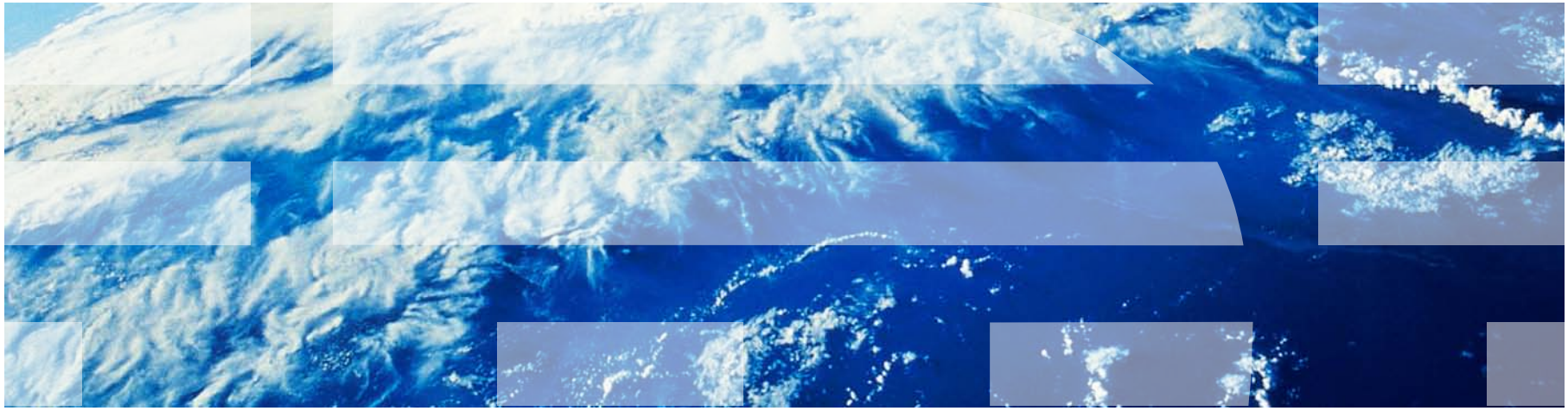
Gregory Neven, IBM Research – Zurich

NIST Meeting on Privacy-Enhancing Cryptography, December 8-9, 2011, Gaithersburg, MD

IBM Identity Mixer (idemix)



Motivation

Online security & trust today:

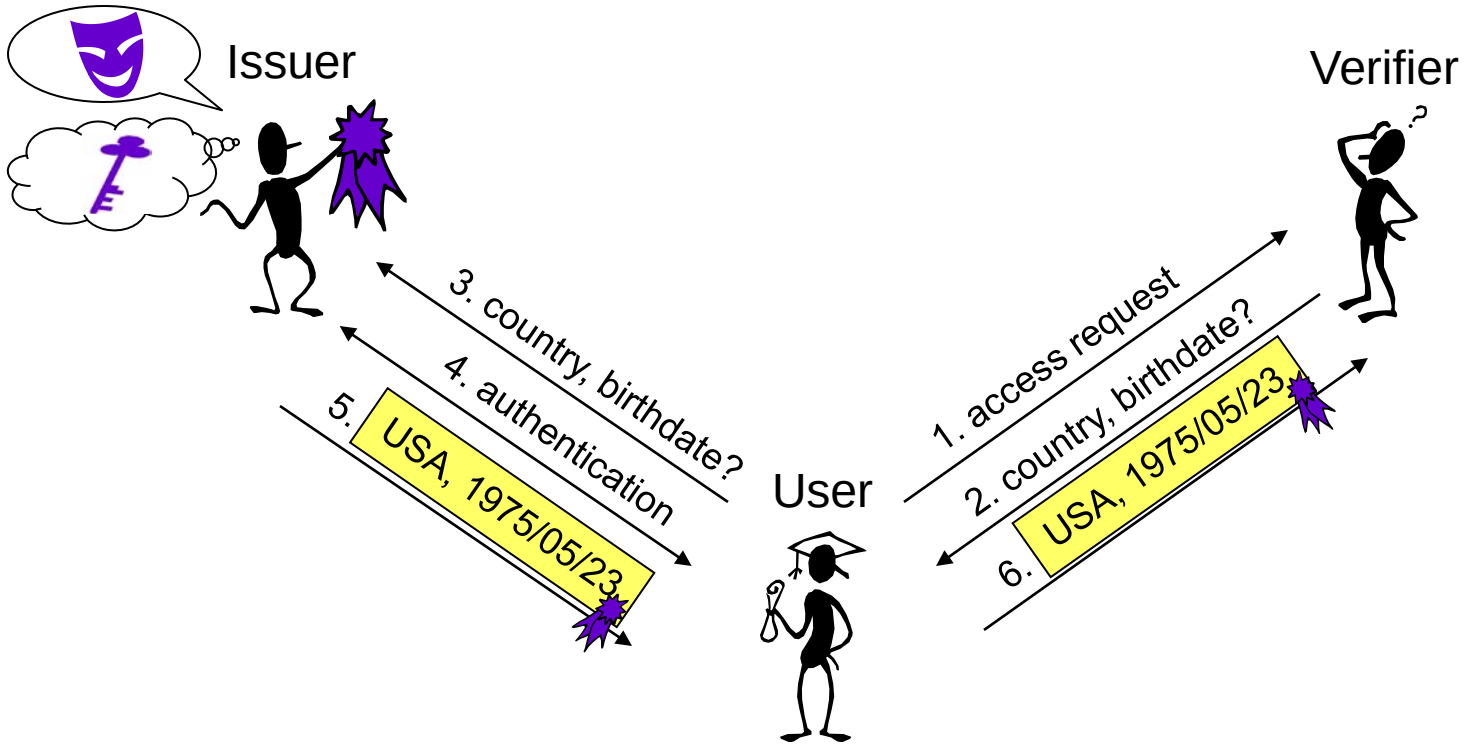
- SSL/TLS does encryption and server-side authentication
- Client-side authentication by username-password
- Mostly self-claimed attributes (except perhaps email, credit card)

