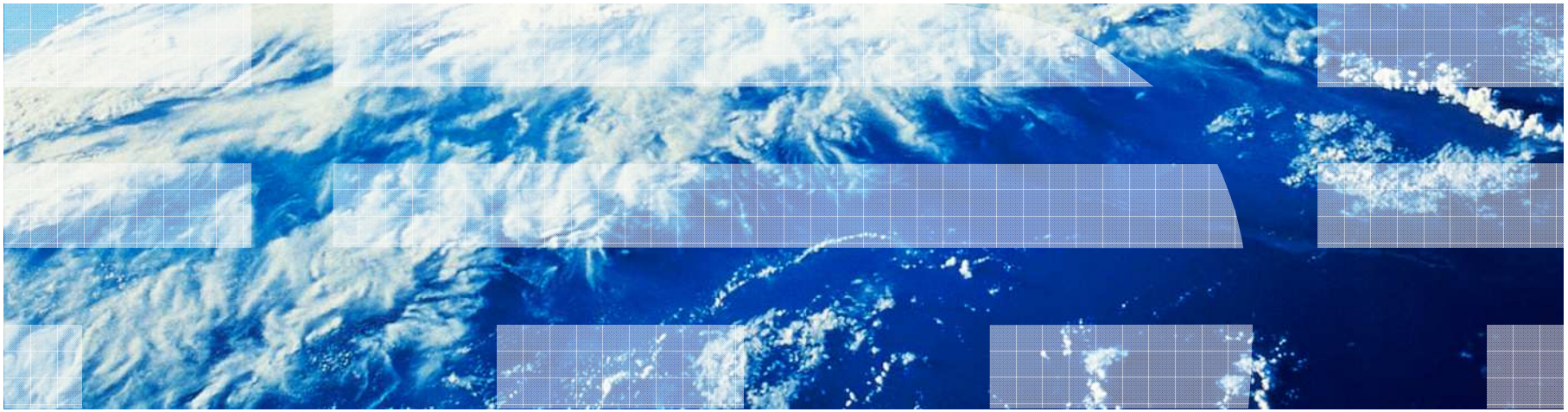
Gregory Neven, IBM Research – Zurich
IFIP Summer School, Trento, Italy, September 6, 2011

Privacy-Preserving Attribute Credentials



© 2011 IBM Corporation


“Neil Armstrong’s Footsteps are still there”
(Robin Wilton, futureidentity)

And we leave traces, lots of traces!



























Computers don’t forget!





- Data storage becomes ever cheaper
  - “store by default”
  - e.g., surveillance cameras, Google Street View with wireless traffic, Apple location history
- Data mining techniques ever better
  - self-training algorithms become more intelligent than their designers
  - not just trend detection, even prediction
  - e.g., flu pandemics, ad clicks, purchases,…
  - what about mortgage defaults, criminal behavior?
  - correlation with illegal criteria, e.g., race, religion?

Everyday privacy threats

- Sacked because of Facebook or Twitter posts
- Burglars using Facebook and Twitter to find targets
- Electronic toll collection data used in divorce cases
- Abuse of stored or transmitted data by malicious employees
  e.g., Telecom Italia wiretapping scandal
- Mother's maiden name, birth date,… often used as backup secret
- Facebook's evolving privacy defaults
  http://mattmckeon.com/facebook-privacy



Brian Fairrington, Cagle Cartoons

- Google Street View storing payload data from wireless networks
- iPhones found to store detailed location history
- Sony loses personal data of about 110 million PlayStation customers

Privacy breaches happen almost daily



Date	Data Origin	Event	# affected
29.08.2011	CDU	Political party membership list leaked online	5 800
22.08.2011	Sky Germany	List of football betting participants stolen	8 000
07.08.2011	Neusehland e.V.	Sensitive patient data found in trash	100 s
01.08.2011	Hatraco / Marktkauf	Customer data stolen by hackers	1 000 000
27.07.2011	DRK Kreisverband	Personal data of children and youngsters leaked online	33
18.07.2011	Rewe	Football and animal card collecters' data stolen	10 000 s
18.07.2011	Rheinbahn	Sensitive employee data leaked	2 700
11.07.2011	Westermann Verlag	Online customer data stolen	10 000 s
04.07.2011	Flughafen Berlin Brandenburg	Data of volunteer test persons leaked	10 000 s
28.06.2011	SPD Sachsen	List of political party website visitors stolen	countless
22.06.2011	Finanzverwaltung Baden-Württemberg	Taxpayers' data lost	countless
20.06.2011	Residents and demonstrators	Dresden police intercepts demonstrators' phone calls and SMSs	10 000 s
14.06.2011	Landgericht Dresden	Court loses journalists' personal data	110
31.05.2011	Neckermann	Gambling customer data stolen	1 200 000
24.05.2011	University Potsdam	Student data accessible online	20 000

Source: www.projekt-datenschutz.de

What can we do?

- Most of the **technology** is there (but have to use it)
- Most of the **legislation** is there (but have to enforce it)
- **Awareness** is growing (but have to raise it even more)

What can we do?

- Most of the **technology** is there (but have to use it)
- Most of the **legislation** is there (but have to enforce it)
- **Awareness** is growing (but have to raise it even more)

Overview of this talk

- Cryptography for privacy
- Privacy-enhancing attribute credentials
- PrimeLife Policy Language (PPL)
- Ongoing work

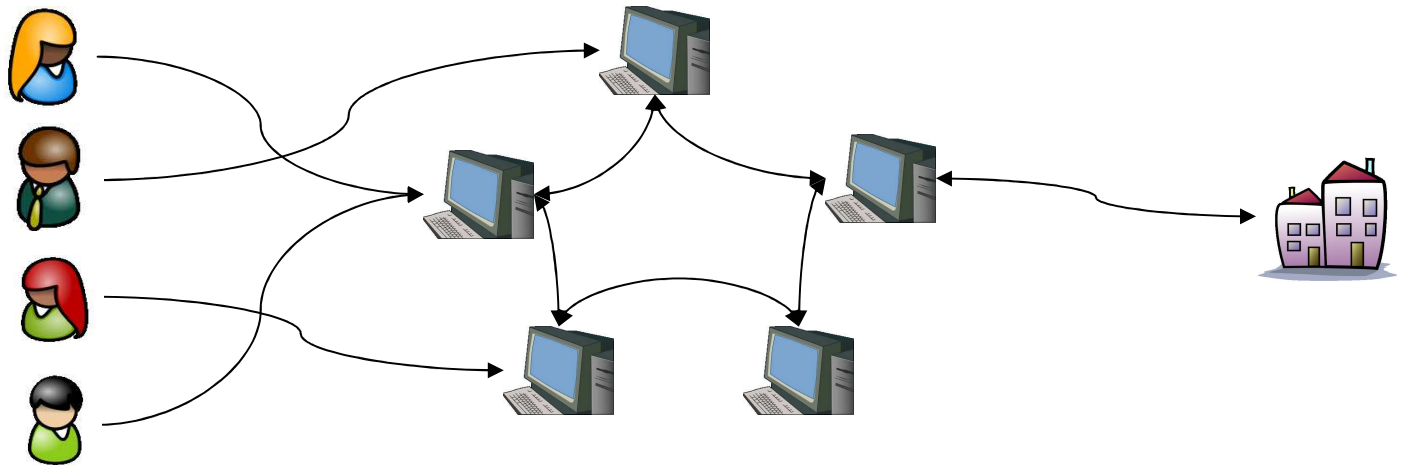
Overview of this talk

- **Cryptography for privacy**
- Privacy-enhancing attribute credentials
- PrimeLife Policy Language (PPL)
- Ongoing work

