Introduction to Privacy-Enhancing Attribute-Based Credentials

Anja Lehmann (IBM Research – Zurich)

ABC4Trust 1st Reference Group Meeting, Zurich, February 13, 2012

A research project funded by the European Commission's 7th Framework Programme

SEVENTH FRAMEWORK PROGRAMME

Outline

- Motivation & Existing Solutions
- Concepts and Features of Privacy-ABCs
  - Basic Functionality
  - Advanced Features
    - Pseudonyms & Key-Binding
    - Advanced Issuance
    - Revocation
    - Inspection
  - Examples: Idemix & U-Prove

Outline

Online security & trust today:

- SSL/TLS does encryption and server-side authentication
- Client-side authentication by username-password
- Mostly self-claimed attributes

Alternative approaches exist

- e.g., SAML, OpenID, Facebook Connect, X.509…

… but have privacy and security issues

User-Authentication

Issuer

I am Alice Doe
and I'm over 18!

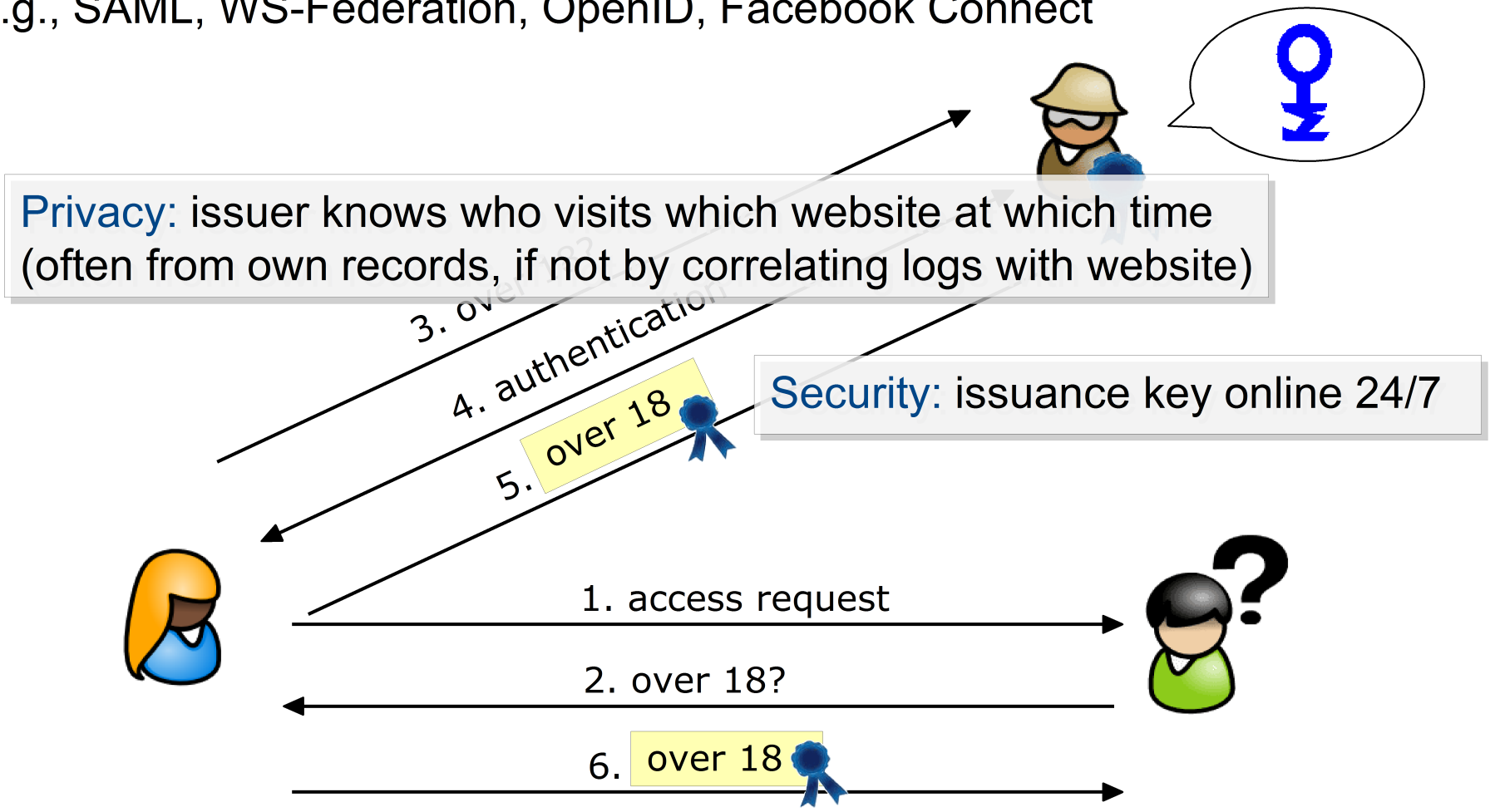
Convince me!
btw … I trust the Issuer

User

Verifier

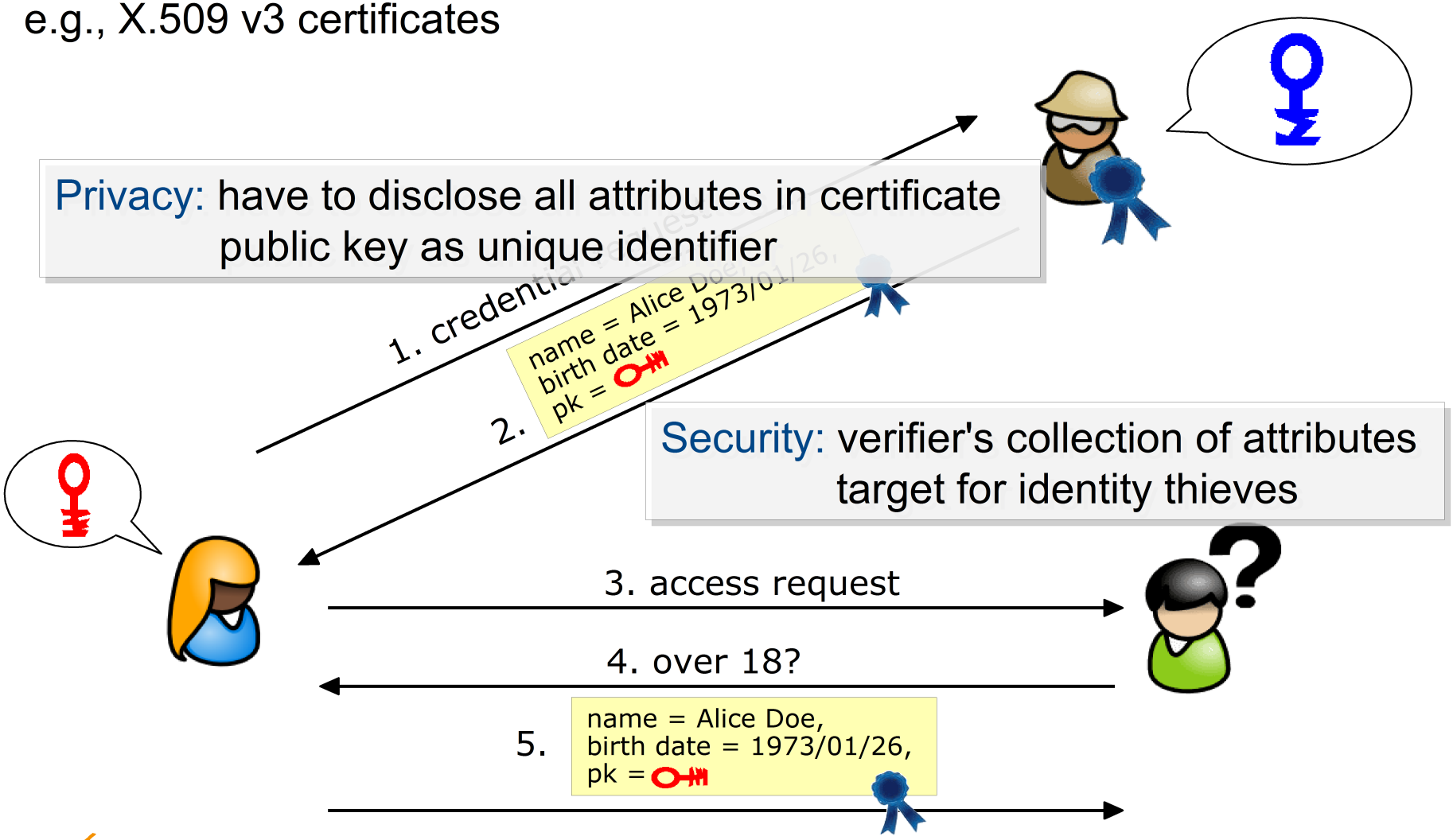
Authentication – Online Solution

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



Authentication – Offline Solution

e.g., X.509 v3 certificates



Privacy-Enhancing Attribute Based Credentials

best of both worlds

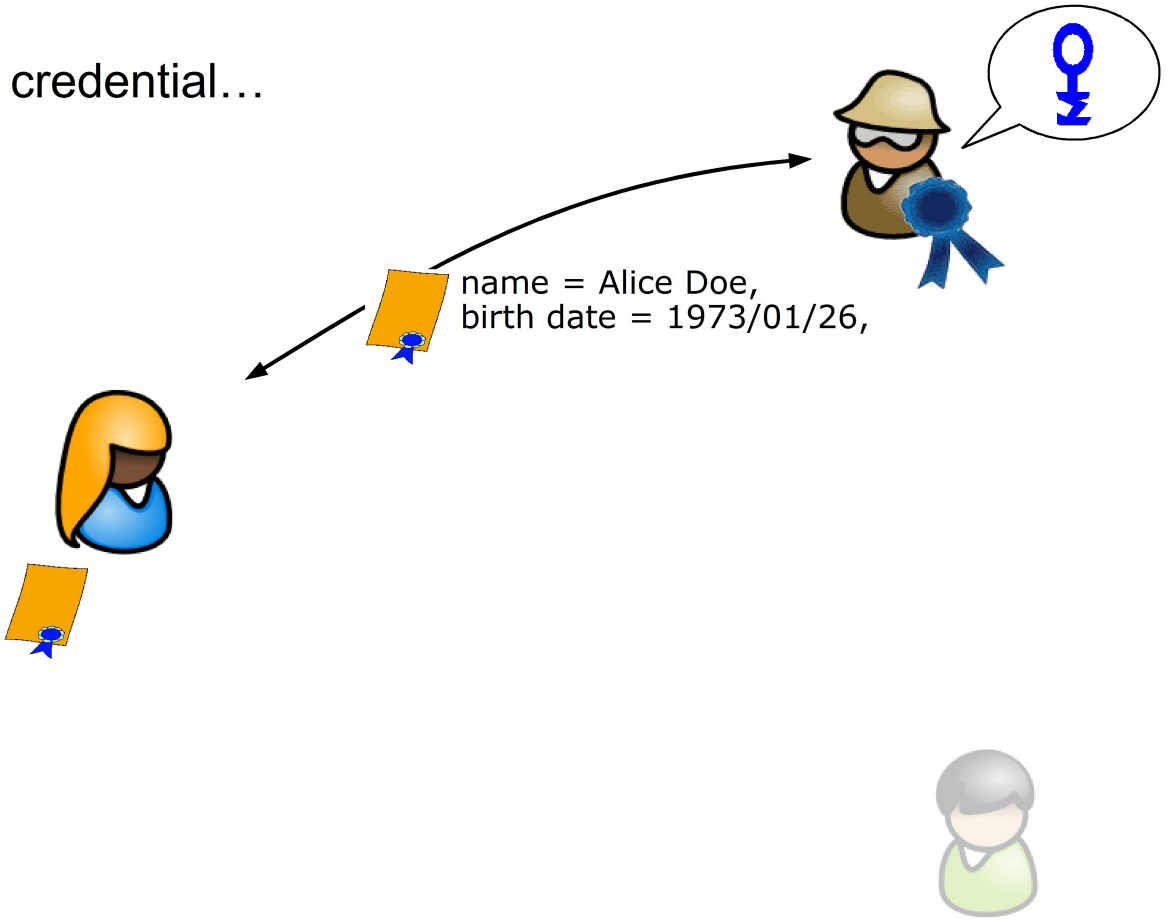
- Privacy: unlinkable transactions,
  minimal information disclosure
- Security: offline issuer
- e.g., Identity Mixer, U-Prove, pairing-based scheme

