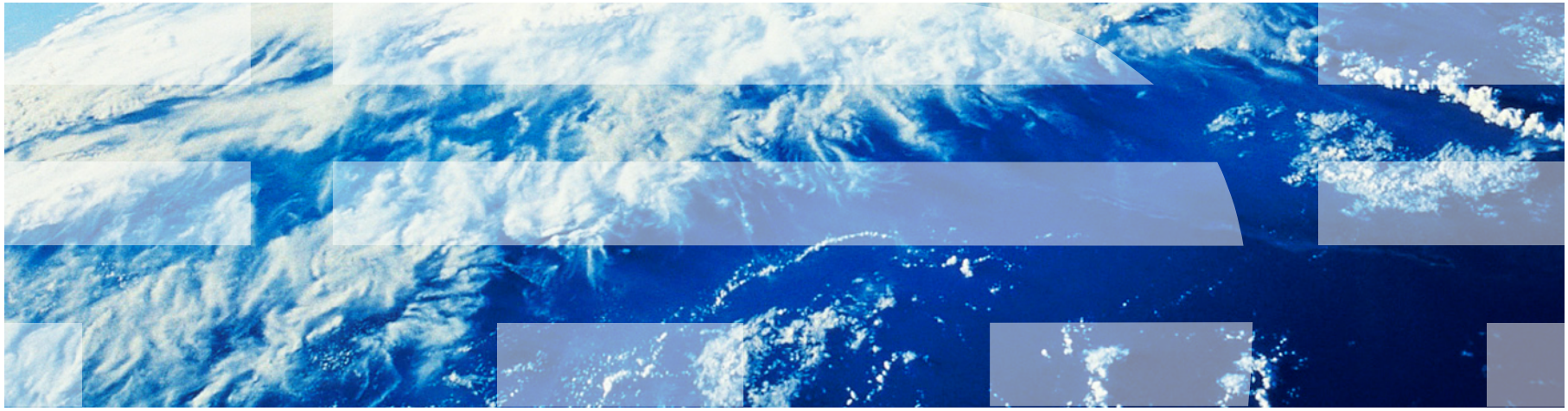
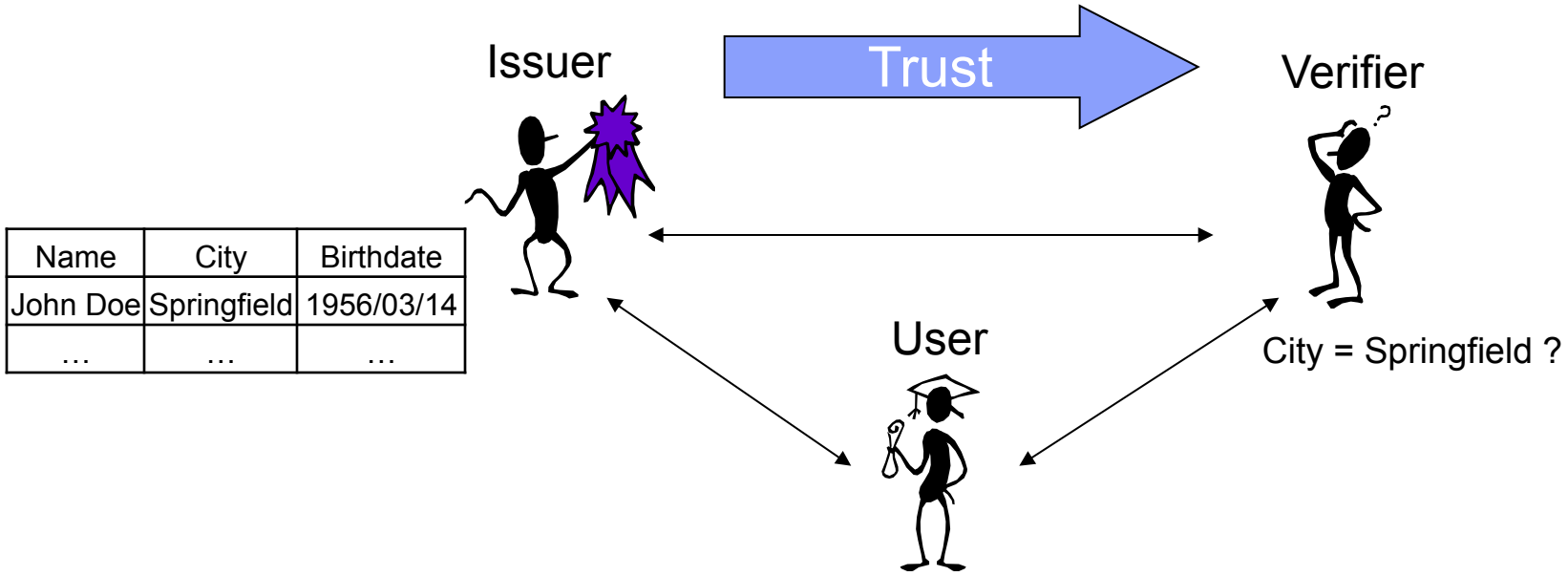
Features and concepts of Privacy-ABCs



