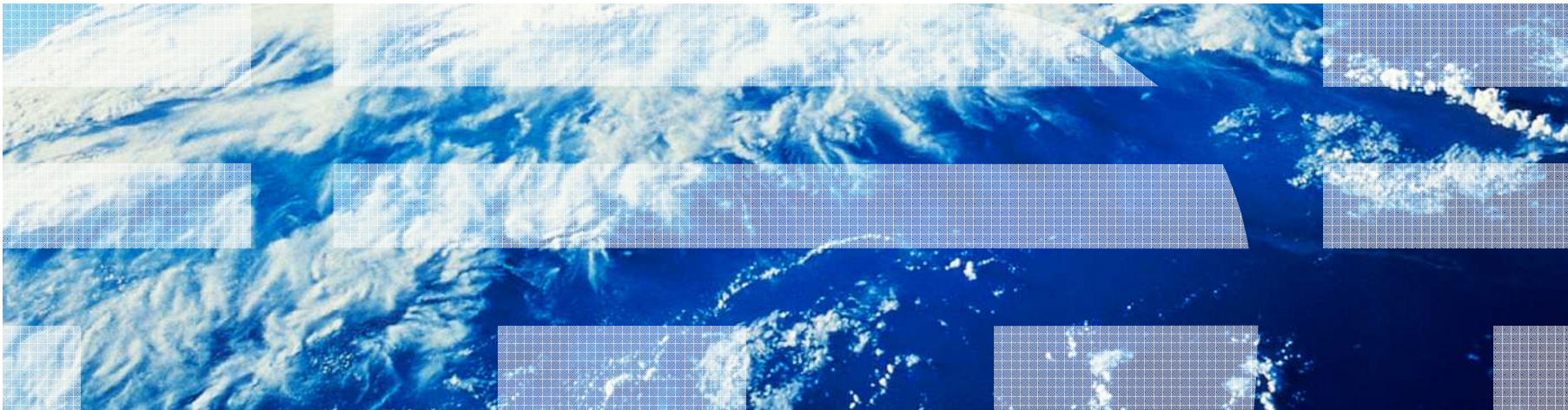


Identity Mixer: From papers to pilots – and beyond



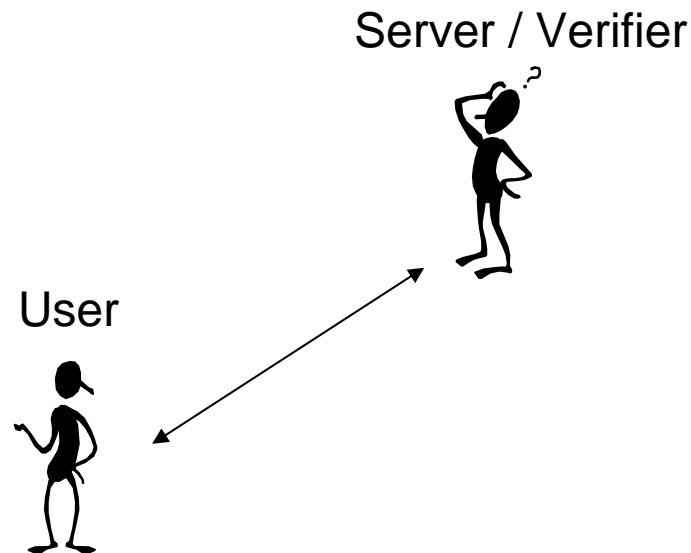
Gregory Neven, IBM Research – Zurich

Motivation



Online security & trust today:

- SSL/TLS for encryption and server authentication
- Username/password for client authentication
- Mostly self-claimed attributes (except email, credit card)



