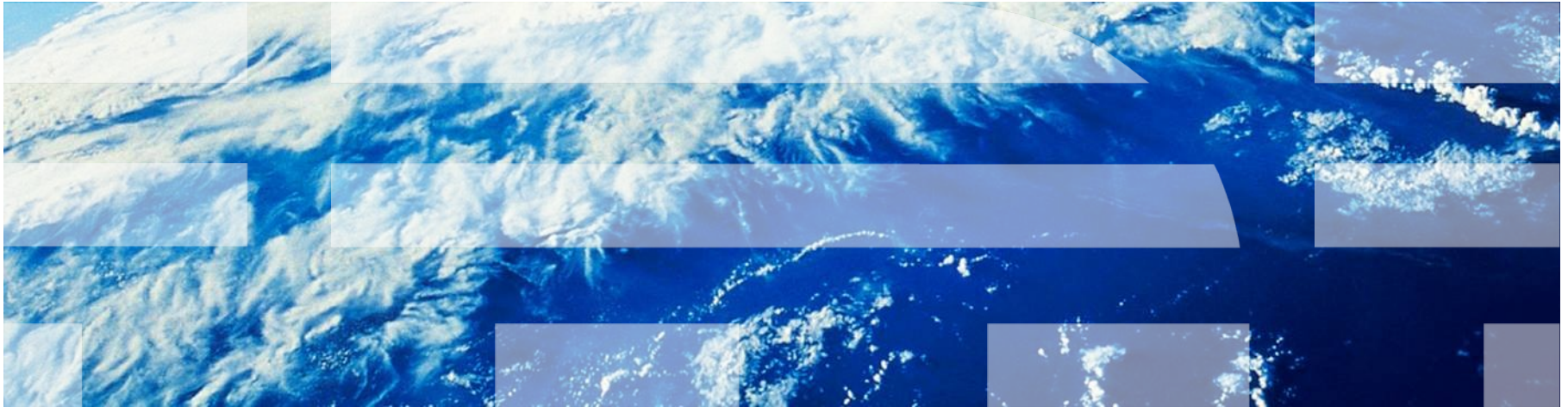


# Privacy



# Privacy



# PrimeLife



# Technology



# Privacy



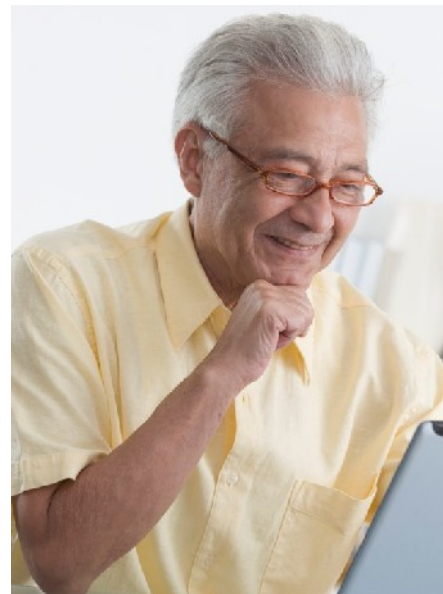
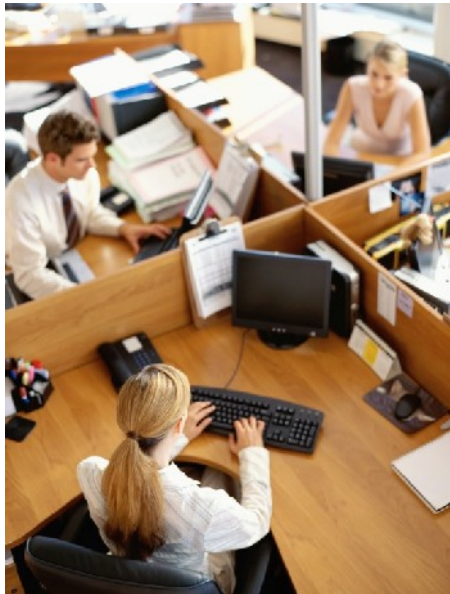
# PrimeLife