Alternative approaches exist

- e.g., SAML, WS-Federation, OpenID, Facebook Connect,…
- but have privacy and security issues

Existing online solutions

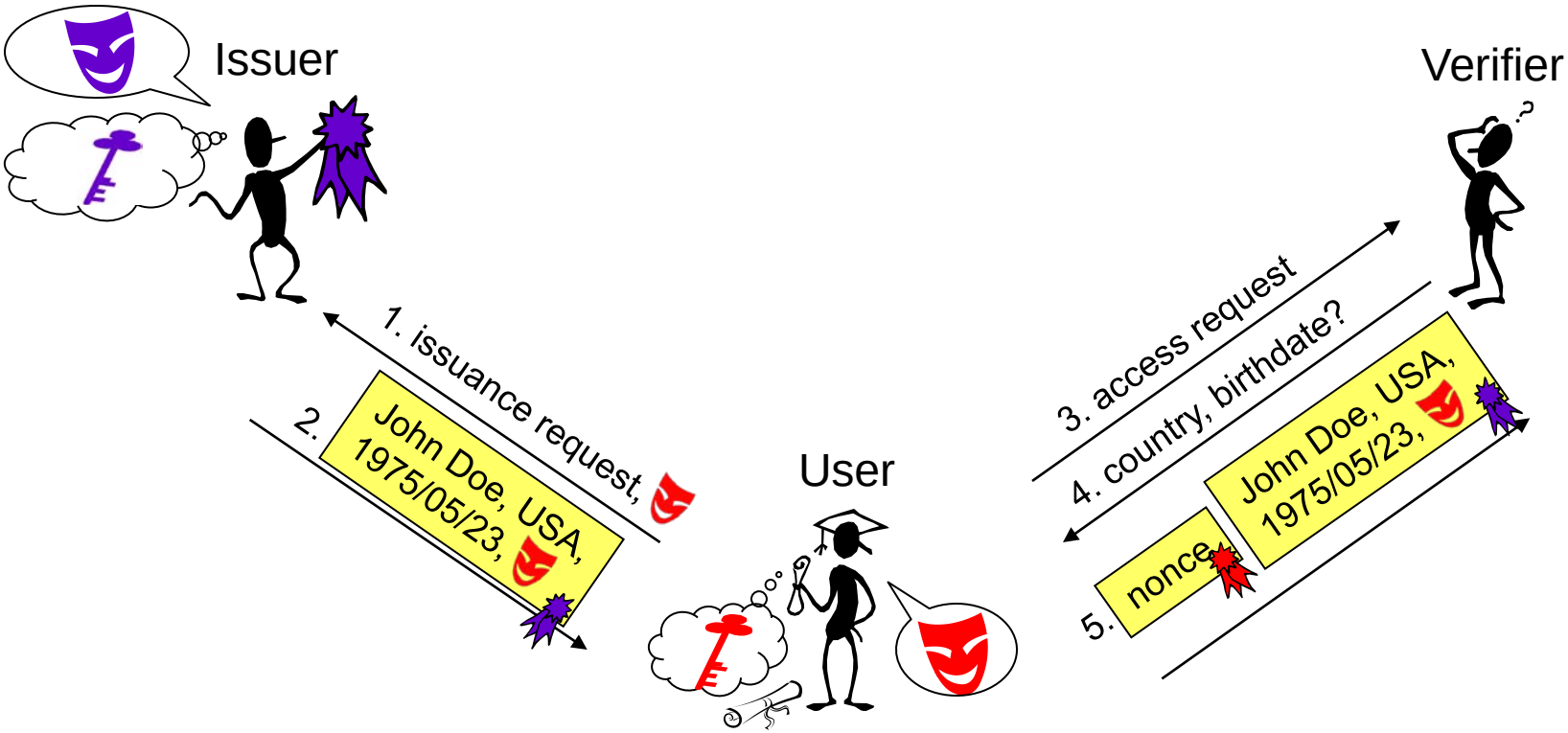
e.g., SAML, WS-Federation, OpenID, Facebook Connect