- Contribution of ABC4Trust
  - unified view on concept & features of Privacy-ABCs
  - common architecture for (Privacy)-ABCs
  - common dataformats for the entire life-cycle of Privacy-ABCs

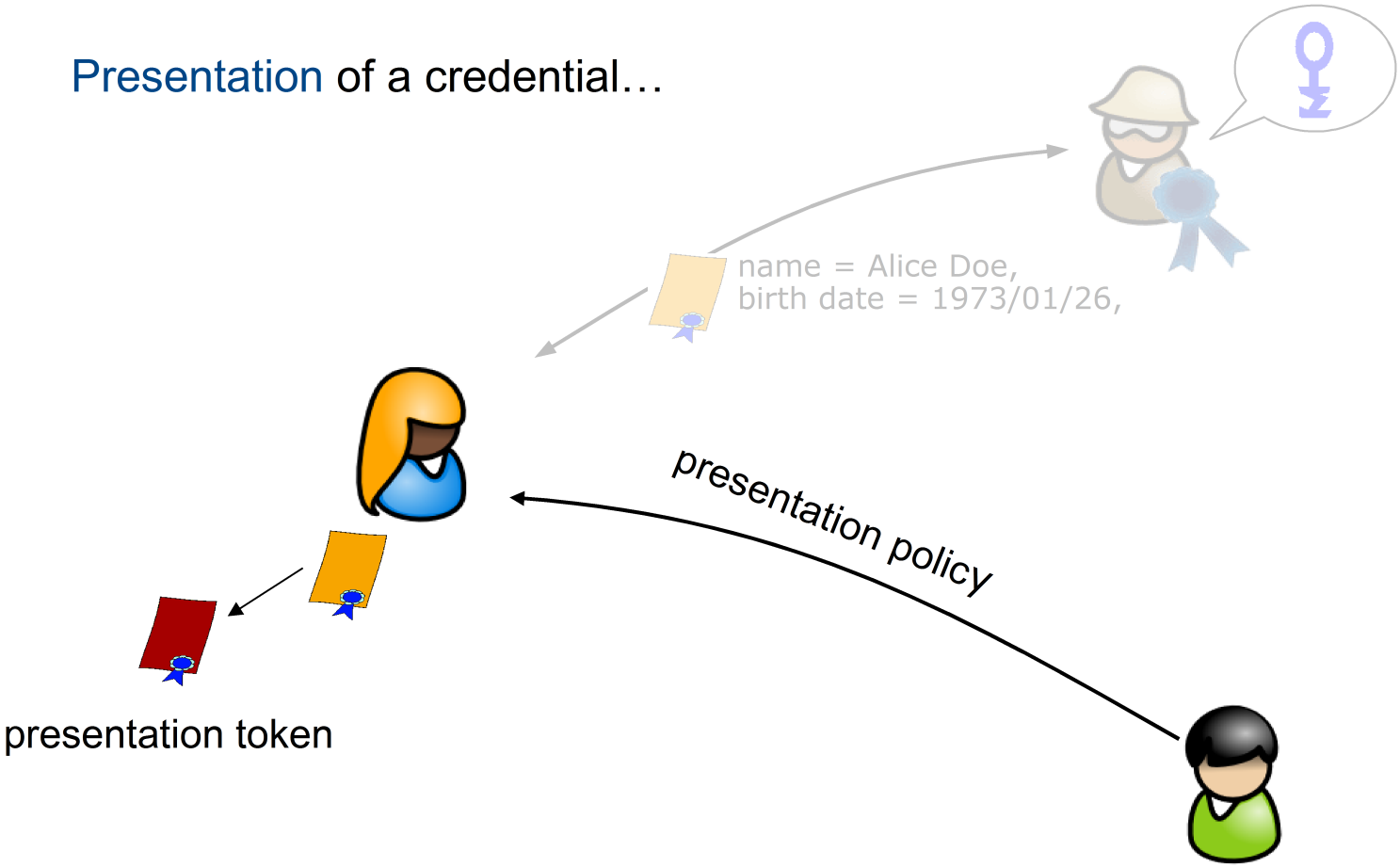
Features & Concepts of Privacy-ABCs

Basic Functionality

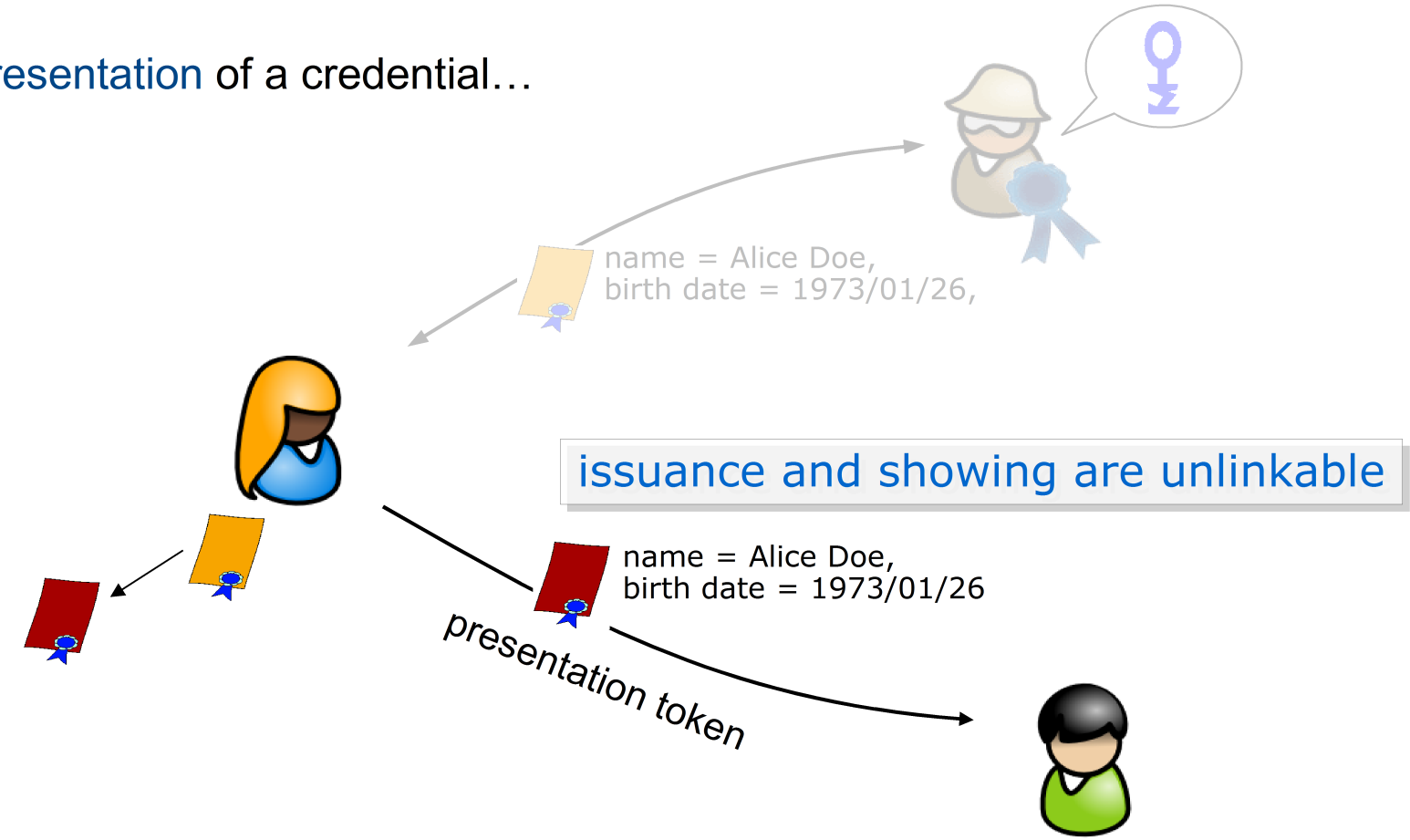
Obtaining a credential…



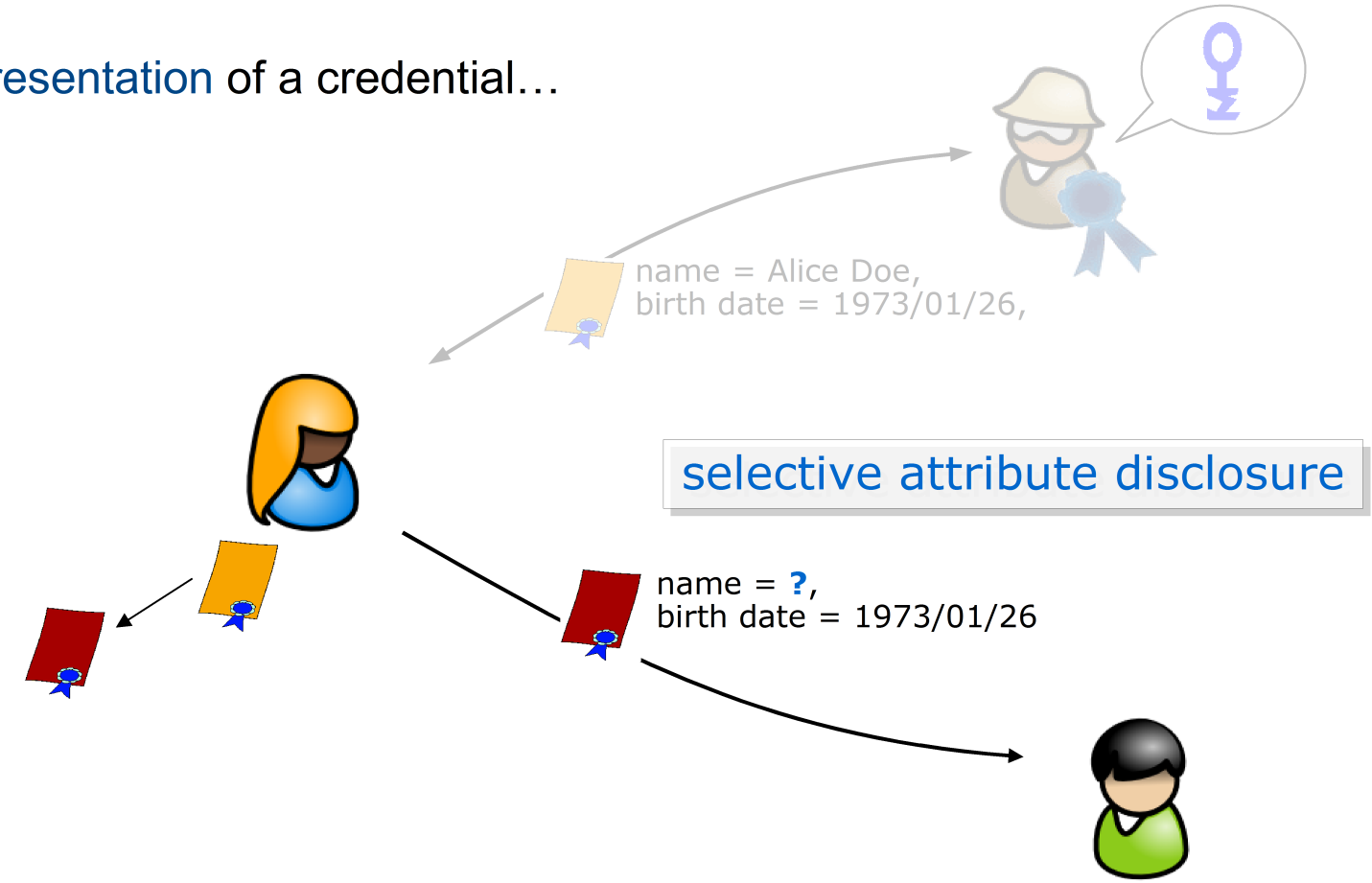