Cryptography at network layer

Anonymous communication at network layer

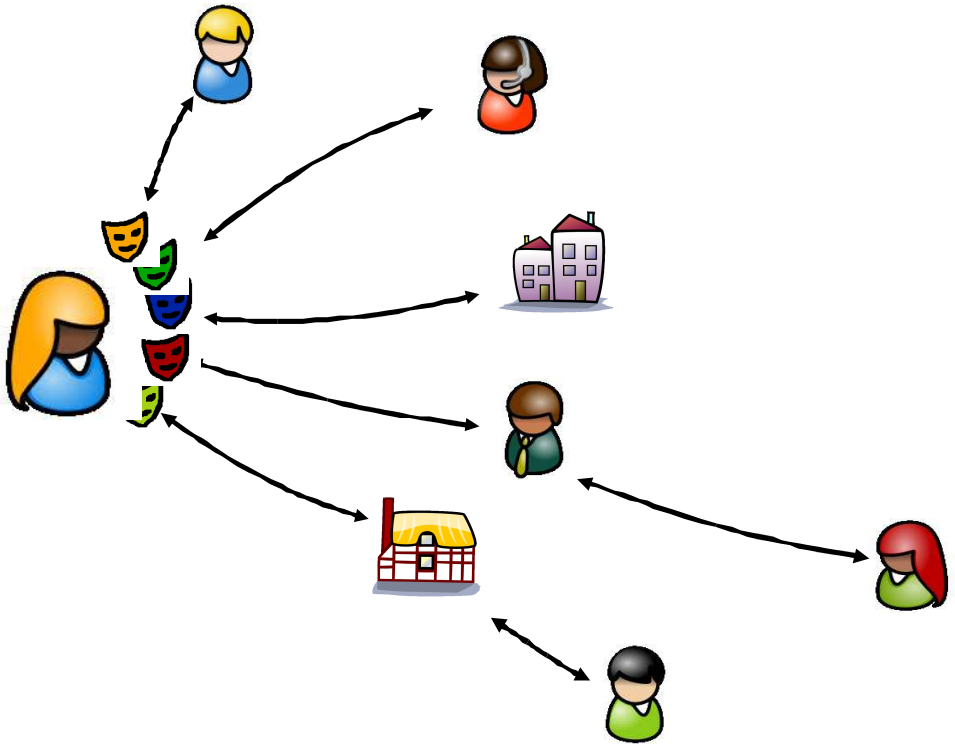
e.g., mix networks, onion routing, DC-nets, …



(at the price of lower bandwidth; physical layer notoriously hard to protect)

Cryptography at identification layer

Anonymous communication at identification layer:
privacy-preserving credentials, e.g., Identity Mixer, U-Prove

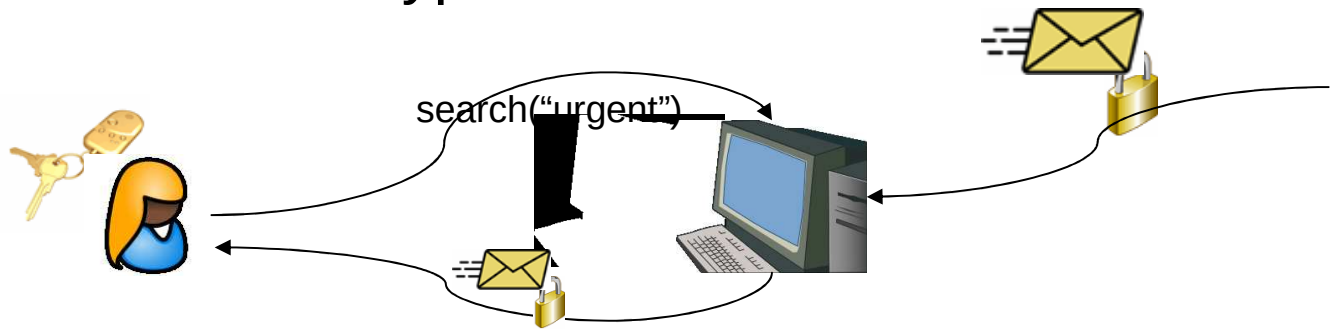


(more details in a moment…)

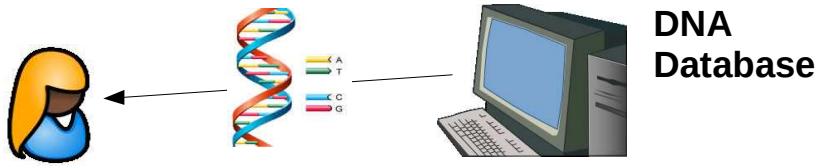
Cryptography at application layer

Anonymous communication at application layer:

e.g., searchable encryption:



e.g., oblivious transfer

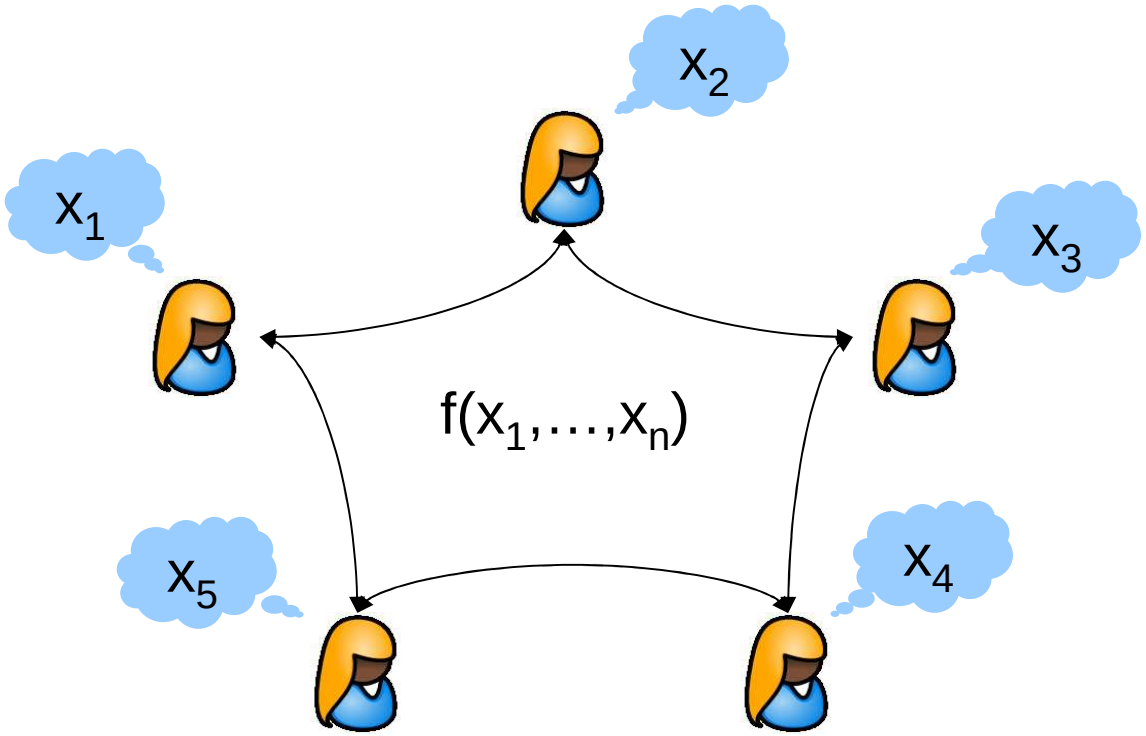


database does not learn who accesses, or which record is accessed

even comes with (anonymous) access control, pricing!

Cryptography at application layer

e.g., secure multi-party computation



Privacy-enhancing attribute-based credentials

- Also kown as
  - privacy-ABCs
  - anonymous credentials
  - ≈ minimal disclosure tokens
- Cryptographic credentials with
  - minimal information disclosure
    - selective attribute disclosure
    - attribute predicates
  - unlinkability by default, linkability when needed
  - untraceability by default, traceability when needed
  - no Big Brother as Identity Provider
- Implementations
  - U-Prove (Microsoft)
  - Identity Mixer (IBM)

