ABC4Trust & PrimeLife Tutorial

Part I: Introduction to Privacy-Preserving Authentication

Outline

- Introduction
  - Motivation
  - Classical Authentication
- General Concepts of Minimal Disclosure Wallets
  - Basic Functionality
  - Pseudonyms and Multiple Tokens
  - Extended Functionality
- Solutions
  - High-Level Crypto Ingredients
  - Idemix and U-Prove

Motivation | Our digital footprints…

facebook

amazon.com

twitter

ebay

Google

Motivation | Computers don’t forget!

Once personal data is released, it can no longer be controlled

- can be distributed
- different pieces can be linked and profiles be made

Digital World makes this even worse

- storage is becoming increasingly cheaper — store by default, e.g.,

  wireless router traffic picked up by Google Street View car

  IPhones stored location data (without user consent)

- data mining more efficient, e.g., Google

  not just trend detection, even prediction

  e.g., flu pandemics, ad clicks, purchases,…

  what about mortgage defaults, criminal behavior?

Motivation | Privacy breaches happen almost daily

„Projekt Datenschutz"

Datenschutzvorfälle in Unternehmen, Organisationen und Behörden und Datenschutz-Aktivitäten der Politik

Suche nach: Suchen

- Home
- Das Projekt
- News
- Blog „Datenschutz"
- Links
- Twitter
- Kontakt/Impressum

Datenschutzvorfälle

Datum	Ort	Datenherkunft	Organisation	Betroffene	Anz. Betroffene	Kurzbeschreibung	
31.05.2011	Frankfurt am Main	Neckermann	Unternehmen	Gewinnspielteilnehmer	1,2 Millionen	1,2 Millionen Neckermann-Kundendaten geklaut	Details...
24.05.2011	Potsdam	Universität	Bildungseinrichtung	Studenten	20.000	Datenpanne an der Uni Potsdam: Liste mit Daten von 20.000 Studierenden einsehbar	Details...
03.05.2011	Tokio	Sony Online Entertainment	Unternehmen	Kunden des Computerspiele-Dienstes	24,6 Millionen	Neue Datenpanne bei Sony: 24,6 Millionen Kundendaten von Sony Online Entertaiment geklaut	Details...
29.04.2011	Paris	Unesco	Organisation	Bewerber	Zehntausende	Unesco stellt Bewerberdaten ungeschützt ins Internet	Details...
27.04.2011	New York	Sony	Unternehmen	Nutzer des PlayStation Network und des Video- und Musikservices Qriocity	75 Millionen	Daten-GAU bei Sony: 75 Millionen Kundendaten gestohlen	Details...
20.04.2011	Oldenburg	Ashampoo GmbH & Co. KG	Unternehmen	Ashampoo-Kunden	Unzählige	Datenklau bei Software-Hersteller Ashampoo	Details...
15.04.2011	Willhelmshaven	Mindfactory AG	Unternehmen	Mindfactory-Kunden	Zehntausende	Opfer von Datenklau: Kundendaten von Mindfactory kursieren im Netz	Details...
07.04.2011	Witten	Zahnarztpraxis	Unternehmen	Patienten	Hunderte	Wilde Müllkippe: Wittener Zahnarztpraxis entsorgt Patientenakten auf öffentlichem Parkplatz	Details...
29.03.2011	Bad Hersfeld	Landratsamt des Landkreises Hersfeld-Rotenburg	Behörde	Bürger des Landkreises Hersfeld-Rotenburg	122.812	Datenklau der besonderen Art: Landratsamt lässt sich Server stehlen	Details...
18.03.2011	Nürnberg	ADAC Nordbayern	Unternehmen	Mitarbeiter und ehrenamtliche Funktionäre	Hunderte	ADAC Nordbayern spioniert Mitarbeiter aus	Details...
14.02.2011	Sachsen, Sachsen-Anhalt	NPD	Partei	Parteimitglieder	Unzählige	Datenleck bei der NPD ermöglicht Einblick in 60.000 E-Mails	Details...

http://www.projekt-datenschutz.de/

Motivation | What are the risks?

- Embarrassment
- Discredit
- Financial Fraud
- Blackmailing
- Identity Theft
- …

None are new just higher (and more severe) due to online availability

→ the less data we share the better

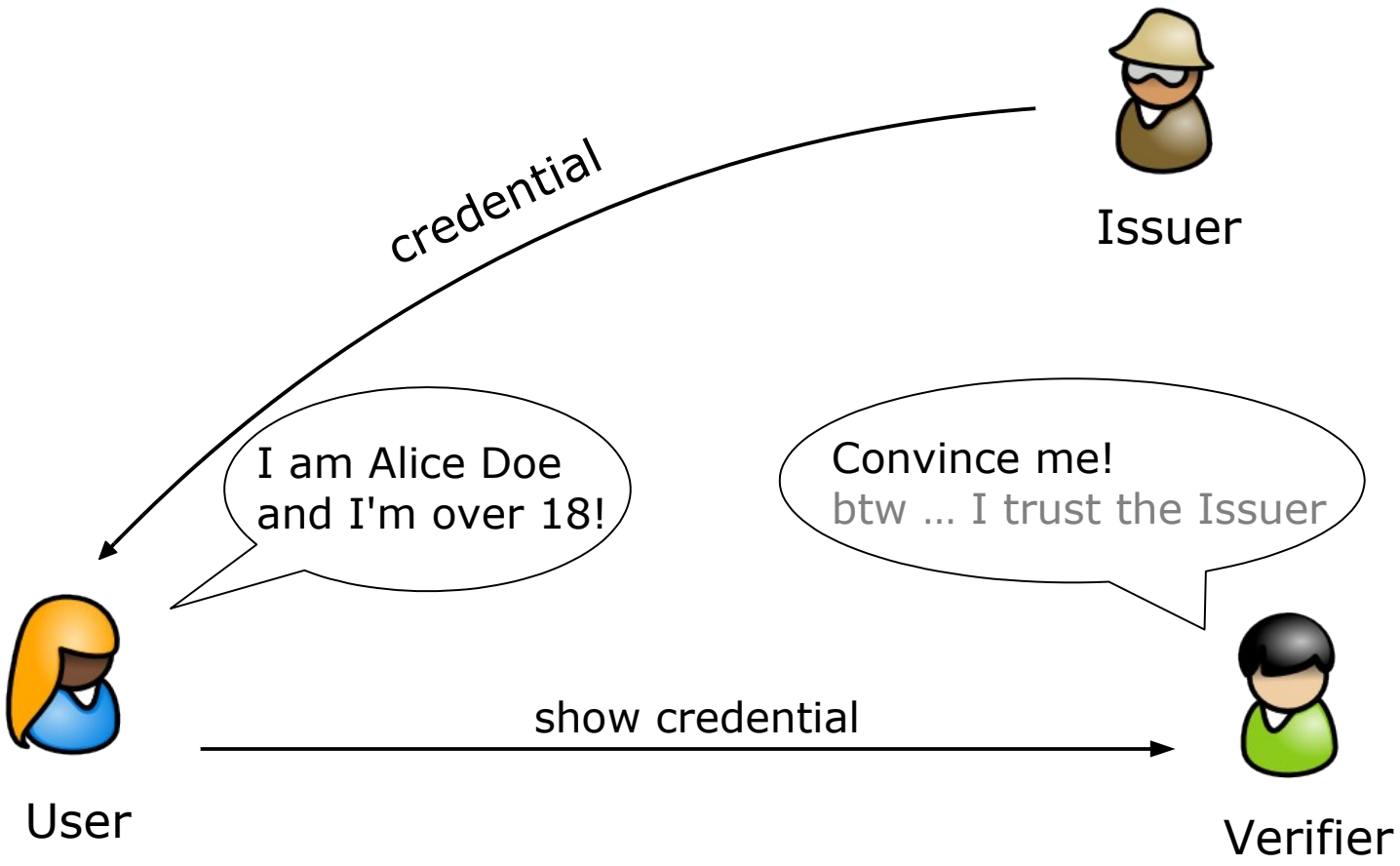
Basic protection techniques:

- release only necessary data

  use cryptography to control and minimize the release of data

- define what should happen with released data
- require from recipient that data be protected

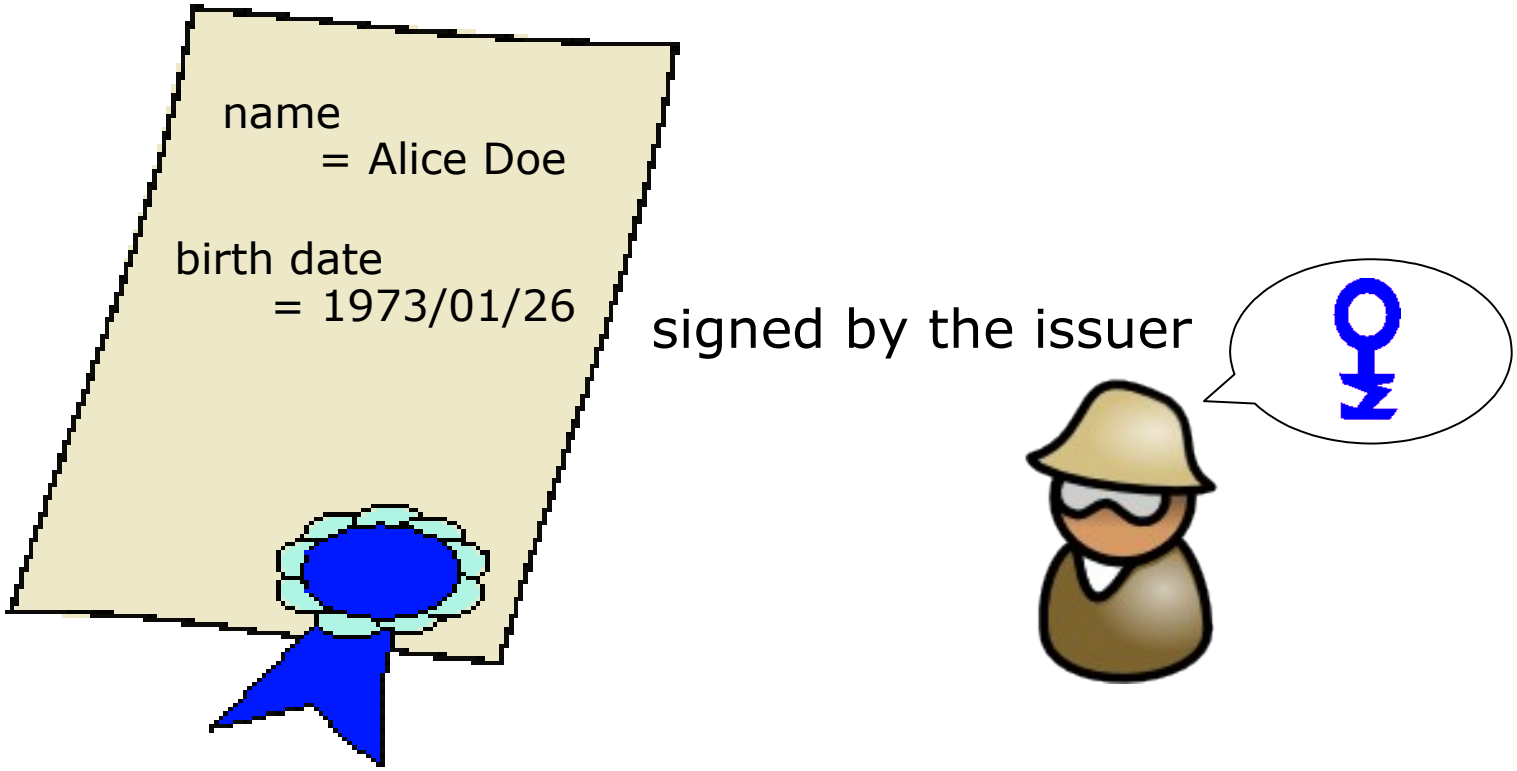
Authentication



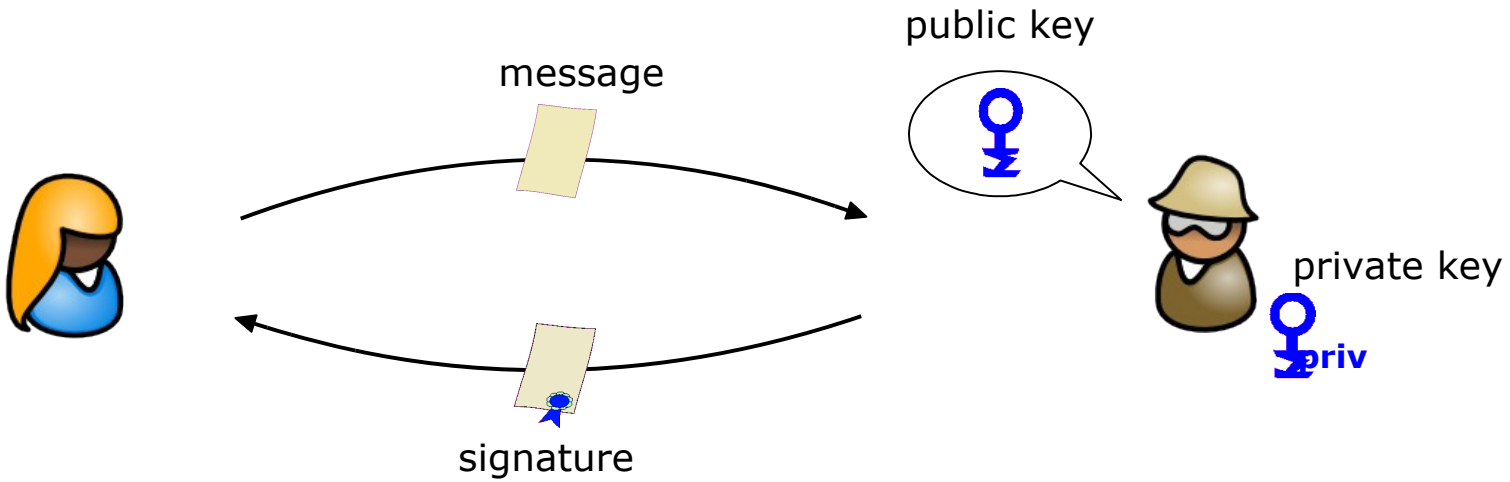
Authentication

credential / certificate

- signed list of attribute-value pairs



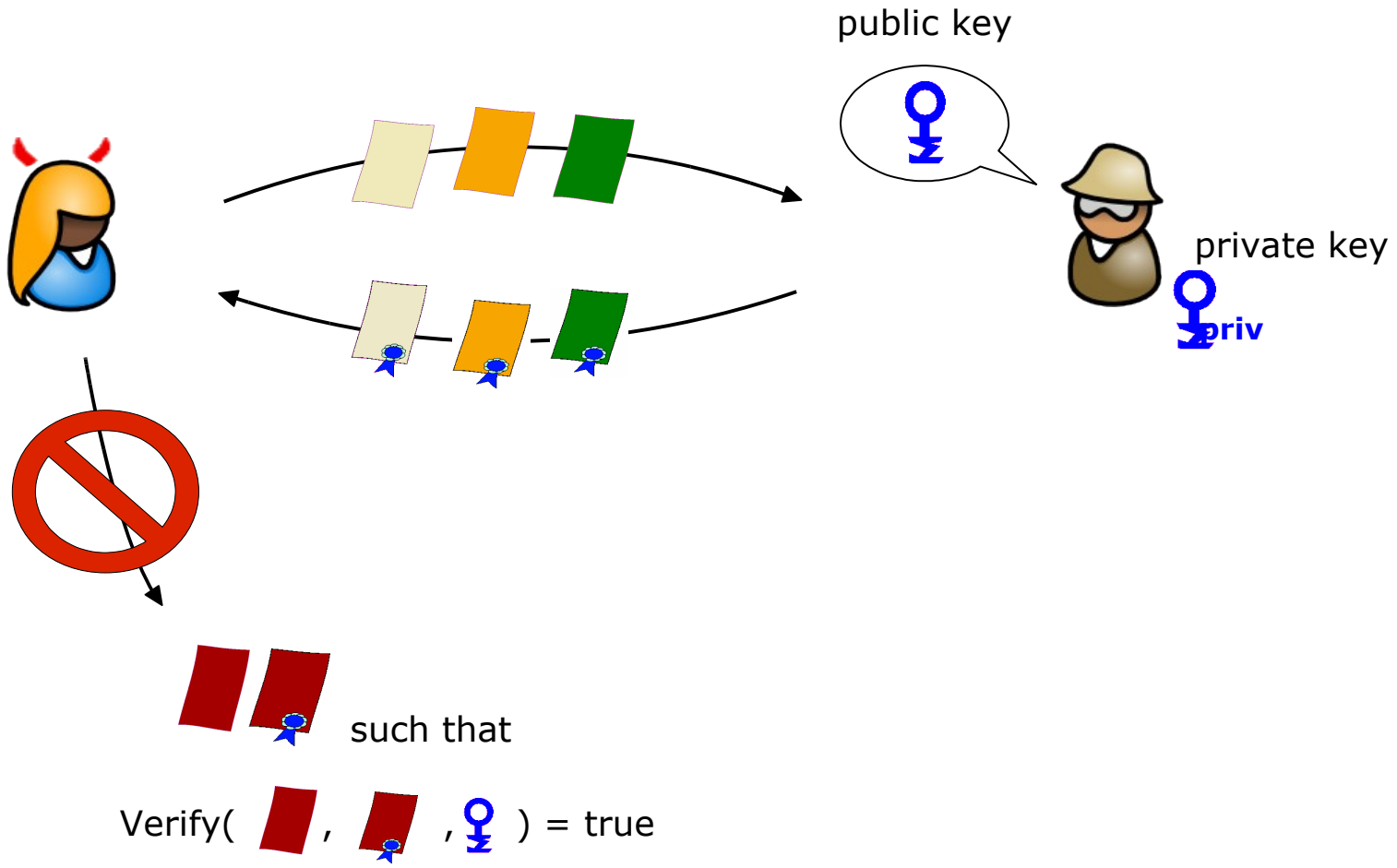
Signature Scheme



Verify(, ,) = true

= Sign(, priv)