Motivation

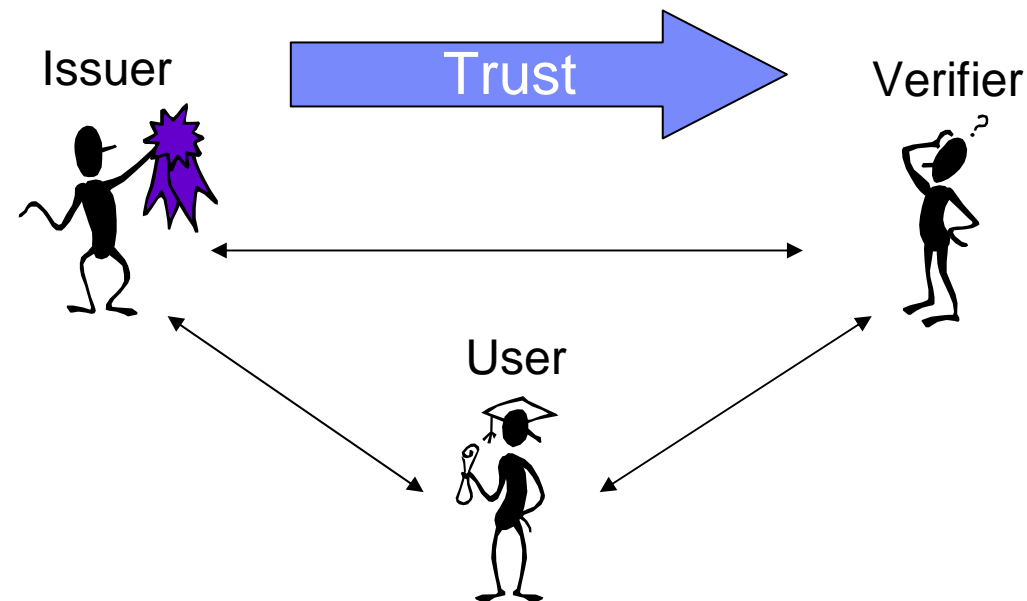


Trusted attribute transfer solutions exist

e.g., SAML, WS-Federation, OpenID, Facebook Connect, X.509 v3

but have privacy issues

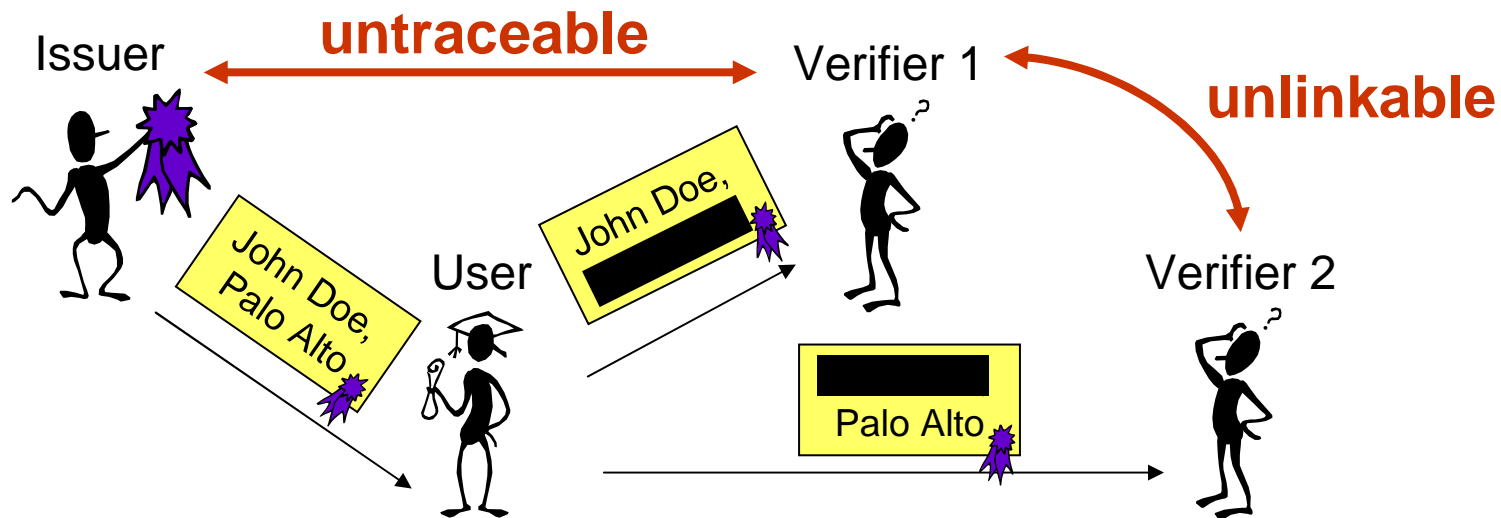
- Online identity provider as “Big Brother”
- Linkability through unique identifiers or public keys



Privacy-preserving Attribute-Based Credentials (Privacy-ABCs)

generalization of

- pseudonym systems [Chaum 81]
- group signatures [Chaum-van Heyst 91]
- anonymous credentials [Camenisch-Lysyanskaya 01]
- identity escrow [Kilian-Petrank 98]
- minimal-disclosure tokens [Brands 99]
- direct anonymous attestation [Brickel-Camenisch-Chen 04]



Overview of this talk



- Features of Privacy-ABCs
- Cryptographic realization
- Non-cryptographic hurdles to deployment
- Current status of Identity Mixer
- Future of Identity Mixer

Overview of this talk



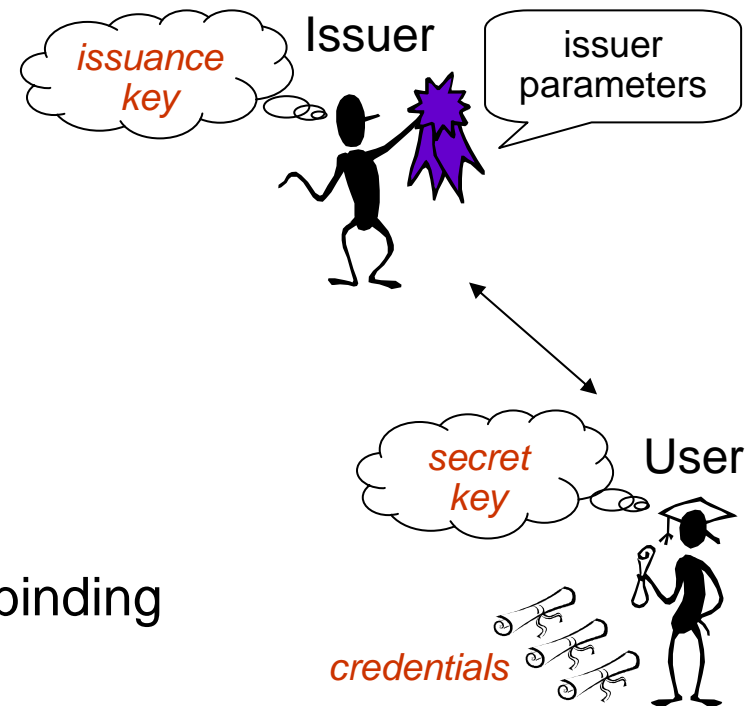
- Features of Privacy-ABCs
- Cryptographic realization
- Non-cryptographic hurdles to deployment
- Current status of Identity Mixer
- Future of Identity Mixer