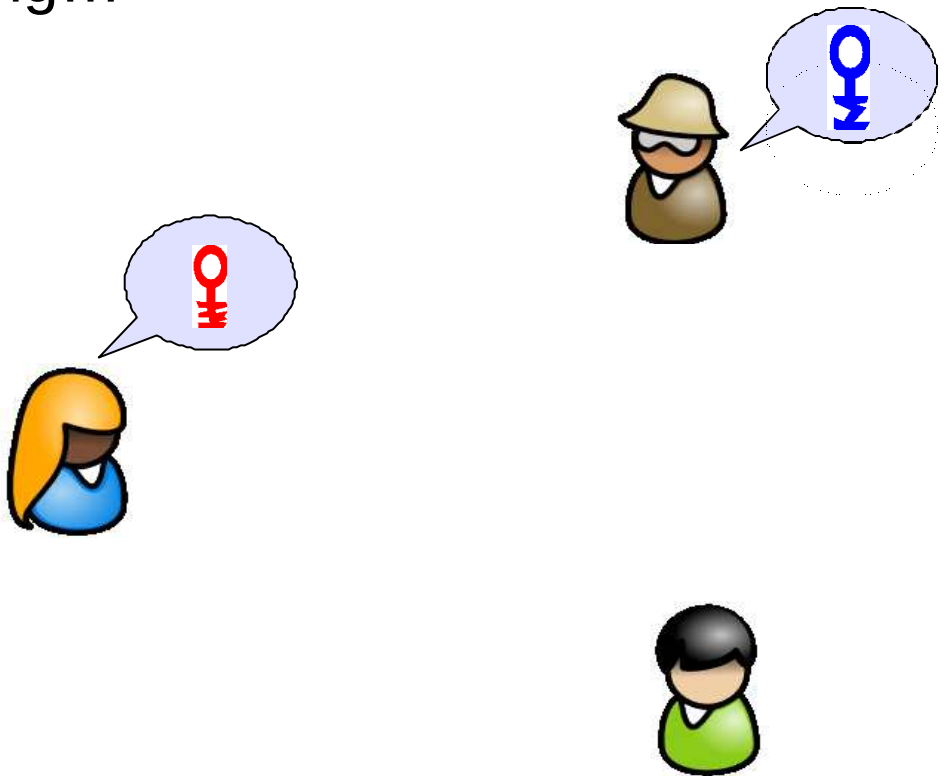
Overview of this talk

- Cryptography for privacy
- **Privacy-enhancing attribute credentials**
- PrimeLife Policy Language (PPL)
- Ongoing projects: ABC4Trust, FI-WARE PPP