Signature Scheme | Unforgeability

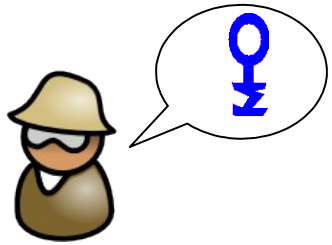


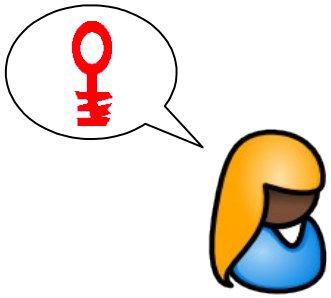
Classical Authentication

Standard Public-Key Certificates

e.g., X.509 certificates

In the beginning…

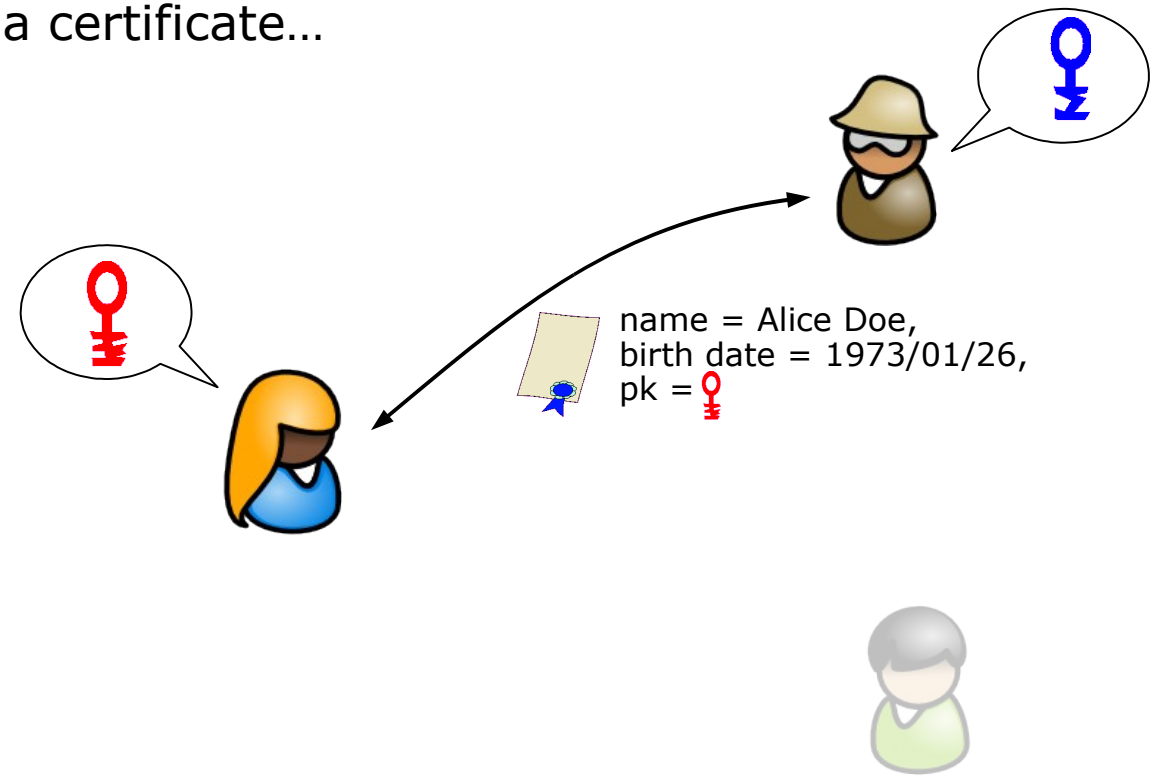




Standard Public-Key Certificates

e.g., X.509 certificates

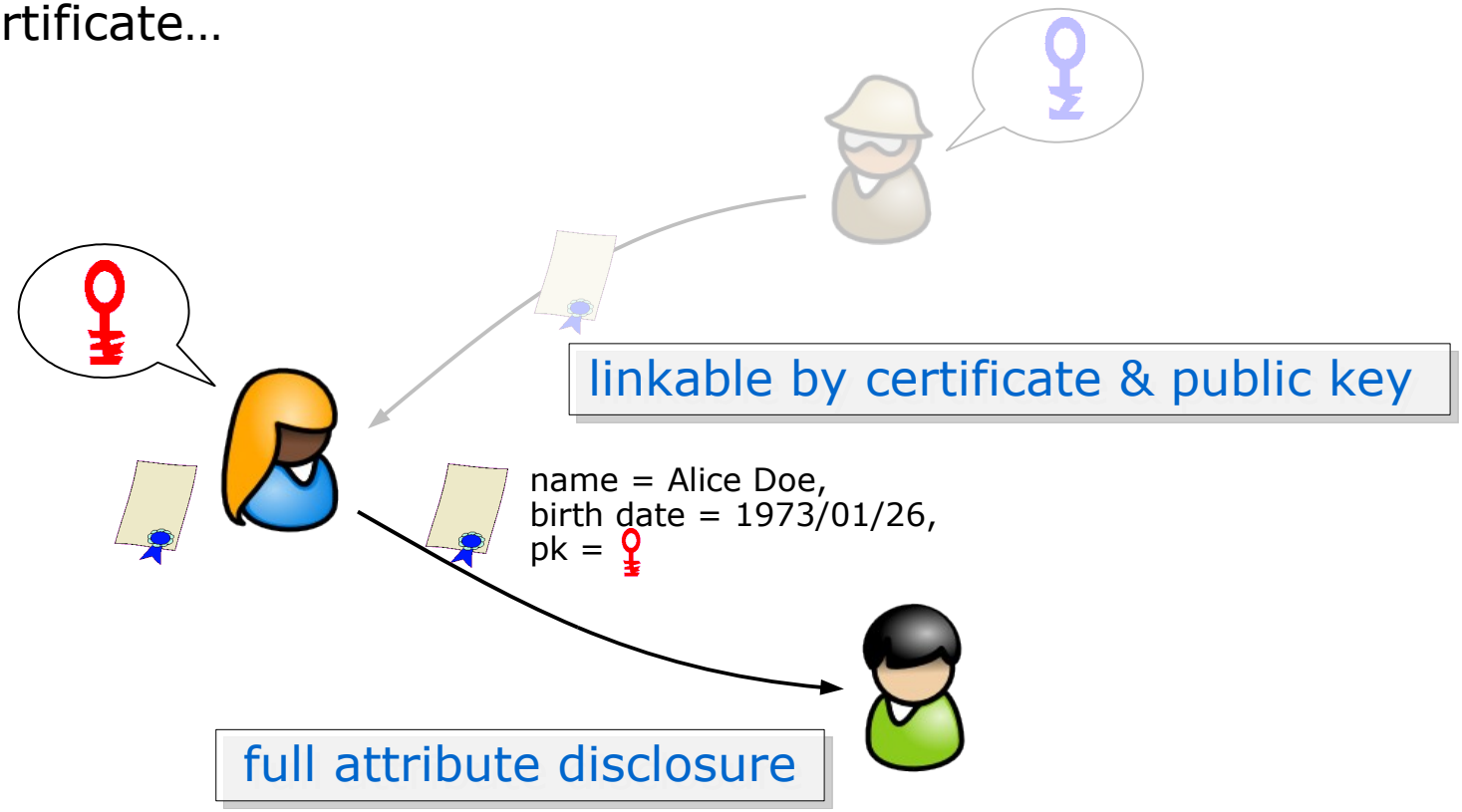
Obtaining a certificate…



Standard Public-Key Certificates

e.g., X.509 certificates

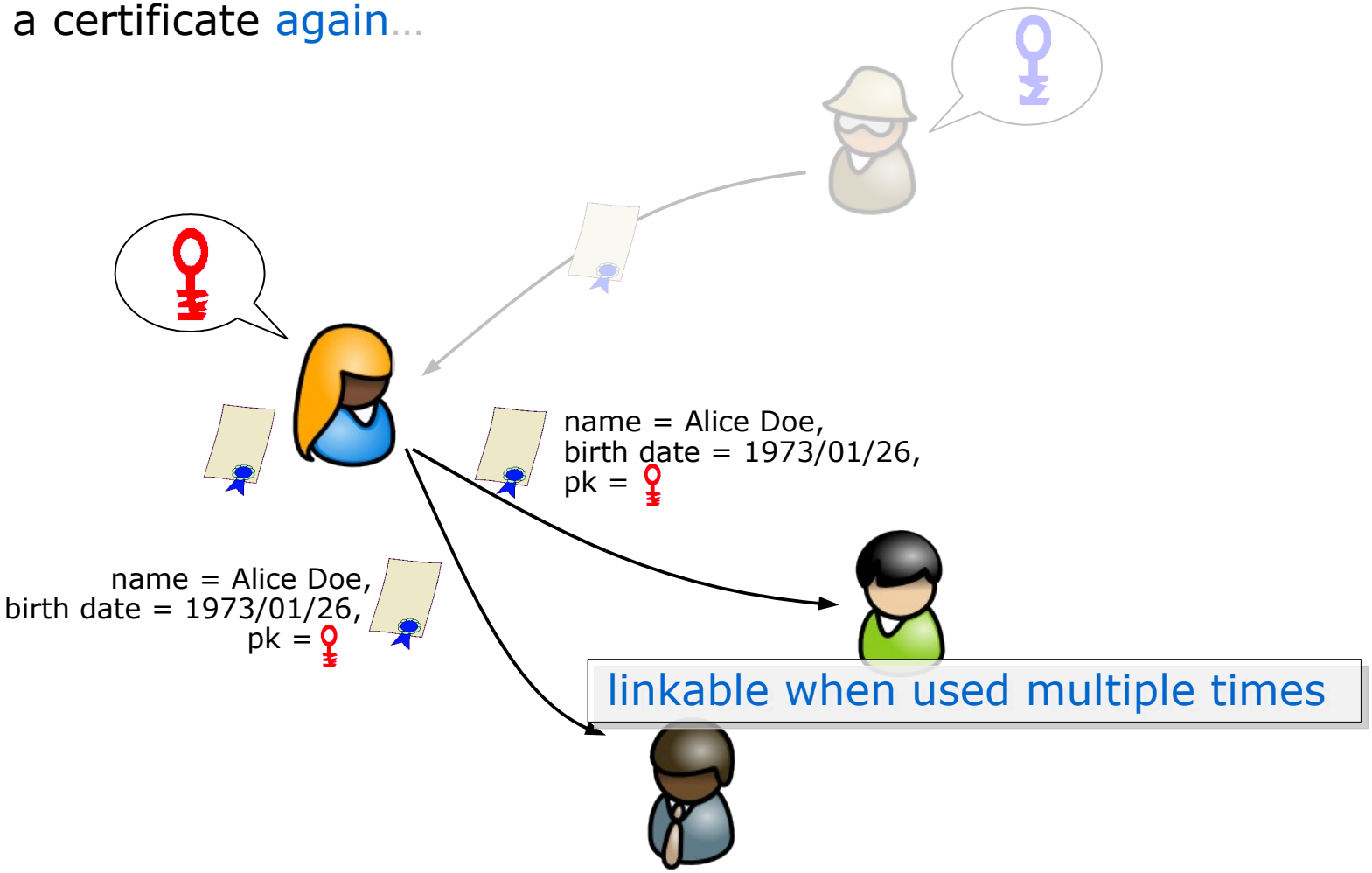
Using a certificate…



Standard Public-Key Certificates

e.g., X.509 certificates

Using a certificate again…



Privacy-Preserving Authentication

Privacy-Preserving Authentication: General Concepts

- Basic Functionality

  Minimal Disclosure *Tokens*

- Pseudonyms and Combining/Binding of Multiple Tokens

  Minimal Disclosure *Wallets*

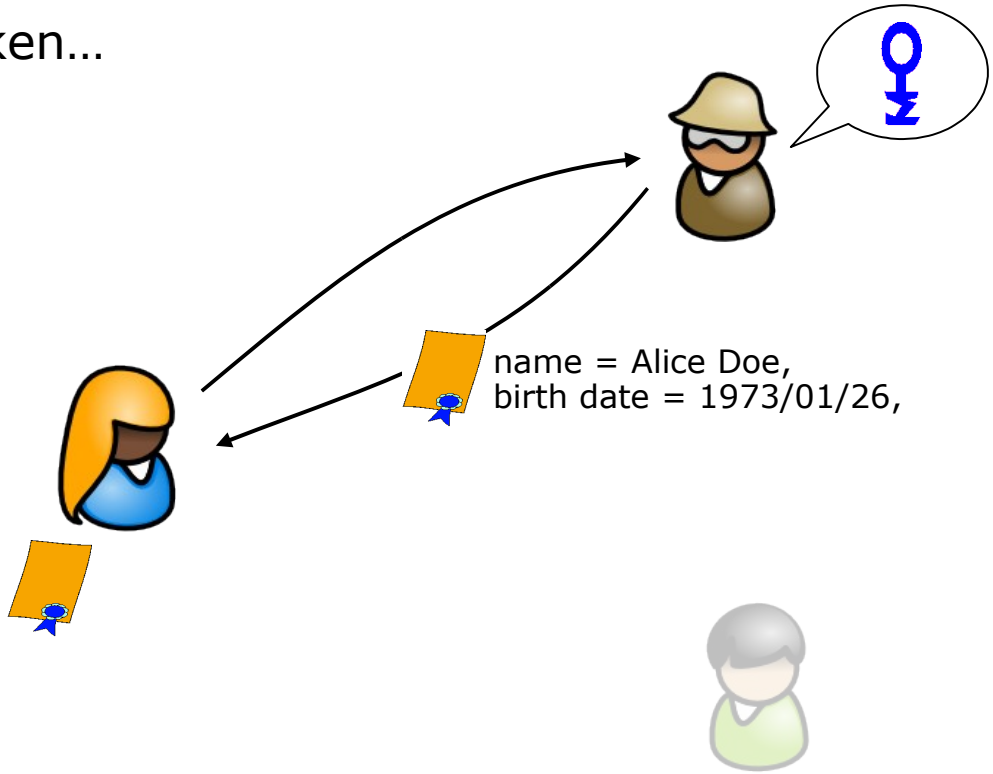
- Extensions
  - Revocation
  - Usage Limitation
  - Inspection
  - ...

Minimal Disclosure Tokens

In the beginning…

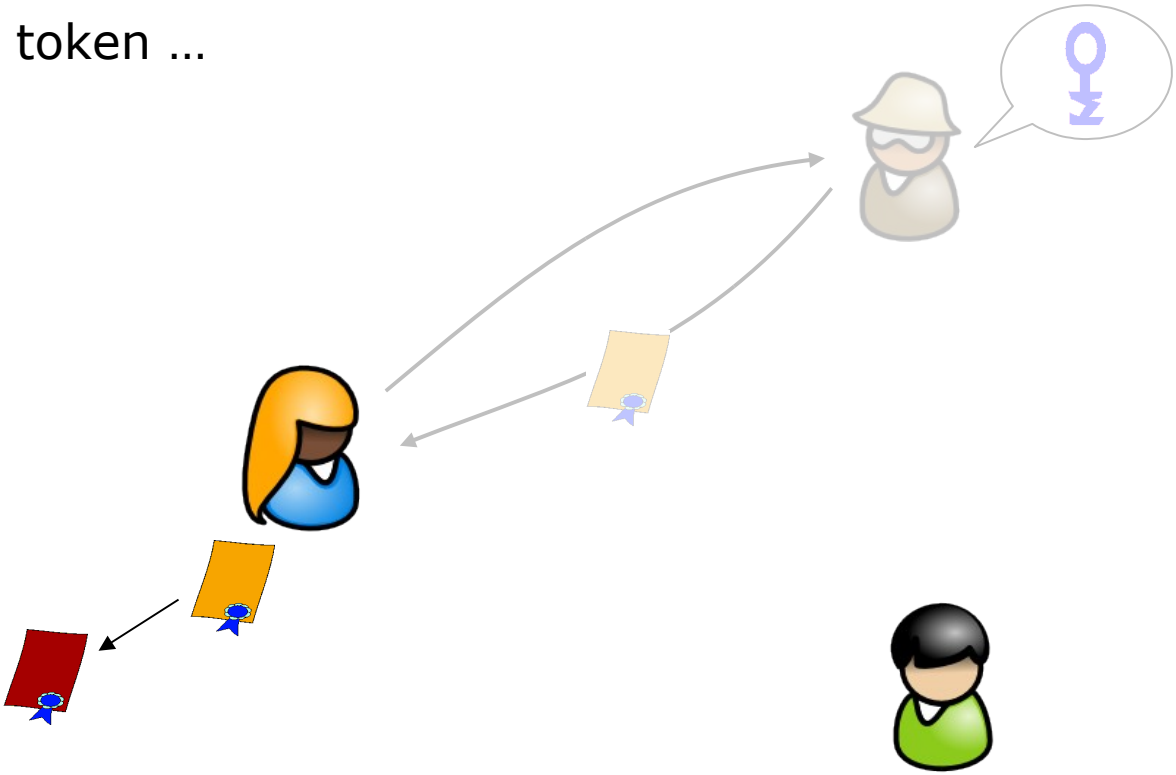
Minimal Disclosure Tokens

Obtaining a token…



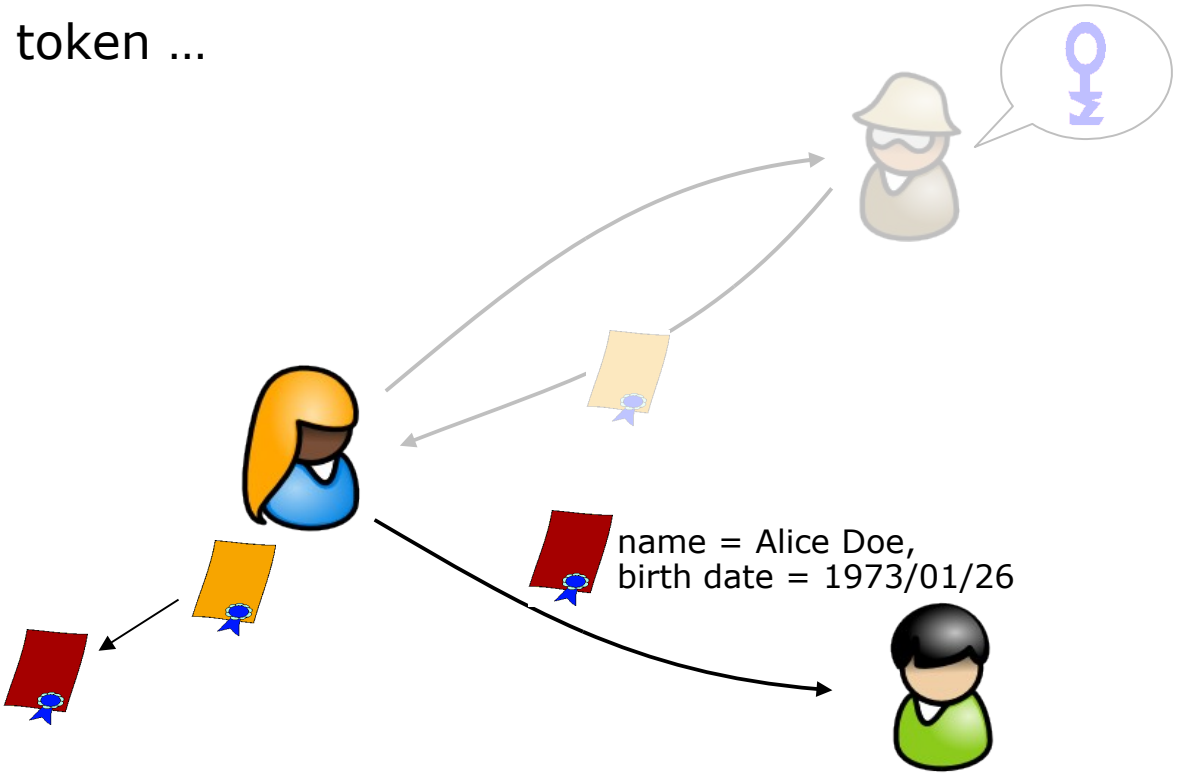
Minimal Disclosure Tokens

Using a token …



Minimal Disclosure Tokens

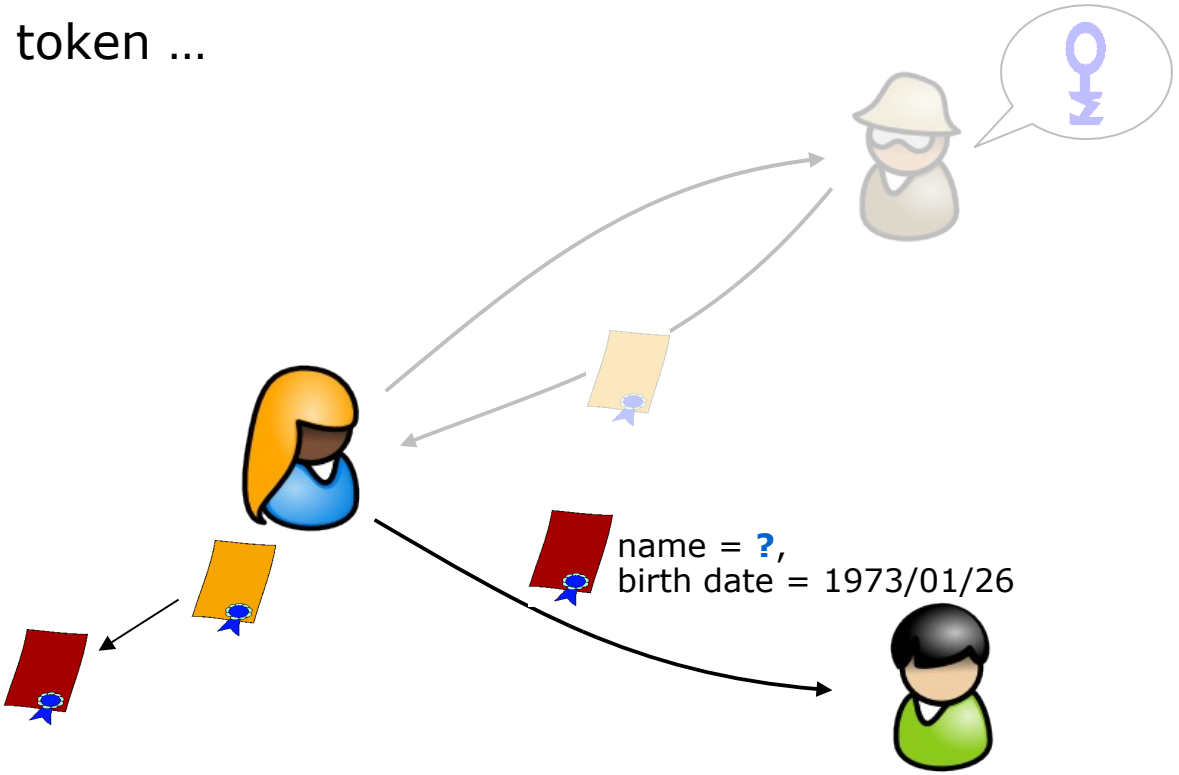
Using a token …



issuance and showing are unlinkable

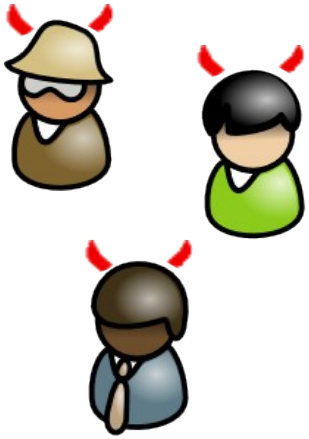
Minimal Disclosure Tokens

Using a token …

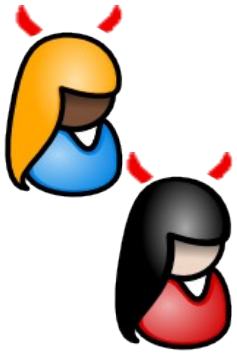


selective attribute disclosure

Minimal Disclosure Tokens



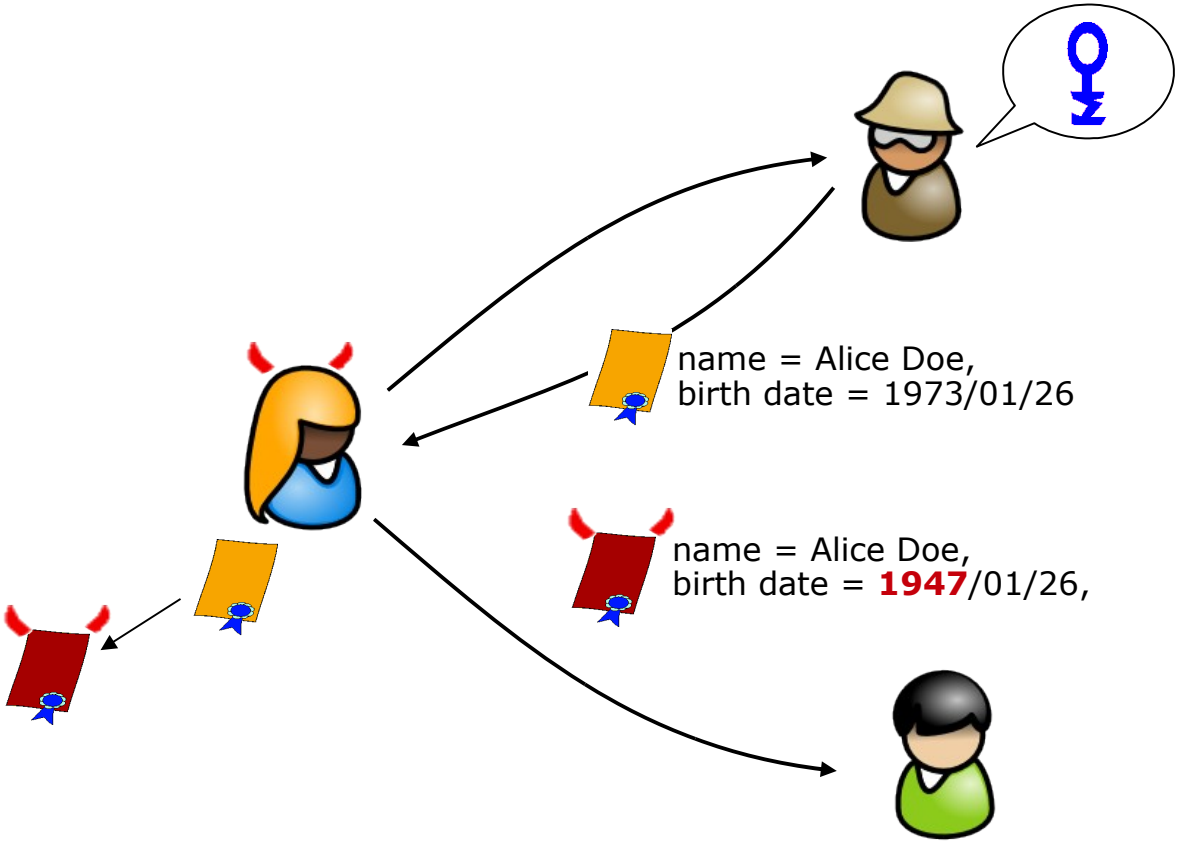
- Protection of user's privacy
  - anonymity
  - unlinkeability (single-use)
  - selective disclosure



- Unforgeability of tokens

Minimal Disclosure Tokens

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



Privacy-Preserving Authentication: General Concepts

- Basic Functionality

  Minimal Disclosure Tokens

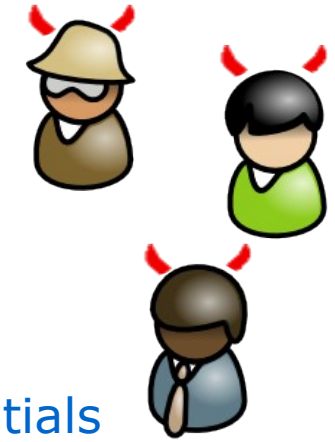
- Pseudonyms and Combining/Binding of Multiple Tokens

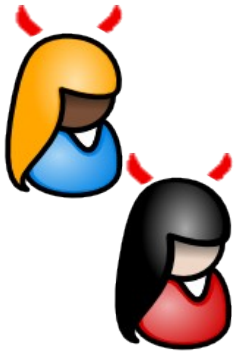
  Minimal Disclosure Wallets

- Extensions
  - Revocation
  - Usage Limitation
  - Inspection
  - ...