Credential issuance



Credential

- list of attribute-value pairs
- certified by issuer
- (optionally) *bound* to user's secret key
 - non-frameability
 - prevent credential pooling
 - secret key on trusted device → device binding



Advanced issuance:

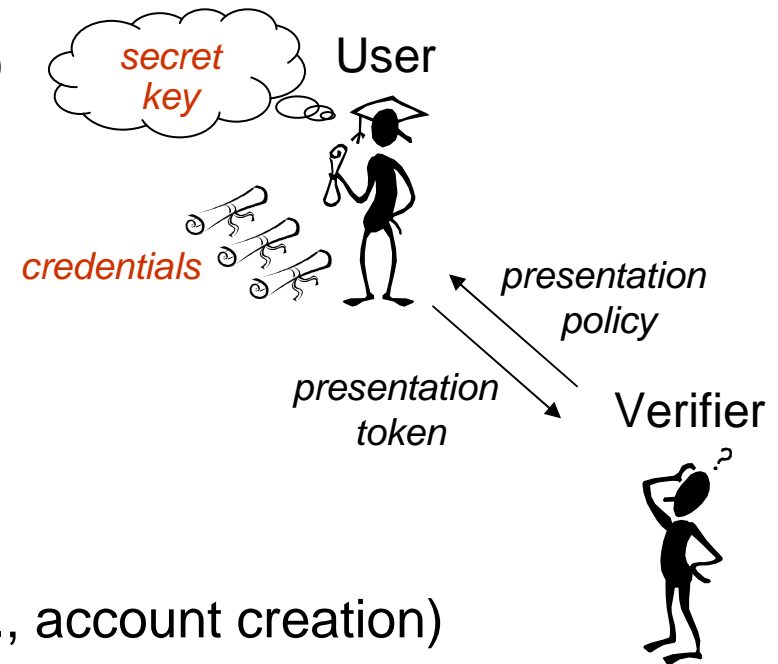
- carry over attributes or key from existing credentials
- issuer-blind attributes
- jointly random attributes

Presentation



Presentation policy (token) requests (reveals)

- attribute values from credential(s)
- predicates over attributes
attribute₁ =, >, < attribute₂ or constant
- *pseudonyms*
 - ≈ unlinkable public key for secret key
 - intentionally create limited linkability (e.g., account creation)
 - re-authenticate later with secret key (no credentials)
 - *scope-exclusive* pseudonym:
unique pseudonym for specific *scope string*



Inspection

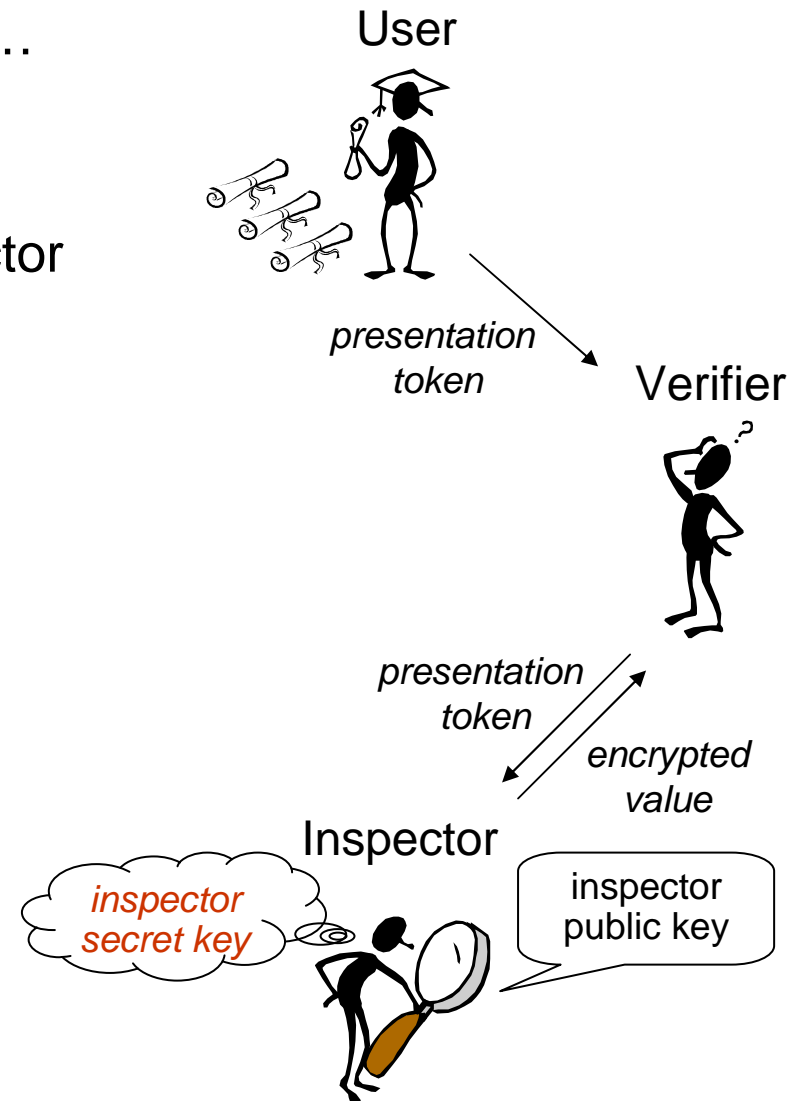
aka opening, tracing, anonymity revocation,...