# Technology



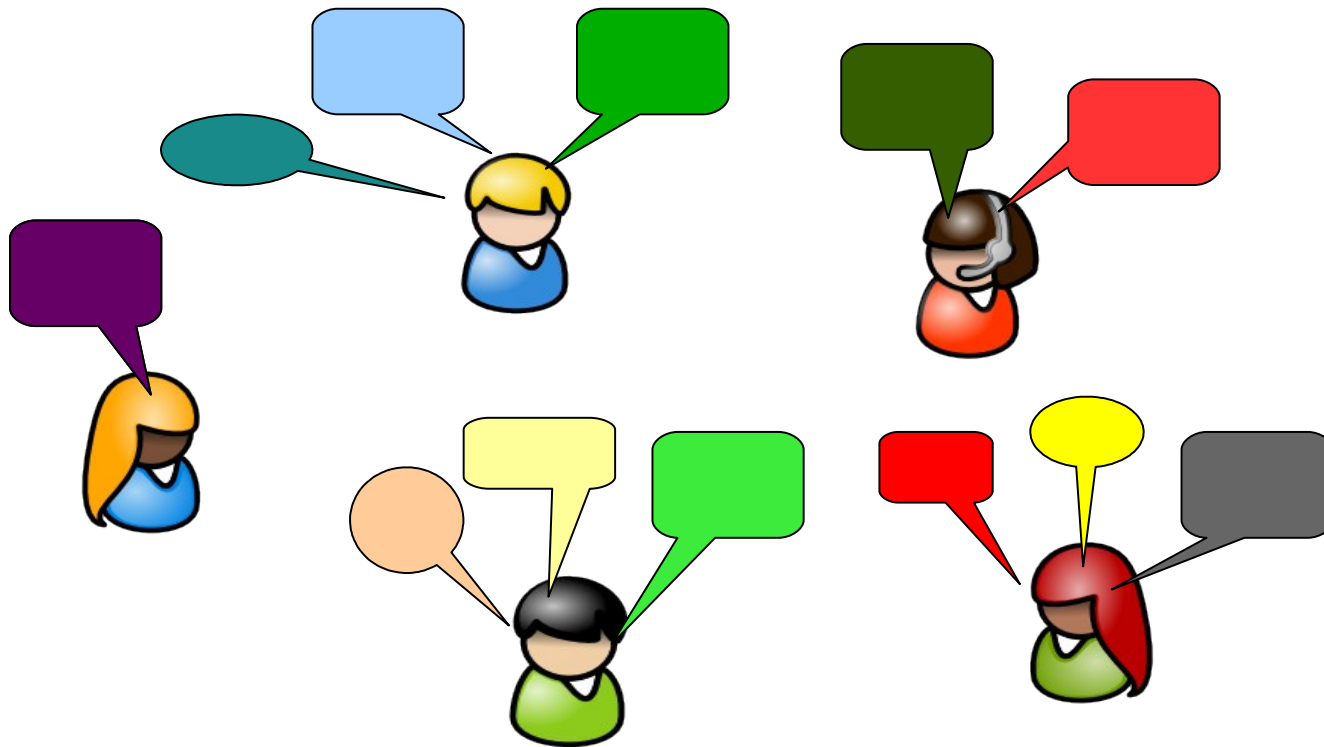
# Who is Privacy About?



# People



# People Who Like to Talk





*“Neil Armstrong’s Footsteps  
are still there”*

(Robin Wilton, Sun Microsystems)