Minimal Disclosure Wallets

- extended version of minimal disclosure tokens:
  - Protection of user's privacy
    - pseudonymity
    - unlinkeability (multi-use)
    - using/combining multiple credentials
    - selective disclosure

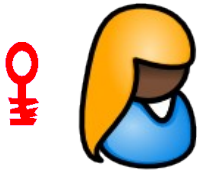




  - Unforgeability of credentials
  - Consistency of credentials (no sharing)

Minimal Disclosure Wallets

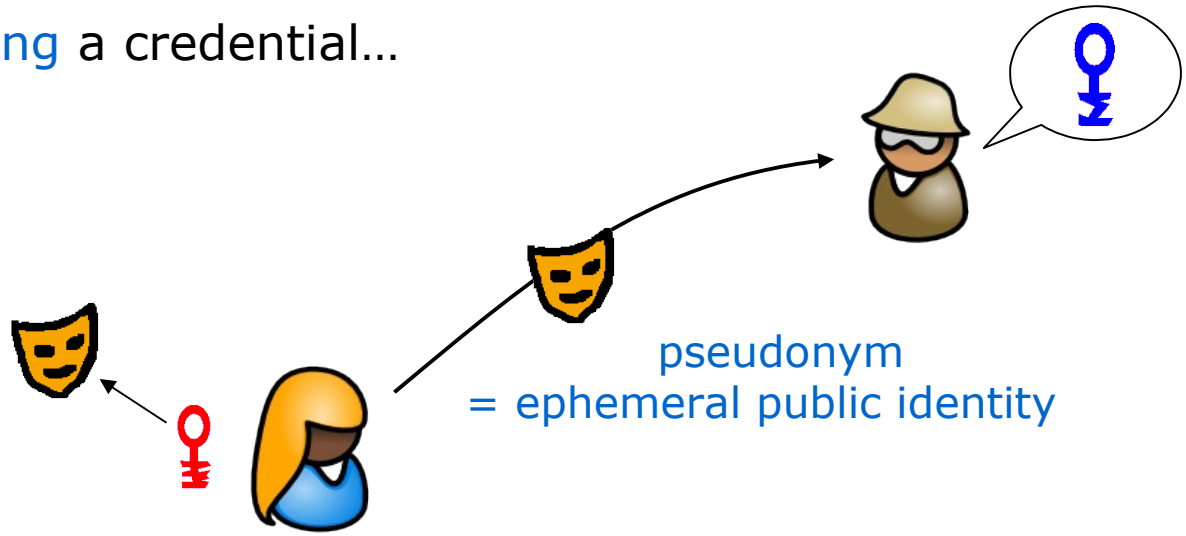
In the beginning…



master key
= unique private identity

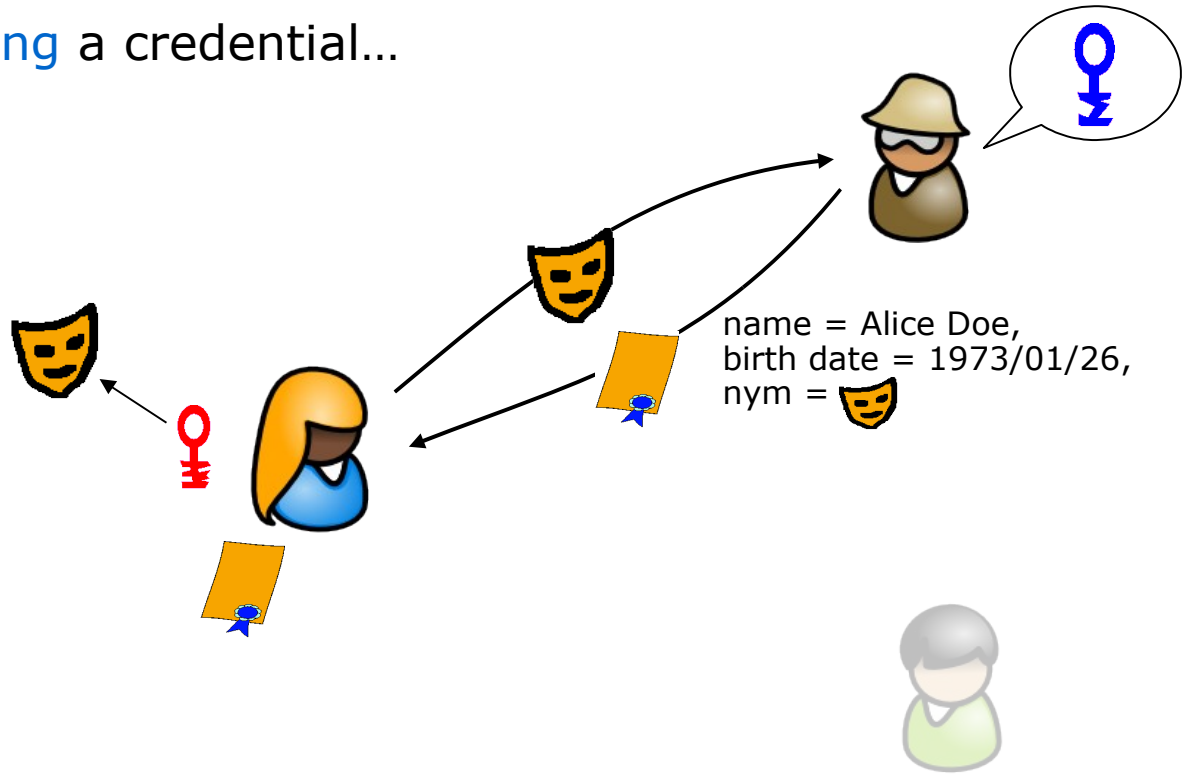
Minimal Disclosure Wallets

Obtaining a credential…



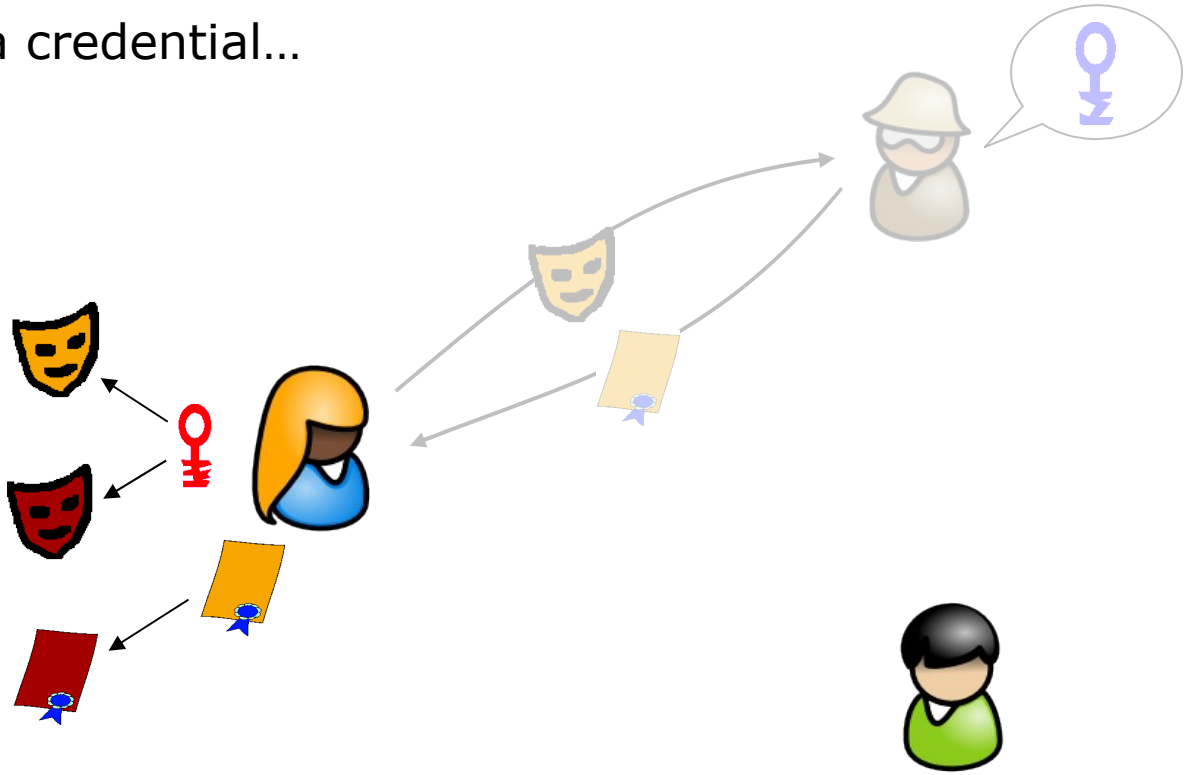
Minimal Disclosure Wallets

Obtaining a credential…



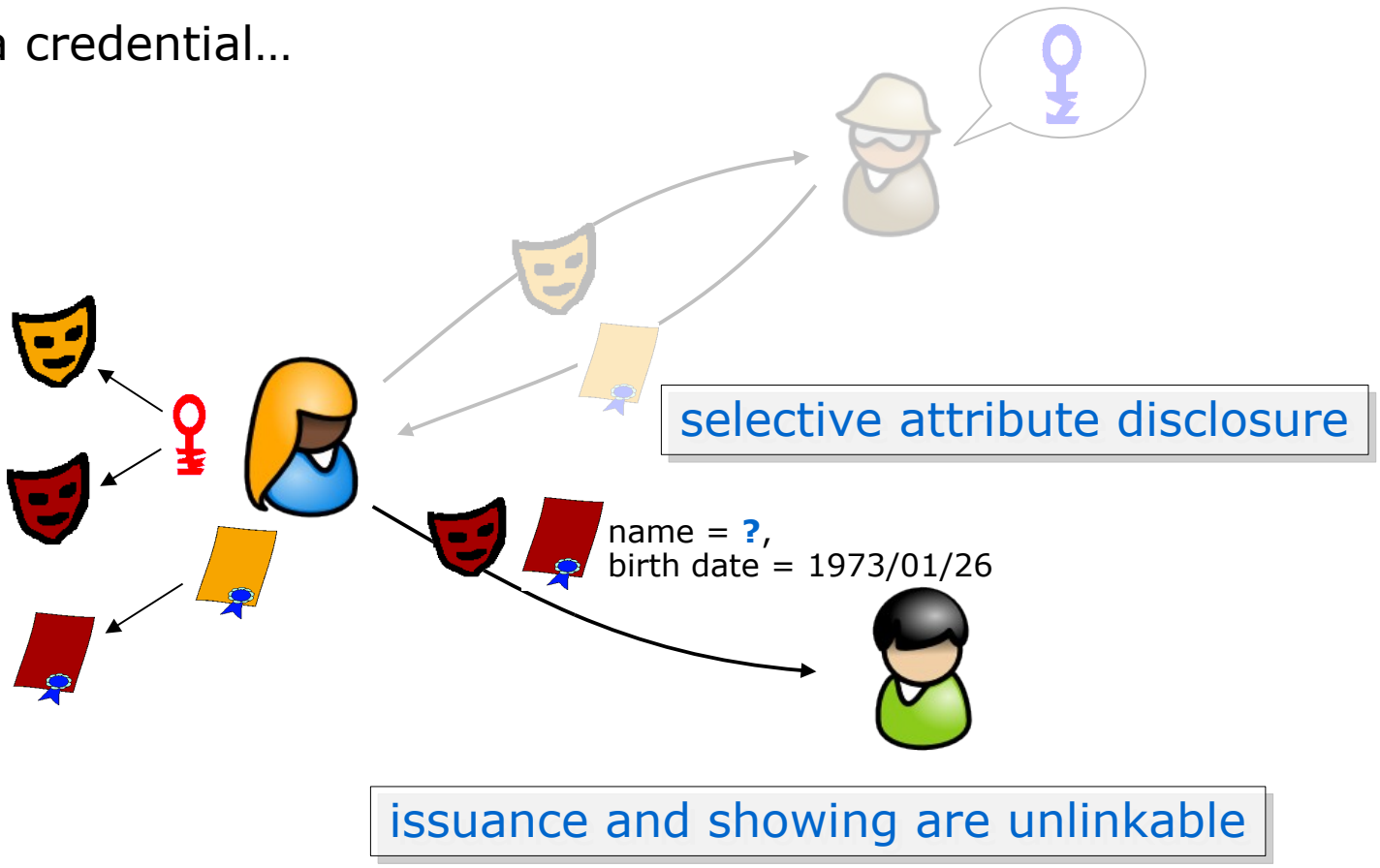
Minimal Disclosure Wallets

Using a credential…



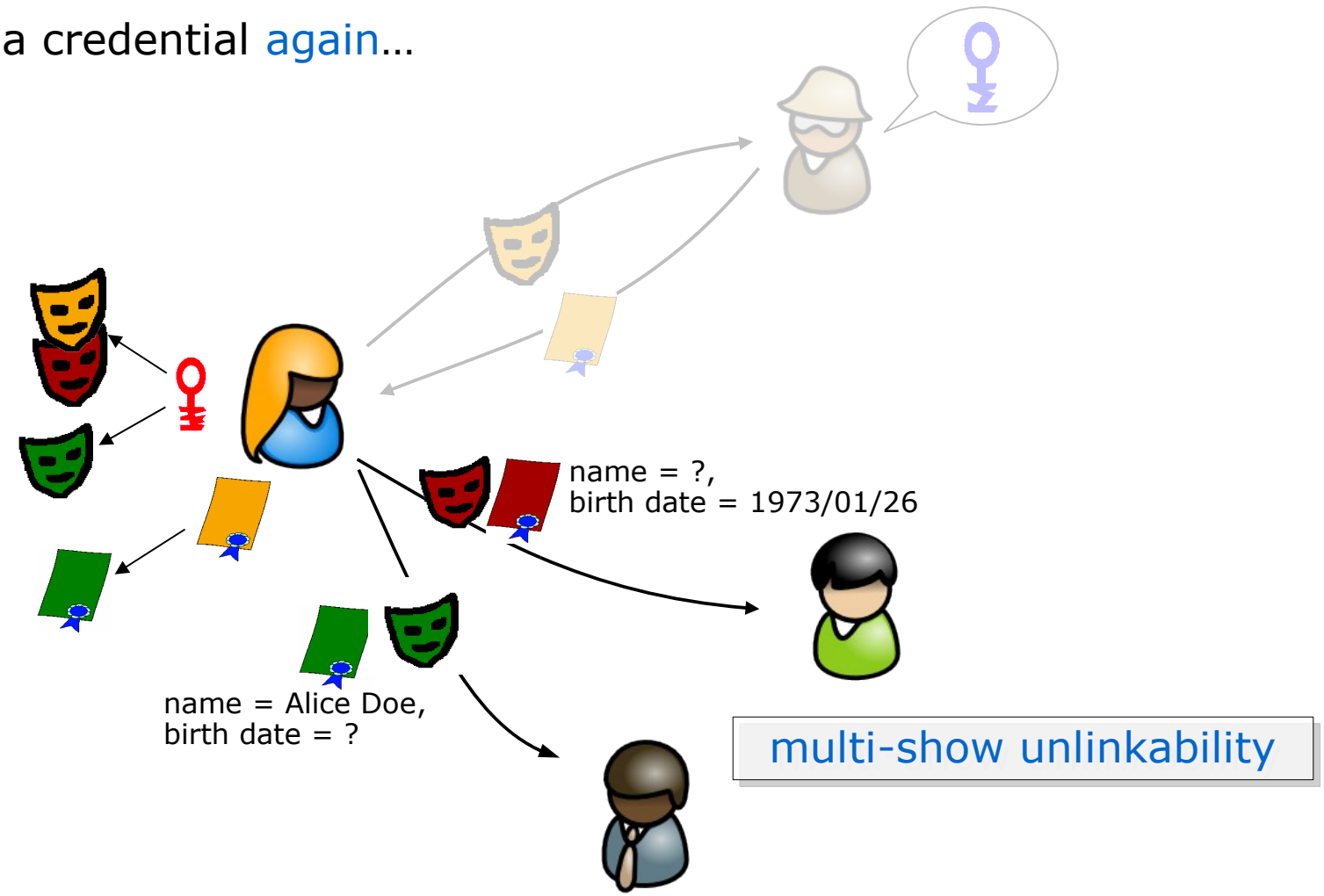
Minimal Disclosure Wallets

Using a credential…



Minimal Disclosure Wallets

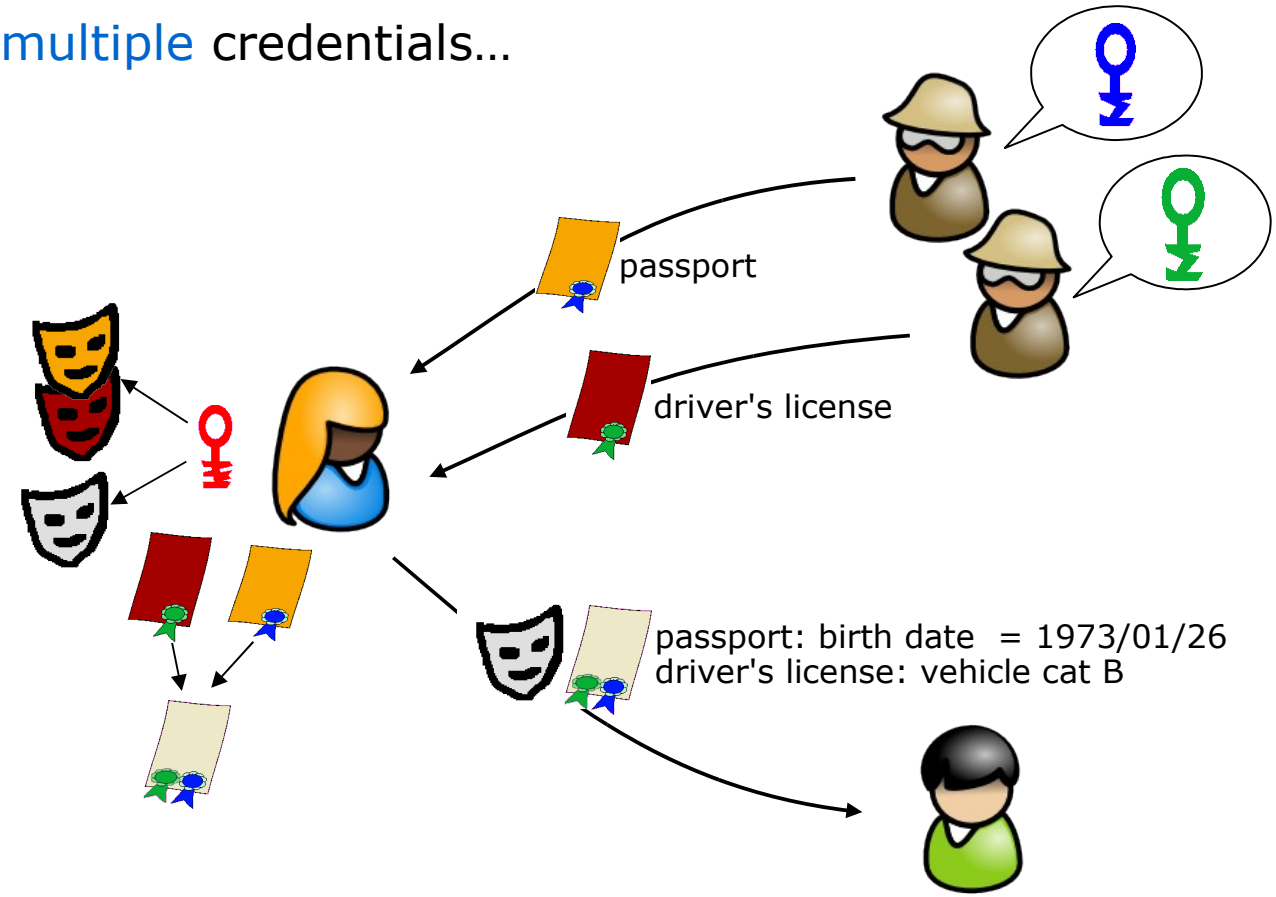
Using a credential again…



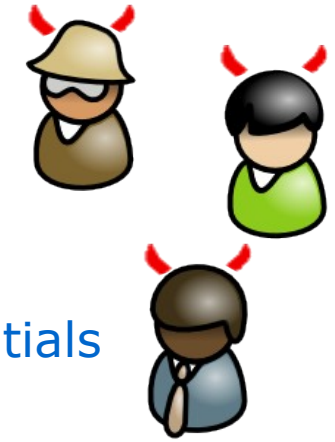
multi-show unlinkability

Minimal Disclosure Wallets

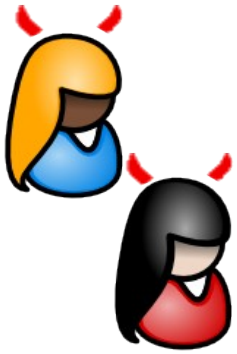
Using multiple credentials…



Minimal Disclosure Wallets



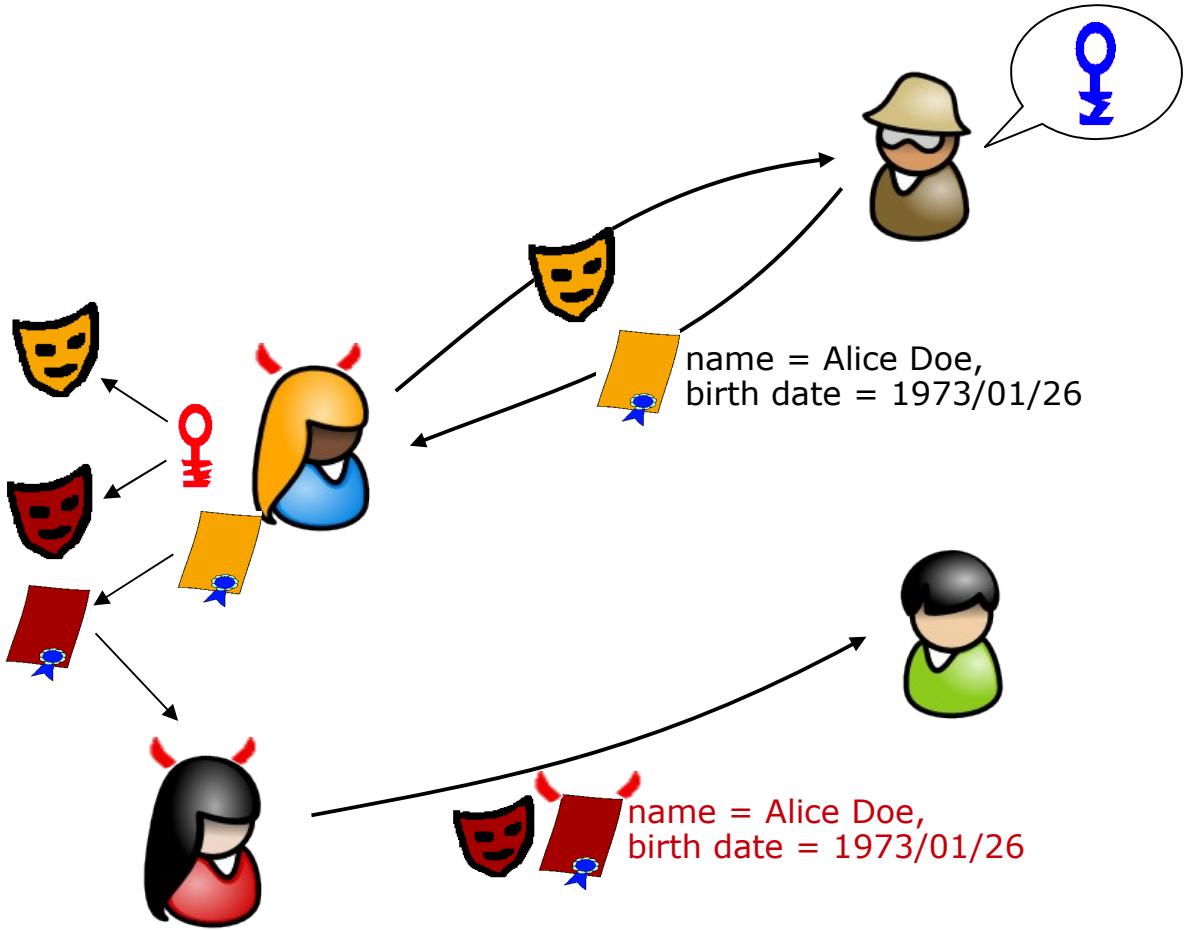
- Protection of user's privacy
  - pseudonymity
  - unlinkeability (multi-use)
  - using/combining multiple credentials
  - selective disclosure



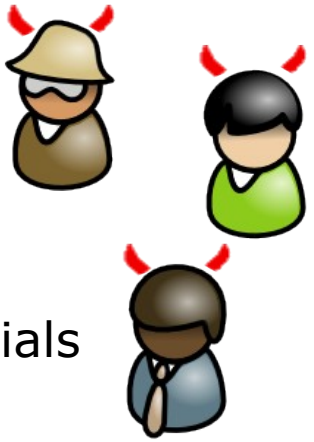
- Unforgeability of credentials
- Consistency of credentials (no sharing)

Minimal Disclosure Wallets

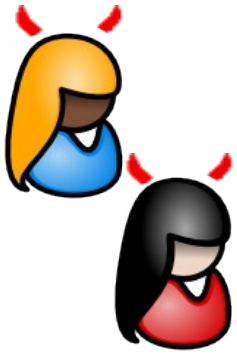
Sharing Prevention: Alice and Eve should not be able to share credential



Minimal Disclosure Wallets



- Protection of user's privacy
  - pseudonymity
  - unlinkeability (multi-use)
  - using/combining multiple credentials
  - selective disclosure



- Unforgeability of credentials
- Consistency of credentials (no sharing)

Privacy-Preserving Authentication: General Concepts

- Basic Functionality

  Minimal Disclosure Tokens

- Pseudonyms and Combining/Binding of Multiple Tokens

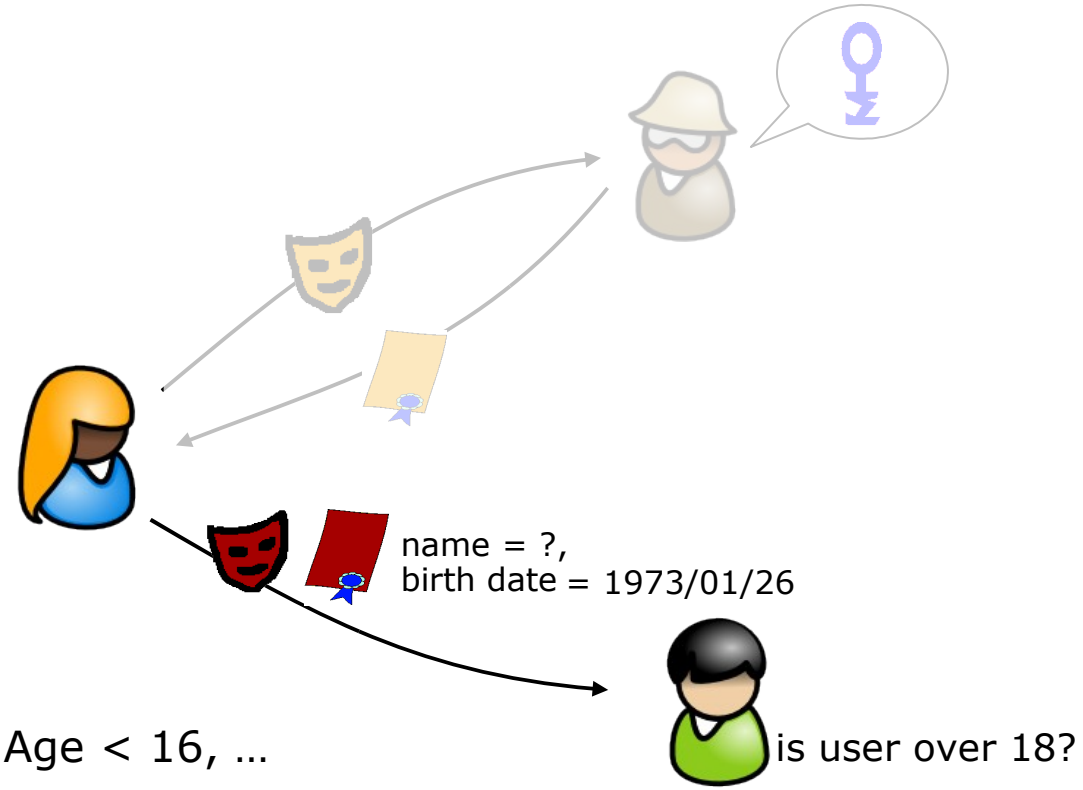
  Minimal Disclosure Wallets

- Extensions
  - Predicates over Attributes
  - Revocation