Presentation of a credential…



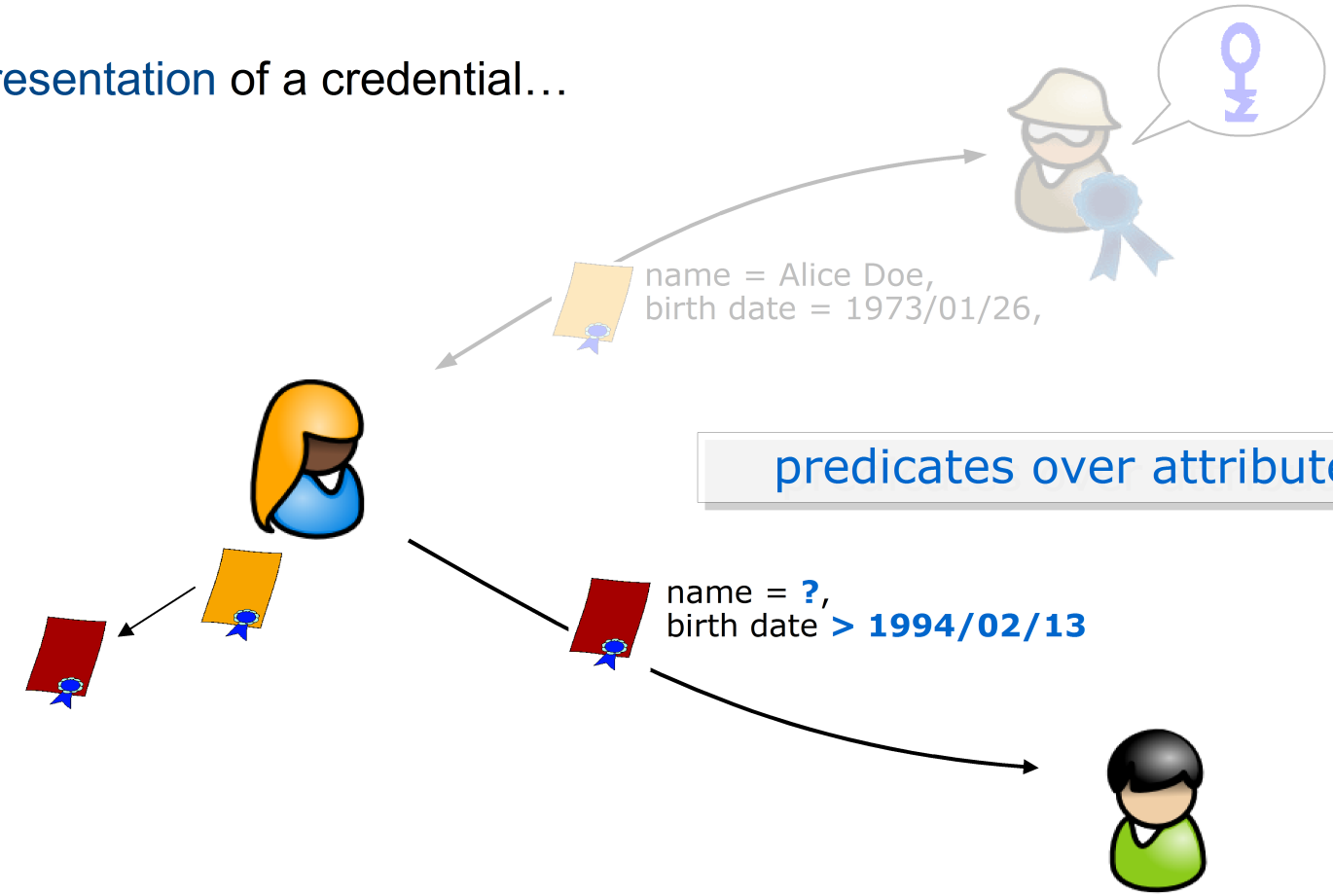
Presentation of a credential…



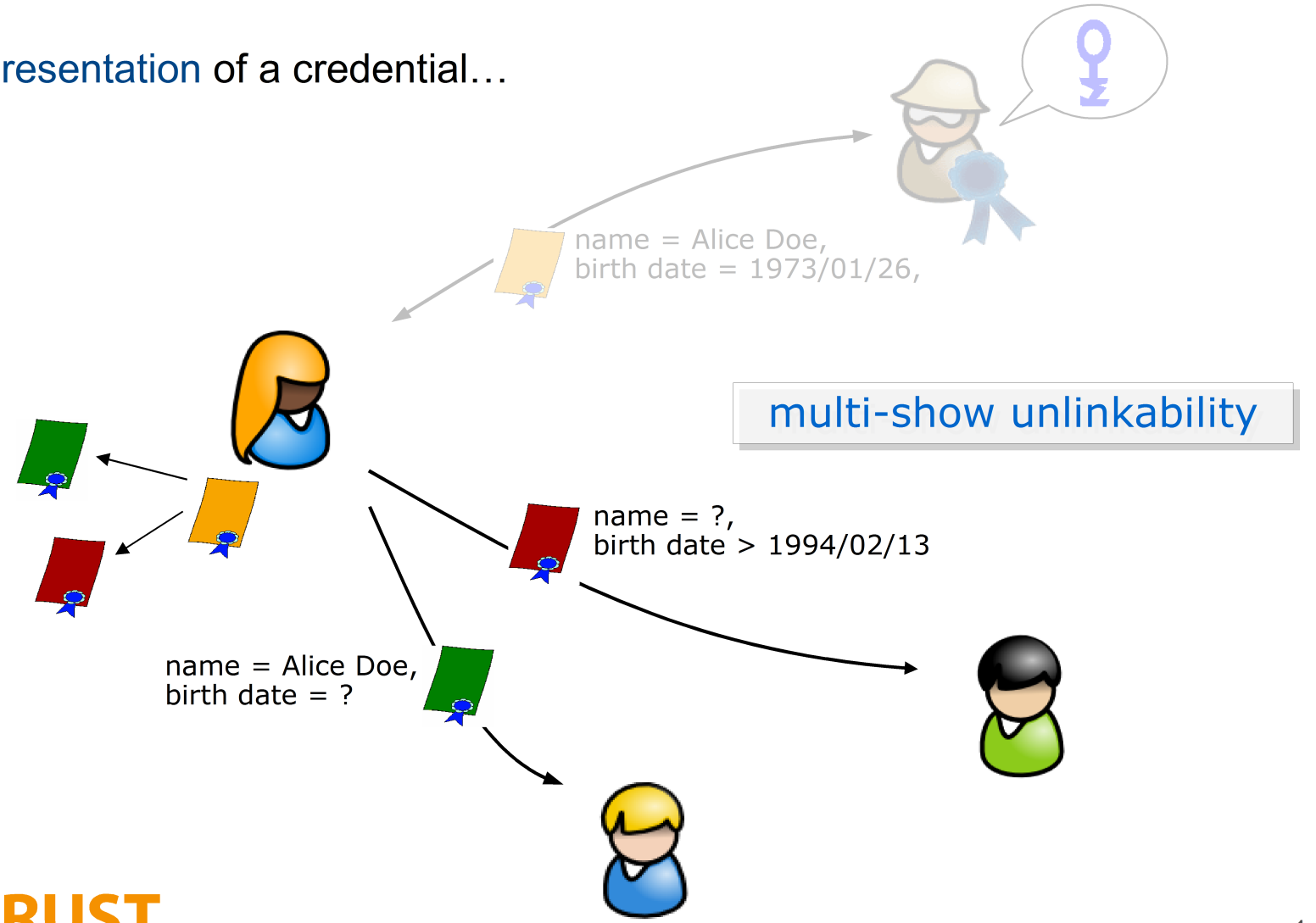
Presentation of a credential…



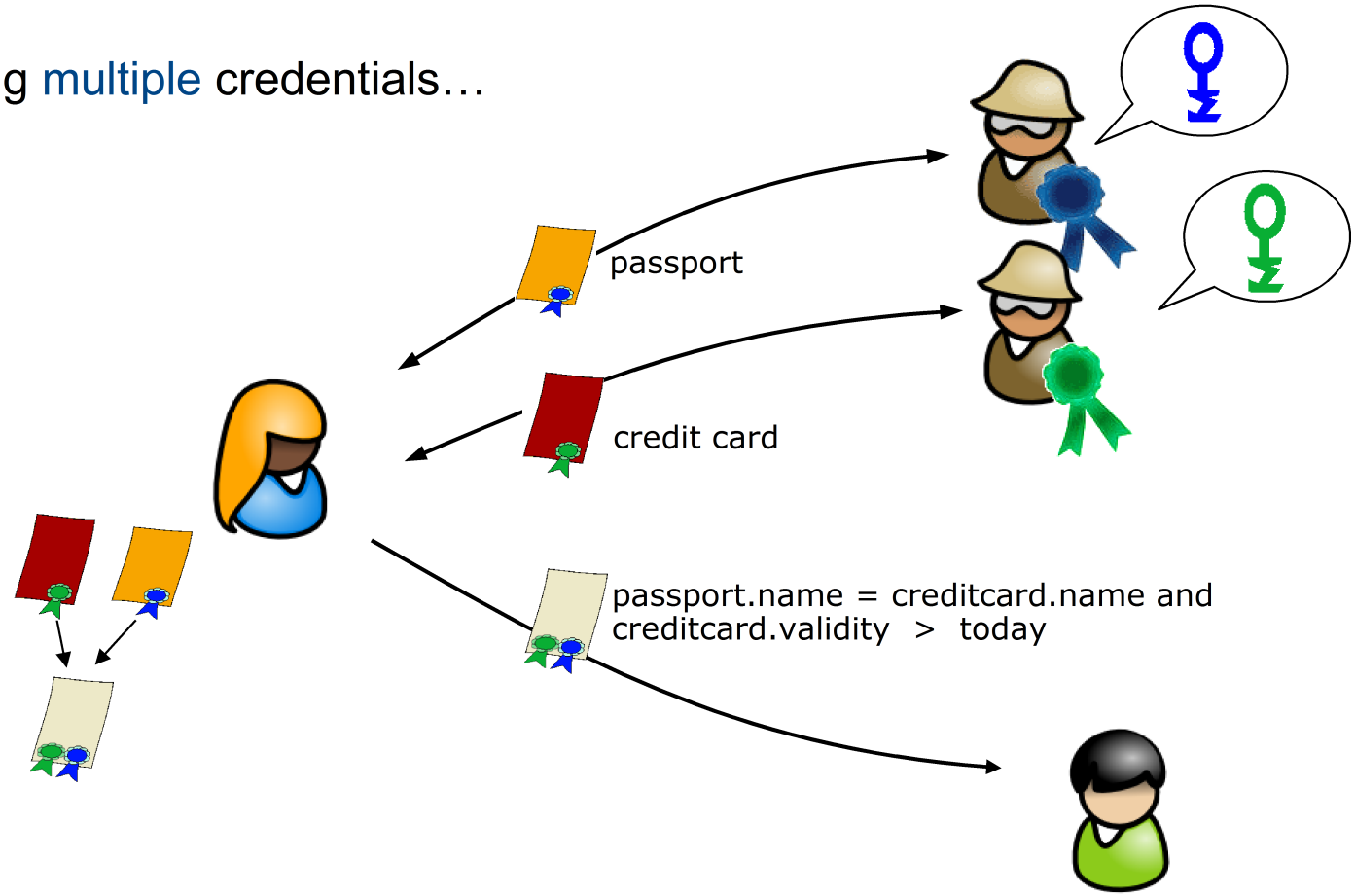
Presentation of a credential…

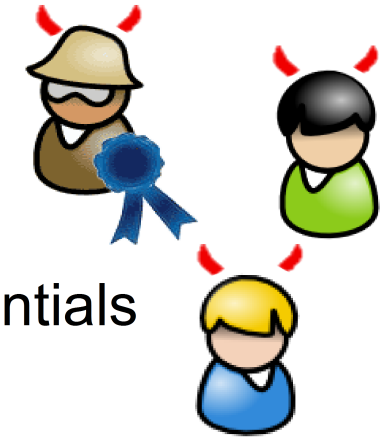


Presentation of a credential…

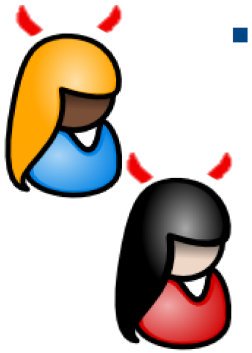