# Computers don't forget

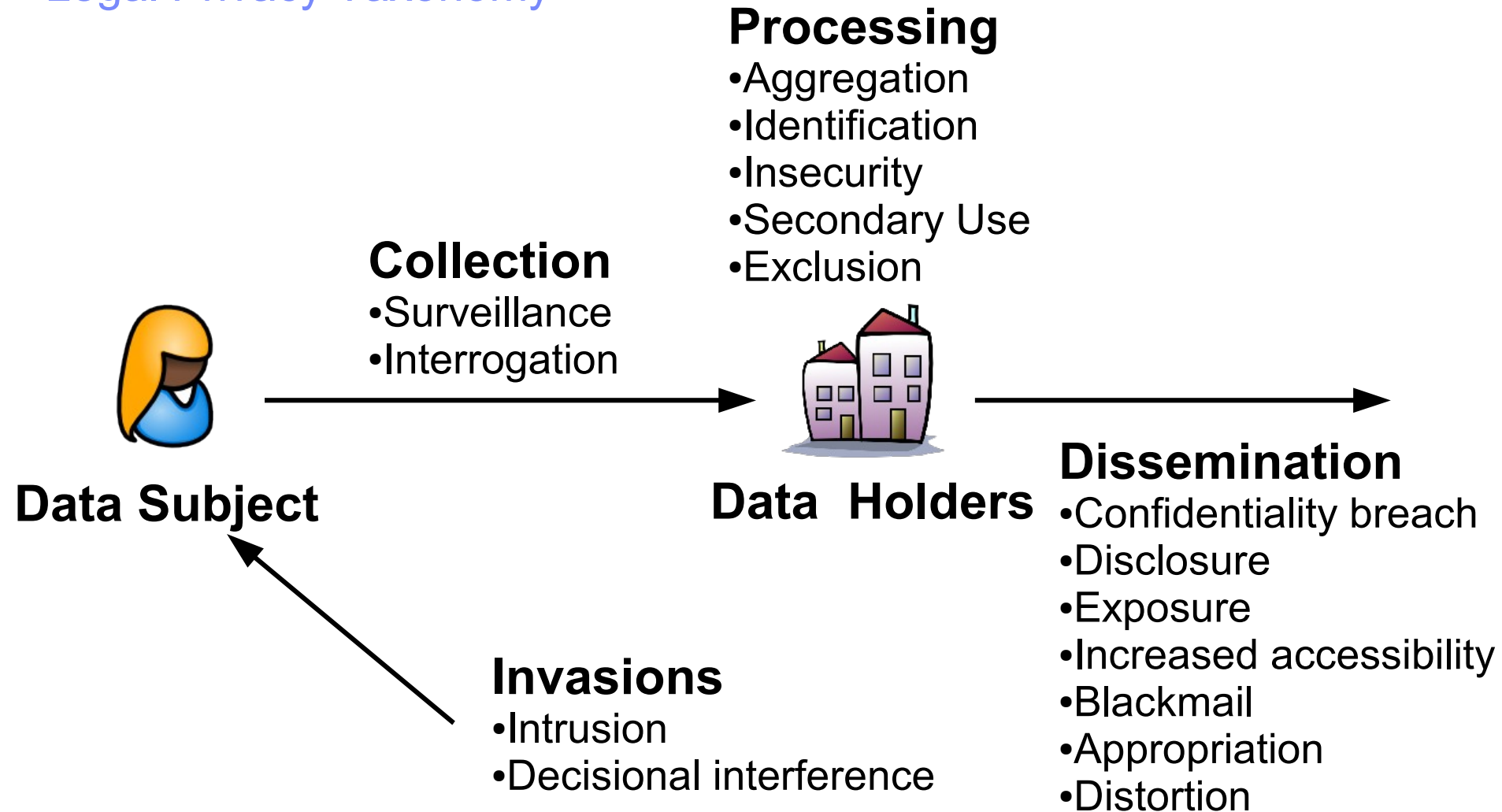


## Consent Paradigm in Privacy

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Alan Westin

# Legal Privacy Taxonomy



# Privacy



# PrimeLife



# Technology





# PrimeLife Consortium



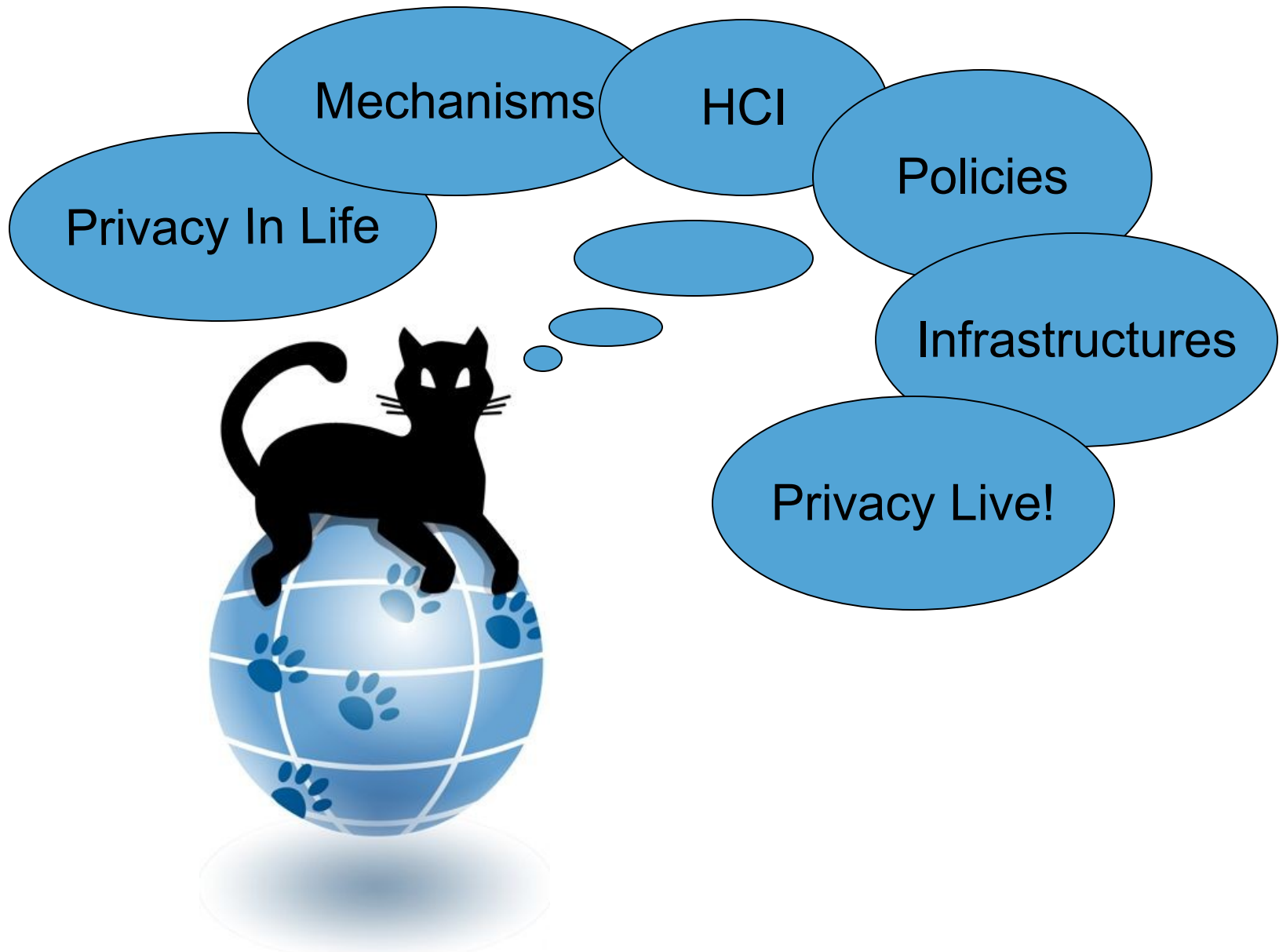