  - Device Binding
  - Inspection
  - Usage Limitation
  - ...

Extended Functionality

- Predicates over attributes
- Credentials on hidden attributes
- Device binding
- Domain pseudonym
- Revocation of credentials
- Inspection of credentials/attributes
- Usage limitation
- Censorable Audit Logs

Predicate Over Attributes



Range Proofs

Age > 18, 10 < Age < 16, …

credit card expiration date > today

Set Membership

status: {children, student, senior}

Logical Combinations

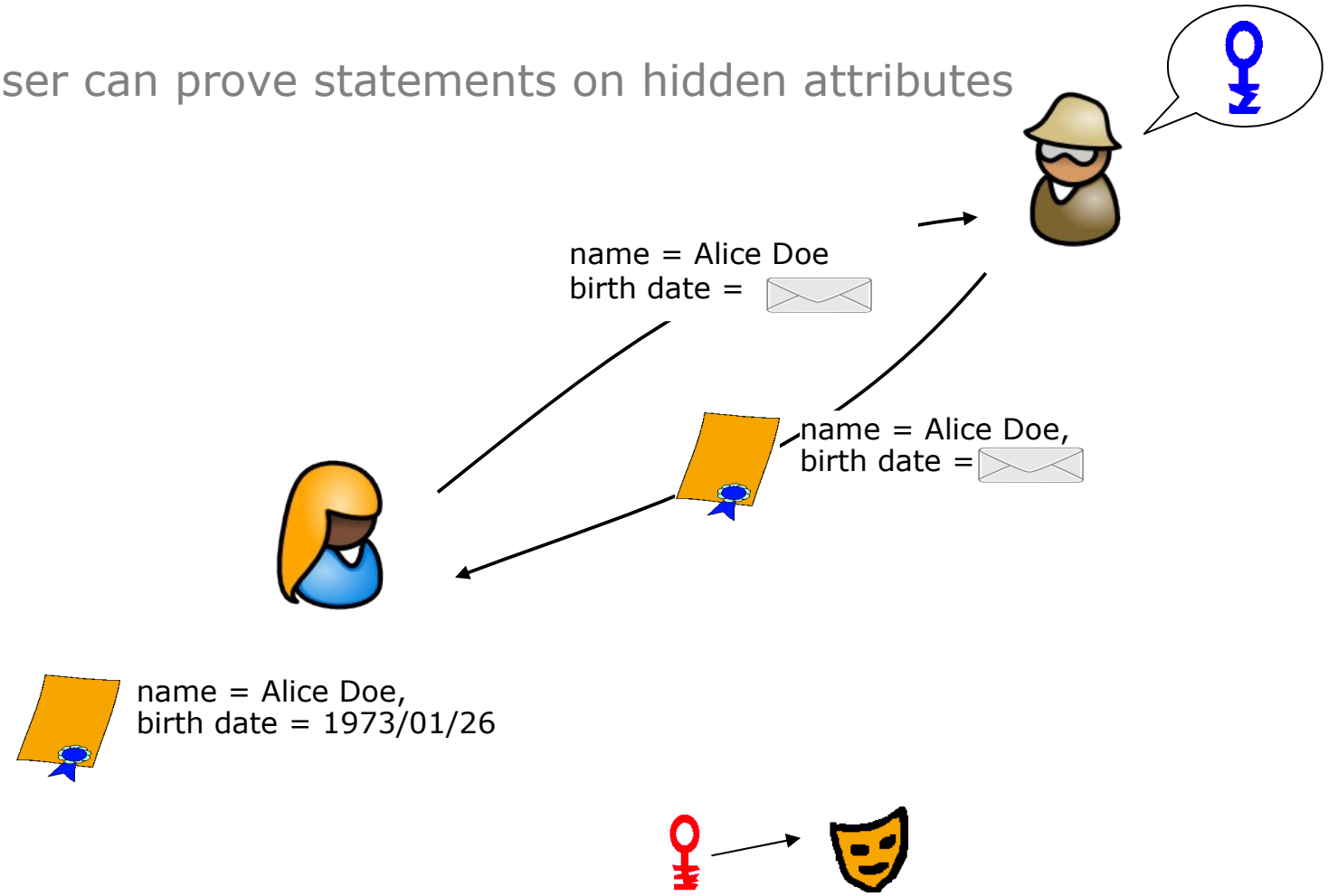
(credit card status = silver *or* gold) *and* valid driver's license

Extended Functionality

- Predicates over attributes
- Credentials on hidden attributes
- Device binding
- Domain pseudonym
- Revocation of credentials
- Inspection of credentials/attributes
- Usage limitation
- Censorable Audit Logs

Credentials on Hidden Attributes

User can prove statements on hidden attributes



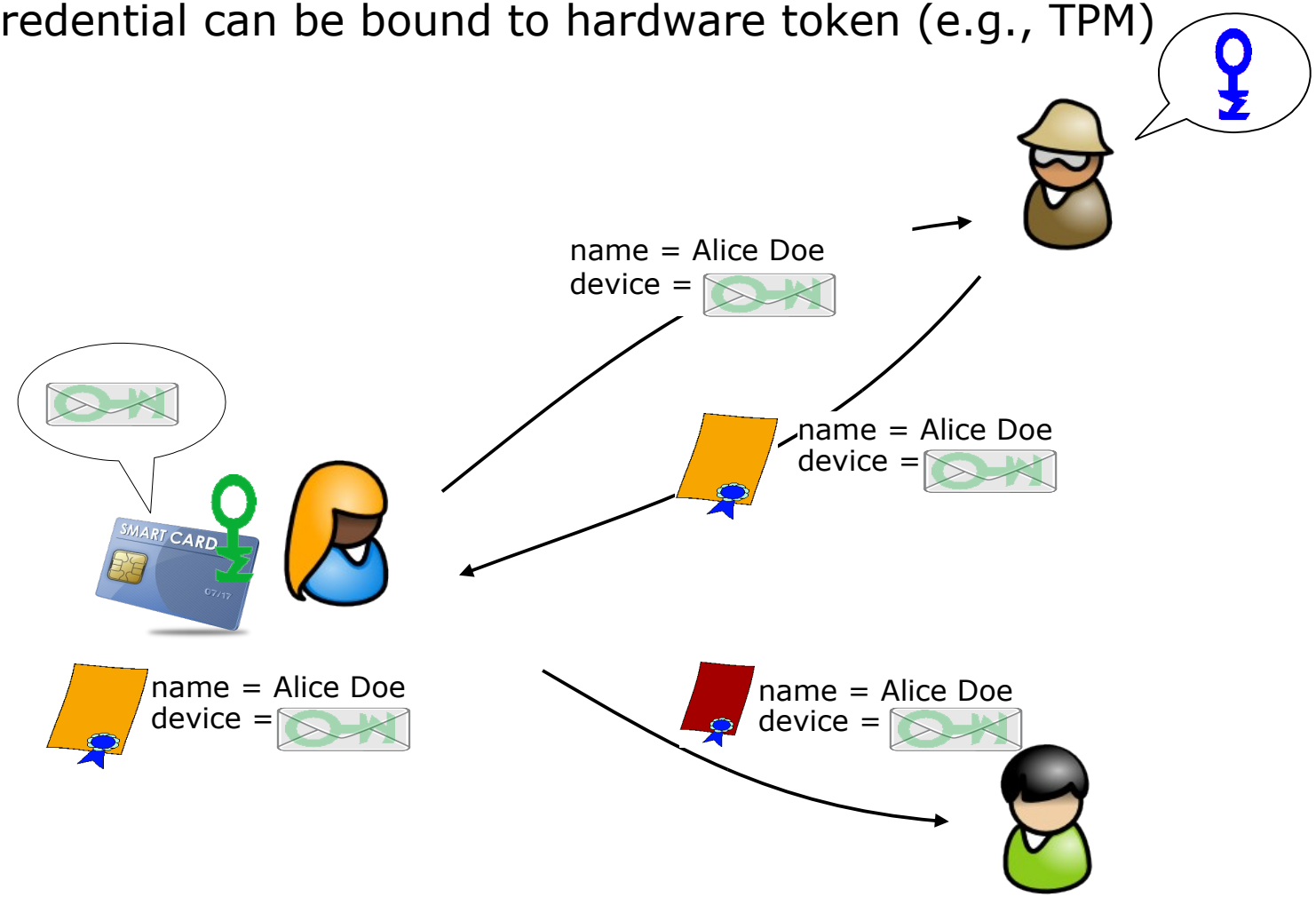
similar to usage of pseudonyms = commitments to master secret

Extended Functionality

- Predicates over attributes
- Credentials on hidden attributes
- Device binding
- Domain pseudonym
- Revocation of credentials
- Inspection of credentials/attributes
- Usage limitation
- Censorable Audit Logs

Device Binding

credential can be bound to hardware token (e.g., TPM)



presentation of credential requires presence of hardware token

Extended Functionality

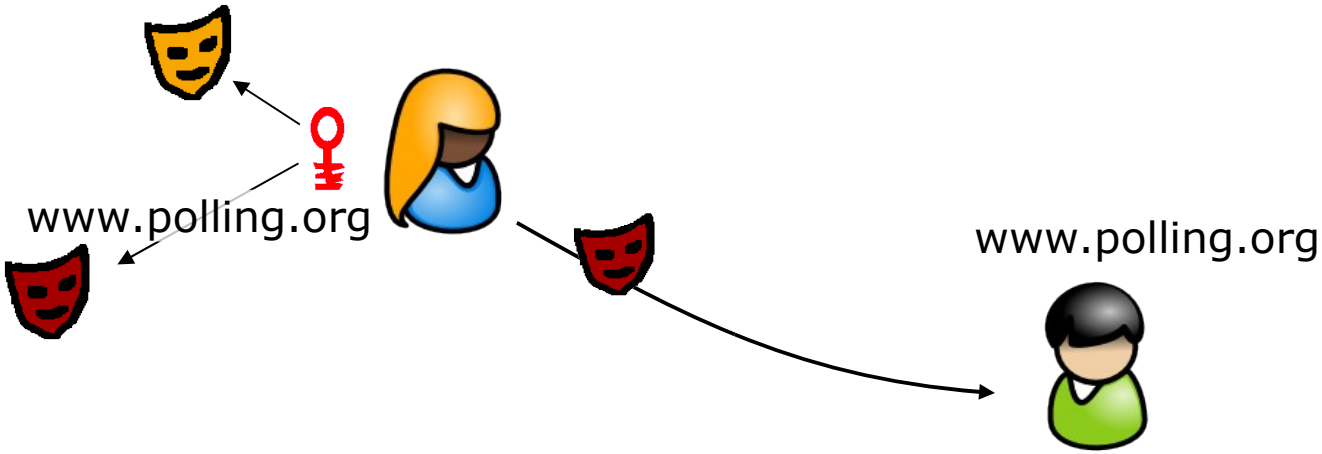
- Predicates over attributes
- Credentials on hidden attributes
- Device binding
- Domain pseudonym
- Revocation of credentials
- Inspection of credentials/attributes
- Usage limitation
- Censorable Audit Logs

Domain Pseudonyms

- sometimes user wants/must be recognized in a certain context

  normal pseudonyms are unlinkable for RPs and Issuers

  domain pseudonym = unique pseudonym for particular domain

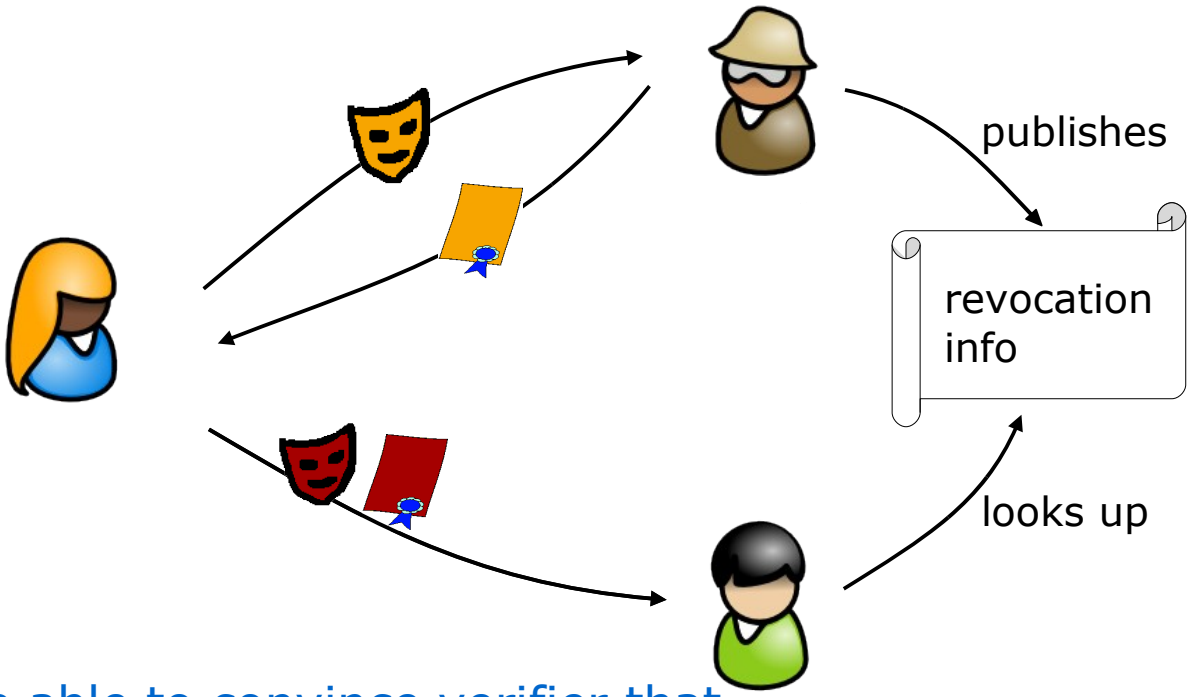


Extended Functionality

- Predicates over attributes
- Credentials on hidden attributes
- Device binding
- Domain pseudonym
- Revocation of credentials
- Inspection of credentials/attributes
- Usage limitation
- Censorable Audit Logs