Standard public-key certificates

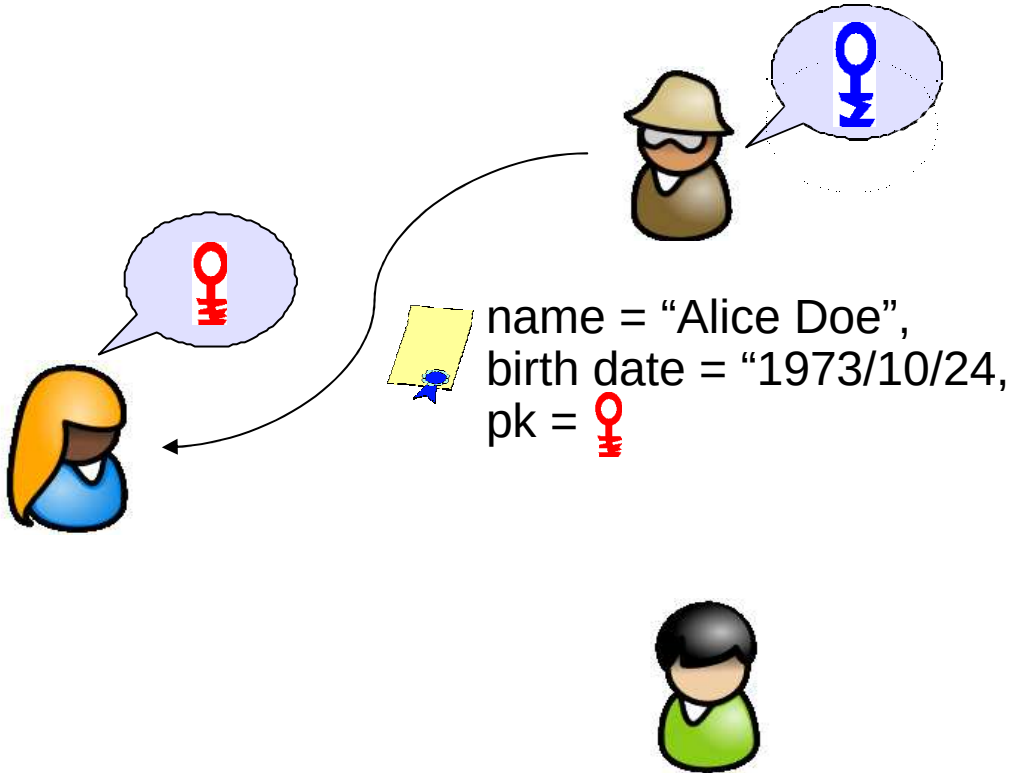
e.g., X.509 certificates

In the beginning…



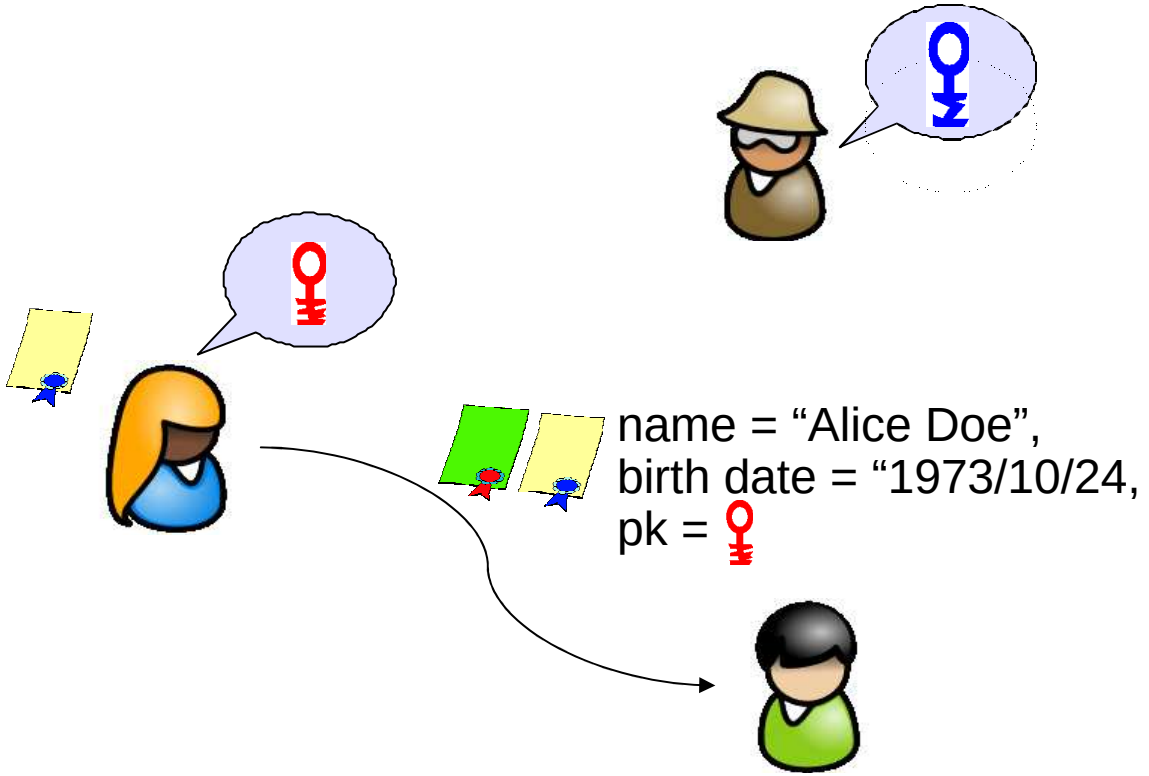
Standard public-key certificates

Obtaining a certificate…



Standard public-key certificates

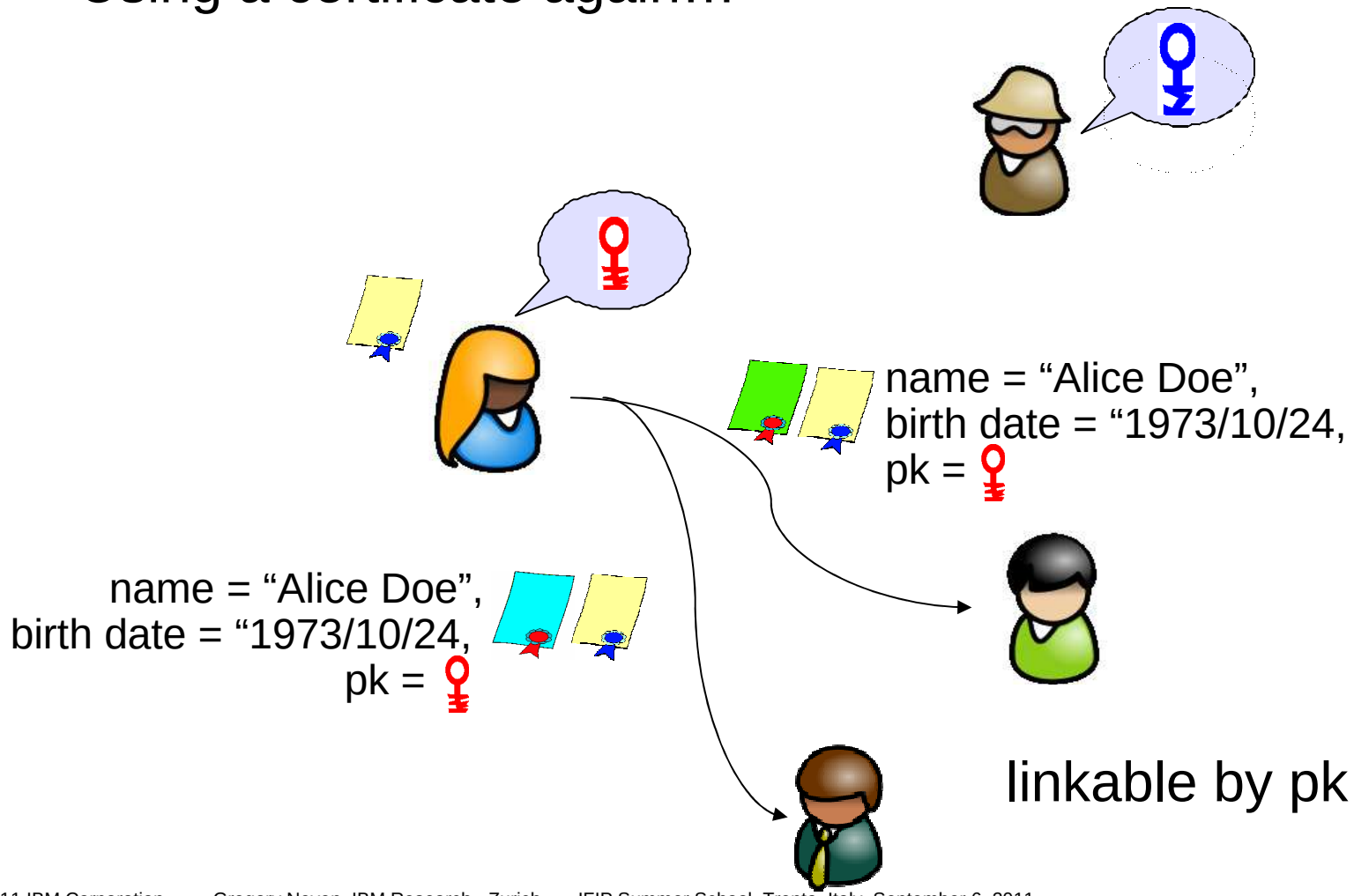
Using a certificate…



full attribute disclosure

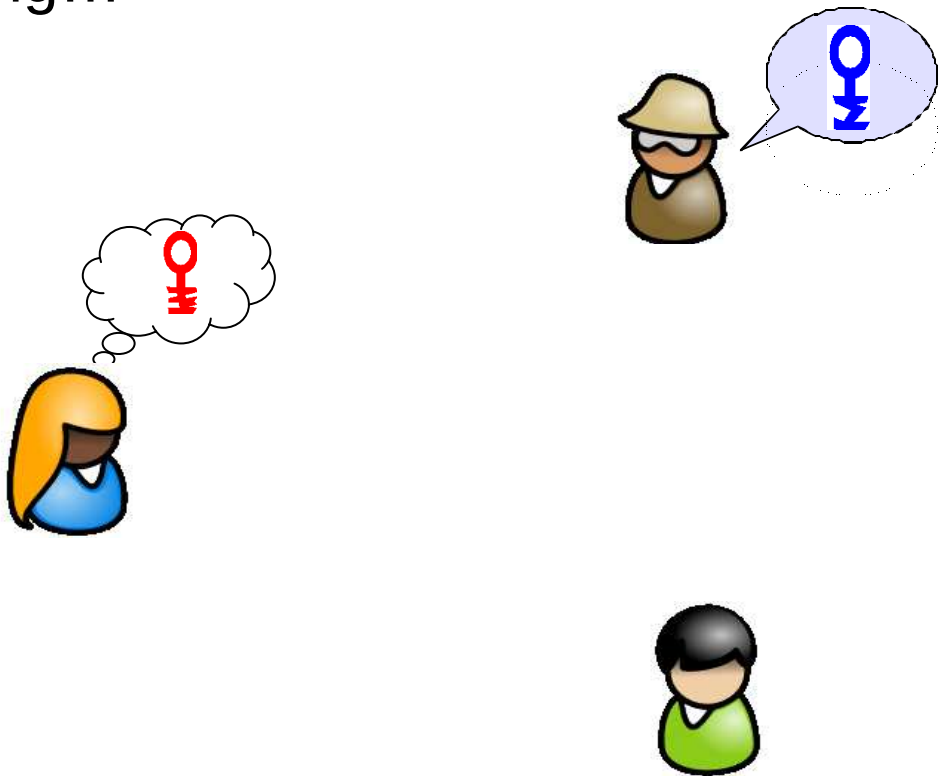