# PrimeLife's Objectives

## Bringing Sustainable Privacy and Identity Management to Future Networks and Services

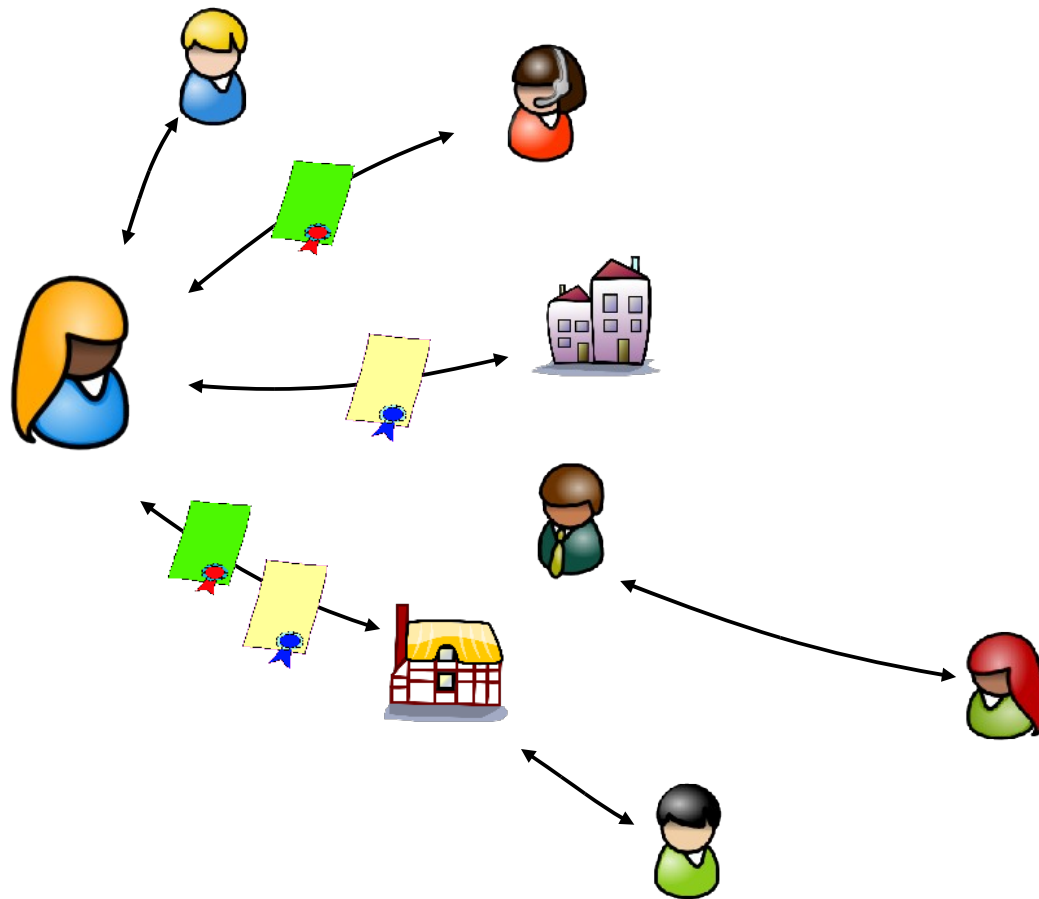
- Fundamentally understanding privacy-enhancing identity management 'for life'
- Bringing Privacy to the future web
- Develop and make tools for privacy friendly identity management widely available – *privacy live!*