Verifiably encrypt attribute value(s) to inspector

- De-anonymization in case of abuse
- Reveal attributes to 3rd party
e.g., credit card details to bank

Many inspectors, chosen at presentation

Token bound to *inspection grounds*



Revocation



Render certain credentials unusable for presentation

Revocation authority publishes

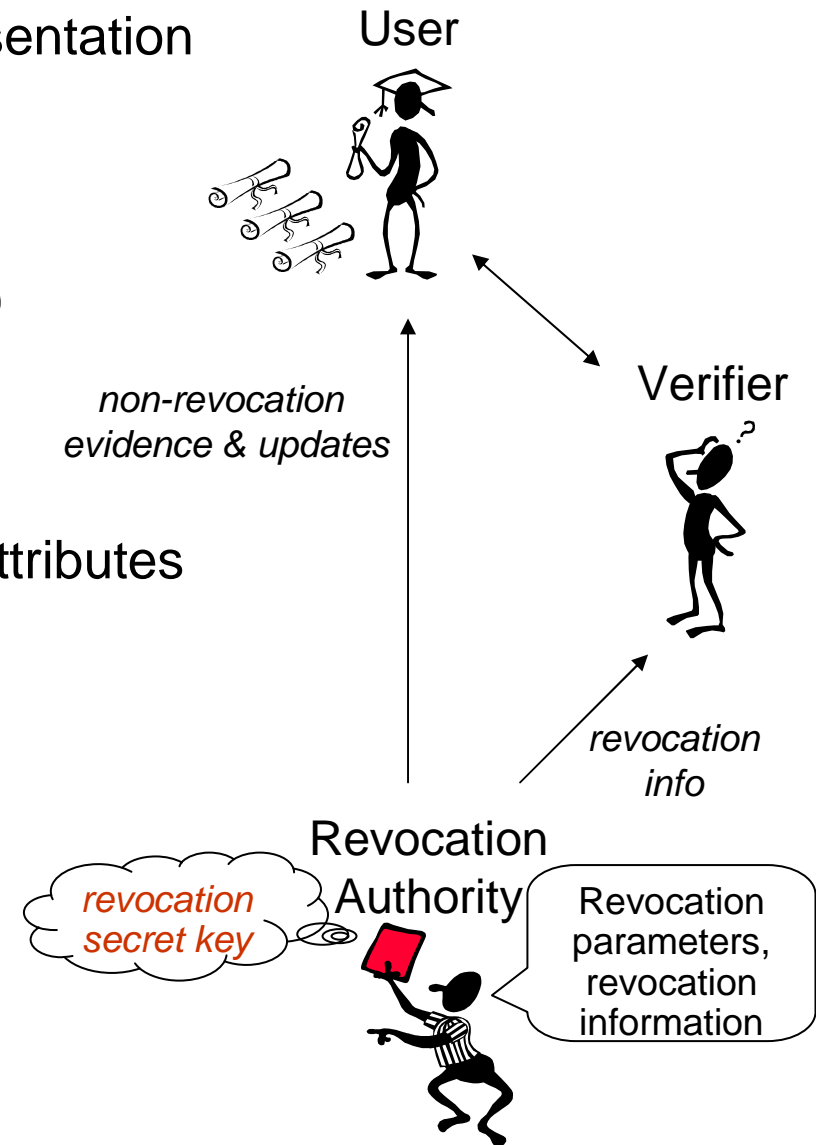
- revocation parameters (public, static)
- revocation information (public, dynamic)

■ Issuer-driven (global) revocation:

- issuer assigns revocation authority
- e.g., credential compromise, changed attributes

■ Verifier-driven (local) revocation:

- verifier assigns revocation authority
- e.g., exclude from service after abuse

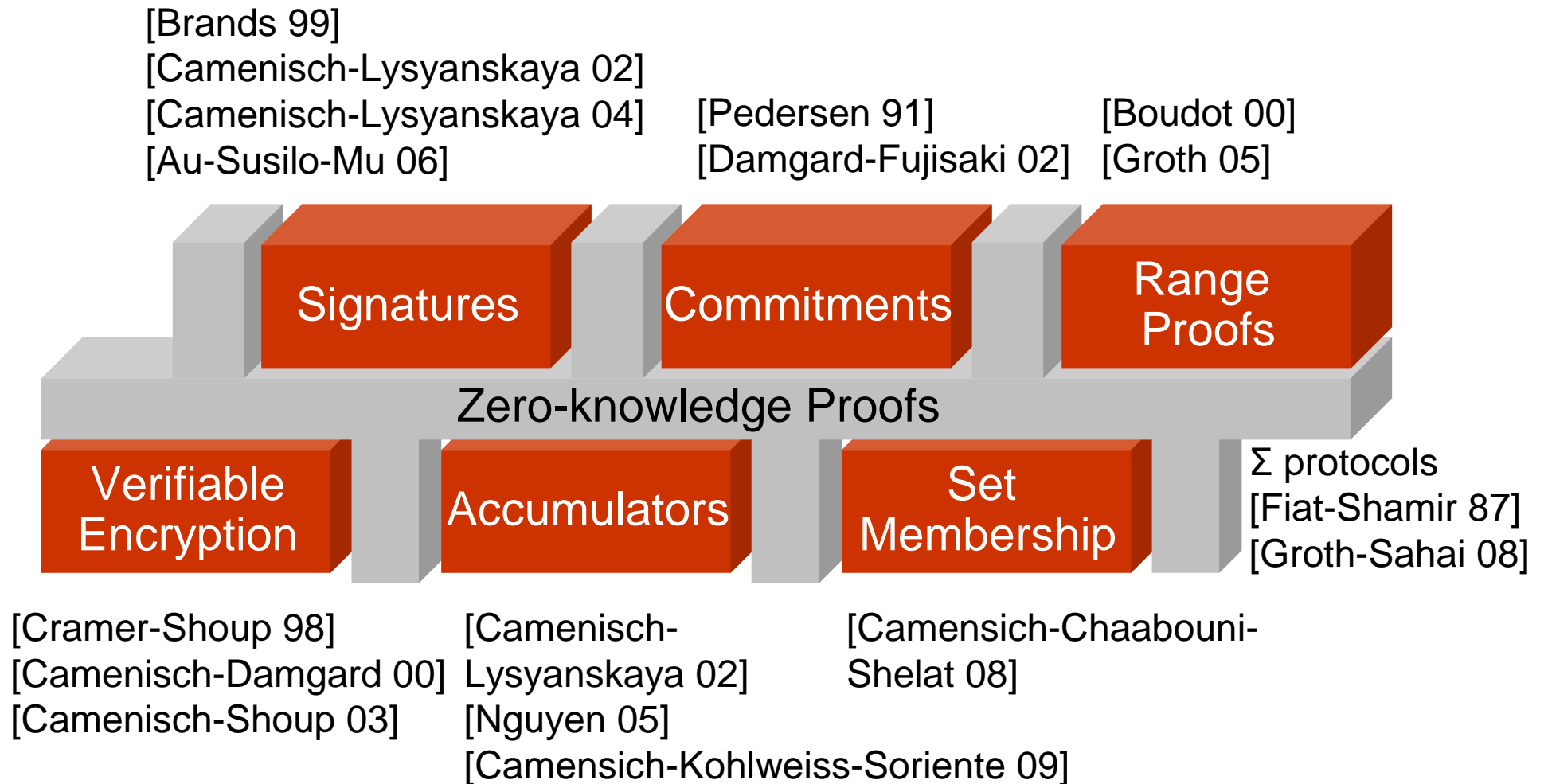


Overview of this talk

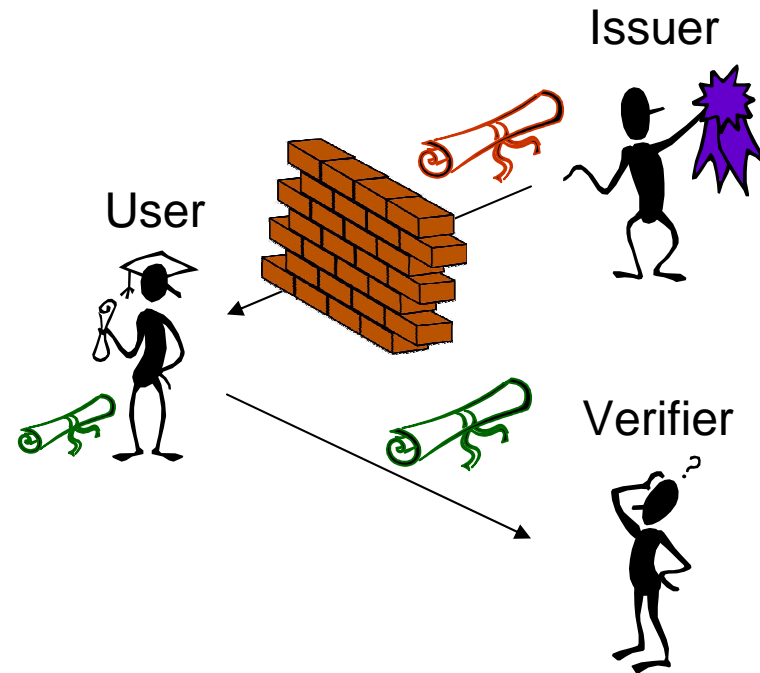
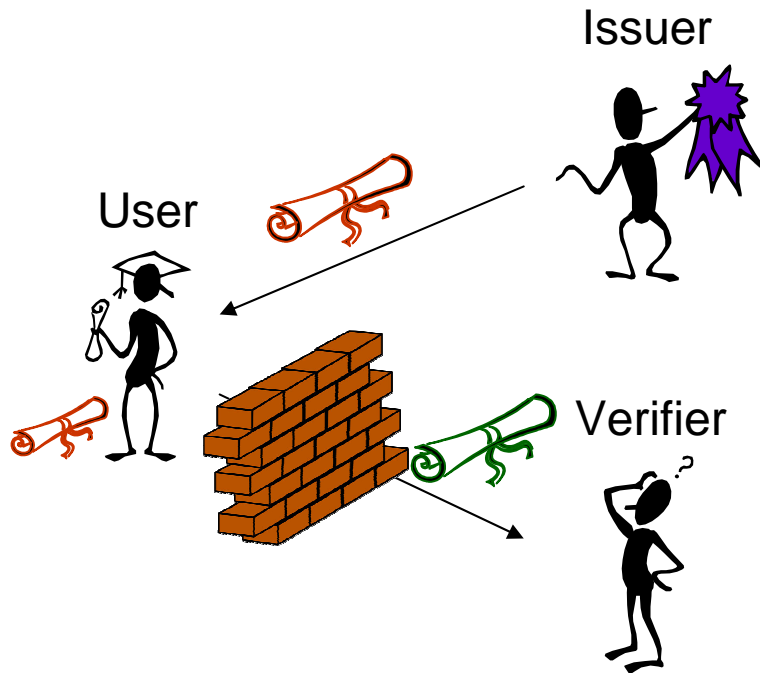