- Privacy: issuer knows who visits which website at which time (often from own records, if not by correlating logs with website)
- Security: issuance key online 24/7

Existing offline solutions

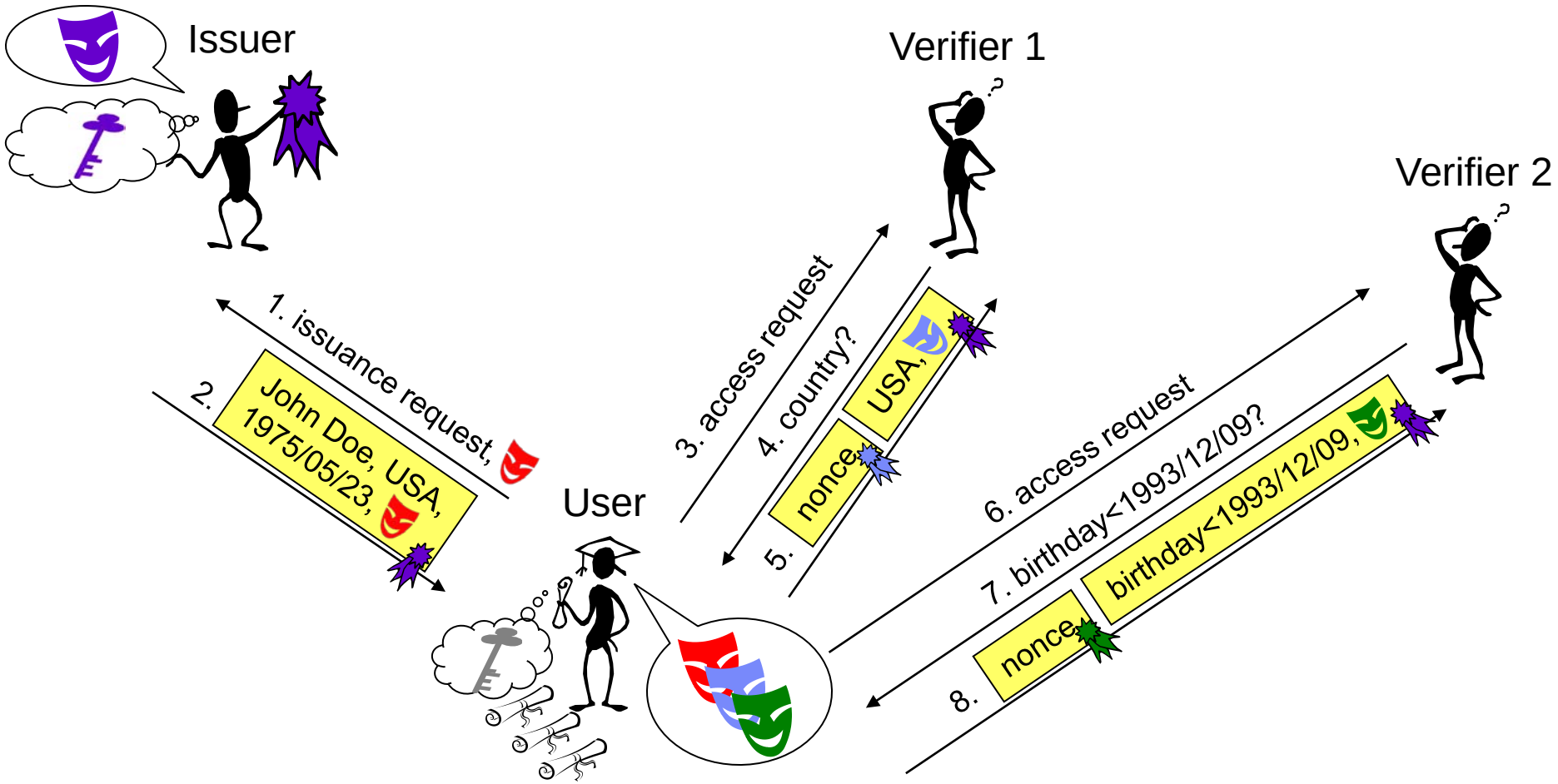
e.g., X.509 v3 certificates



- Privacy: have to disclose all attributes in certificate
  public key as unique identifier
- Security: verifier's collection of attributes target for identity thieves

Best of both worlds: private credentials

e.g., Identity Mixer, U-Prove, pairing-based schemes