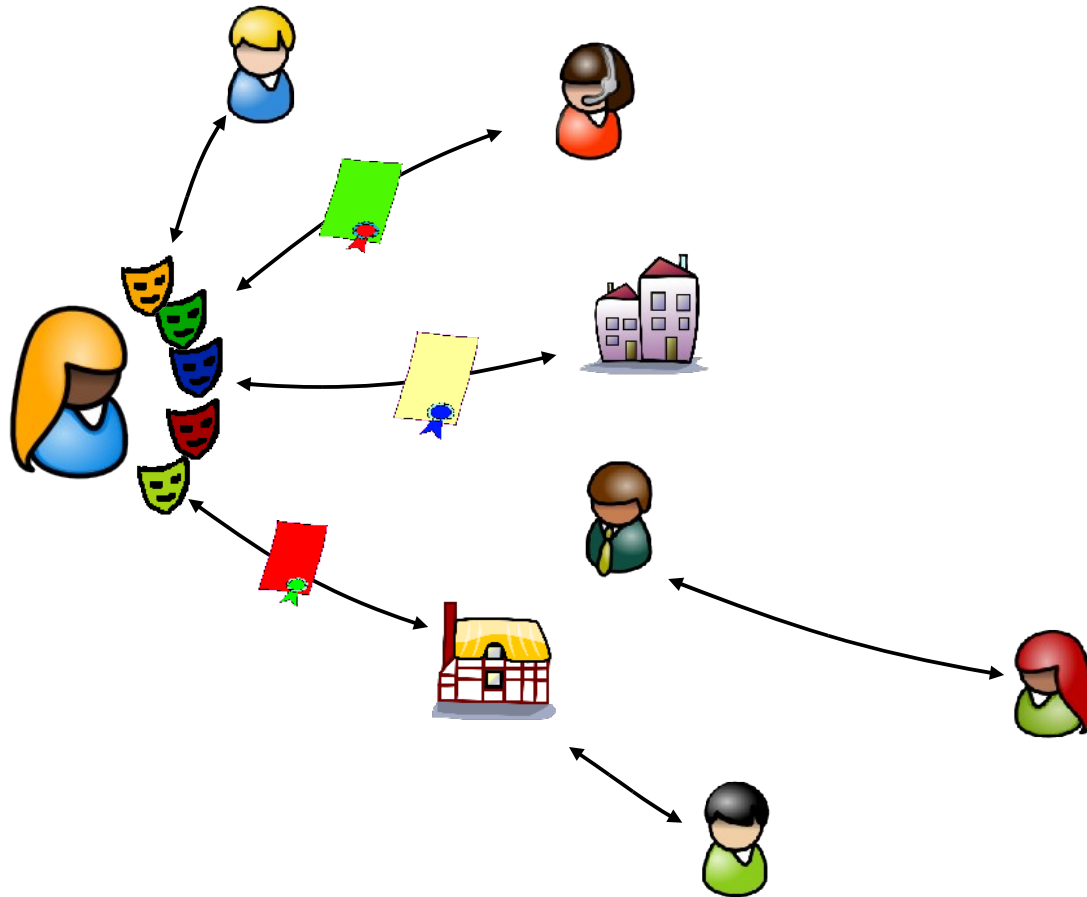
# PrimeLife's 6 Activities



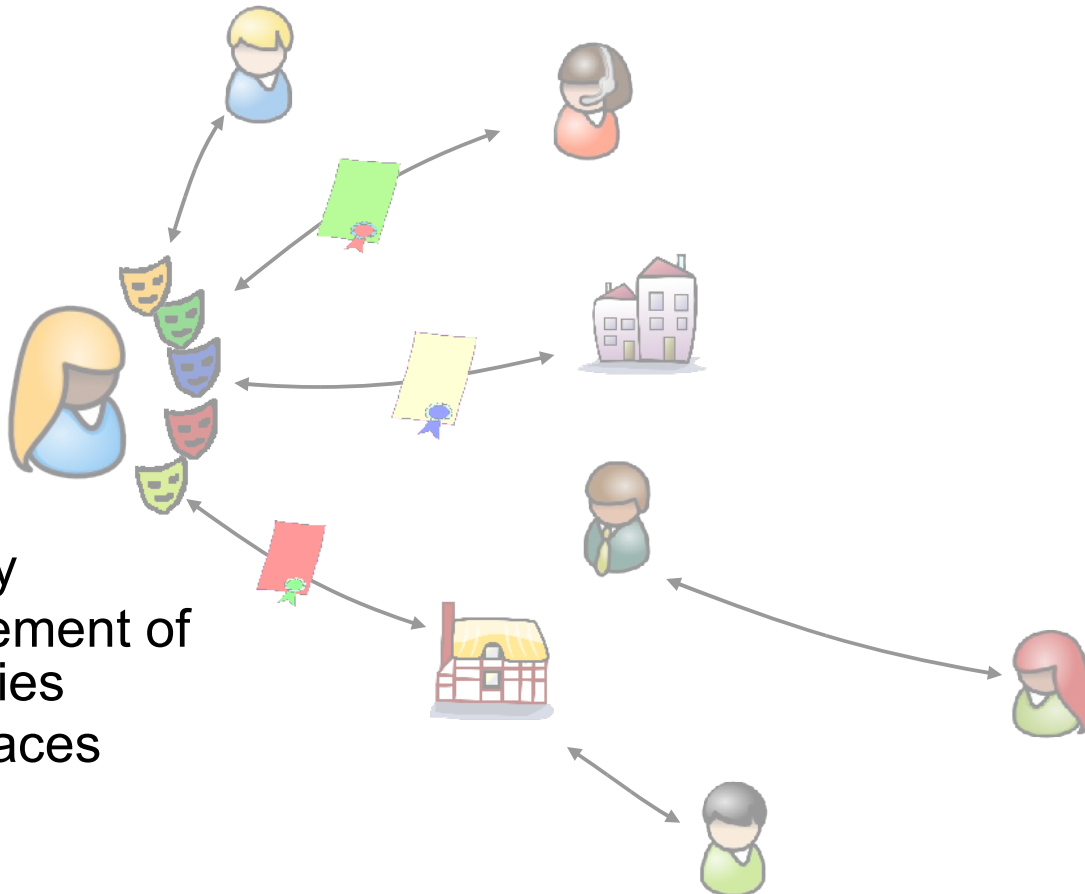
# Scenario



# PrimeLife's approach



# PrimeLife's