Using multiple credentials…



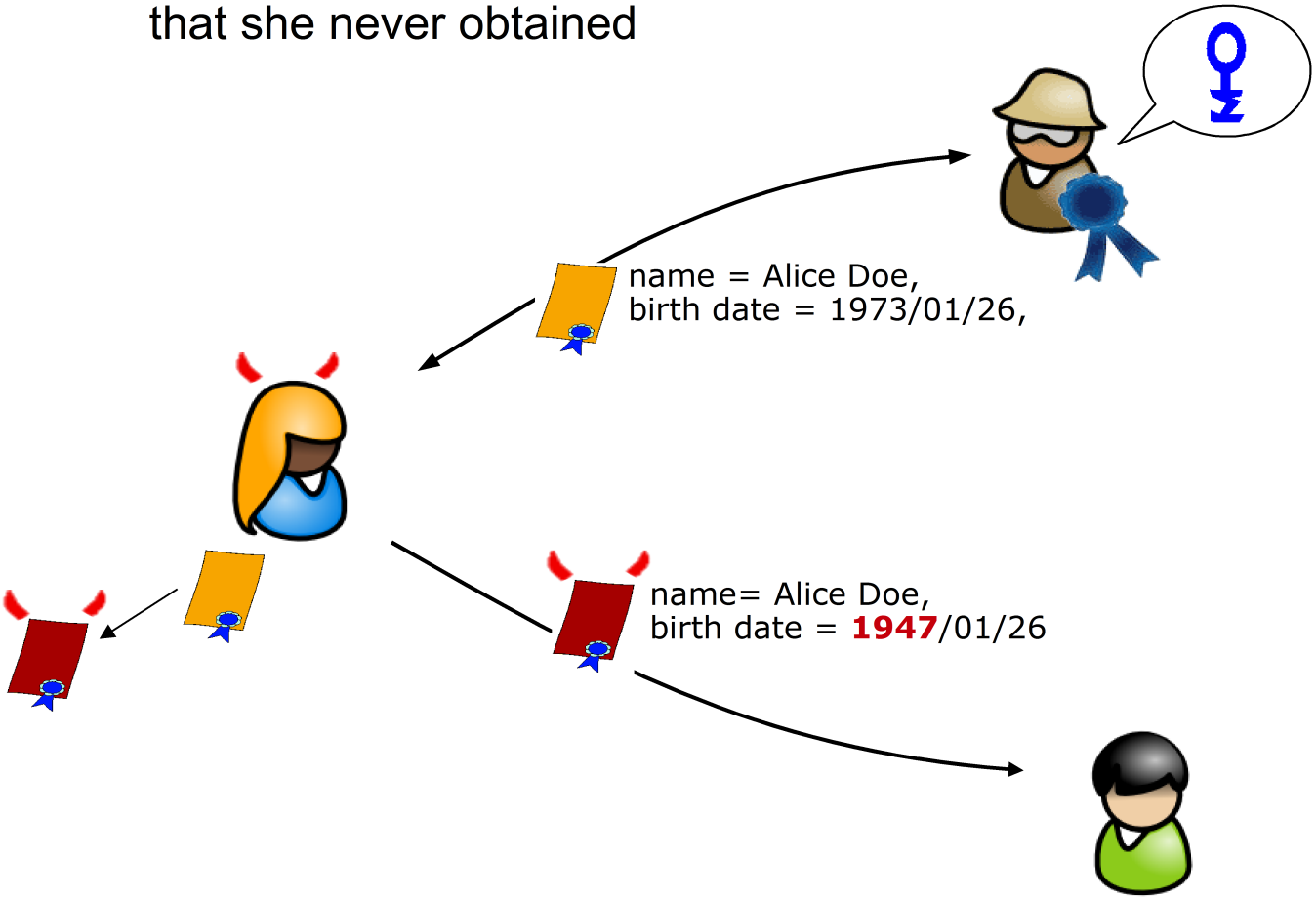


- Protection of user's privacy
  - unlinkability (multi-use)
  - using/combining multiple credentials
  - selective disclosure
  - predicated over attributes



- Strong authentication
  - unforgeability of presentation tokens

Unforgeability: Alice should not be able to show a token for a credential that she never obtained