- Privacy: unlinkable pseudonyms, minimal information disclosure
- Security: offline issuer

And there's more

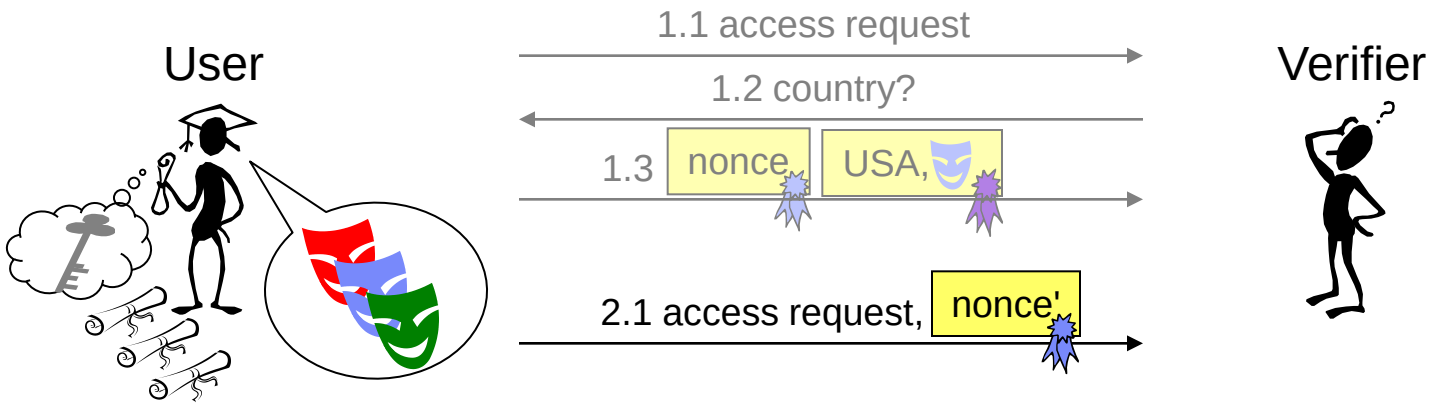
Full privacy isn't always what we want

- Permanent accounts → re-authenticate under previous pseudonym
- Sybil attacks → limit #pseudonyms per user for particular website
- Misbehavior, fraud, abuse → exclude and/or identify culprit
- Credential loss or exposure → revocation

We can do all this without sacrificing privacy!