approach



- Privacy Policy
- Easy Management of *Partial* Identities
- Usable Interfaces

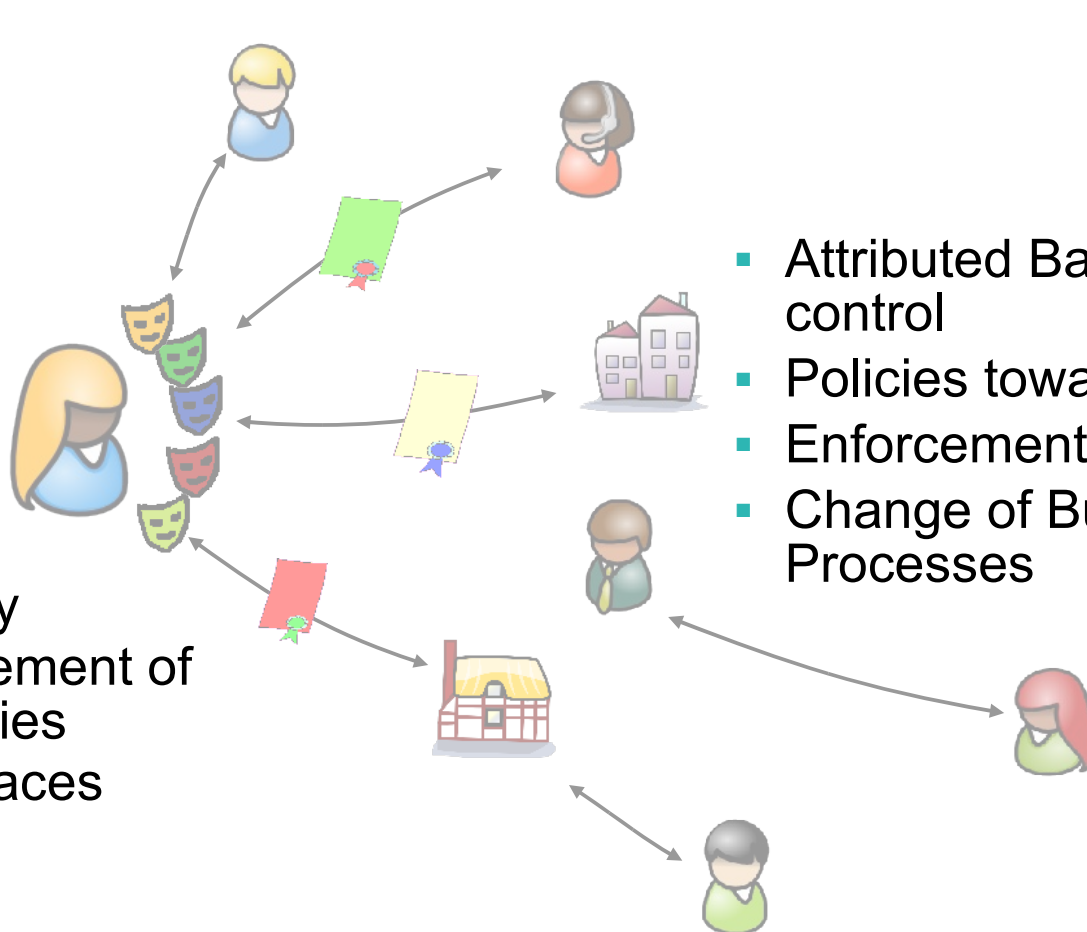
(Anonymous Communication)