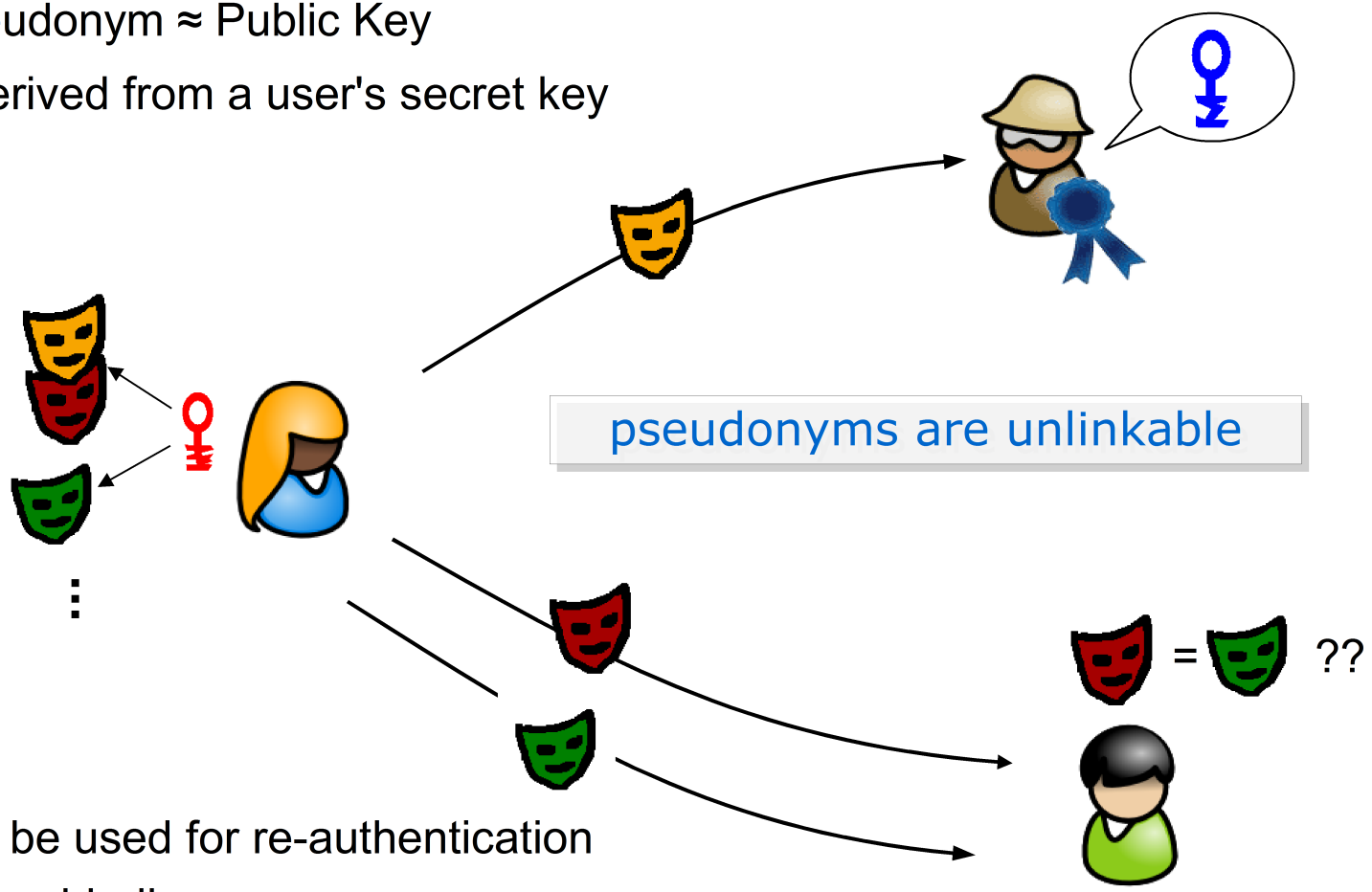


there is more ....

- Pseudonyms & Key Binding
- Advanced Issuance
- Revocation
- Inspection
- ...

Pseudonym ≈ Public Key

- derived from a user's secret key

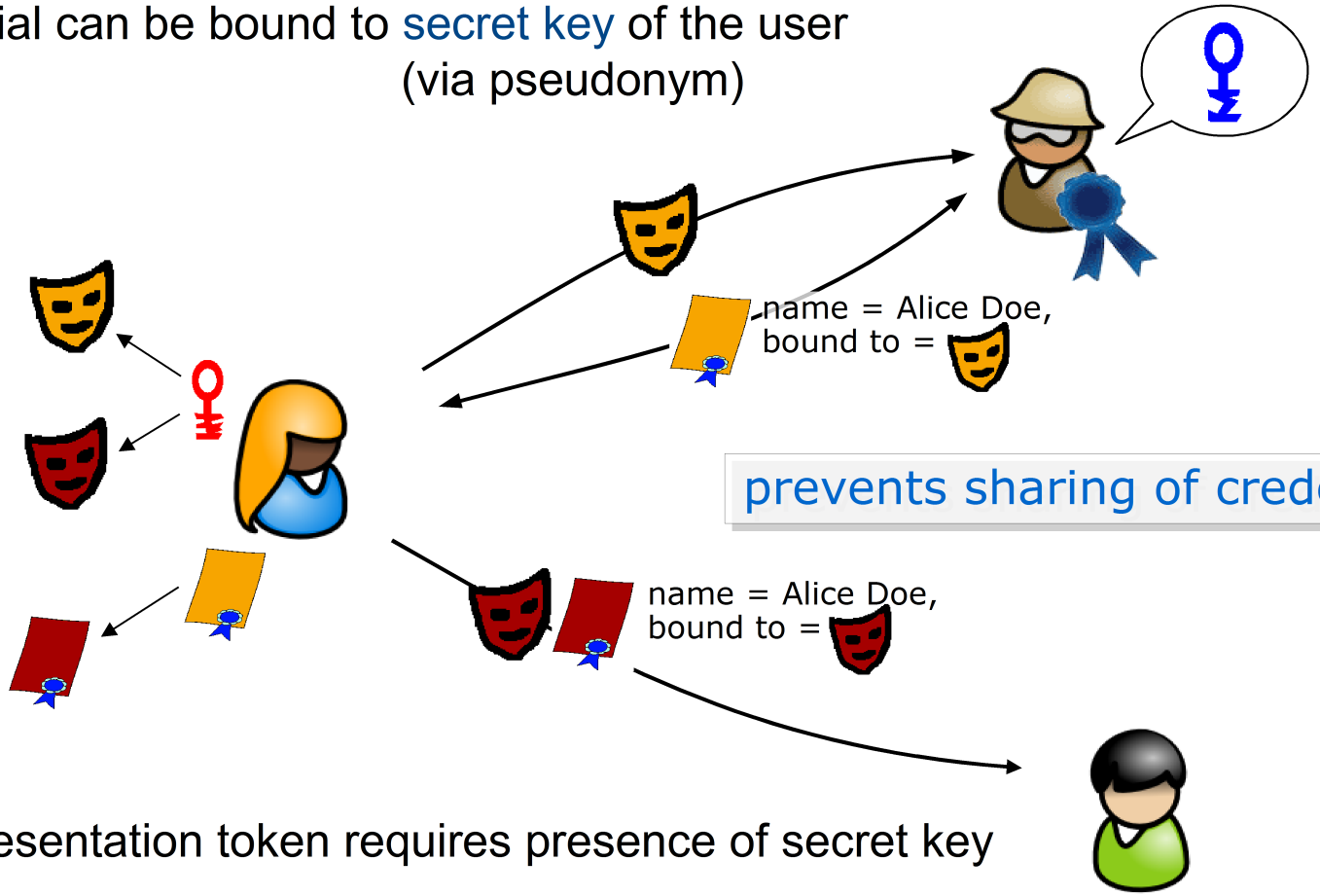


can be used for re-authentication

or key binding ...

Privacy-ABCs | Key Binding

credential can be bound to secret key of the user
(via pseudonym)