Anonymous Credential Revocation

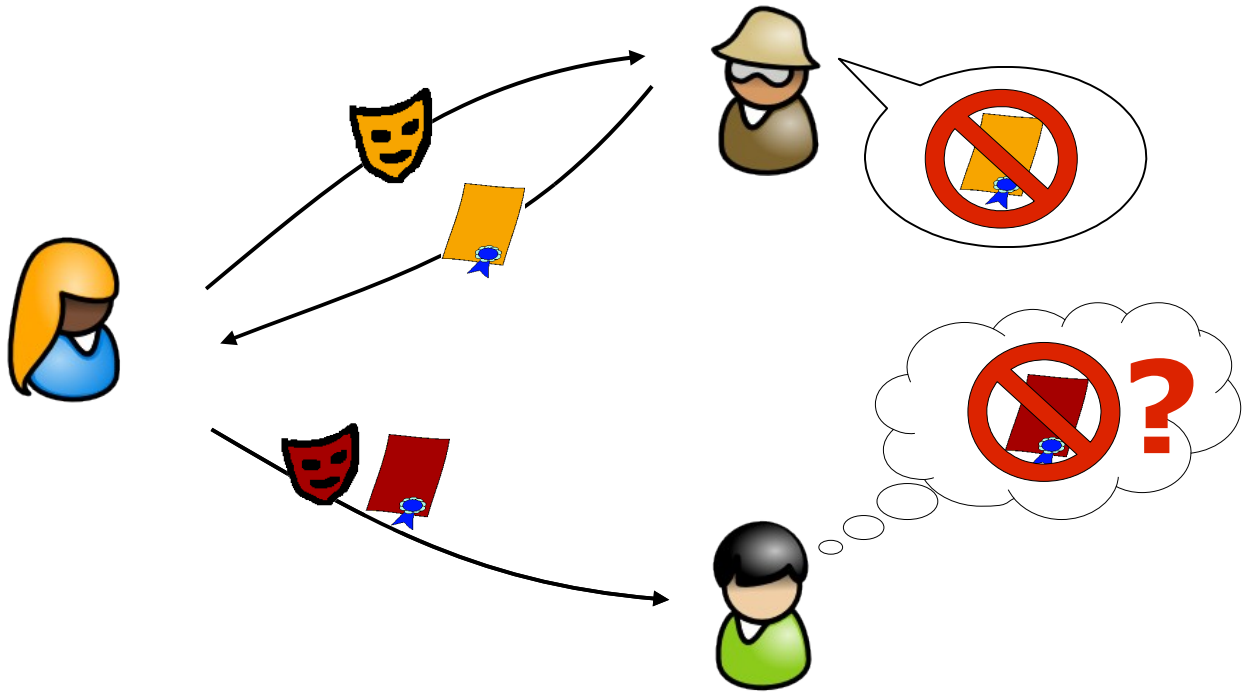
- various reasons to revoke credential
  - user lost credential / secret key
  - misbehavior of user



Alice should be able to convince verifier that her credential is among the good ones!

Anonymous Credential Revocation

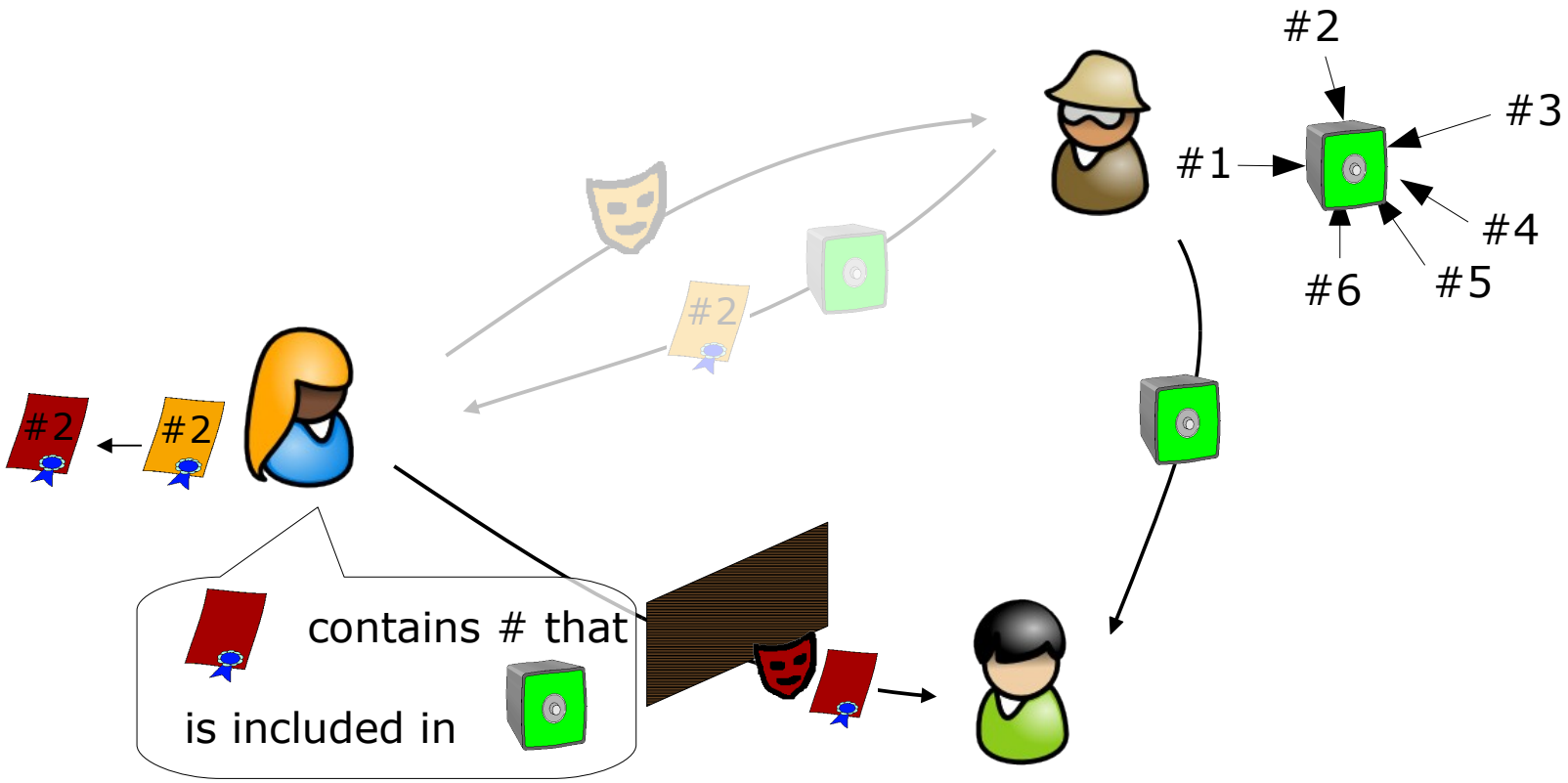
- Pseudonyms ⟶ standard revocation lists don't work



Anonymous Credential Revocation

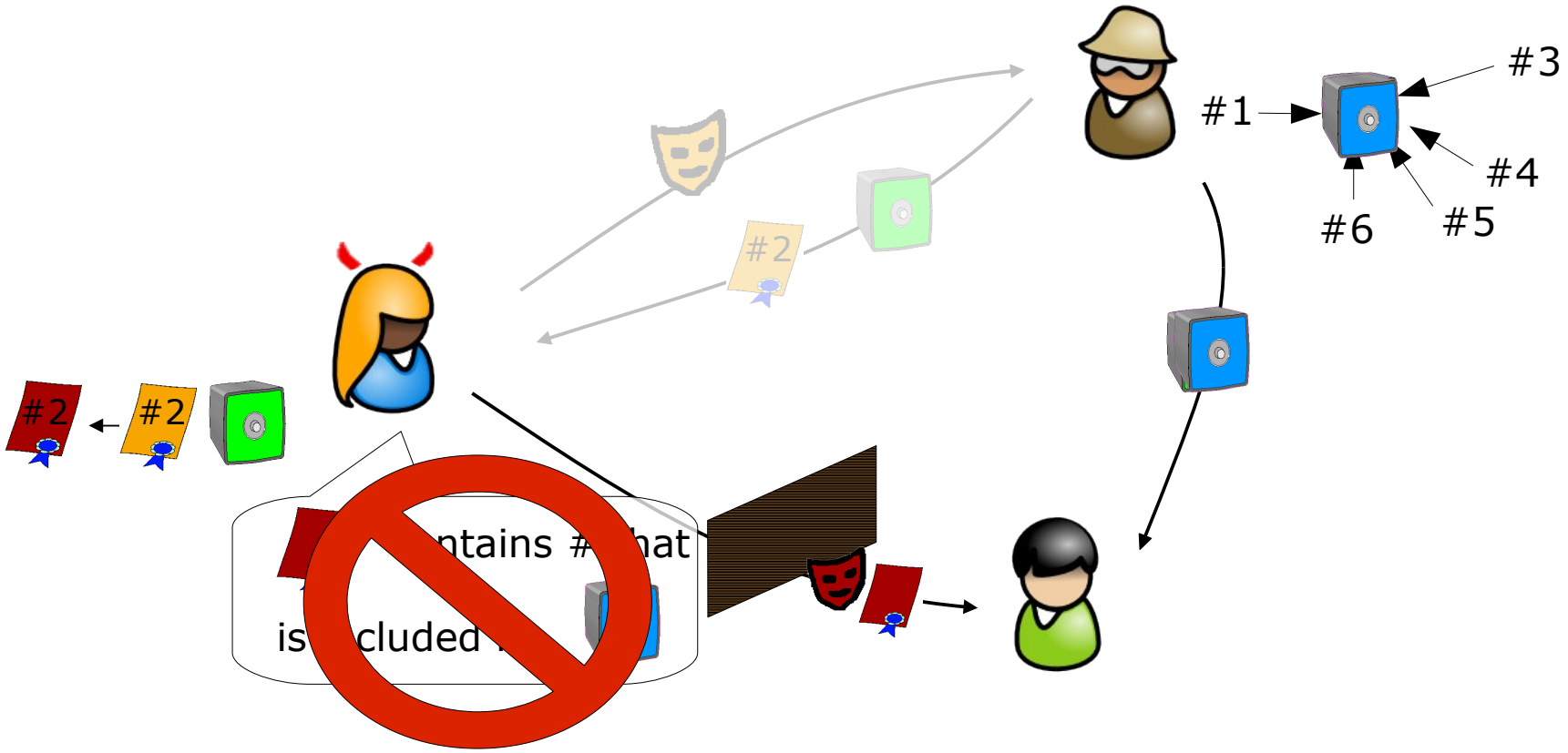
credentials contain random serial number #

Issuer accumulates all "good" serial numbers



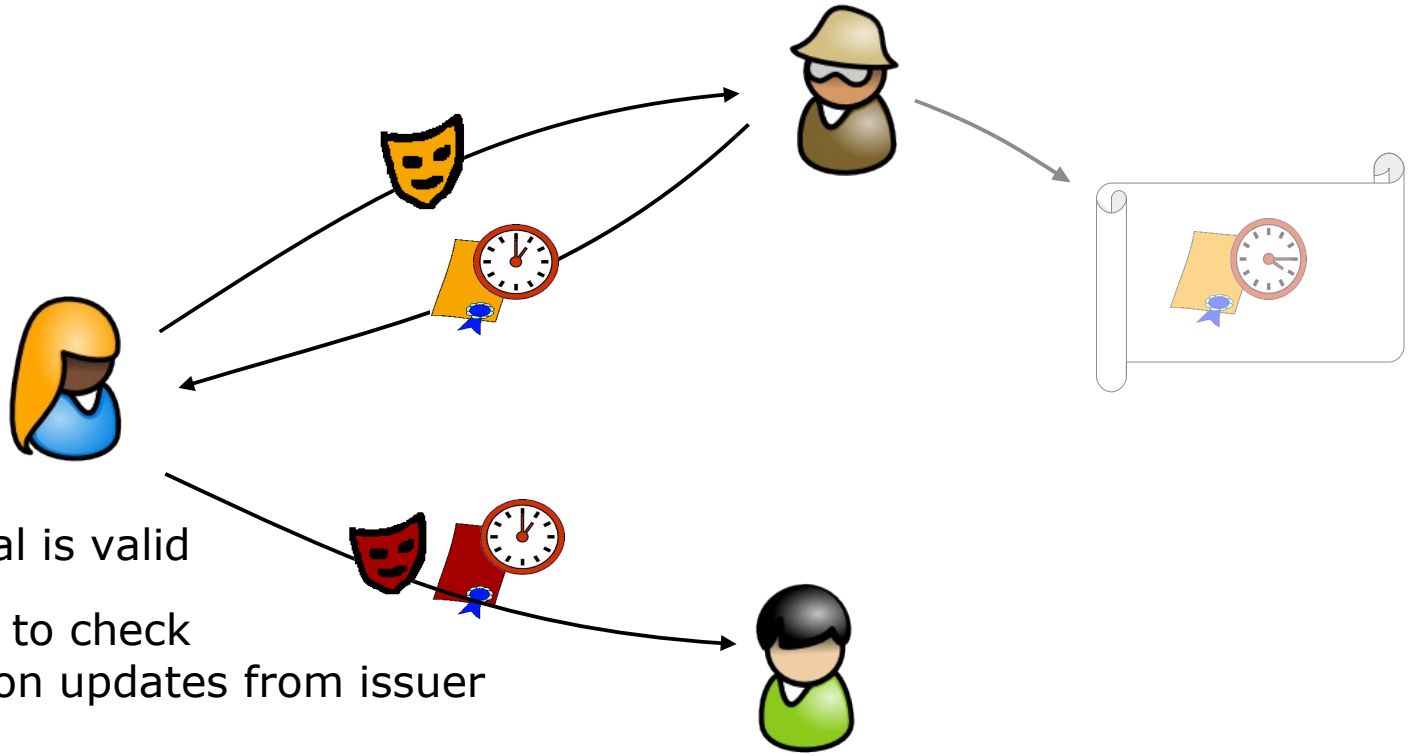
Anonymous Credential Revocation

to revoke #2 issuer publishes new accumulator (& new updates for unrevoked credentials)



Anonymous Credential Revocation

Update of Credentials: encode validity time as attribute



if credential is valid

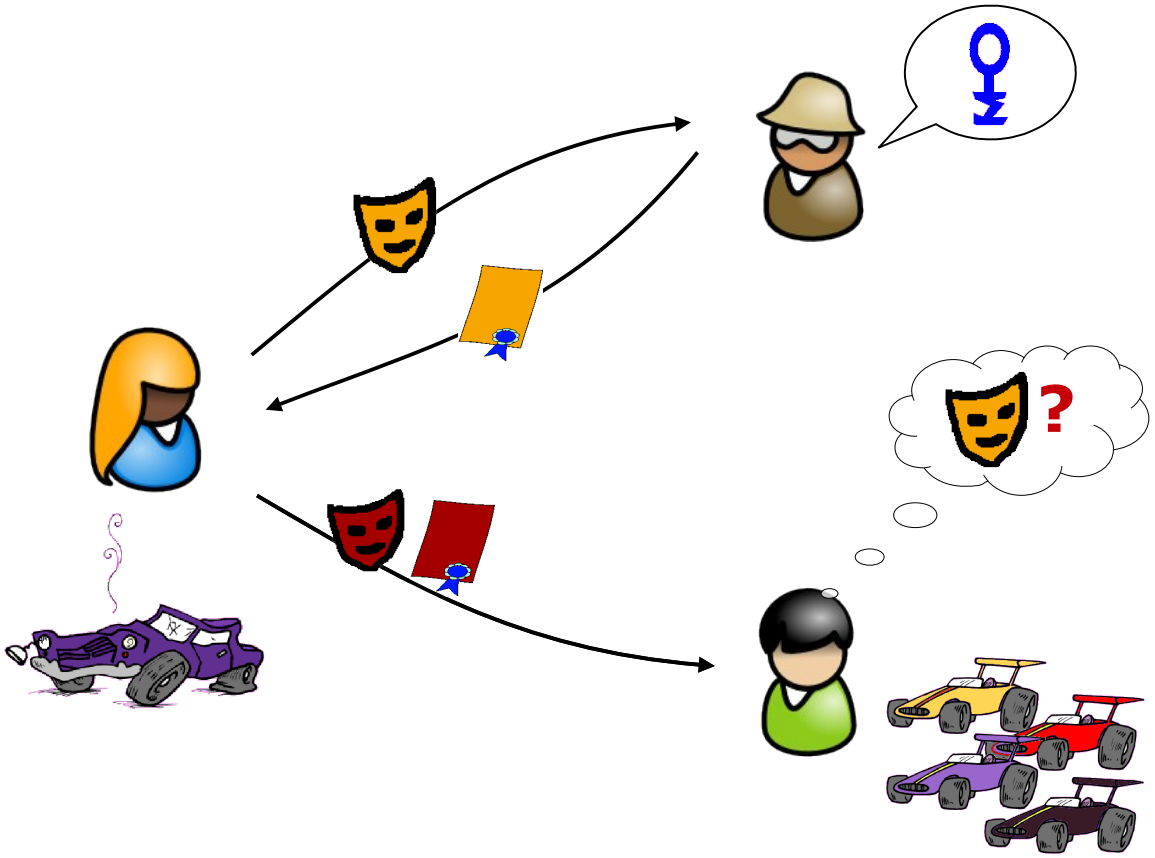
→ no need to check
revocation updates from issuer

no additional effort for verifier

Extended Functionality

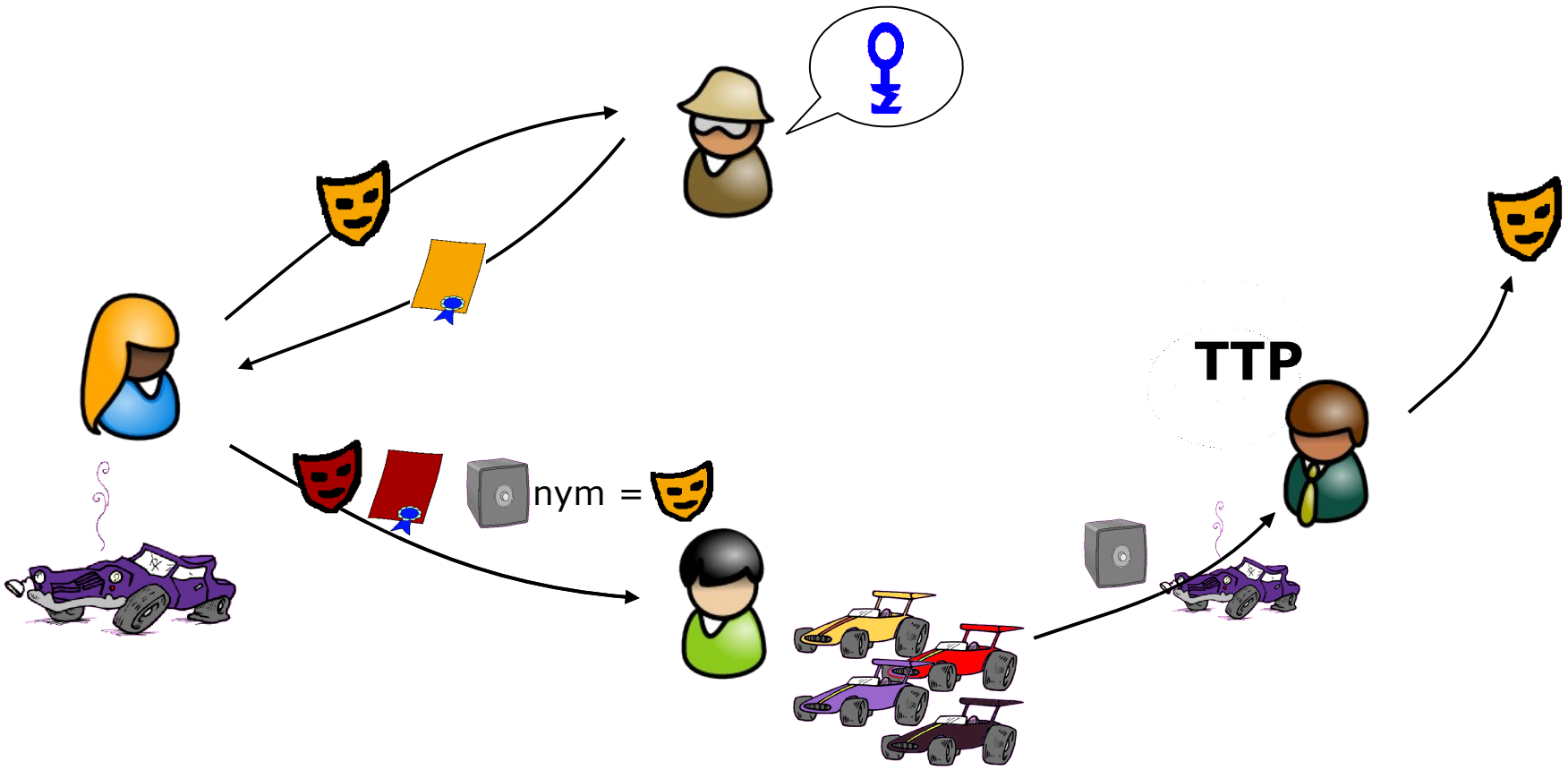
- Predicates over attributes
- Credentials on hidden attributes
- Device binding
- Domain pseudonym
- Revocation of credentials
- Inspection of credentials/attributes
- Usage limitation
- Censorable Audit Logs