- Features of Privacy-ABCs
- Cryptographic realization
- Non-cryptographic hurdles to deployment
- Current status of Identity Mixer
- Future of Identity Mixer

Cryptographic realization



Two approaches



- Multi-use
- Damgard, Camenisch-Lysyanskaya
- 
- Strong RSA, pairings (LMRS, q-SDH)

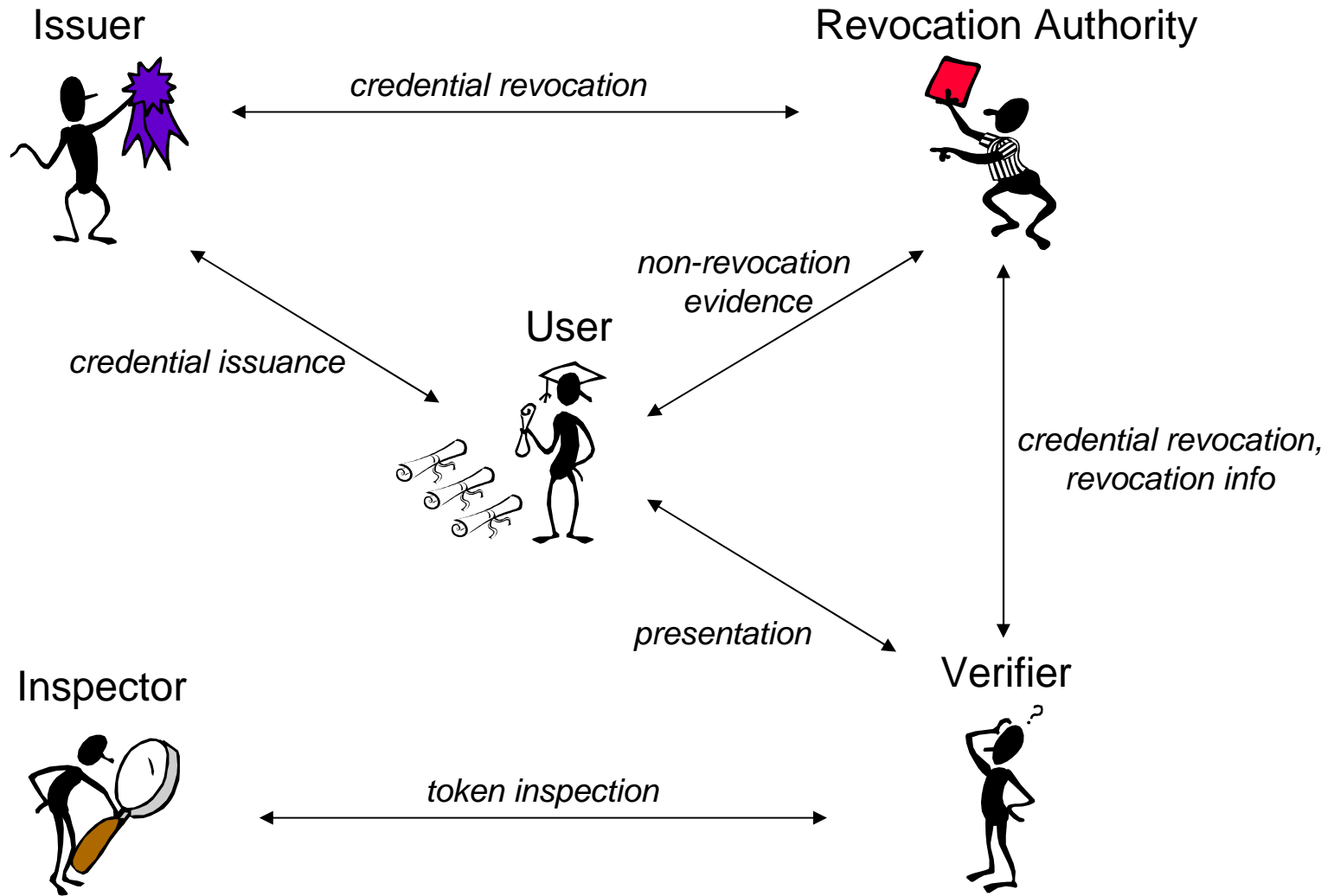
- One-time use (multi through batching)
- Chaum, Brands
- 
- Related to discrete logs, RSA,...