# PrimeLife's approach



- Privacy Policy
- Easy Management of *Partial* Identities
- Usable Interfaces

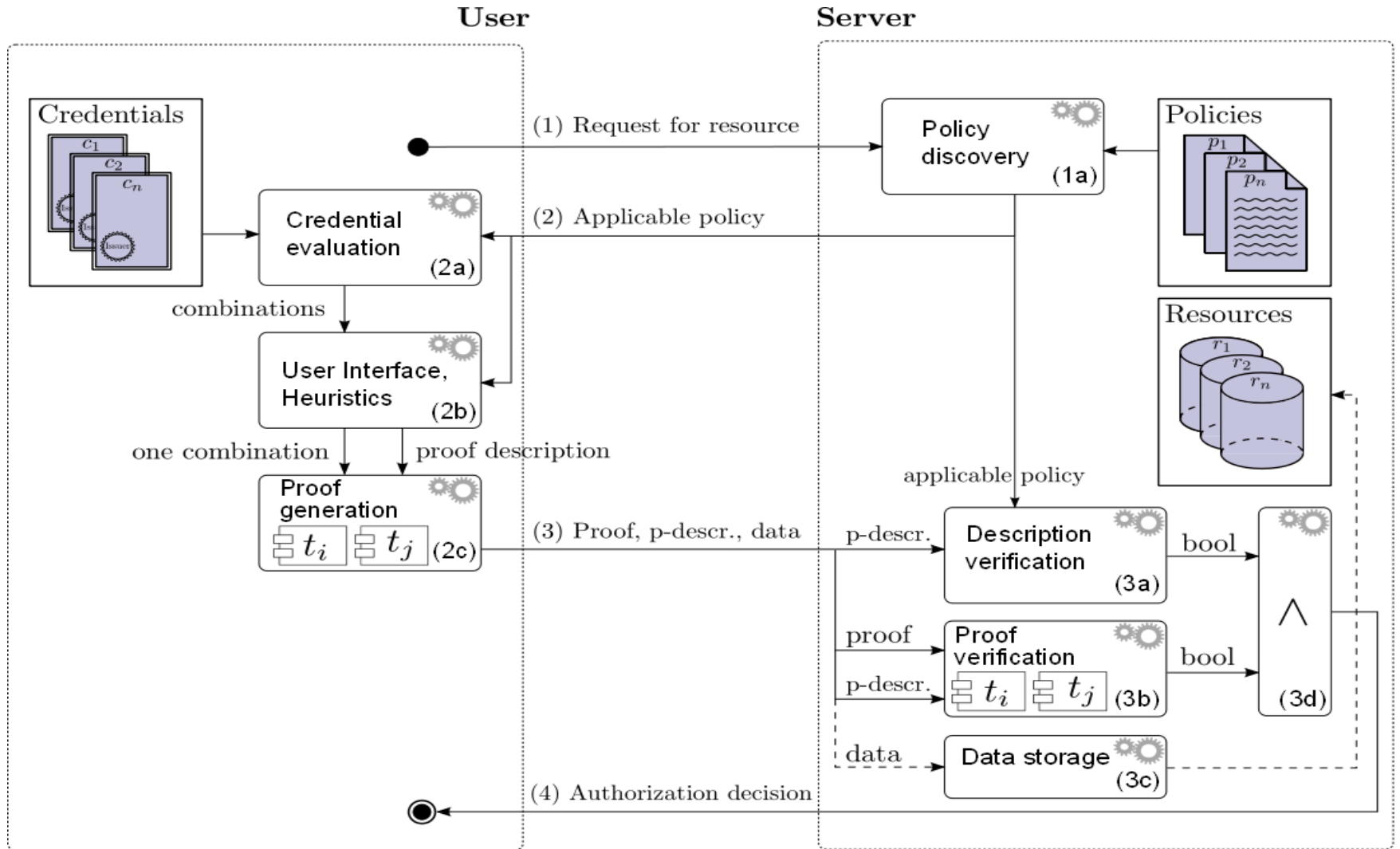


- Attributed Based Access control
- Policies towards users
- Enforcement of Policies
- Change of Business Processes

(Anonymous Communication)