Inspection of Credentials/Attributes



Alice rents a car and breaks it: ID needs to be retrieved

Inspection of Credentials/Attributes



Alice rents a car and breaks it: ID needs to be retrieved

- Can verifiably encrypt any certified attribute *(optional)*
- TTP is off-line & can be distributed to lessen trust

Extended Functionality

- Predicates over attributes
- Credentials on hidden attributes
- Device binding
- Domain pseudonym
- Revocation of credentials
- Inspection of credentials/attributes
- Usage limitation
- Censorable Audit Logs

Usage limitation

- Limited Spending
  - credential is only allowed to be spent at most n times
  - challenge: recognize n+1 usage, w/o sacrificing unlinkeability

"online solution"

- if user wants to spend credential the n+1 time

  he is caught immediately & access is denied
- requires a common state of all verifiers

"offline solution"

- if user has spent the credential > n times

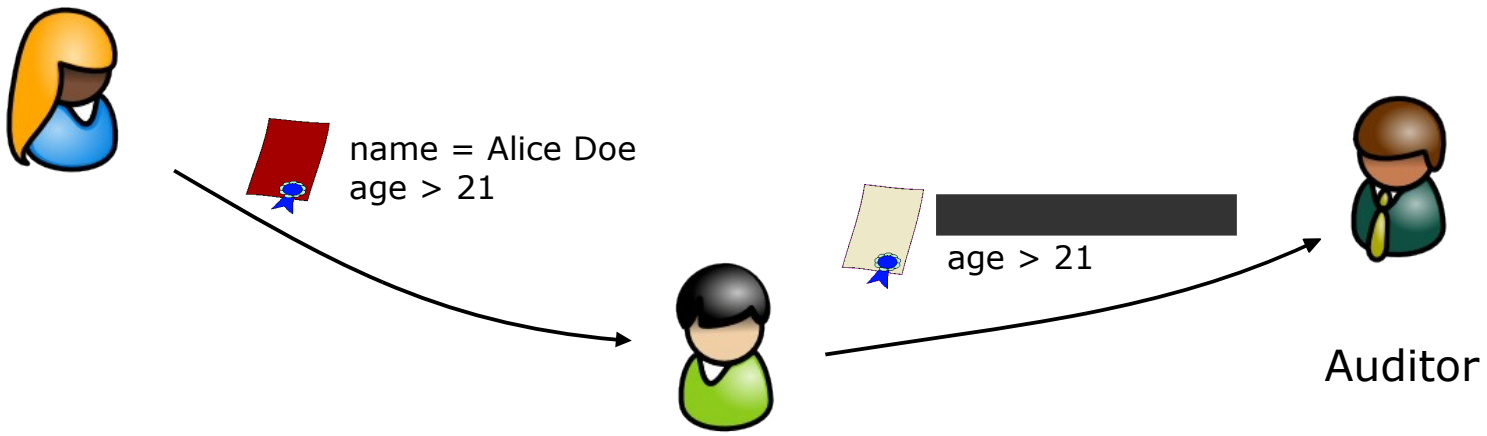
  → will be detected and reveals his identity

Extended Functionality

- Predicates over attributes
- Credentials on hidden attributes
- Device binding
- Domain pseudonym
- Revocation of credentials
- Inspection of credentials/attributes
- Usage limitation
- Censorable Audit Logs

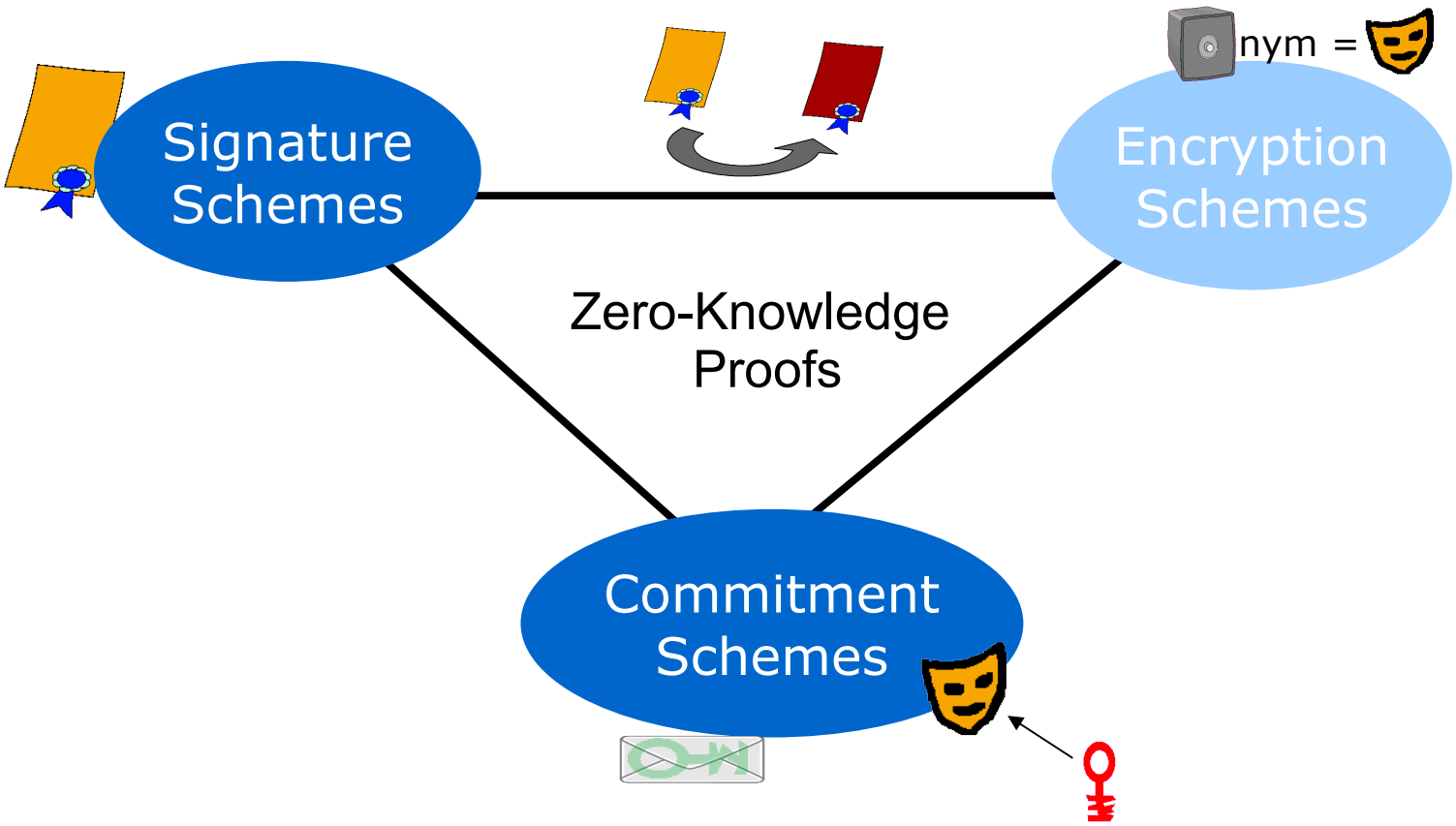
Censorable Audit Logs

- relying parties can remove information from presented token
- sanitized token is still verifiable wrt Issuer



Solutions: Idemix & U-Prove

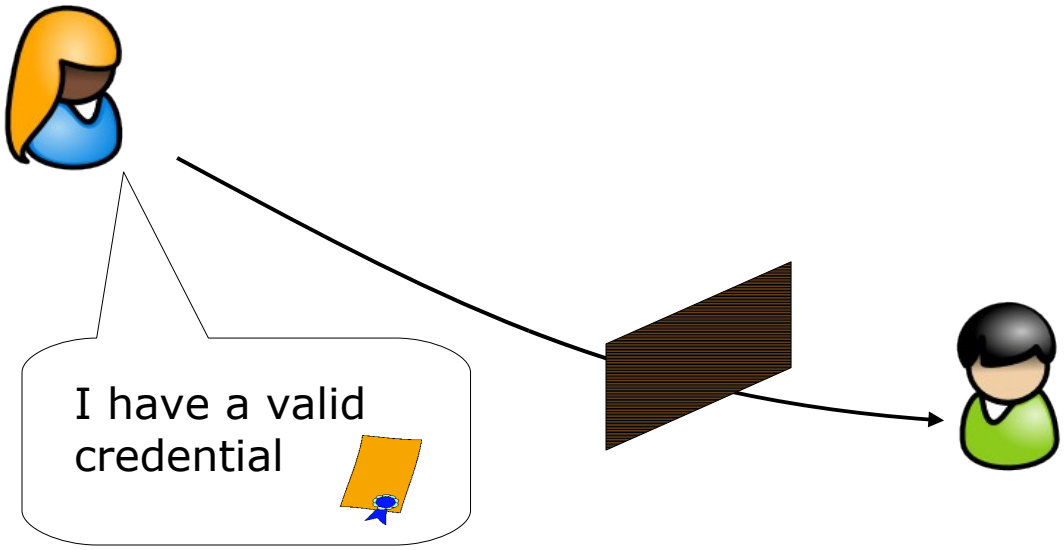
Solutions | Cryptographic Ingredients



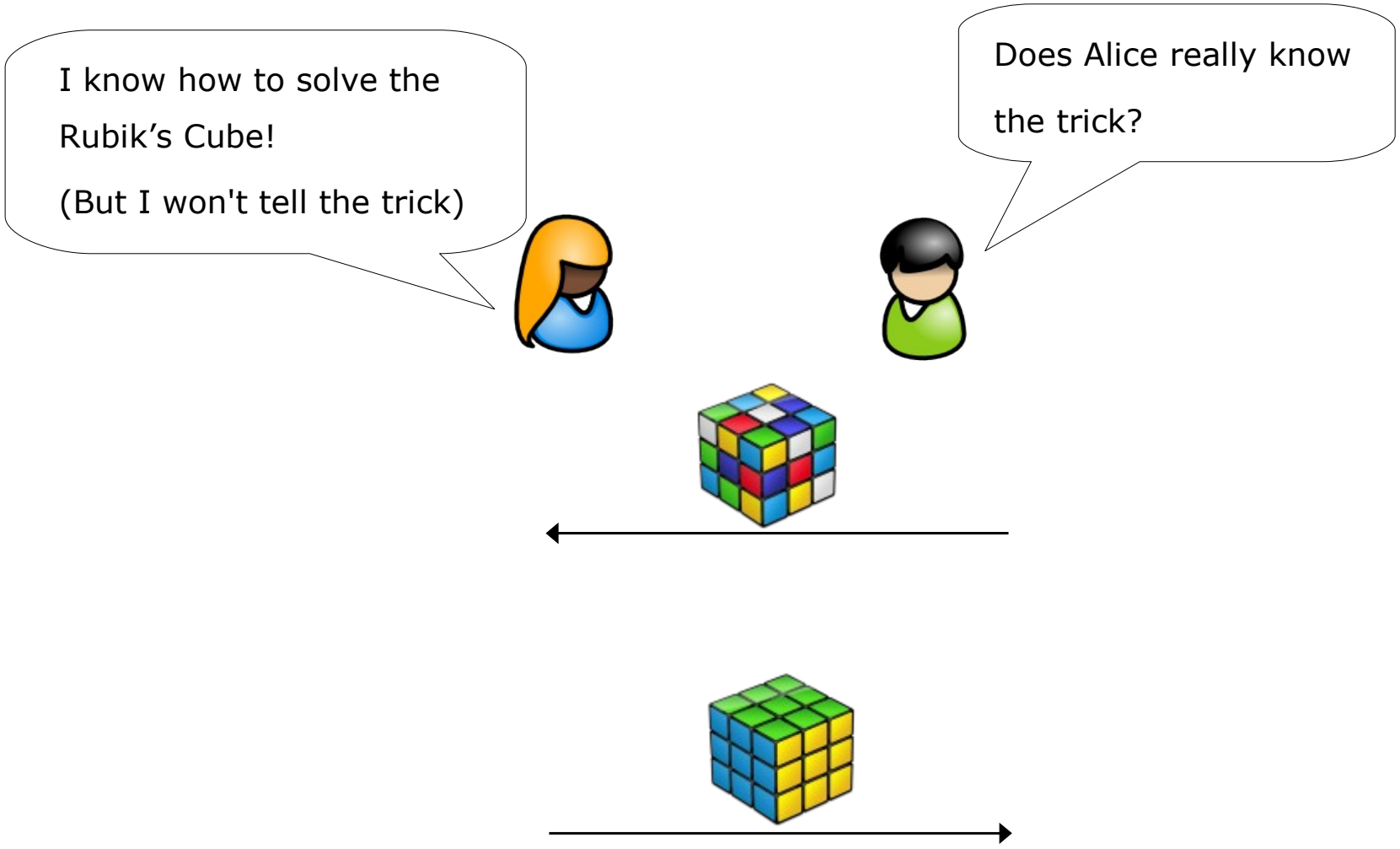
Prover Alice wants to convince verifier Bob that

she knows a secret

...but without him learning the secret!

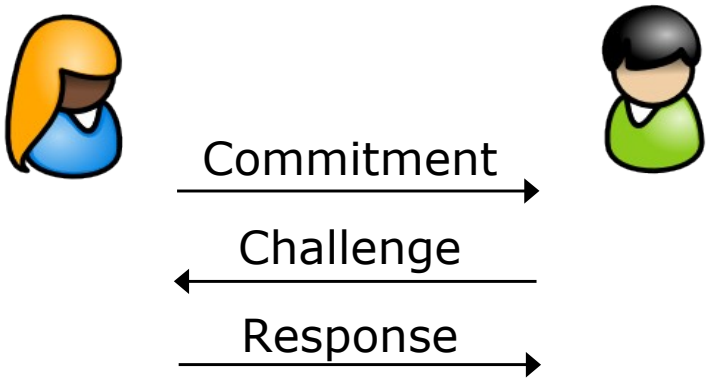


- Toy Example: Rubik's Cube



repeat until Bob is convinced ...

- interactive proof



- properties:

  zero-knowledge

  verifier learns nothing about the prover's secret

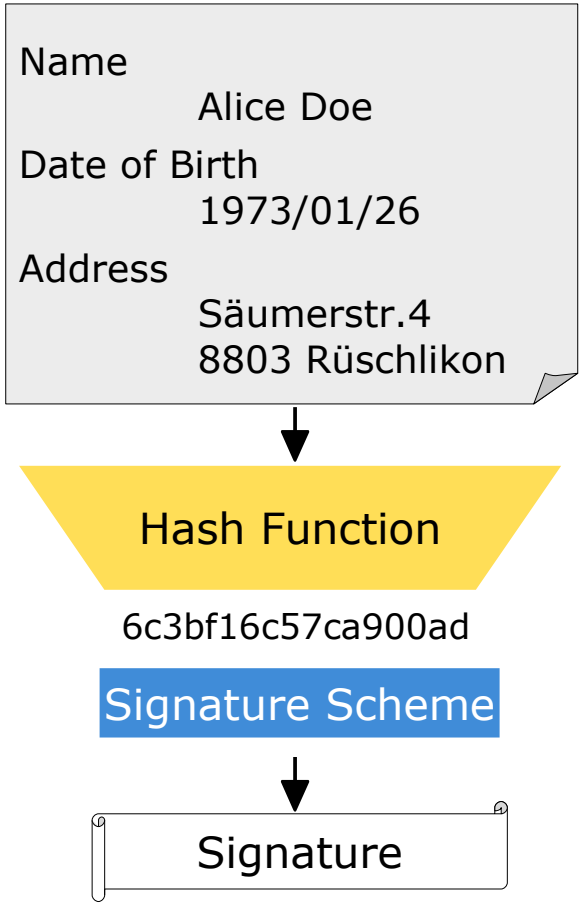
  soundness

  prover can convince verifier only if she knows the secret

  completeness

  if prover knows the secret she can always convince the verifier

- need for "special" signatures, i.e., standard signatures wont work:

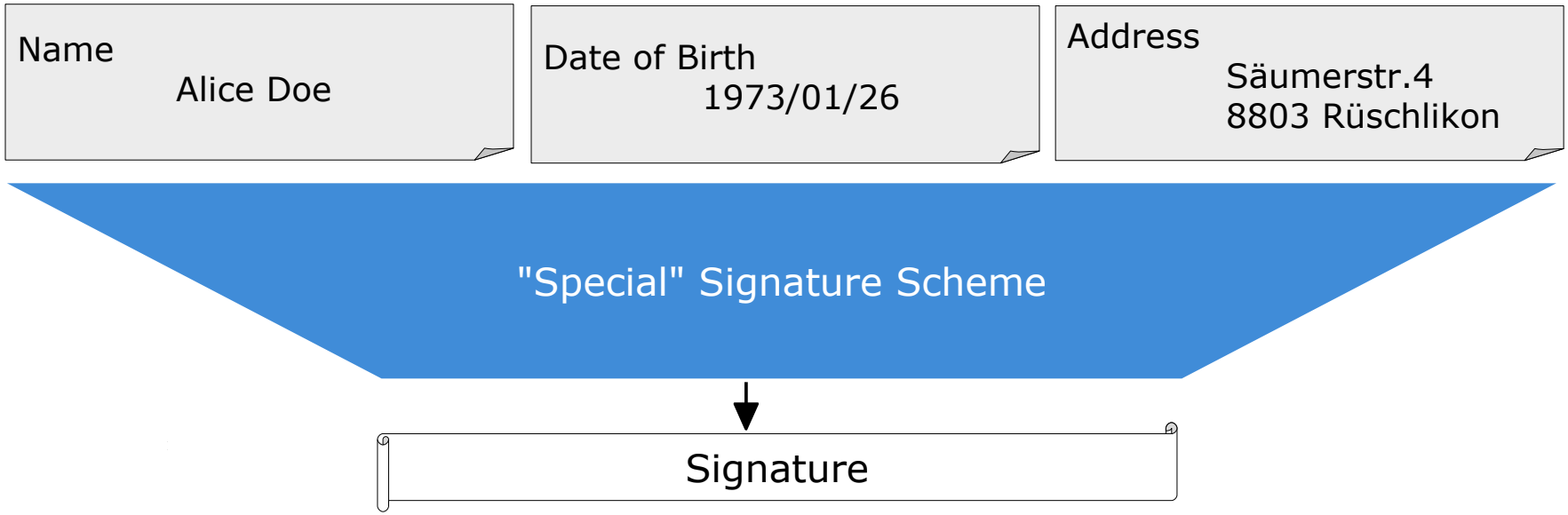


only the short hash value gets signed

verification requires to recompute the hash

→ full message (i.e., all attributes) must be disclosed

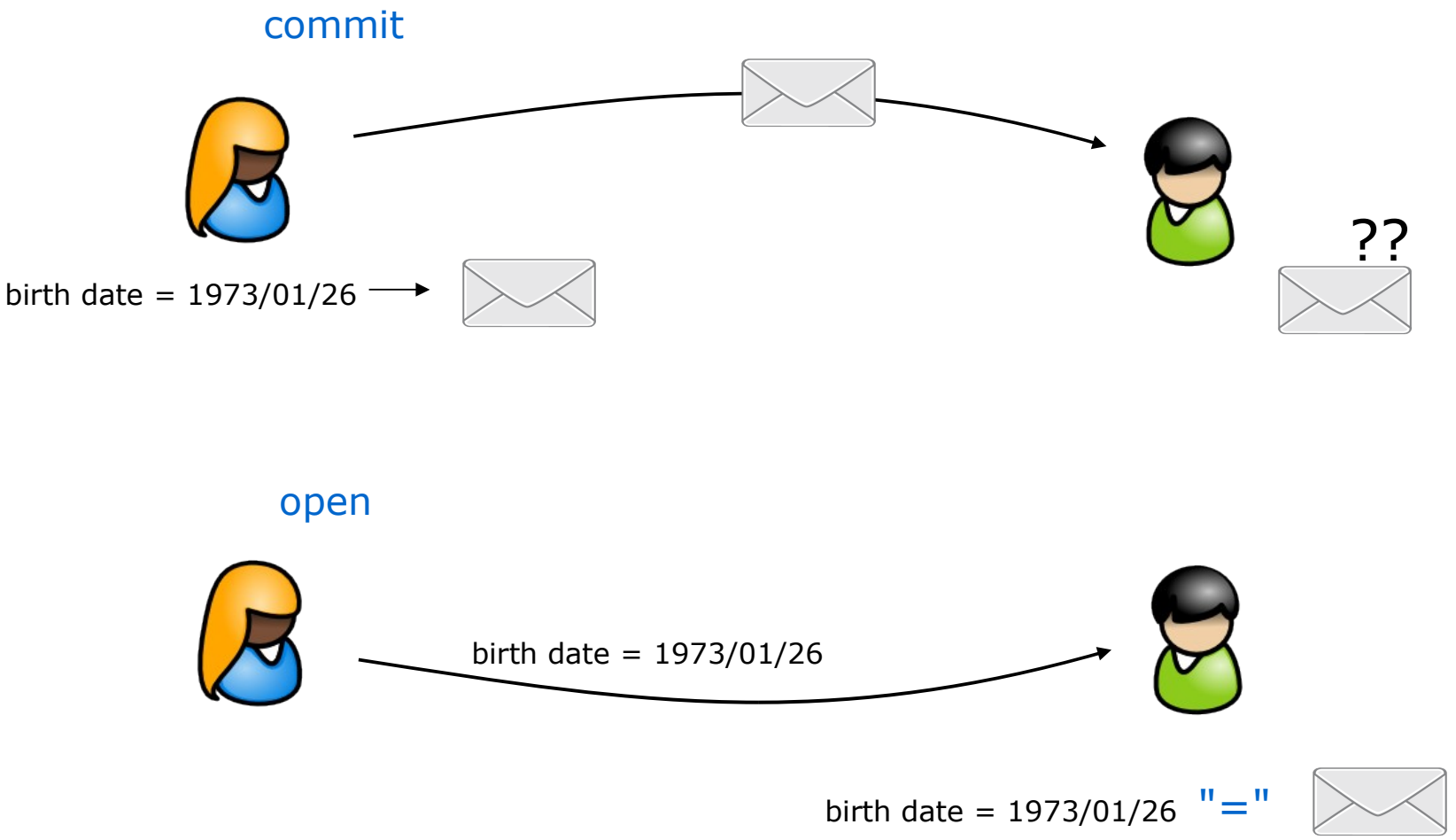
- "special" signatures: sign multiple message blocks & don't hash