Overview of this talk

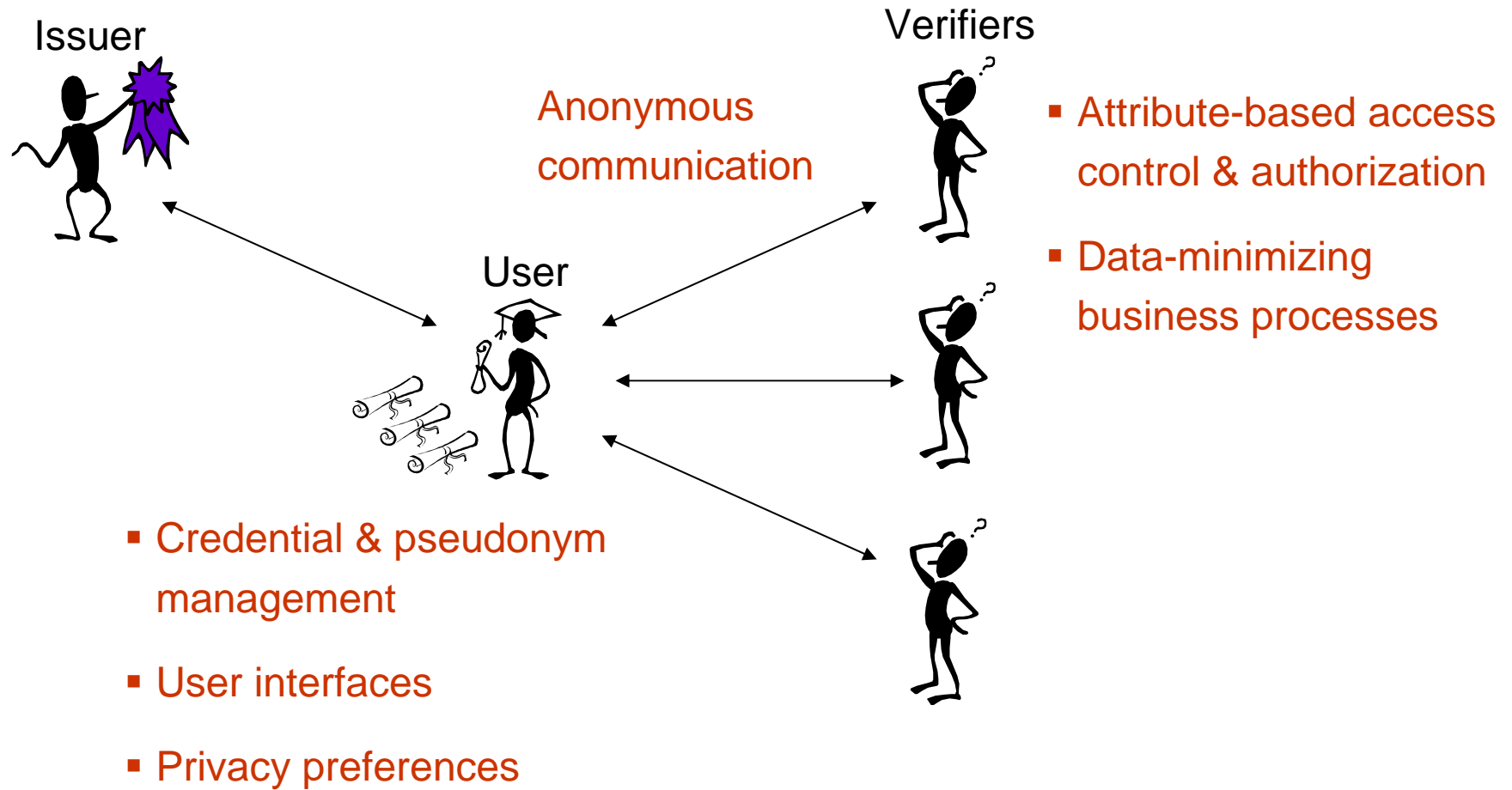


- Features of Privacy-ABCs
- Cryptographic realization
- **Non-cryptographic hurdles to deployment**
- Current status of Identity Mixer
- Future of Identity Mixer

Privacy-ABCs: the full picture



Deploying Privacy-ABCs



■ Policy languages

- which (combinations of) attributes/predicates from which credentials
- issuance, presentation, revocation, inspection,...
- hide cryptographic details from application developers

```
1 <PresentationPolicyAlternatives>
2   <PresentationPolicy PolicyUID="revealCivicNr">
3     <Message>
4       <Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</Nonce>
5     </Message>
6     <Credential Alias="schoolcred">
7       <CredentialSpecAlternatives>
8         <CredentialSpecUID>http://abc4trust.eu/wp6/credspec/credSchool
9       </CredentialSpecUID>
10      </CredentialSpecAlternatives>
11     <IssuerAlternatives>
12       <IssuerParametersUID>http://abc4trust.eu/wp6/soderhamn/IssParams/school
13     </IssuerParametersUID>
14     </IssuerAlternatives>
15     <DisclosedAttribute AttributeType=
16       "http://abc4trust.eu/wp6/credspec/credSchool/civicNr"/>
17   </Credential>
18 </PresentationPolicy>
19 </PresentationPolicyAlternatives>
```

- APIs and data formats
 - multiple entities and methods
- Public-key infrastructure for issuer parameters
- Ontologies
 - urn:mynamespace:firstname [?] = urn:yournamespace:givenname
- Credential backup & revocation
- Securing layers below
 - cookies, browser history
 - IP addresses, traffic analysis
 - device fingerprinting
- Integration into access control frameworks
- Standardization