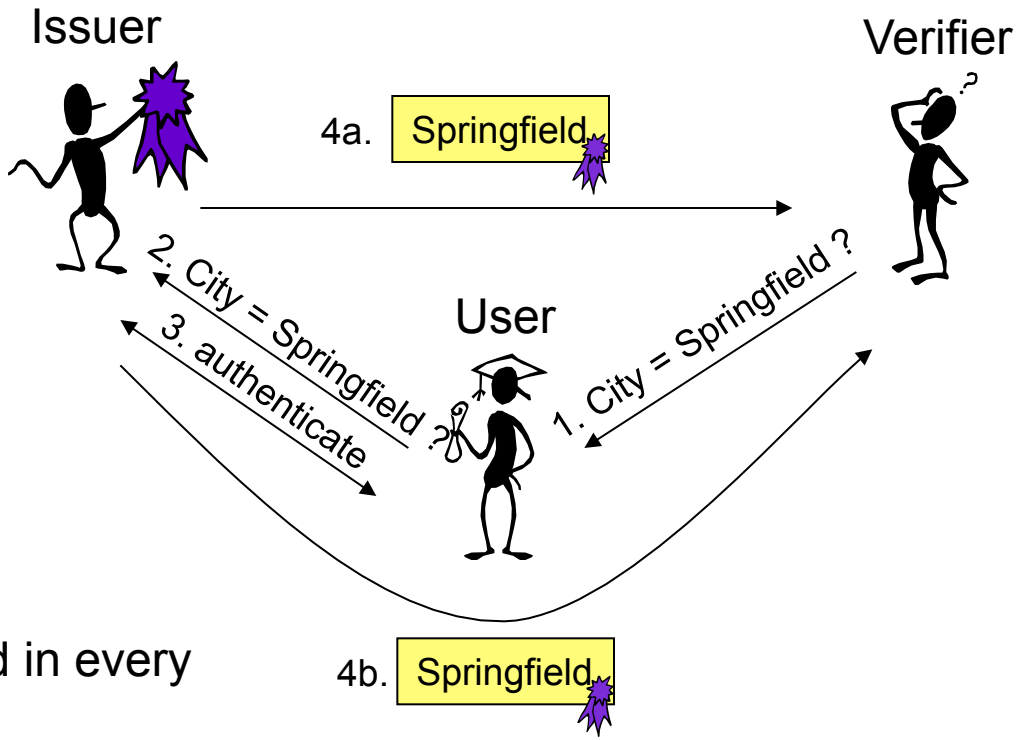
Gregory Neven, IBM Research – Zurich

Trusted attribute transfer



Existing solutions with online issuer

e.g., SAML, WS-Federation, OpenID,
Facebook Connect,…

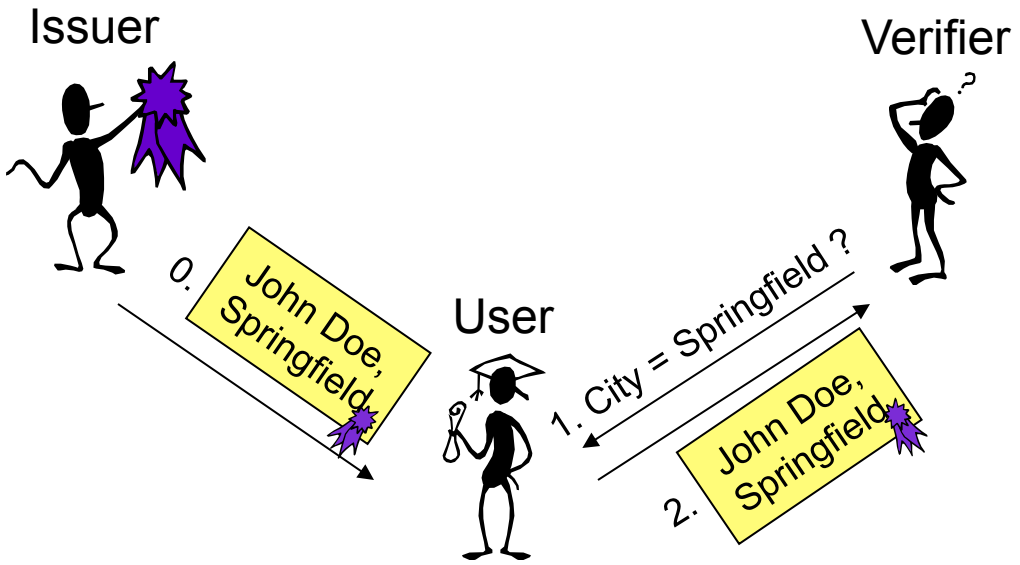


Privacy & security risks:

- Big Brother Issuer: involved in every transaction
- User linkable across verifiers (usually)
- User database & issuance key on online server

Existing solutions with offline issuer

e.g., X.509 v3 certificates

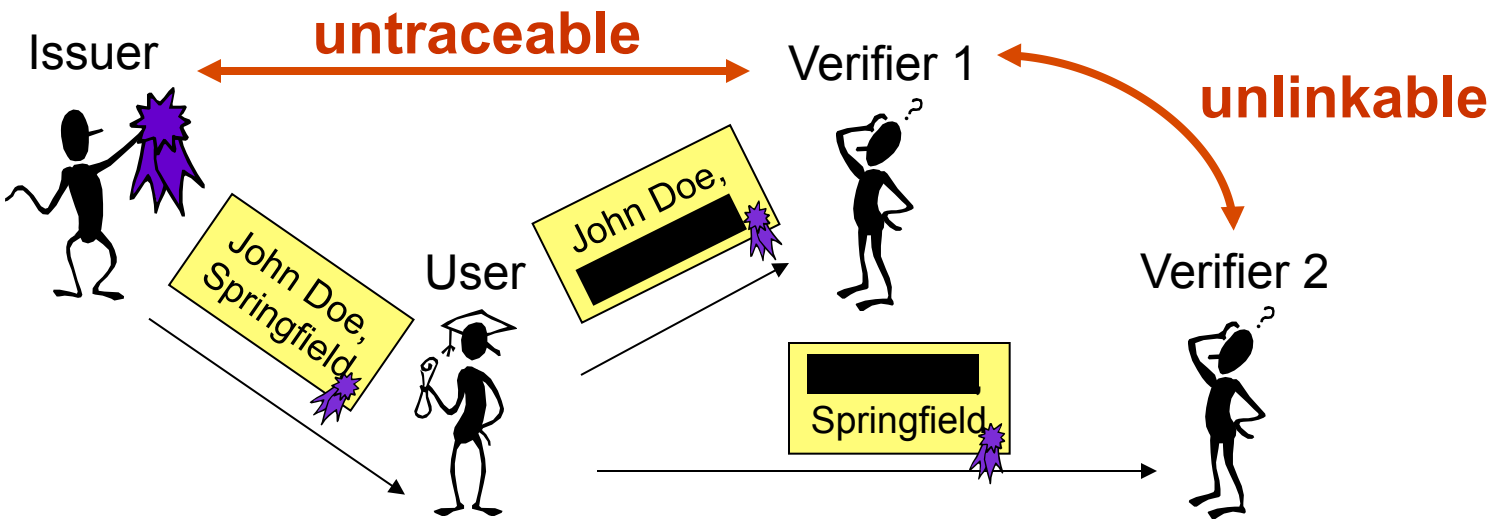


Privacy risks:

- Always reveal full attributes
- Linkable across verifiers by certificate

Privacy-ABCs

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



Features of Privacy-ABCs

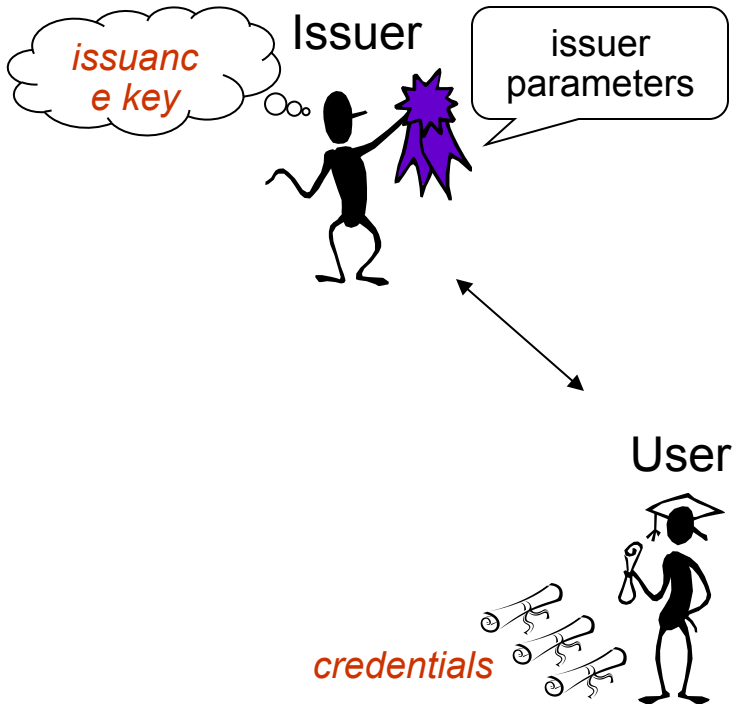
In this talk:

- Credential issuance
- Presentation & pseudonyms
- Inspection
- Revocation

Credential issuance

Credential

- list of attribute-value pairs
- certified by issuer
- Advanced issuance:
  - blindly issued attributes
  - carried-over attributes

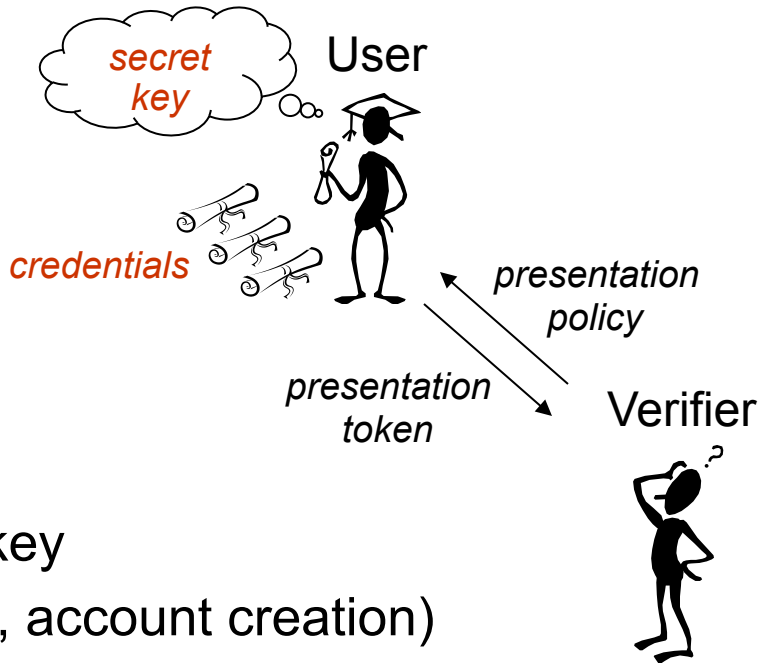


Presentation

Presentation policy (token) requests (reveals)

- selected attributes from credential(s)
- predicates over attributes

  attribute_1 =,>,< attribute_2 or constant
- *pseudonyms*
  - ≈ unlinkable public keys for user's secret key
  - – intentionally create limited linkability (e.g., account creation)
  - – *scope-exclusive* pseudonym: unique yet unlinkable



Inspection & revocation

Inspection

- Attribute value encrypted to trusted inspector
- Token bound to *inspection grounds*: conditions to decrypt
- E.g., de-anonymization in case of abuse

Revocation

- Render credentials unusable for presentation
- E.g., credential compromise, changed attributes

Conclusion

- Privacy by default
  - Unlinkable authentication
  - Selective attribute disclosure
  - Attribute predicates
- Linkability/identification when required
  - Pseudonyms
  - Inspection
- Easy integration into applications
  - XML schema specifications
  - Web service APIs
  - Open-source (EPL) implementation: https://github.com/p2abcengine
- Learn more
  - http://www.abc4trust.eu
  - Longer talk in Track 7 (eAuthentication)