Standard public-key certificates

Using a certificate again…

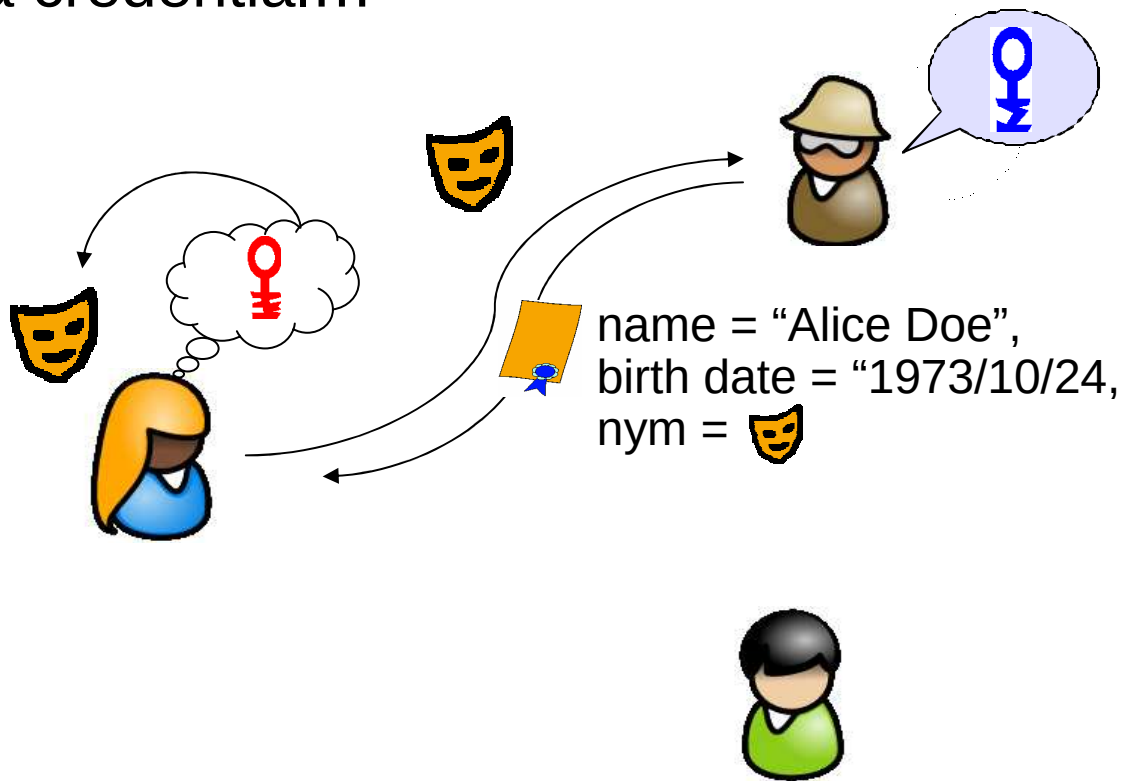


e.g., Identity Mixer, U-Prove

In the beginning…

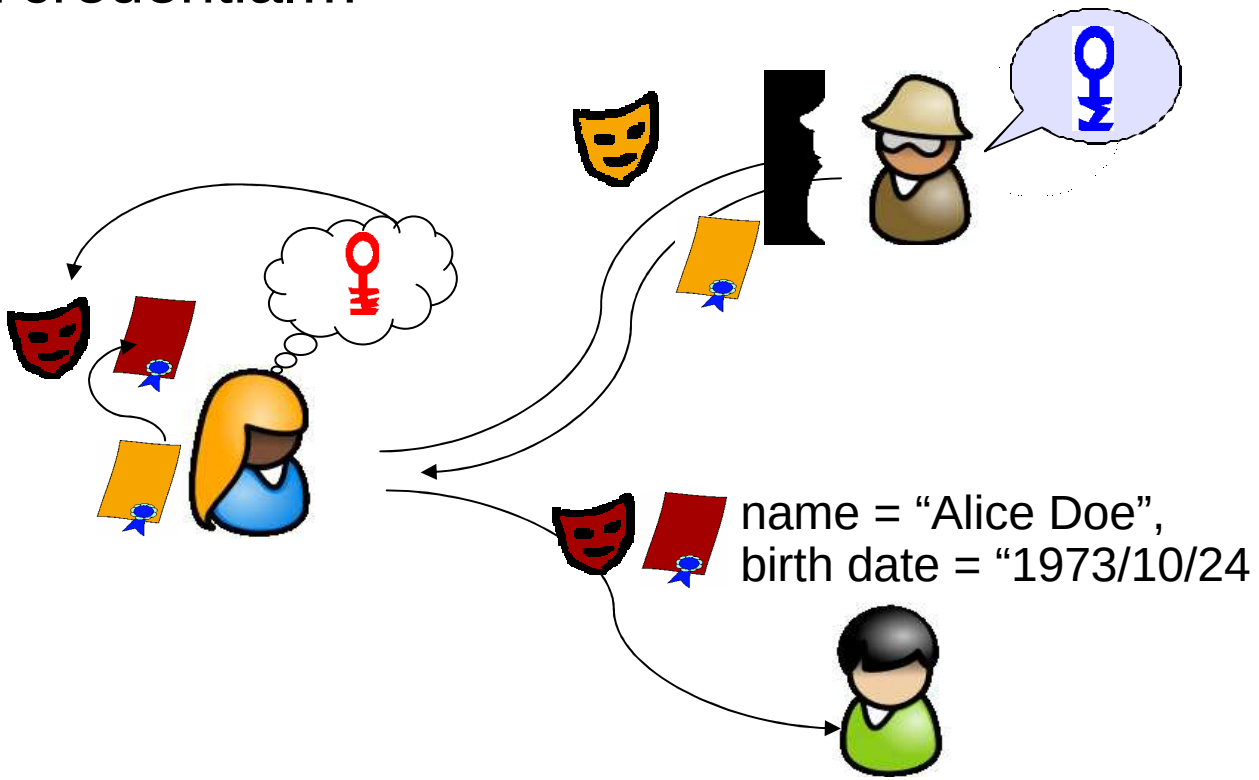


Obtaining a credential…



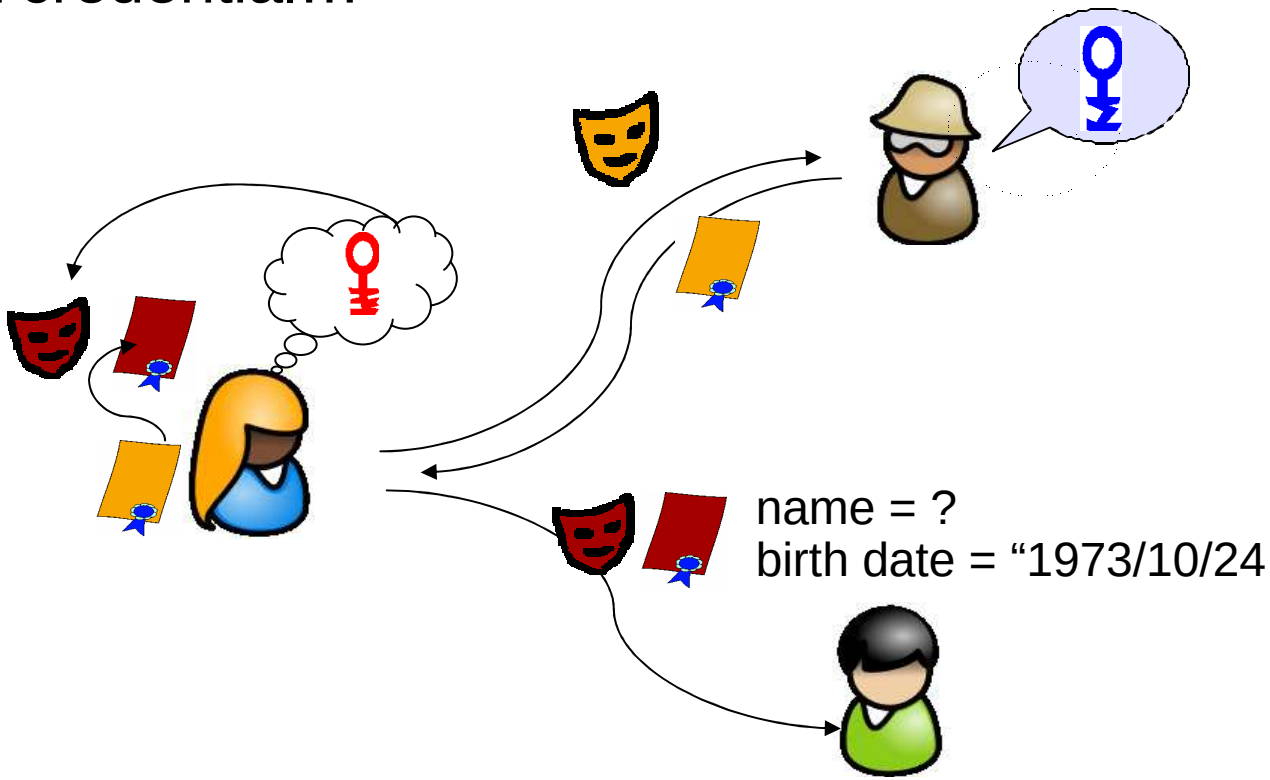
© 2011 IBM Corporation

Using a credential…



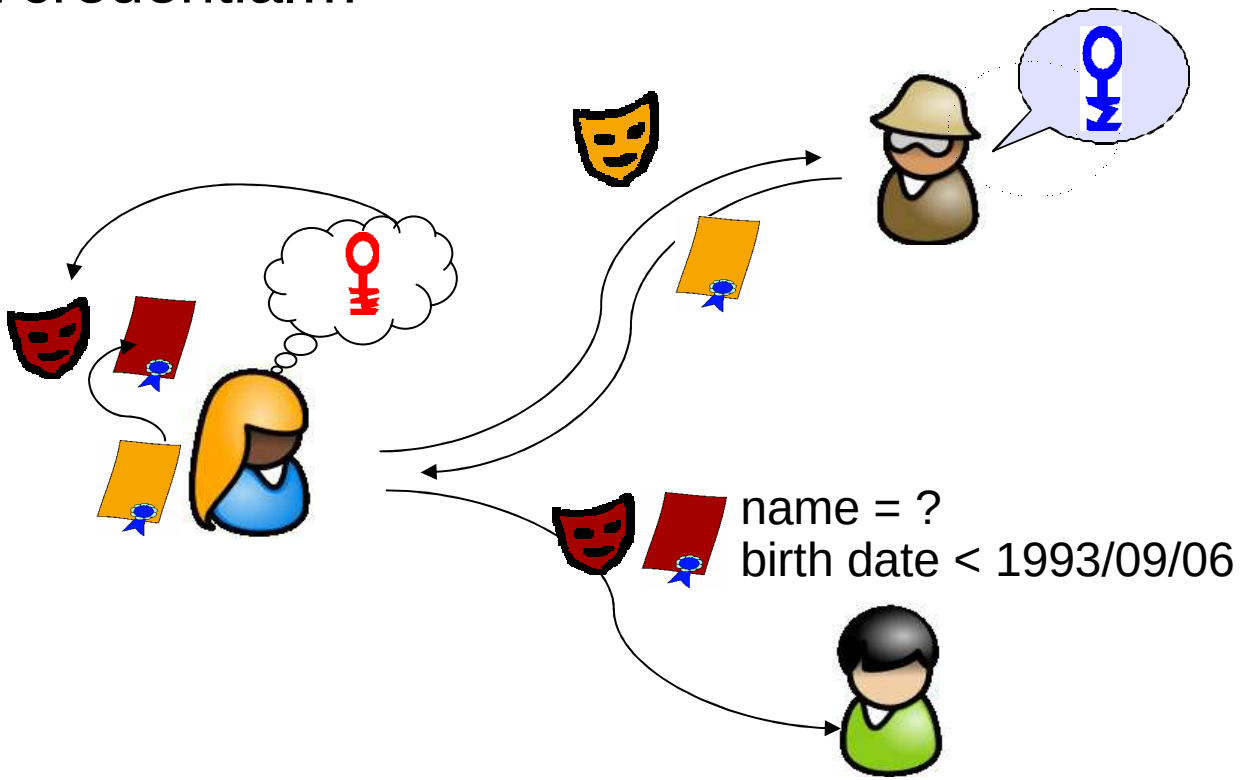
unlinkable by pseudonym

Using a credential…



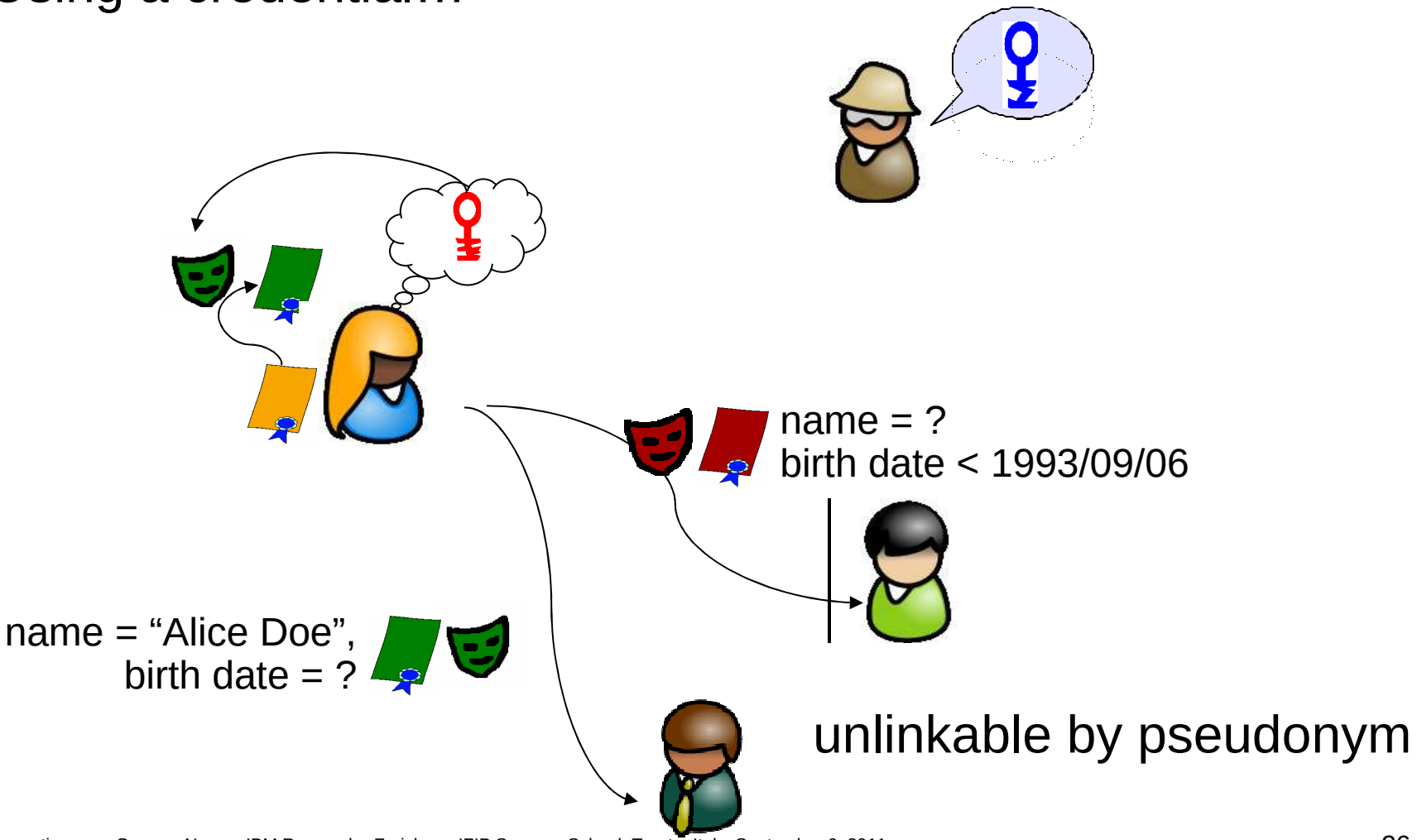