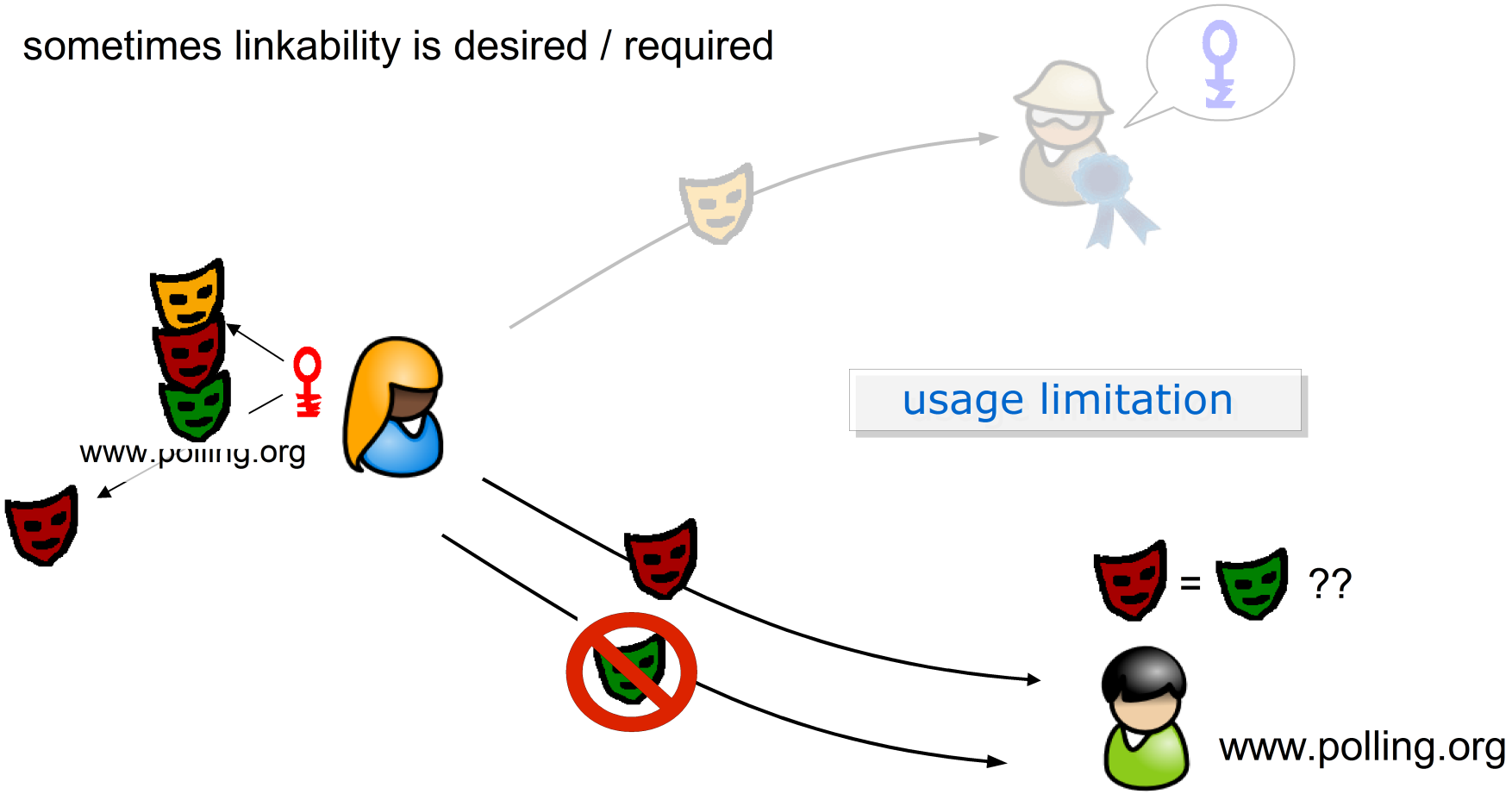


prevents sharing of credentials

presentation token requires presence of secret key

Privacy-ABCs | Scope-Exclusive Pseudonyms

sometimes linkability is desired / required

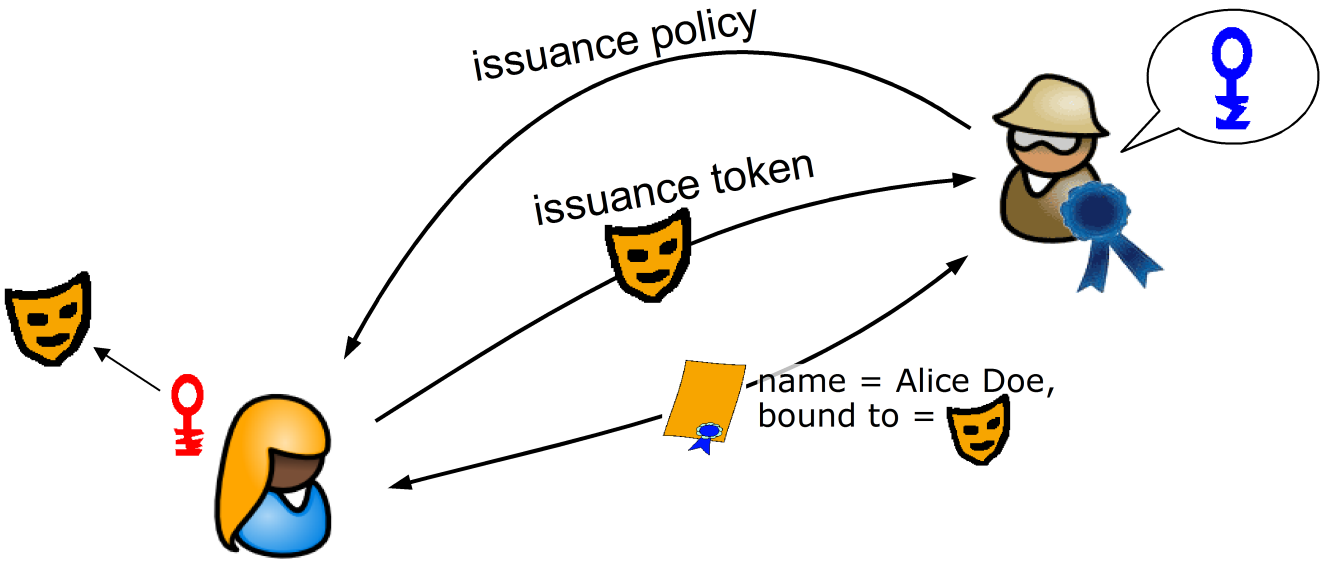


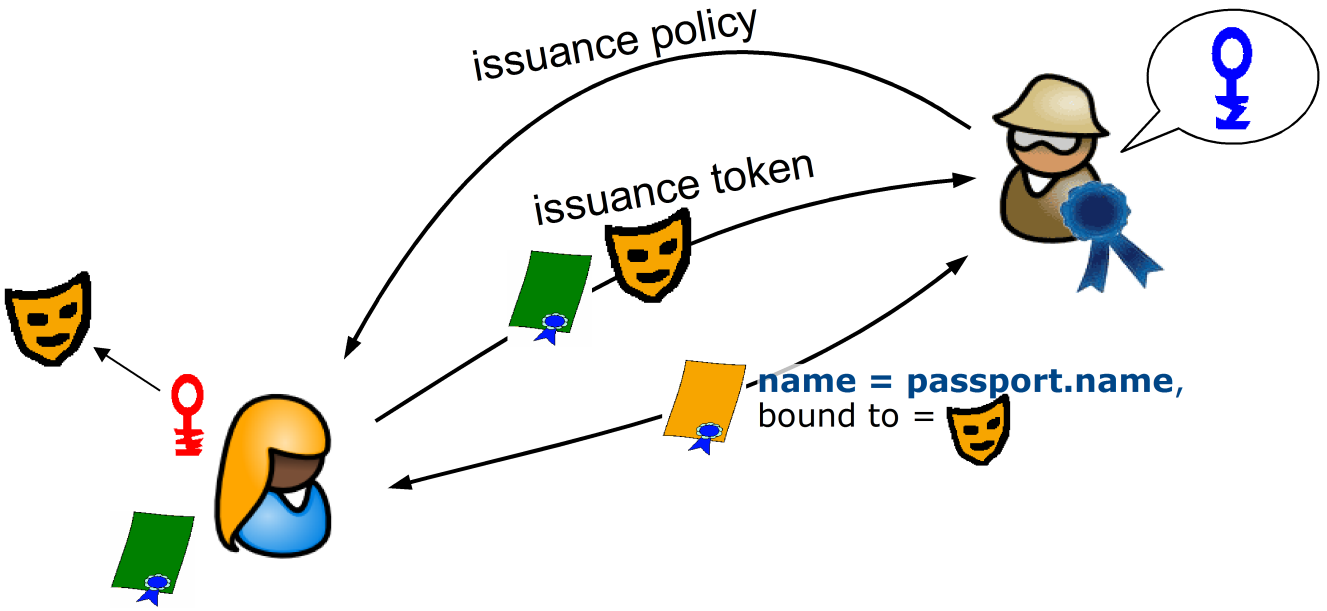
scope-exclusive pseudonym = unique for each scope

there is more ....

- Key Binding & Pseudonyms
- Advanced Issuance
- Revocation
- Inspection
- ...

- so far: Issuance "from scratch"
  - Issuer knows all the attributes he is certifying
- advanced issuance:
  - issued credentials contain attributes that are hidden from the Issuer


issuance policy
issuance token
name = Alice Doe,
bound to =



- key binding
- carried-over attributes
- jointly random attributes
  - ▸ Issuer doesn't learn the attributes

there is more ....

- Key Binding & Pseudonyms
- Advanced Issuance
- Revocation
- Inspection
- ...

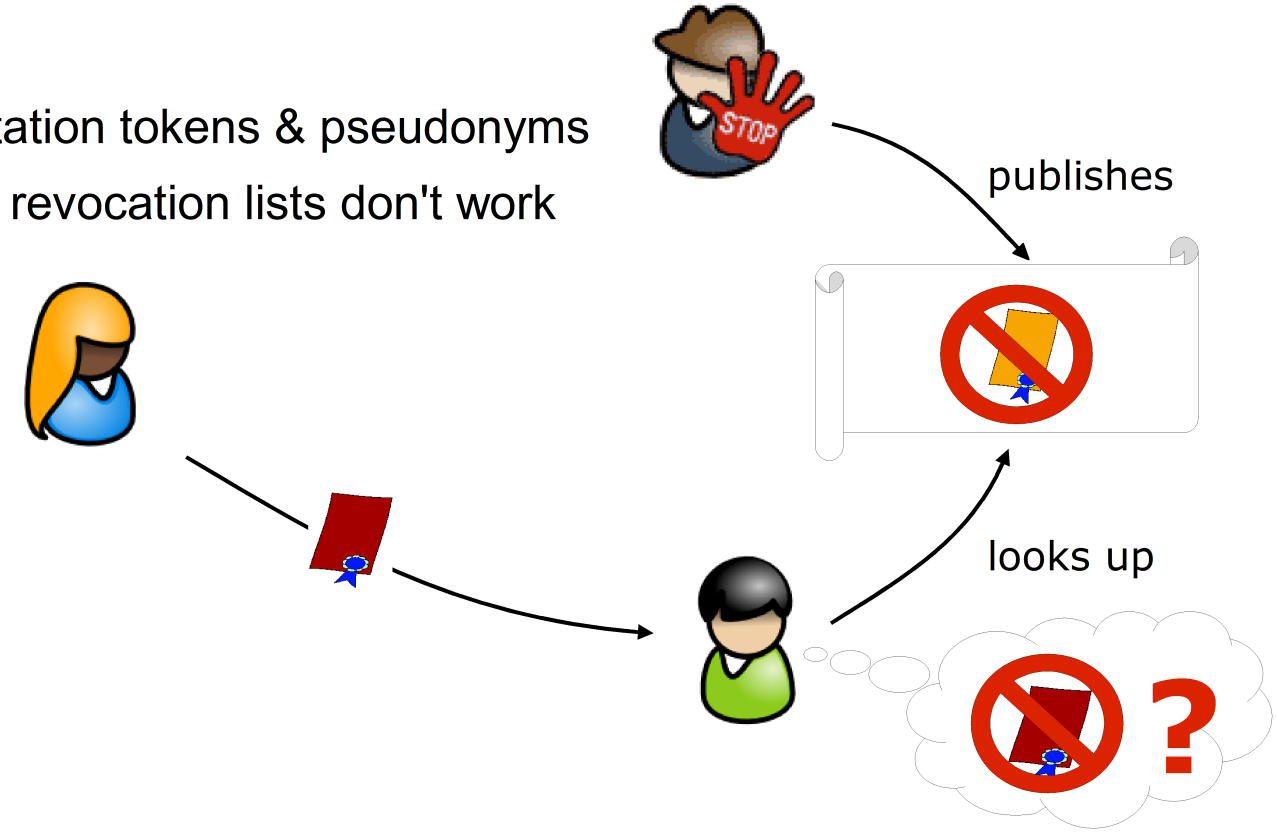
Privacy-ABCs | Revocation

various reasons to revoke a credential

- user lost credential / secret key
- misbehavior of user

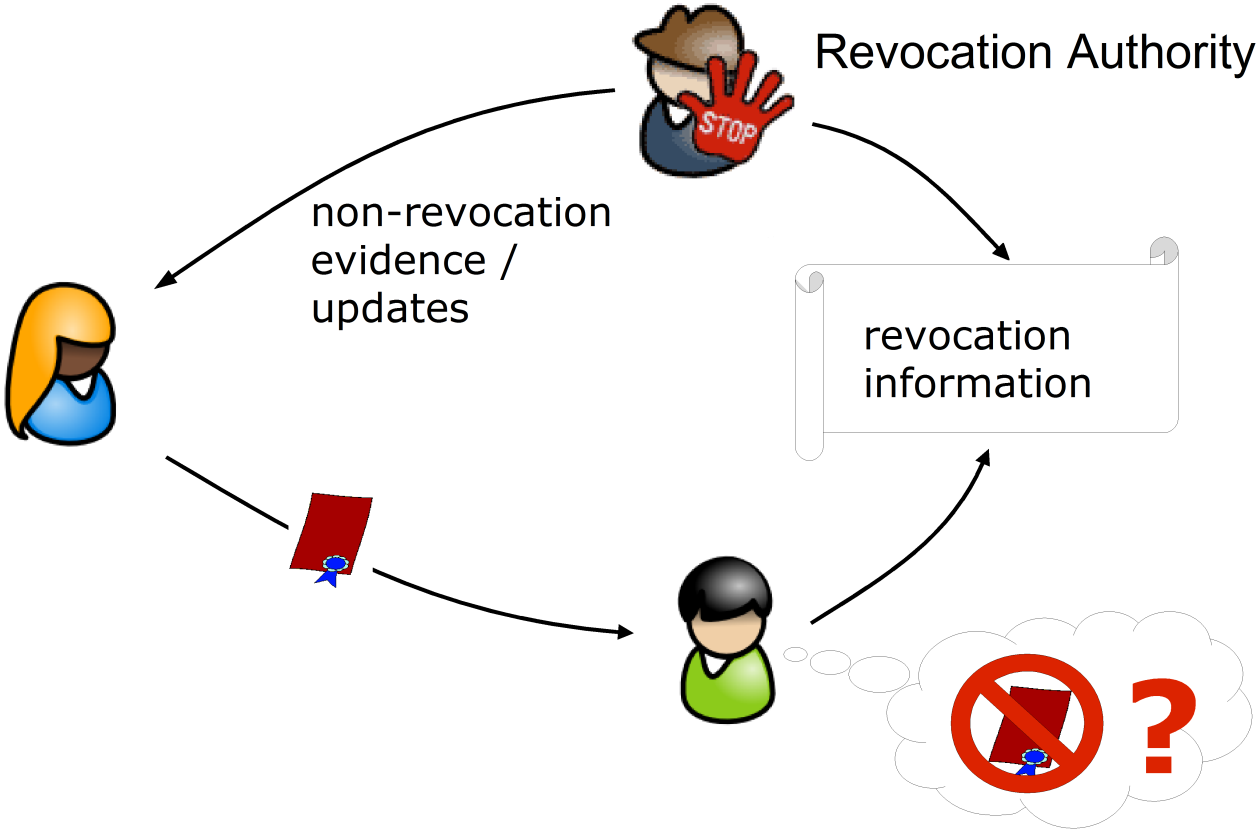
unlinkable presentation tokens & pseudonyms

→ standard revocation lists don't work



Cryptography to the rescue

- privacy-friendly revocation mechanisms (white list or black list)
- prove that user's credential is (or is not) on list



Who specifies the Revocation Authority?