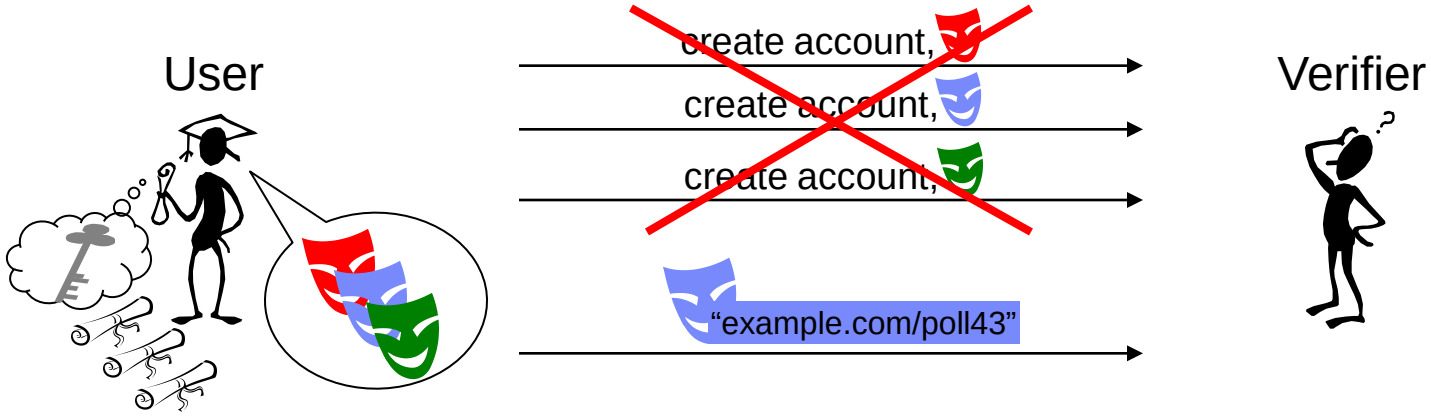
Privacy when possible, identification when needed.

Permanent pseudonyms



- Voluntary linkability between sessions
- Account linked to pseudonym
- Re-authenticate using user secret

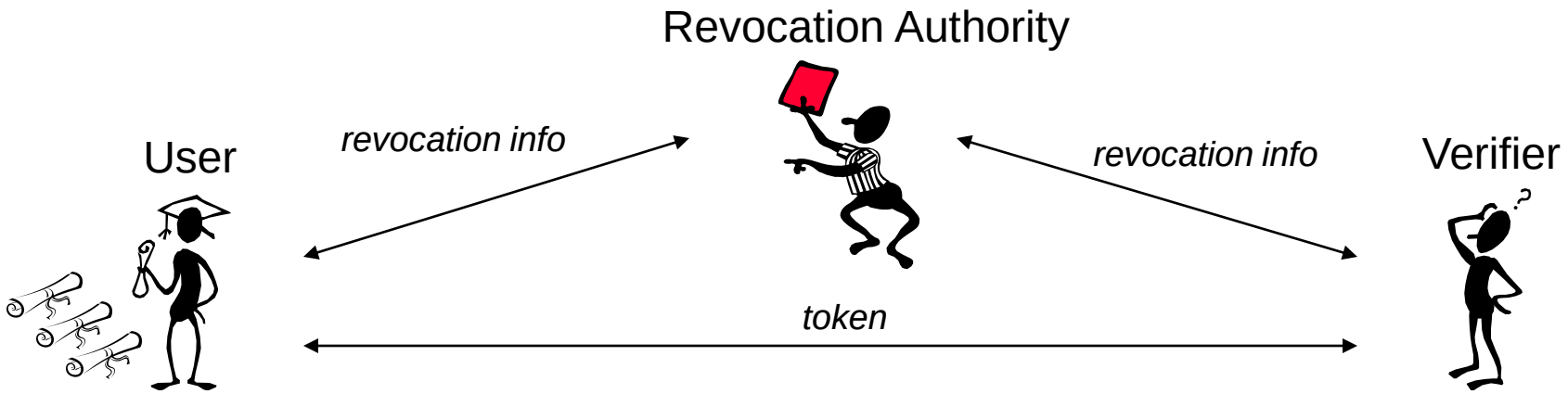
Usage limitation by scope-exclusive pseudonyms