selective attribute disclosure

Using a credential…

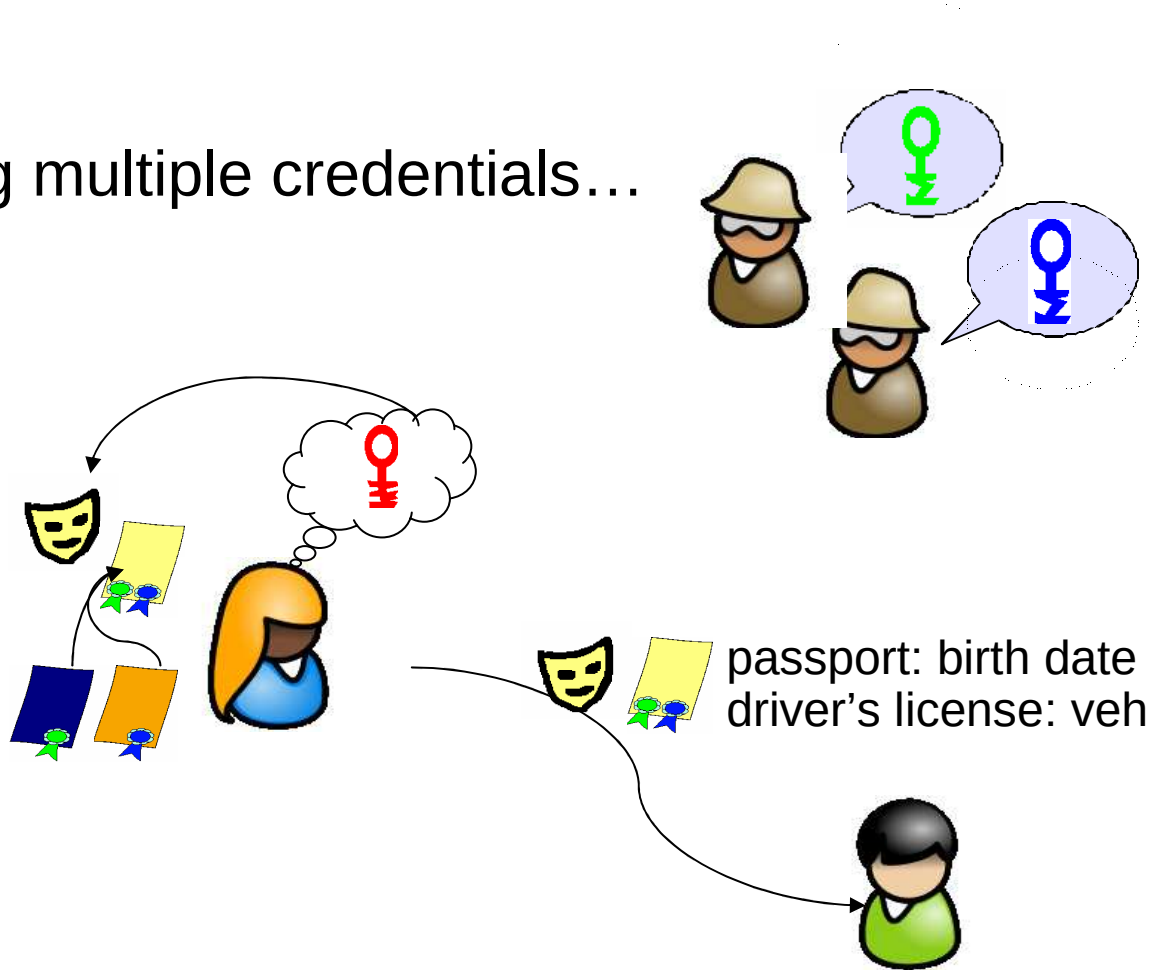


attribute predicate disclosure

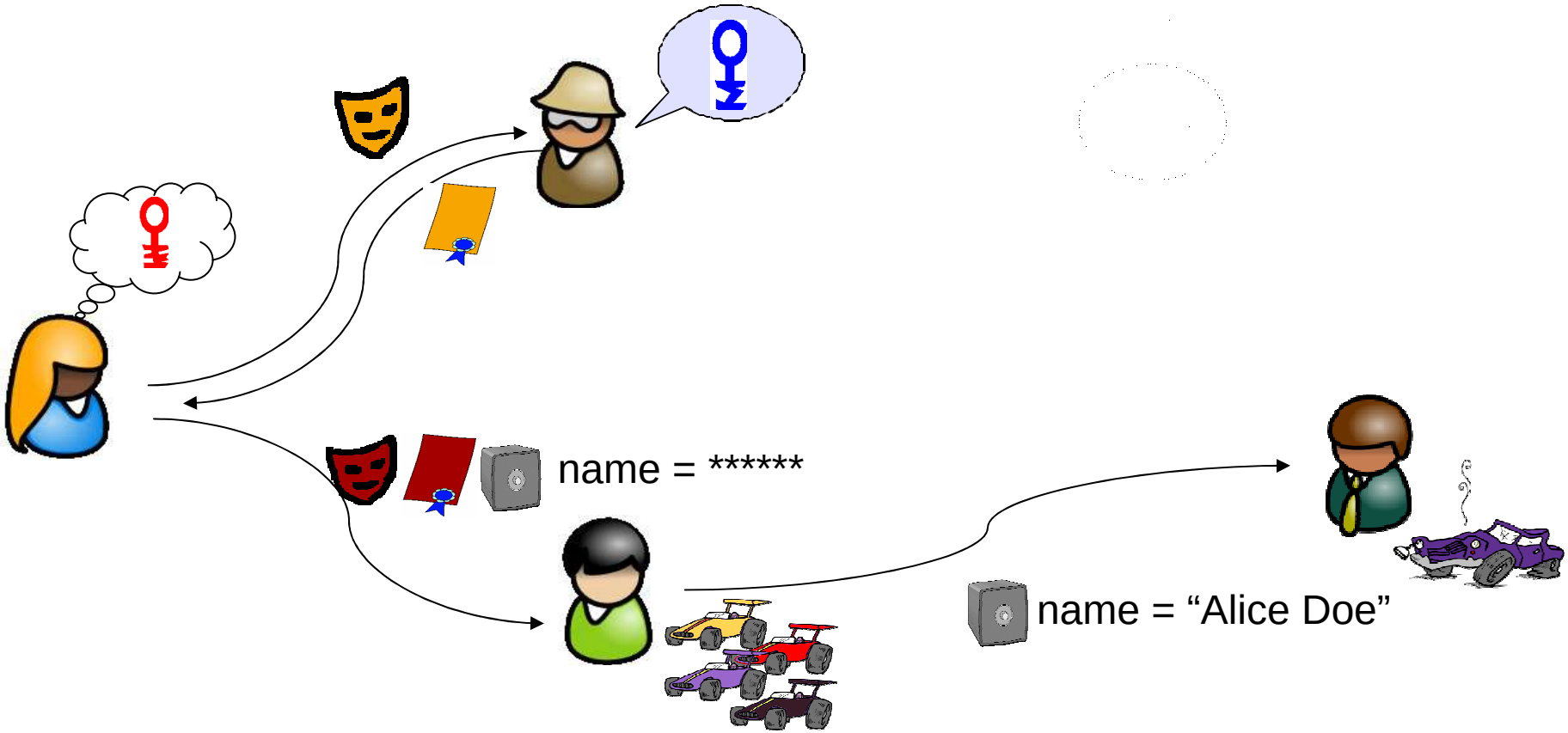
Using a credential…



Showing multiple credentials…

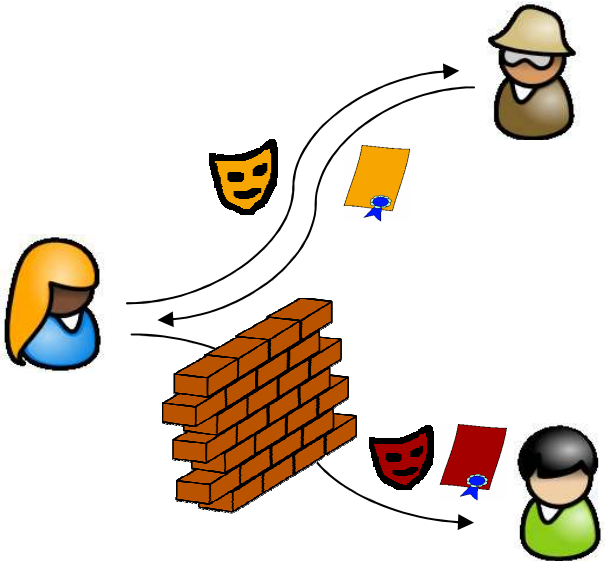


Attribute escrow through verifiable encryption



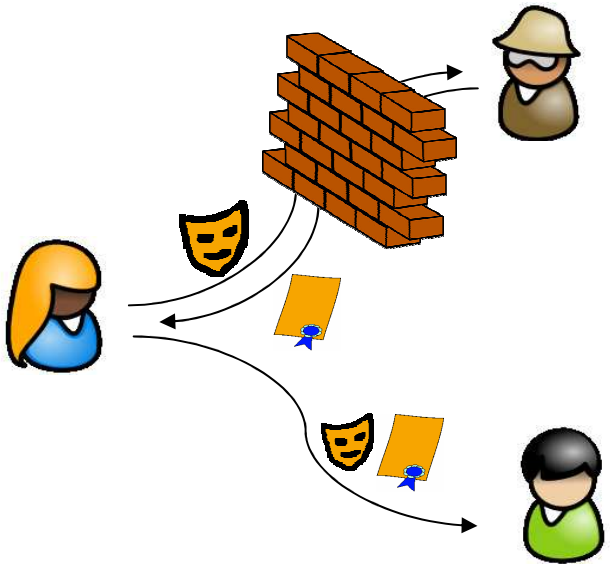
How it works: two approaches

Zero-knowledge proofs



- multi-use
- Damgard, Camenisch-Lysyanskaya (Identity Mixer)
- strong RSA, pairings (LMRS, q-SDH)

Blind signatures



- one-time use
- Chaum, Brands et al. (U-Prove)
- discrete logs, RSA,…

Learn more? Crypto tutorial tomorrow afternoon!

Overview of this talk

- Cryptography for privacy
- Privacy-enhancing attribute credentials
- **PrimeLife Policy Language (PPL)**
- Ongoing work

