on Dec 12, 1998
- 7 Waterdrive
- CH 8003 Zurich
- Single
- Expires Aug 4, 2018

Mplex Customer
- #1029347
- Premium Subscription
- Expires Jan 13, 2016

Movie Streaming Service
Watching the movie with the traditional solution

This is a privacy and security problem!

- identity theft
- profiling
- discrimination

Aha, you are
- Alice Doe
- born on Dec 12, 1998
- 7 Waterdrive
- CH 8003 Zurich
- Single
- Expires Aug 4, 2018

Mplex Customer
- #1029347
- Premium Subscription
- Expires Jan 13, 2016

Movie Streaming Service
Watching the movie with the traditional solution

With OpenID and similar solutions, e.g., log-in with Facebook
Watching the movie with the traditional solution

With OpenID and similar solutions, e.g., log-in with Facebook

Aha, Alice is watching a 12+ movie

Alice

Movie Streaming Service
Watching the movie with the traditional solution

With OpenID and similar solutions, e.g., log-in with Facebook

Aha, you are
- Alice@facebook.com
- born on Dec 12, 1998
- Alice's friends are ....
- Alice's public profile is ...

Mplex Customer
- #1029347
- Premium Subscription
- Expires Jan 13, 2016

Aha, Alice is watching a 12+ movie

Alice

Movie Streaming Service
Privacy-ABCs solve this.

When Alice authenticates to the Movie Streaming Service with Privacy-ABCs, all the service learns is that Alice

- has a subscription &
- is older than 12

and no more.
Privacy-protecting authentication with Privacy-ABCs

Like PKI
- but does not send credential
- minimal attribute disclosure

Alice
- valid subscription
- eID with age ≥ 12

Movie Streaming Service

Privacy-ABC
eID & voucher
Privacy-protecting authentication with Privacy-ABCs

Like PKI

- but does not send credential
- minimal attribute disclosure

Aha, you have
- subscription &
- are older than 12
...enjoy the movie!
Let's watch a movie then!
ABC4Trust and the cloud

helping Issuers and Service Provider to use Privacy-ABCs
ABC4Trust and the cloud

Application Layer

- Credential Wallet

Policy Layer

- User ABC Engine
  - policy credential matcher
  - storage
  - evidence generation orchestration
  - credential mgr

- Verifier ABC Engine
  - policy token matcher
  - storage
  - evidence verification orchestration
  - token mgr

Crypto Layer

- Crypto Engine (e.g. Idemix)
  - Sig
  - Enc
  - Com
  - ZKP

all running in the cloud as a service
ABC4Trust and the cloud

- **Application layer**
  - Credential Wallet
  - Browser/Application

- **Policy layer**
  - User ABC Engine
    - policy credential matcher
    - storage
    - evidence generation orchestration
    - credential mgr
  - Crypto Engine (e.g. Idemix)
    - Sig
    - Enc
    - Com
    - ZKP

- **Crypto layer**
  - Verifier ABC Engine
    - policy token matcher
    - storage
    - evidence verification orchestration
    - token mgr
  - Crypto Engine (e.g. Idemix)
    - Sig
    - Enc
    - Com
    - ZKP

All running in the cloud as a service
Benefits of running ABC4Trust services in the cloud

- Cloud services reduce the complexity for Issuer and Verifier
  - No complex installation and configuration of the ABC4Trust components
  - No maintenance
  - Cloud offers tools to simplify service integration, e.g.:
    - Issuer: Interface to LDAP etc. → credential specs can be derived automatically
    - Service Provider: Integration tools for access control, MySQL, preconfigured PKI
Benefits of running ABC4Trust services in the cloud

- Relying on cloud/web services is already common deployment model
  - Use of external service for authorization is common practice (e.g. Facebook login) → simple integration/migration
  - Small business often rely on cloud infrastructure anyway
  - Issuer and Verifier could run their own cloud
Drawbacks of running ABC4Trust services in the cloud

- Cloud provider learn user attributes during issuance and verification
  - But Privacy-ABCs already help to minimize the revealed information (less PII)
  - No need for single provider as in OpenID/Facebook
    → Multiple issuance/verification services reduce trust requirements
ABC4Trust and the cloud

All running in the cloud as a service

User ABC Engine
- policy credential matcher
- evidence generation orchestration
- storage
- credential mgr

Verifier ABC Engine
- policy token matcher
- evidence verification orchestration
- storage
- token mgr

Crypto Engine (e.g. Idemix)
- Sig
- Enc
- Com
- ZKP

application layer

policy layer

crypto layer

Credential Wallet

Browser/Application

presentation policy

presentation token

request resource
ABC4Trust and the cloud

Application layer

Credential Wallet

Policy layer

User ABC Engine
- policy credential matcher
- evidence generation orchestration
- storage
- credential mgr

Verifier ABC Engine
- policy token matcher
- evidence verification orchestration
- token mgr

Crypto layer

Crypto Engine (e.g. Idemix)
- Sig
- Enc
- Com
- ZKP

web-based user wallet

all running in the cloud as a service
Web-based user wallet

- **Benefits:**
  - No dedicated software needed – access via Browser
  - Credentials can be used from multiple devices
  - User has choice of whom to trust – no need for single entity as in OpenID

- **Drawbacks:**
  - User has to trust the wallet provider with all data
  - Verifier has to trust wallet provider to properly protect credential access

→ Wallet on user device (e.g. phone) still preferable!
Summary

- Cloud is just a deployment model that makes integration easier
  → helps to get Privacy-ABCs started and
  privacy & security is better than with currently used mechanisms

**Demo: idemixdemo.zurich.ibm.com**

**Twitter Chat – 28 January at 16:00 CET (Data Privacy Day)**
How: You just need a Twitter handle and use #identitymixer
What: Live discussion & exciting news about Identity Mixer

- eMail
  - Anja Lehmann: anj@zurich.ibm.com
  - Jan Camenisch: jca@zurich.ibm.com

- Links
  - www.zurich.ibm.com/idemix
  - www.abc4trust.eu