"Scope-exclusive" pseudonyms

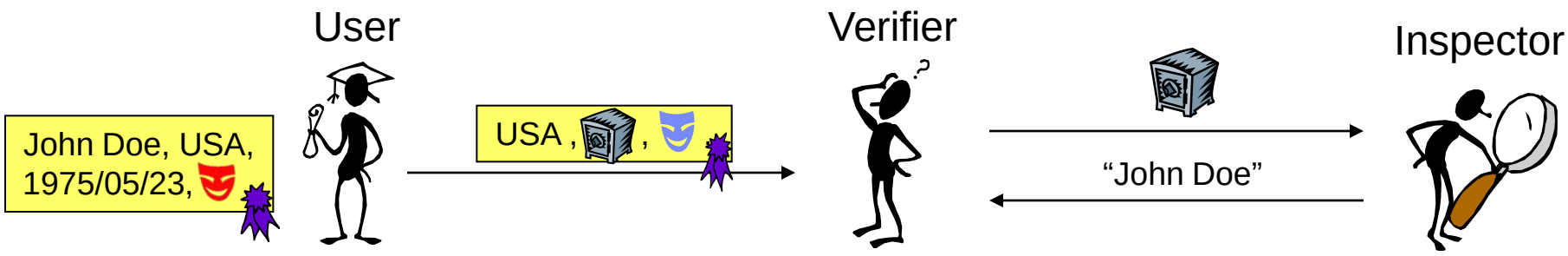
- Cryptographically unique pseudonym for given "scope string"
- Limit number of pseudonyms for particular domain, web page,…
  e.g., enforce "one user, one vote" in online polls
  e.g., enforce maximum usage per time period

Revocation



- No unique identifiers → traditional CRLs no longer work!
- Cryptography to the rescue
  - Several compatible privacy-friendly revocation mechanisms (white list or black list)
  - Prove that user's credential is (or is not) on list

Inspection

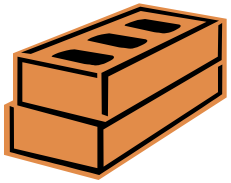


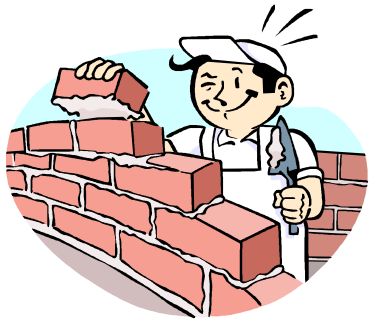
- Dedicated 3rd party (inspector) can recover additional attributes
- Access policy specifies
  - Inspector's public key
  - Which attribute(s) from which credential(s) can be recovered
  - Inspection grounds: circumstances that mandate uncovering
- Main use cases
  - De-anonymization in case of abuse
  - Reveal attributes to 3rd party, e.g., credit card details to bank

Building blocks

Signatures on blocks of messages

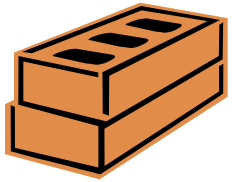
- Camenisch-Lysyanskaya (Identity Mixer, RSA)
- Brands (U-Prove, discrete logarithms)
- Camenisch-Lysyanskaya (bilinear maps)
- Belinkiy et al. (P-signatures, bilinear maps)
- Gordon et al. (lattices)

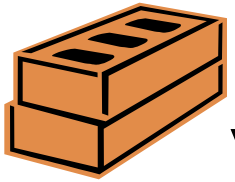




Zero-knowledge proofs

- Schnorr with Fiat-Shamir (random oracle)
- Groth-Sahai (pairings, standard model)





Revocation

- Short-lived credentials [CKS10]
- Credential revocation lists [BS04, BDD07, NFHF09]
- Dynamic accumulators [CL02, N05, ATSM09, CKS09, AN11]

Verifiable encryption

- Camenisch-Shoup (exponents)
- Cramer-Shoup (group elements)
- Camenisch-Damgaard (any)

Identity Mixer in the real world

- More information on http://idemix.wordpress.com
- Open-source Java library available at http://www.primelife.eu/results/opensource
- Common Idemix/U-Prove formats being developed in ABC4Trust project

Technology is there, ready to be used!