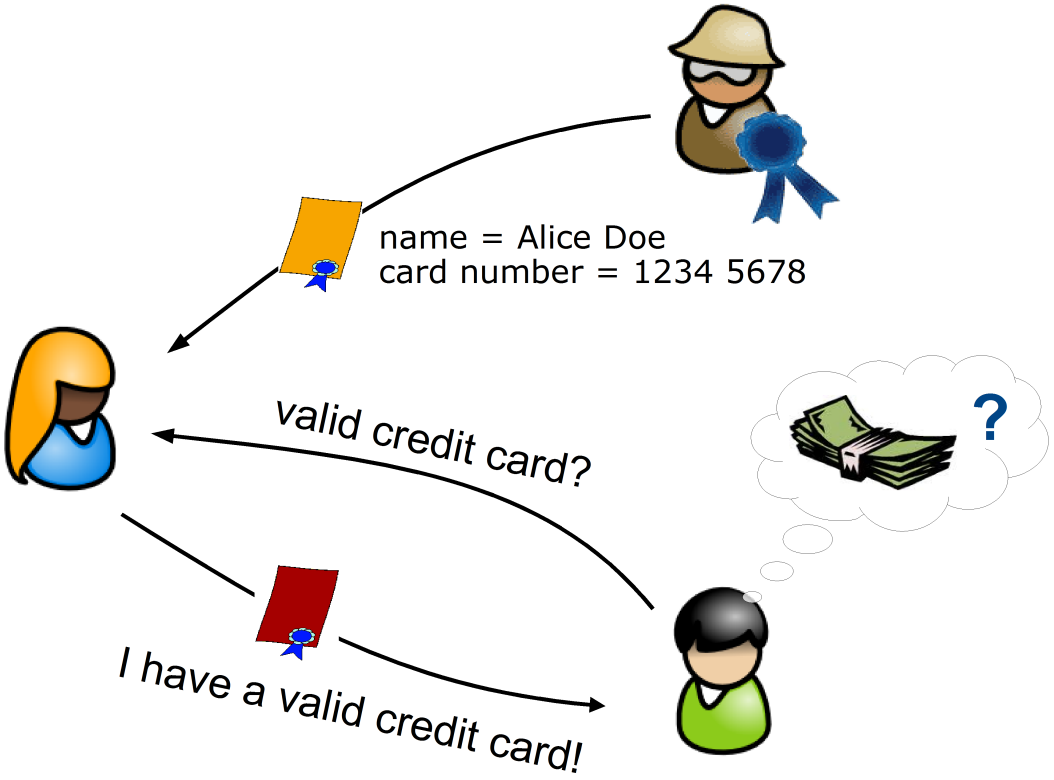
- **Issuer**-driven revocation
  - credential gets globally revoked
    - e.g. if credential got lost or compromised
  - revoked by unique revocation handle (hidden by default)
  - credential must always be proven to be valid

- **Verifier**-driven revocation
  - credential/attributes get revoked only for particular domain/purposes
    - e.g. no-fly list for passengers (passport still valid)
  - verifier specifies whether and which RA to consider
  - revocation based on any (combination of) attributes

there is more ....

- Key Binding & Pseudonyms
- Advanced Issuance
- Revocation
- Inspection
- ...

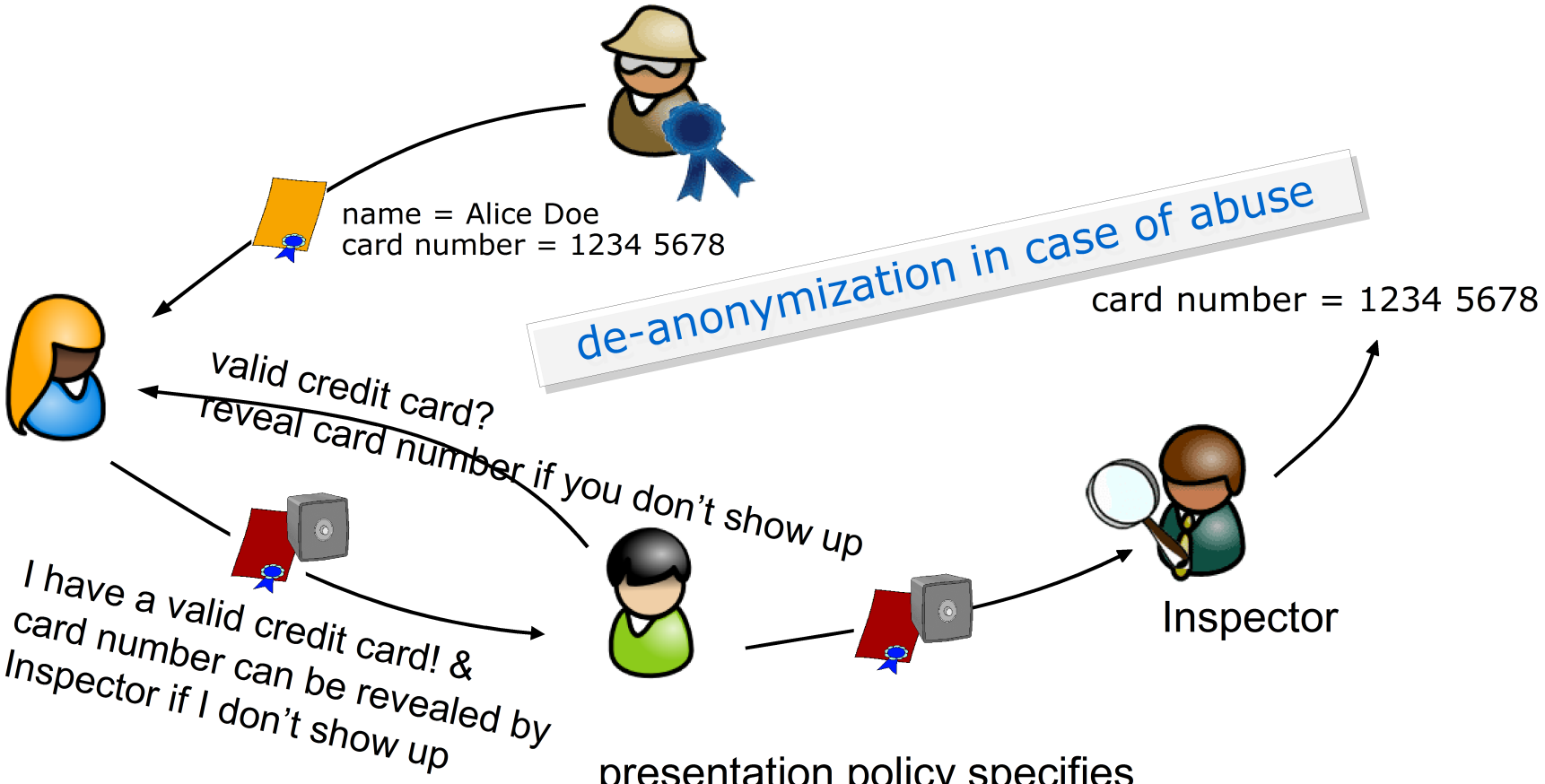
Privacy-ABCs | Inspection



Alice books a hotel, but never shows up

… credit card number must be retrieved to charge for 1st night

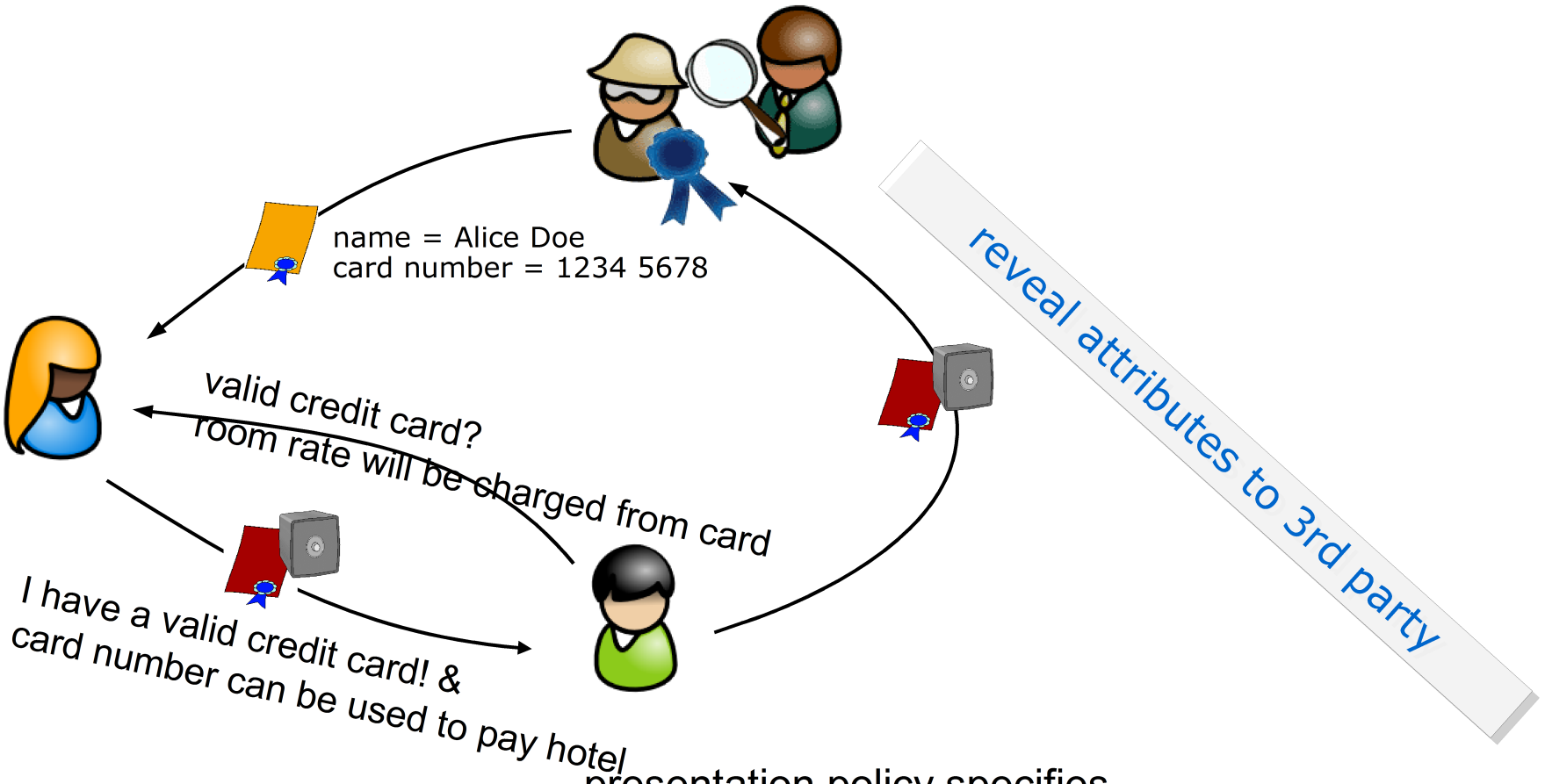
Privacy-ABCs | Inspection



presentation policy specifies

- Inspector's public key
- which attribute(s) from which credential(s)
- Inspection grounds