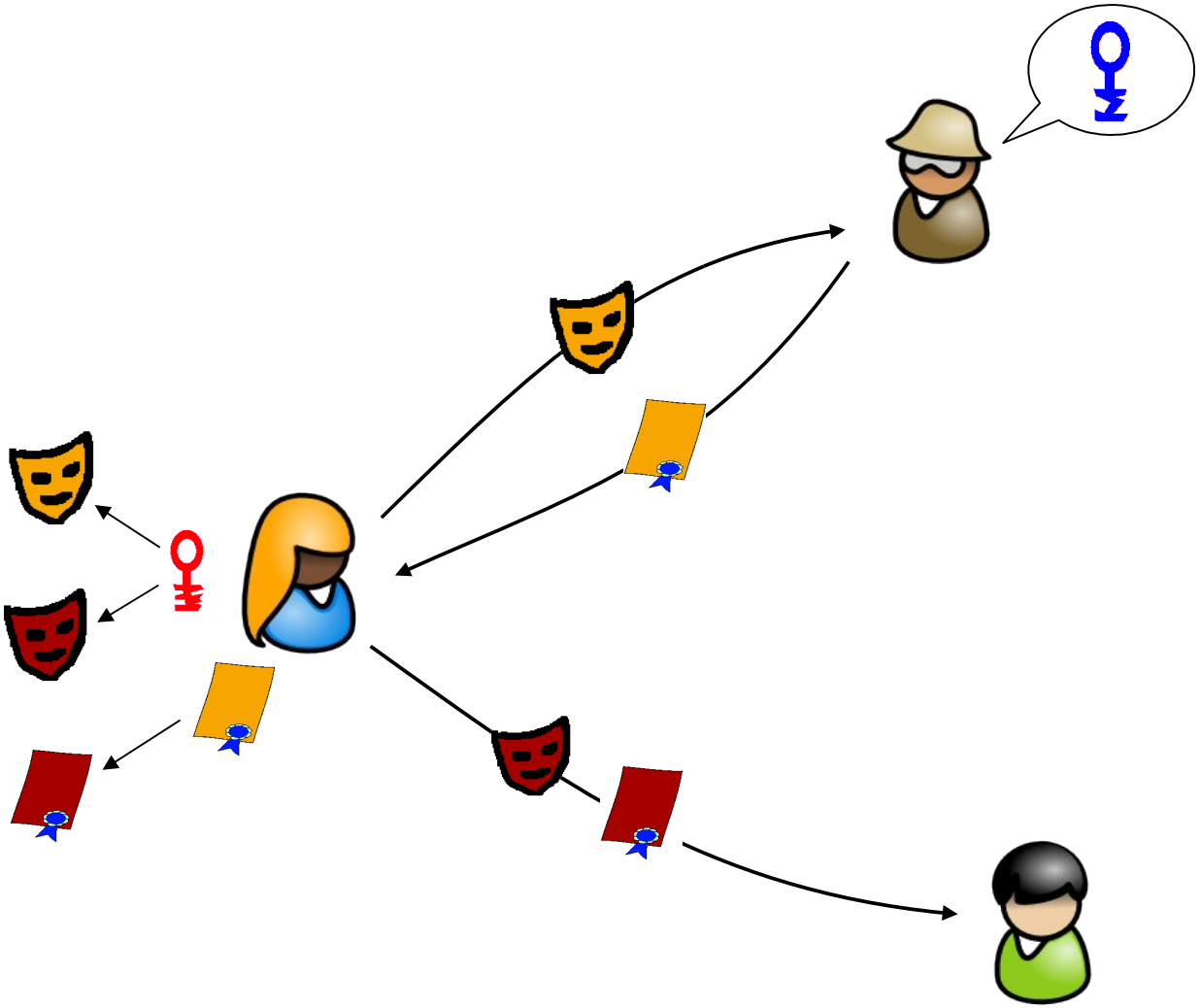
multiple message blocks + structure of signature scheme allow selective disclosure
i.e., not all messages blocks are required to verify a signature

plain (i.e., not hashed) message blocks allow predicate proofs

Cryptographic Ingredients | Commitment Schemes

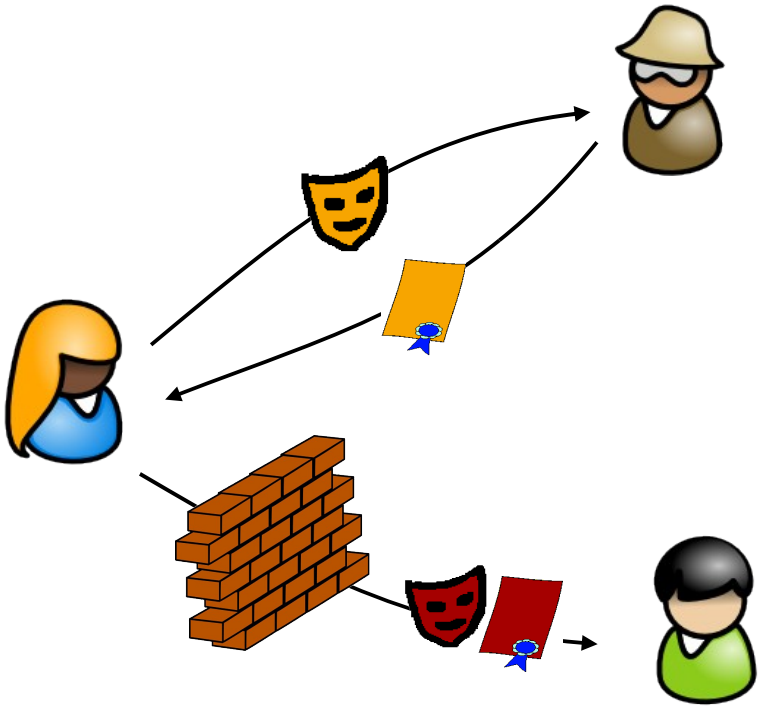


Minimal Disclosure Wallets | Recap



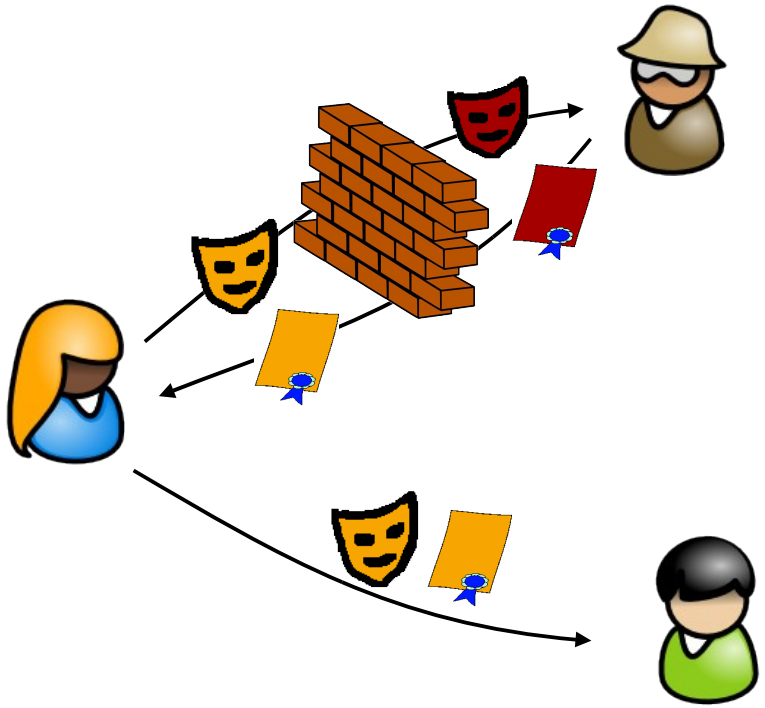
Minimal Disclosure Wallets - Two Approaches