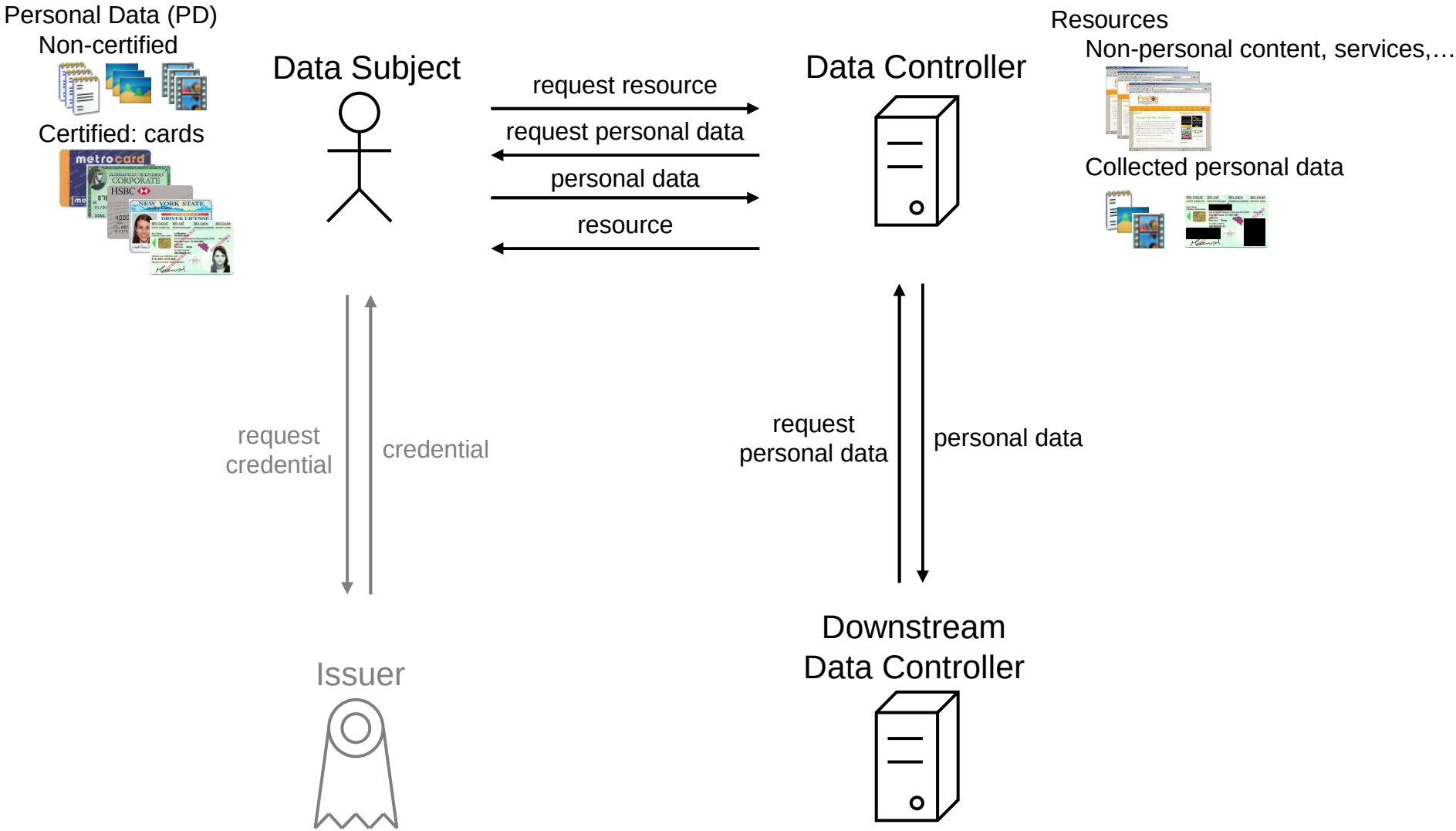
XACML

- eXtensible Access Control Markup Language, developed by OASIS
- Industry standard specifying
  - XML-based access control policy language
  - XML-based access request/response protocol language
  - processing model
- Access decisions based on attributes of
  - Subject (e.g., username, role)
  - Protected resource (e.g., file name, URL, content,…)
  - Action (e.g., read, write,…)
  - Environment (e.g., date, time,…)
- Extension points: can define new attributes, data types, functions, obligations, rule/policy combining algorithms

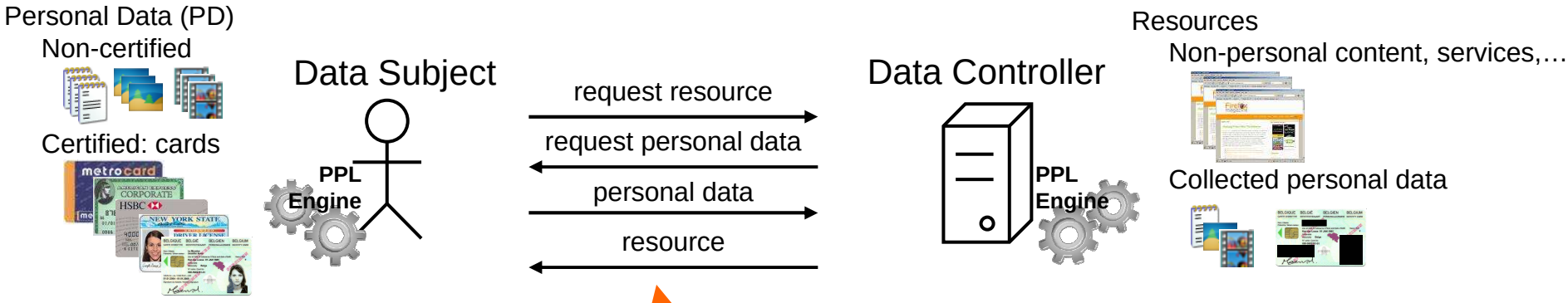
SAML

- Security Assertion Markup Language, by OASIS
- Protocol language for communicating
  - user authentication information
  - user attribute information
  - authorization decision information
- Main use cases
  - Single sign-on (SSO)
  - Identity federation
  - Attribute provision
- SAML profile of XACML
  - Translate SAML attributes into XACML attributes
  - Use SAML to carry XACML policies, authorization decisions,…

PrimeLife Policy Language (PPL) scenario



Structure of PPL



Specific Policy:
over specific personal data (e.g. birth date)
- **Access control policy (ACP):**
  who can access (e.g. PrivacySeal silver)
- **Data handling preferences (DHPrefs):**
  how is to be treated when revealed
  - **Authorizations** (e.g. marketing purposes, forwarded to PrivacySeal gold)
  - **Obligations** (e.g. delete after ≤2y)

Generic Preferences:
DHPrefs over implicitly revealed personal data (e.g. IP address, cookies,…)
- **Authorizations** (e.g. admin purposes)
- **Obligations** (e.g. delete after ≤2y)

SAML

XACML

Specific Policy:
over specific resource (e.g. BuyService)
- **Access control policy (ACP):**
  who can access
  - cards to possess (e.g. ID card)
  - personal data to reveal (e.g. nationality)
  - conditions to satisfy (e.g. age>18)
- **Data handling policy (DHP):**
  how revealed personal data will be treated
  - **Authorizations** (e.g. marketing purposes)
  - **Obligations** (e.g. delete after 1y)

Generic Policy:
DHP over implicitly revealed personal data (e.g. IP address, cookies,…)
- **Authorizations** (e.g. admin purposes)
- **Obligations** (e.g. delete after 1y)

Main features of PPL

- Card-based access control
- Integrated two-sided data handling
- Symmetric architecture
- Policy sanitization
- Based on existing standards: XACML & SAML

Card abstraction



- Card contains
  - list of attribute-value pairs
  - *pre-evidence*: technology-specific meta-data to
    - protect attribute integrity
    - prove card ownership
- Card *issuer* vouches for attributes wrt *owner* (identity/authority)
- Hierarchy of card *types:* define attributes contained
- Instantiating technologies: X.509, SAML, CardSpace, OpenID, Kerberos, trusted LDAP, Identity Mixer, U-Prove,…

Card-based access control example

- Policy: requirements on owned cards, e.g.,

  own p::Passport **issued-by** admin.ch, fgov.be, governo.it

  own c::Creditcard **issued-by** visa.com, amex.com

  reveal c.number, c.expdate

  where p.name = c.name ^ p.bdate < today-18Y

  ^ c.expdate > today ^ p.expdate > today+1M

- Authentication = *claim* over owned cards + *evidence*, e.g.,

  own p::Passport **issued-by** admin.ch

  own c::Creditcard **issued-by** visa.com

  reveal c.number = “1234567890”

  reveal c.expdate = “31/12/2012”

  where p.name = c.name ^ p.bdate < 22/03/1993 ^ p.expdate > 22/04/2011

Overview of this talk

- Cryptography for privacy
- Privacy-enhancing attribute credentials
- PrimeLife Policy Language (PPL)
- **Ongoing work**

Ongoing EU projects



- Common framework/API/token format for U-Prove and Identity Mixer
- Feature set covering full credential lifetime
  - Issuance
  - Presentation
  - Revocation
  - Tracing
- Led by Goethe University Frankfurt, members include Microsoft and IBM



Identity Mixer to be contributed to/integrated with Future Internet security infrastructure

Conclusion

- Most of the **technology** is there (but have to use it)
- Most of the **legislation** is there (but have to enforce it)
- **Awareness** is growing (but have to raise it even more)