Technical hurdles to deployment

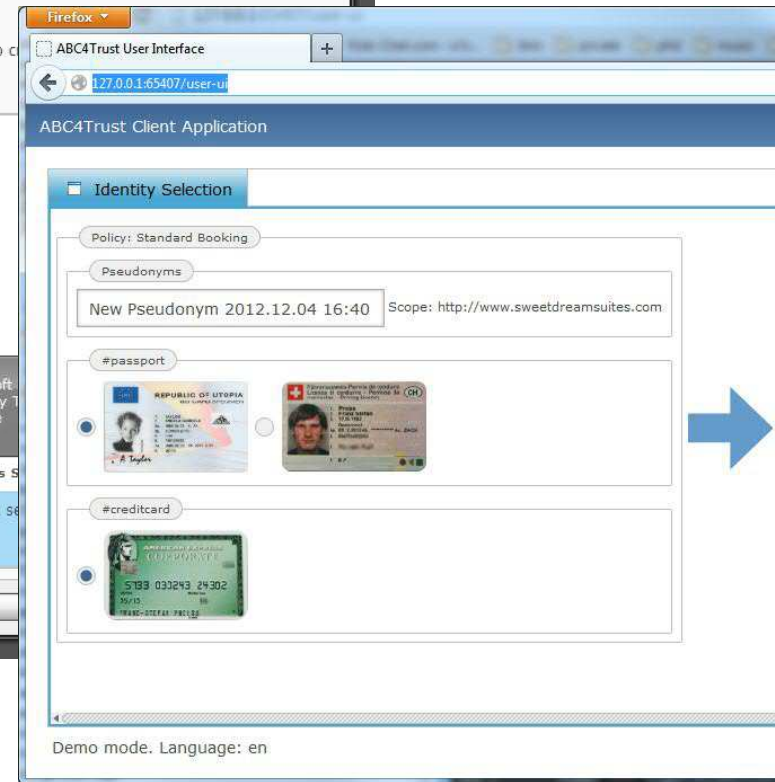
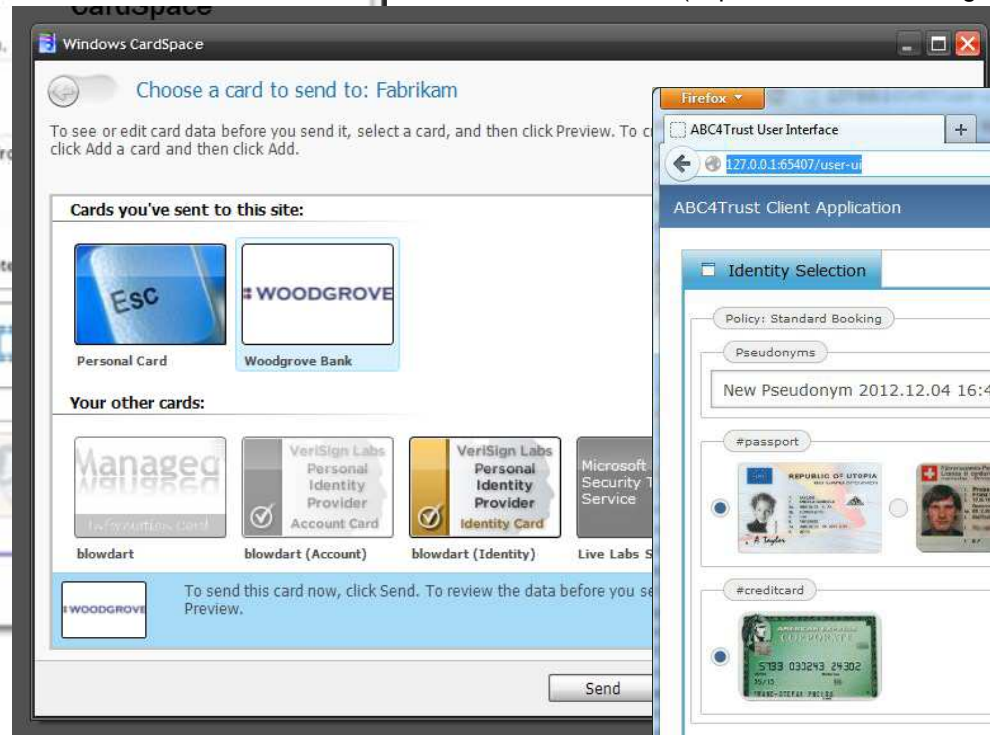


■ User interfaces

Source: Paul Trevithick (<http://www.incontextblog.com>)



Source: Paul Trevithick (<http://www.incontextblog.com>)



Non-technical hurdles to deployment



- Business case: who pays for privacy?
 - companies have inverse incentive (data mining)
 - government/legal incentives: regulation, fines, class-action lawsuits
 - German eID has privacy features
 - no issuers because no verifiers – and vice versa
 - cfr. SSL: market enabler

- Education
 - end users (create demand)
 - developers, industry leaders,...
 - paradoxical features challenge intuition
 - confusing crypto terminology (e.g., zero knowledge, witness,...)

- Legal issues
 - crypto is highly patented
 - software licenses

Overview of this talk



- Features of Privacy-ABCs
- Cryptographic realization
- Non-cryptographic hurdles to deployment
- **Current status of Identity Mixer**
- Future of Identity Mixer

Current status



- More research papers than can fit on this slide ☺
- <http://www.zurich.ibm.com/security/idemix/>

- EU projects



- Open-source code
 - Core crypto library: <https://prime.inf.tu-dresden.de/idemix/>
 - Credential-based policy engine:
<http://primelife.ercim.eu/results/opensource/140-abcauth>
 - ABC4Trust reference implementation: <https://abc4trust.eu> (soon)
- ABC4Trust pilots
 - Patras University: student course evaluation
 - Soderhamn high school: pupil interaction & counselling

Overview of this talk



- Features of Privacy-ABCs
- Cryptographic realization
- Non-cryptographic hurdles to deployment
- Current status of Identity Mixer
- **Future of Identity Mixer**

What the future may bring



- Standards: policy languages, cryptographic formats
 - ISO: SC17/18013 and SC27
 - OASIS: SAML Attribute predicate profile
- Better user interfaces
- Deploy Identity Mixer for eID, toll roads, public transportation
- Quantum-resistant Privacy-ABCs