Zero-Knowledge Proofs



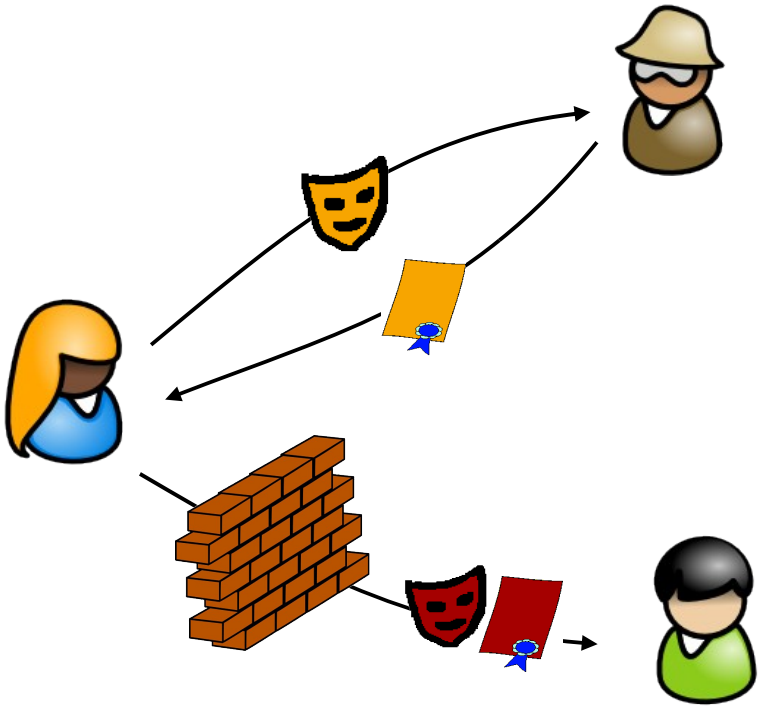
Idemix

Blind Signatures



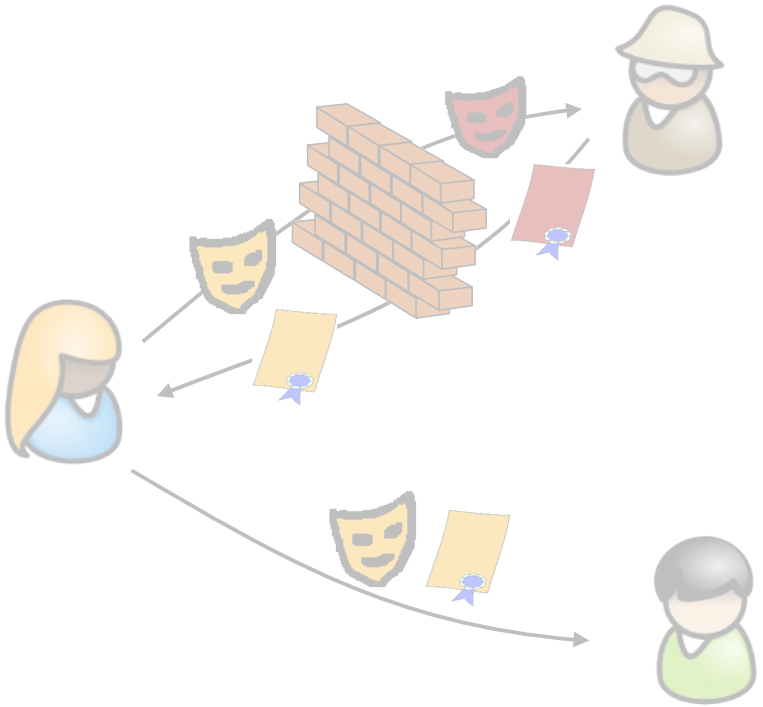
U-Prove

Zero-Knowledge Proofs



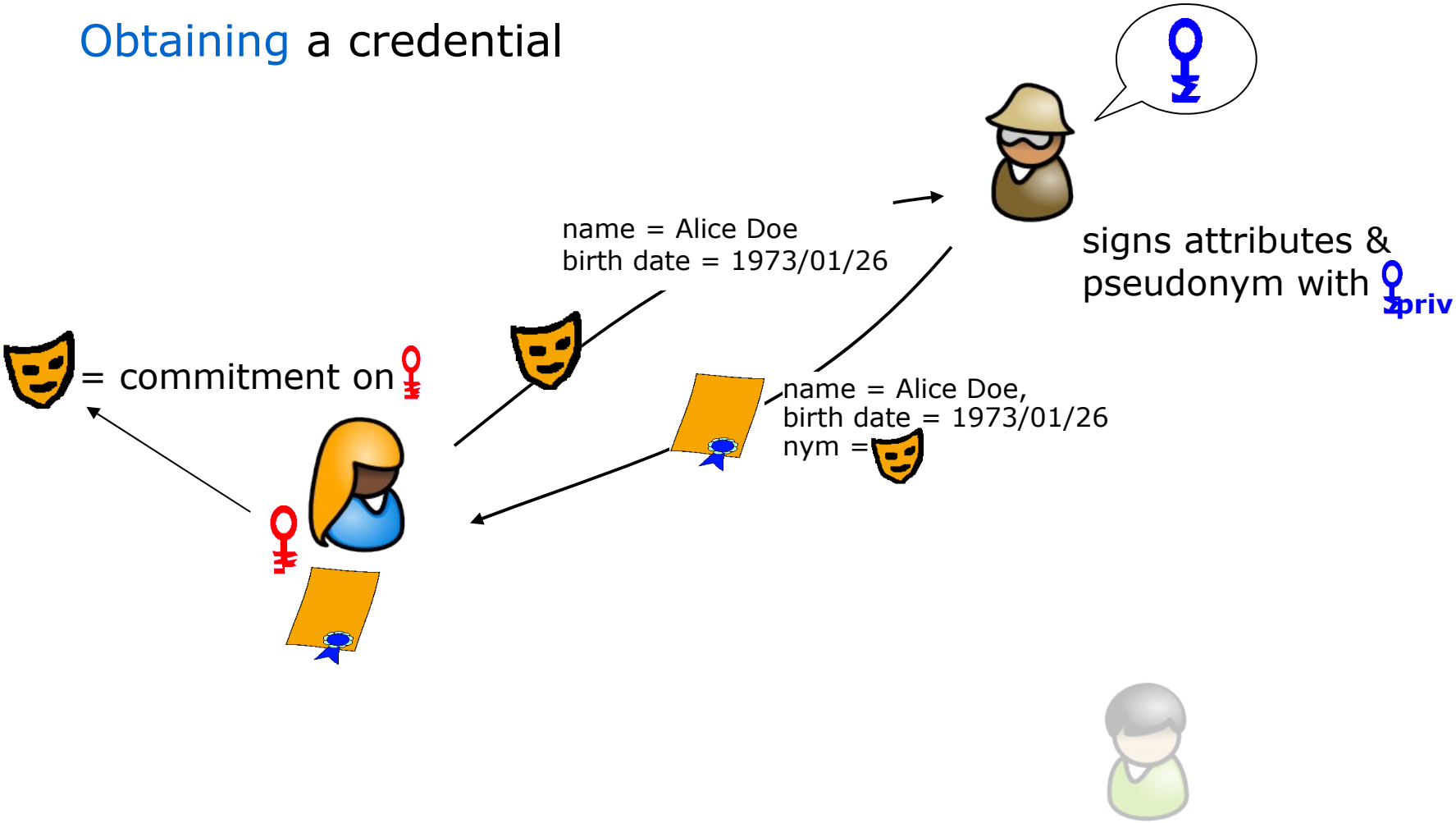
Idemix

Blind Signatures

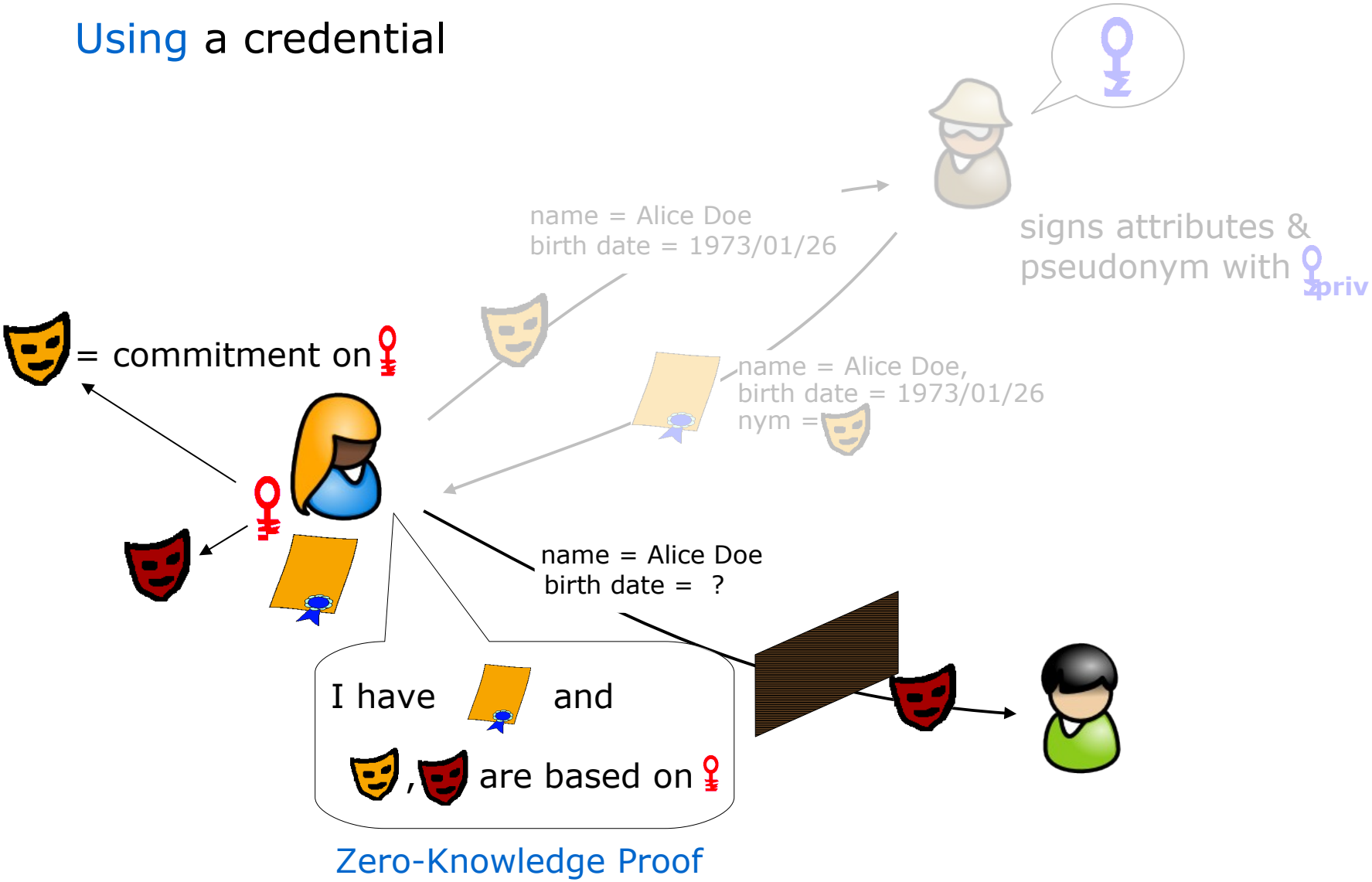


U-Prove

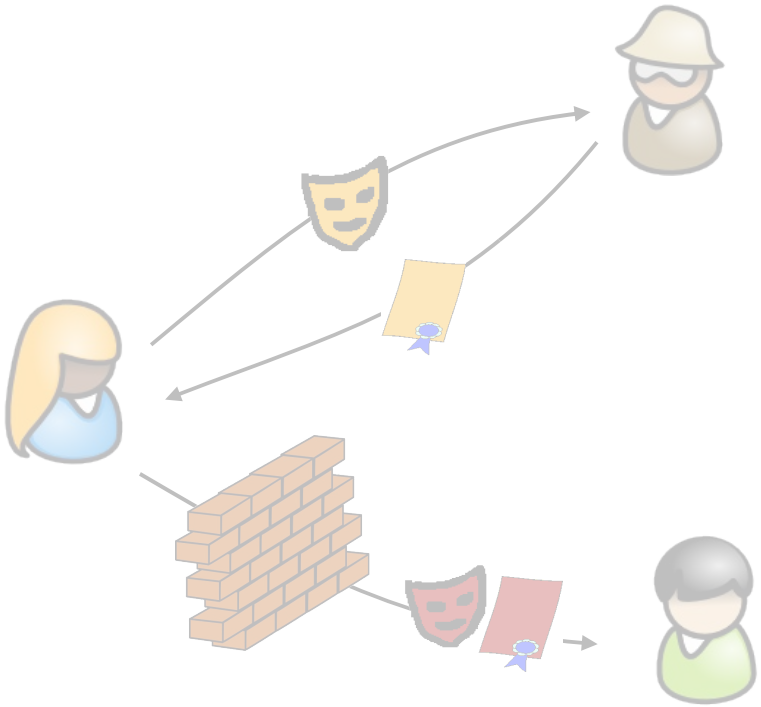
Obtaining a credential



Using a credential

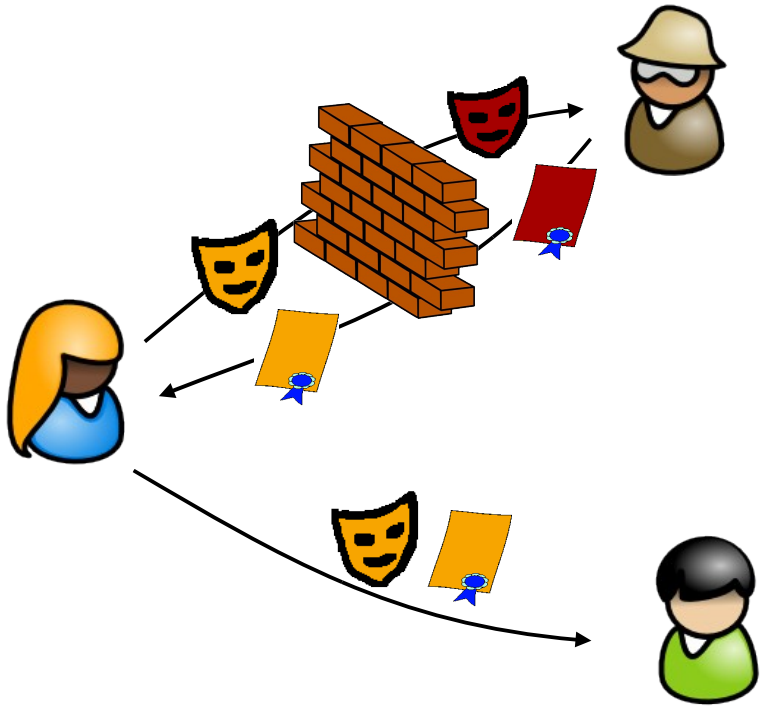


Zero-Knowledge Proofs



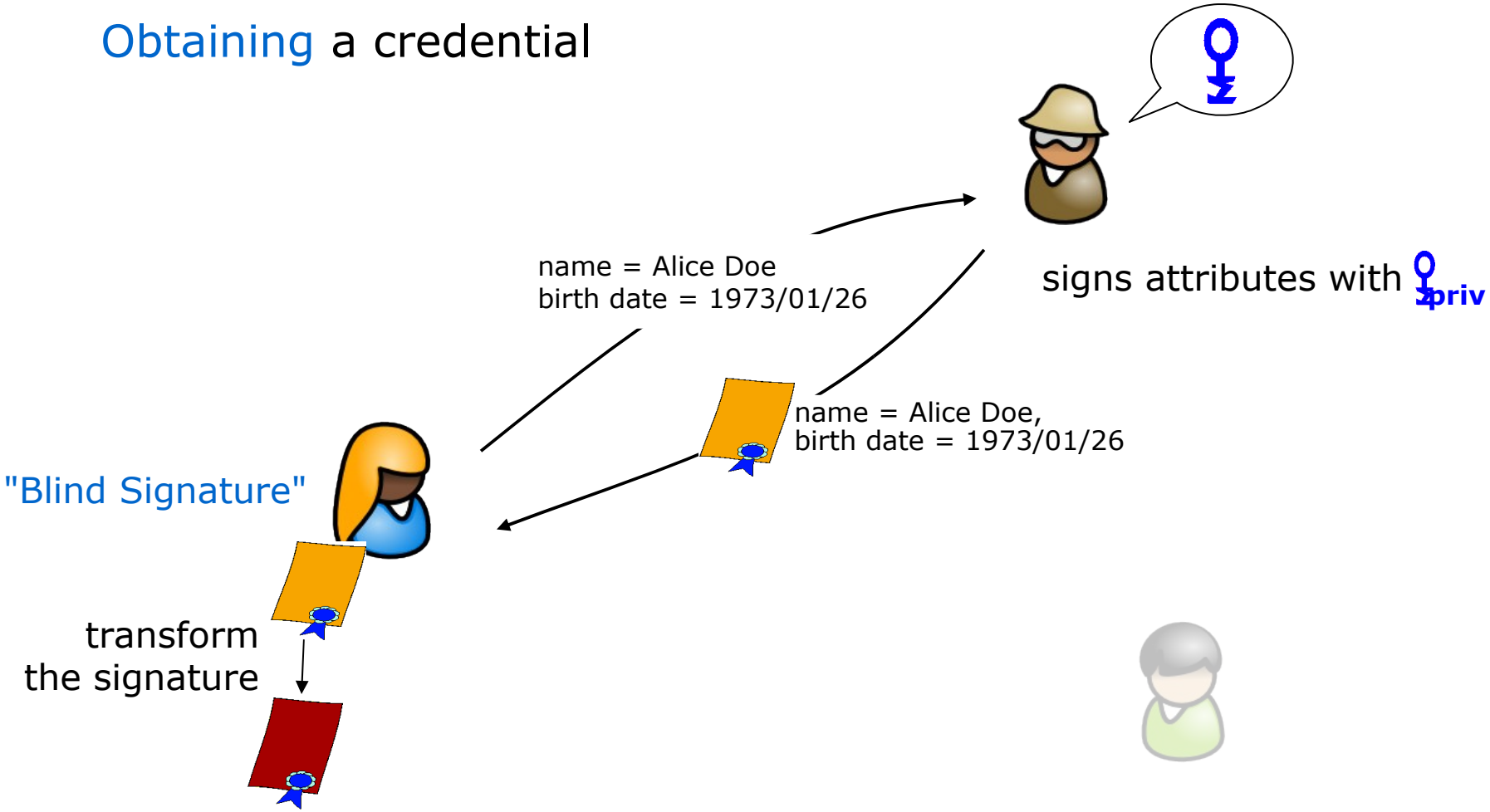
Idemix

Blind Signatures

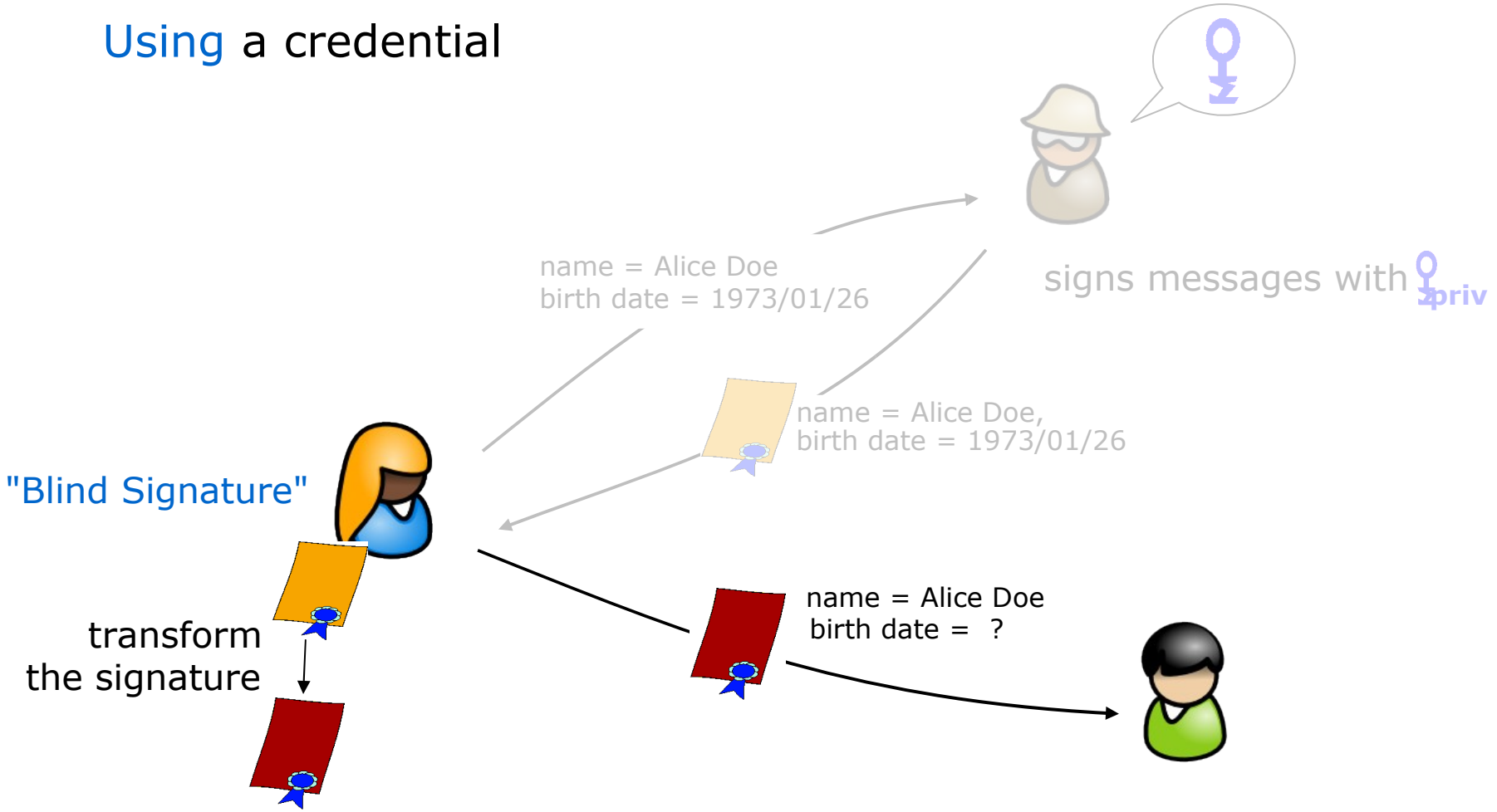


U-Prove

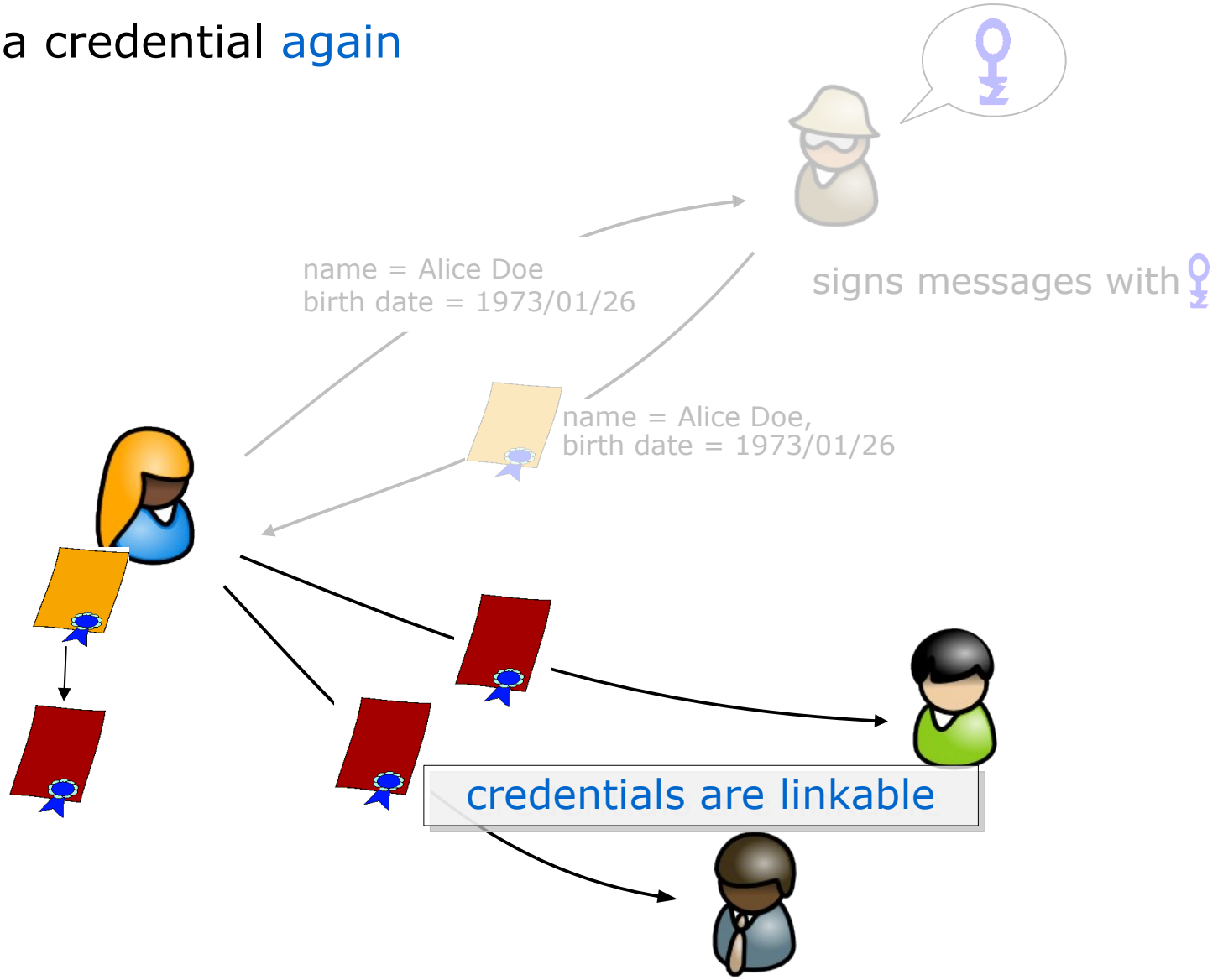
Obtaining a credential



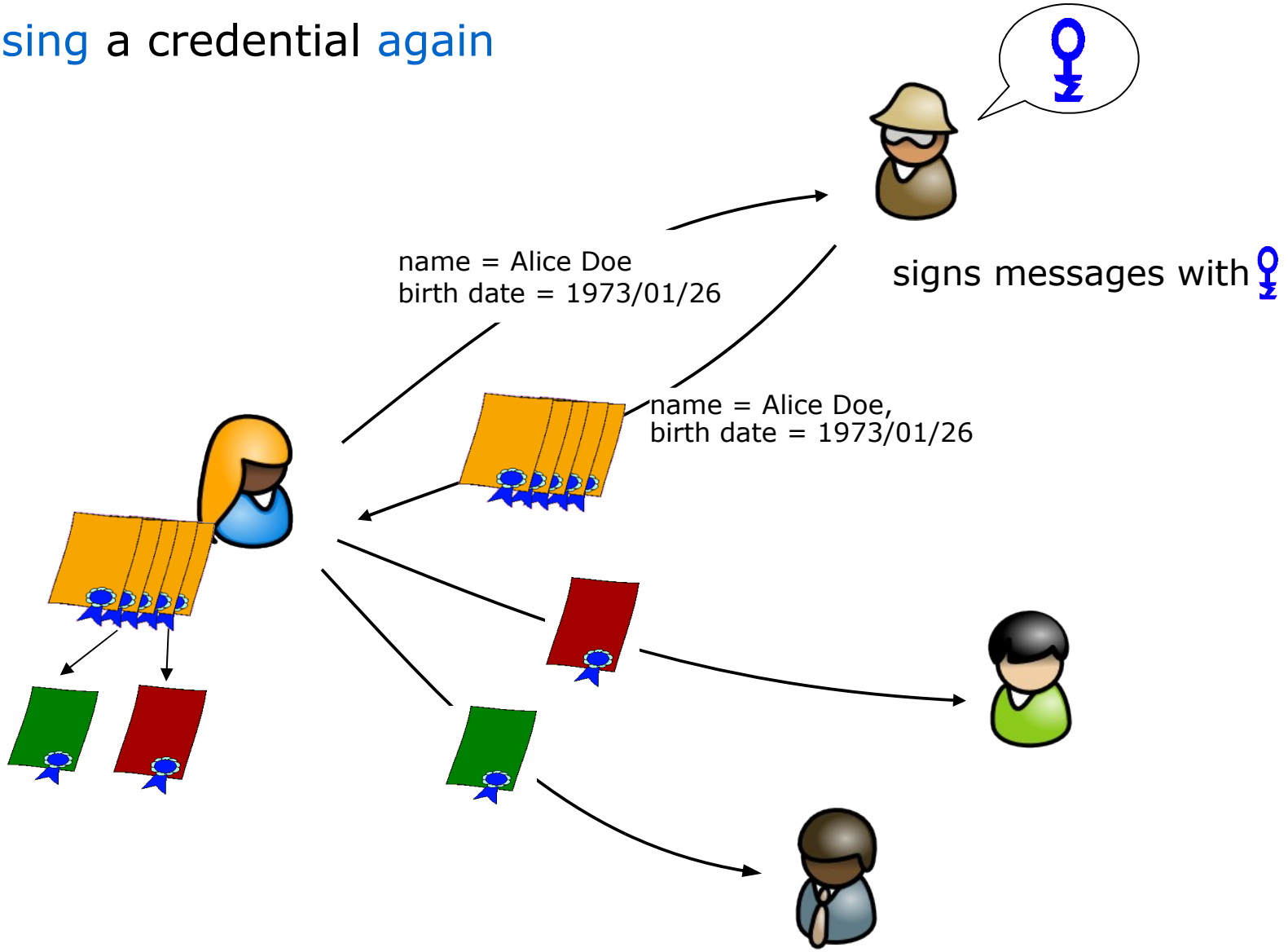
Using a credential



Using a credential again

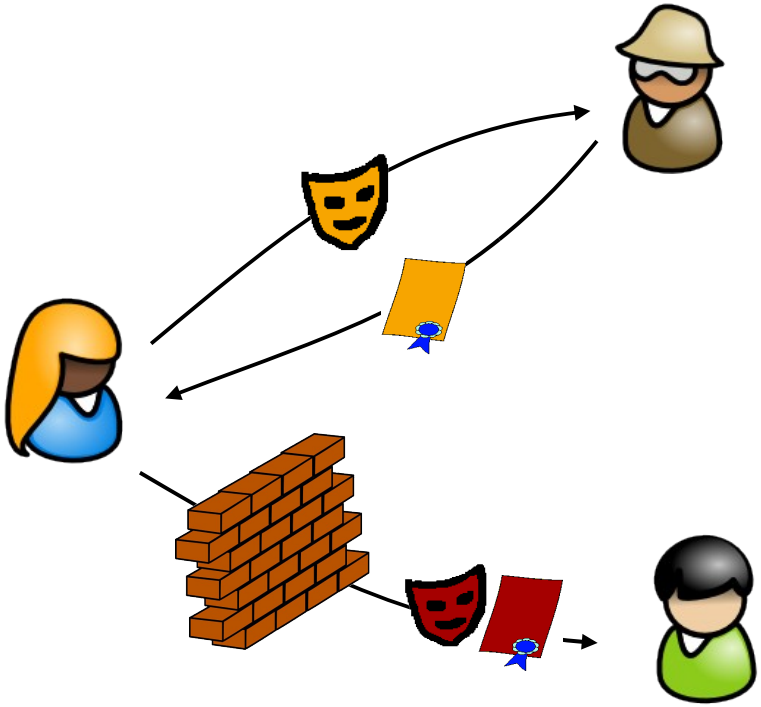


Using a credential again



Minimal Disclosure Wallets - Two Approaches

Zero-Knowledge Proofs

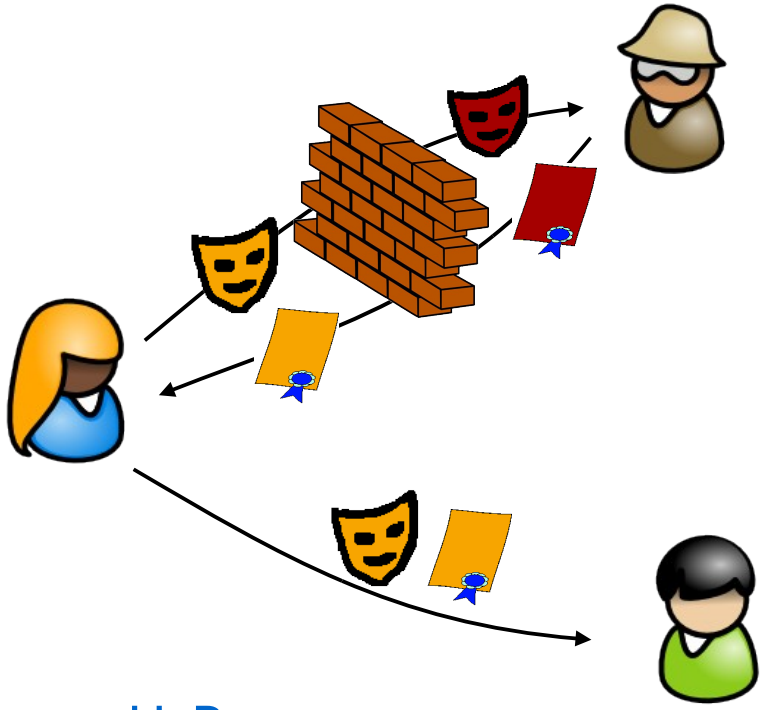


Idemix (Identity Mixer)

Damgard, Camenisch&Lysyanskaya

Strong RSA, pairings (LMRS, q-SDH)

Blind Signatures

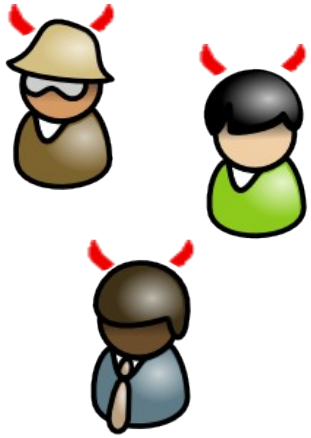


U-Prove

Chaum, Brands et al.

Discrete Logs, RSA,..

- Protection of user's privacy
  - pseudonyms
  - unlinkeability (multi-use)
  - selective attribute disclosure

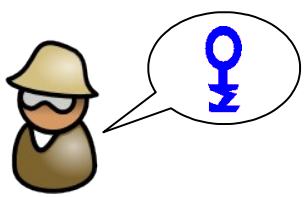


- Using multiple credentials

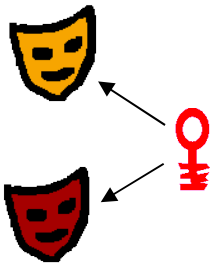
- Unforgeability of credentials
- Consistency of credentials (no sharing)


Summary

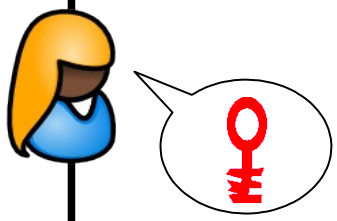
Minimal Disclosure Wallets vs. Classical Certificates



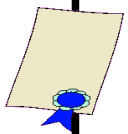
each issuer has public key of signature scheme



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

Summary

- minimal disclosure wallets allow controlled release of personal data
  - strong yet privacy preserving authentication
  - unlinkable use of credentials - prevents profiling
- efficient solutions for minimal disclosure tokens/wallets exist
  - Idemix & U-Prove
    - share similar mathematical structure (interoperable)
  - implementations are available
- various extensions possible
  - revocation, inspection, device binding,..
  - techniques can be combined with Idemix & U-Prove