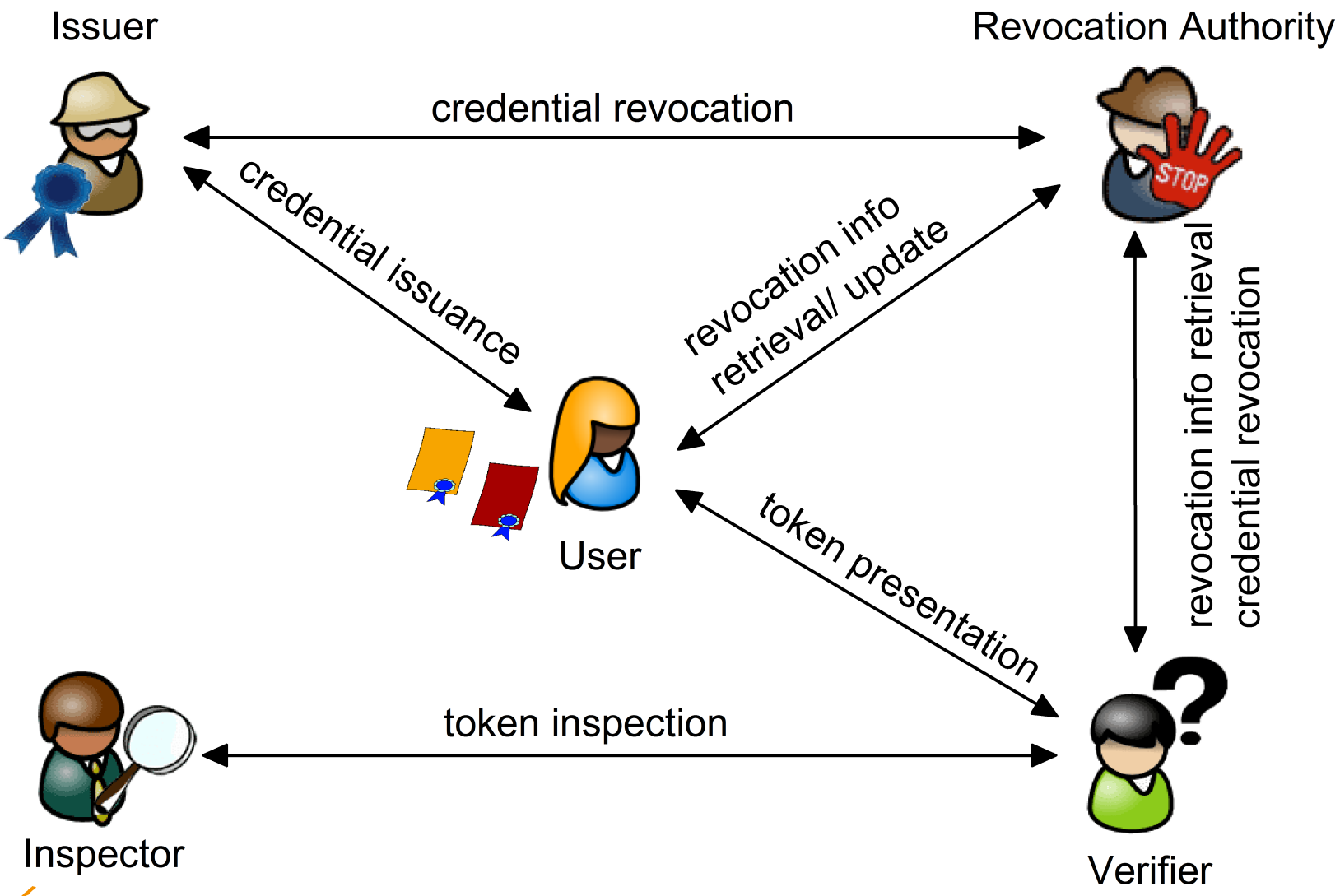
Privacy-ABCs | Inspection



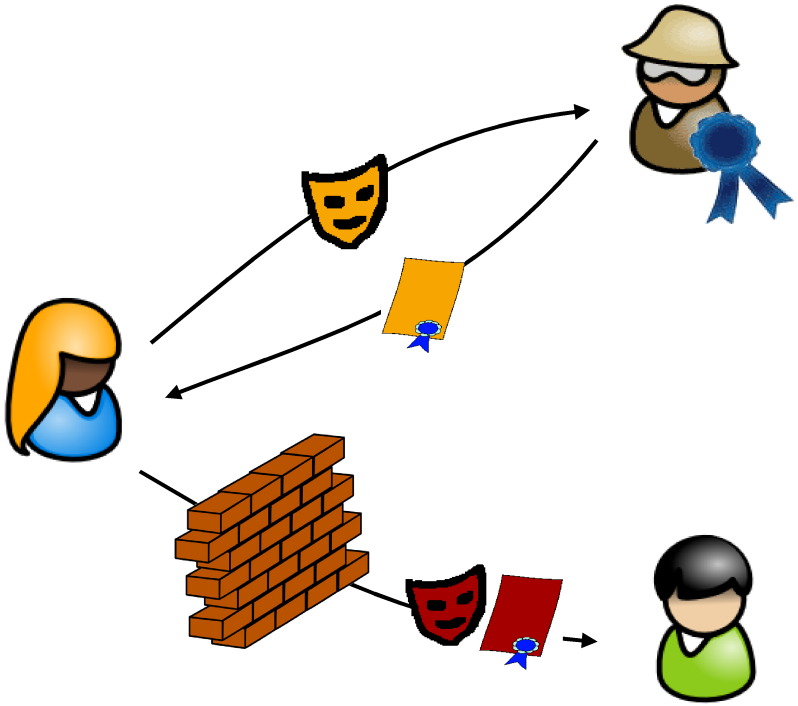
presentation policy specifies

- Inspector's public key
- which attribute(s) from which credential(s)
- Inspection grounds

Privacy-ABCs | Summary of Entities & Features



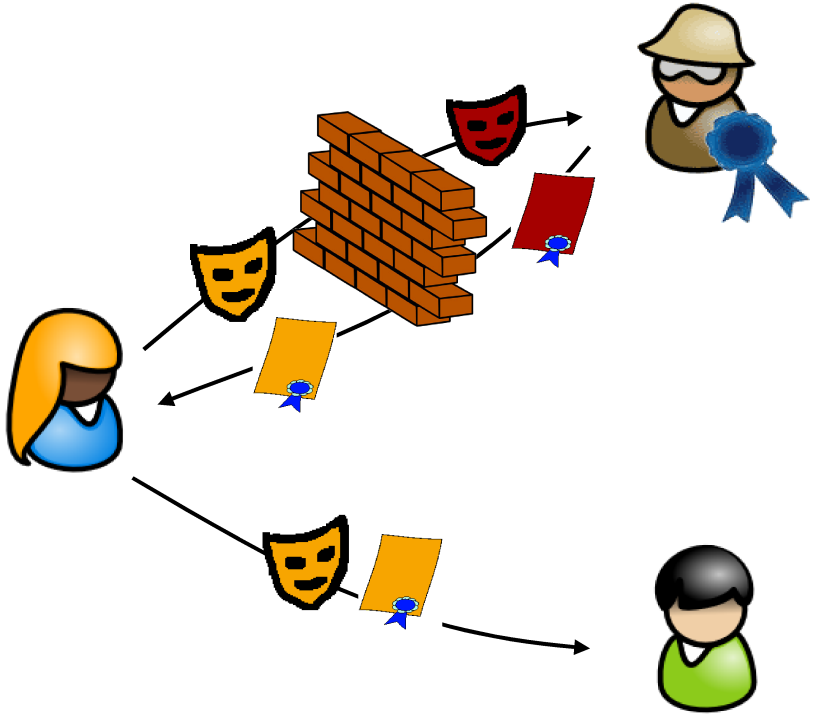
Zero-Knowledge Proofs



Idemix (Identity Mixer)

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

Blind Signatures



U-Prove

Chaum, Brands et al.
Discrete Logs, RSA,..

Privacy-ABCs | Summary

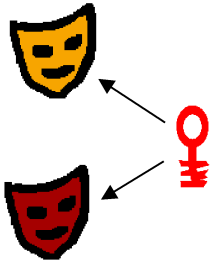
- Privacy-ABCs allow for strong yet privacy-friendly authentication
  - description and terminology for common concepts & features
    - selective disclosure of attributes
    - pseudonyms & key binding
    - advanced issuance (carried-over attributes)
    - inspection, revocation
  - Idemix & U-Prove are two instantiations of Privacy-ABCs

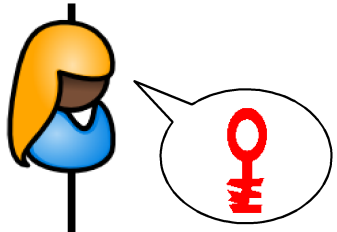
  next talk:
  - common dataformats for the entire life-cycle of Privacy-ABCs
    - credential specifications, presentation policy & token, …
    - support all the presented privacy features

Questions ?

Privacy-ABCs vs. Classical ABCs

each issuer has public key of signature scheme





each user has a single secret key but many public keys

each user has a single public key

certificate = signature on user's secret key + attributes

attributes might be hidden from issuer

certificate = signature on user's public key + attributes

using certificate

prove knowledge of certificate

- prove that different certificates contain same secret key
- selectively reveal attributes

reveal certificate