# PrimeLife's Approach



# Privacy



# PrimeLife



# Technology



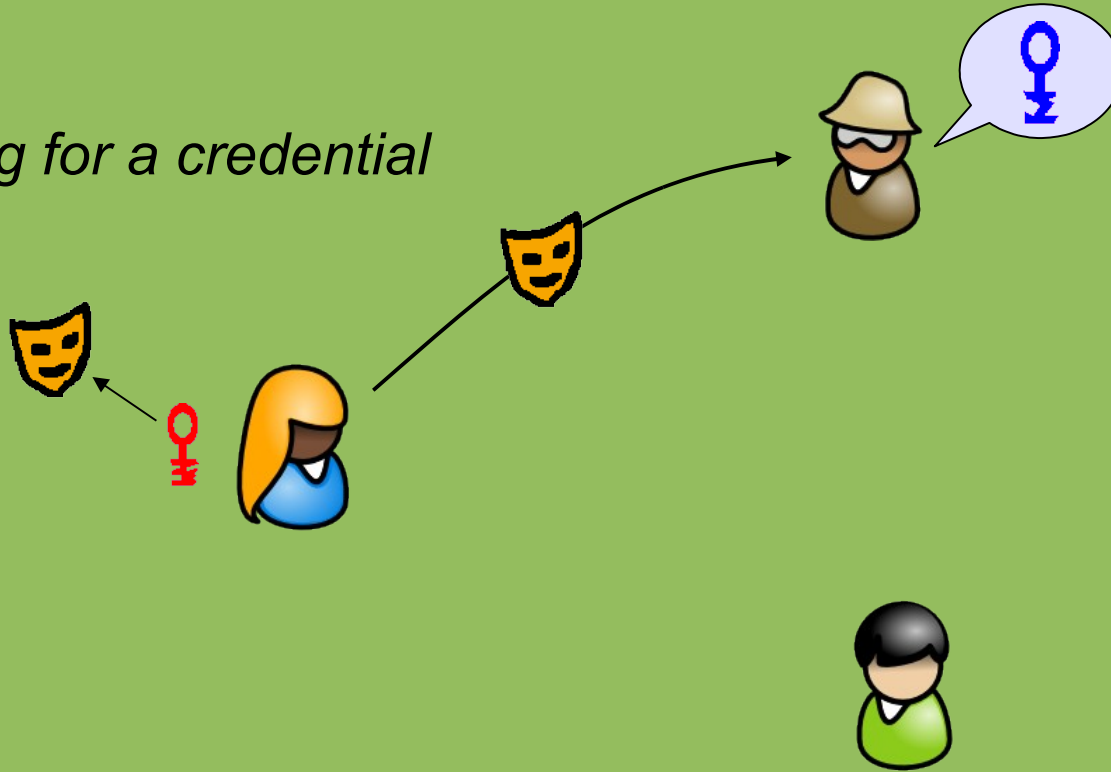
# Private Credentials: How to Build Them

*In the beginning...*



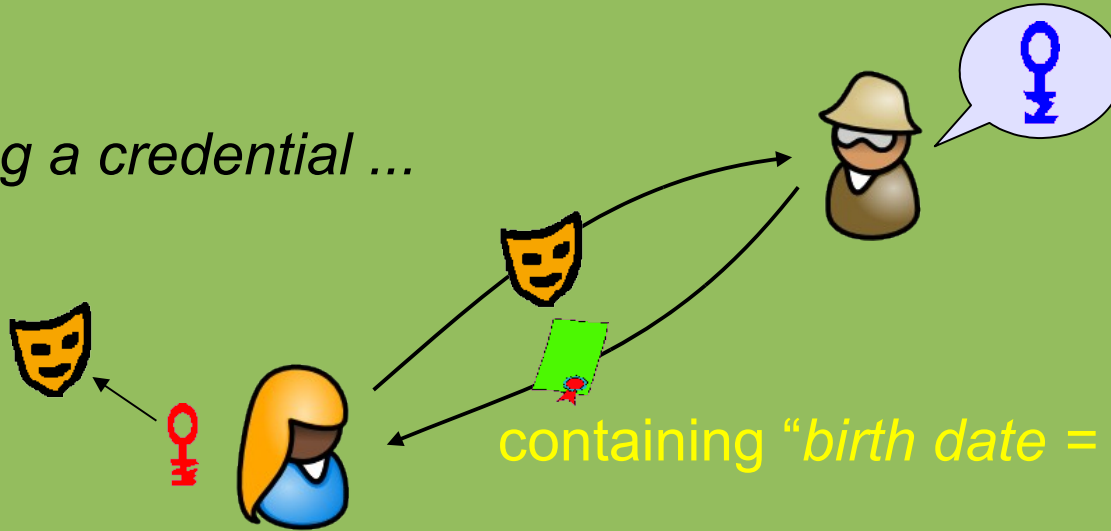
# State of the Art: How to Build Them

*asking for a credential*



# State of the Art: How to Build Them

*getting a credential ...*

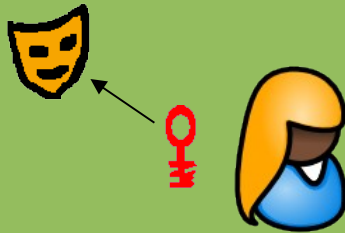


containing "birth date = April 3, 1987"



# State of the Art: How to Build Them

*showing a credential ...*



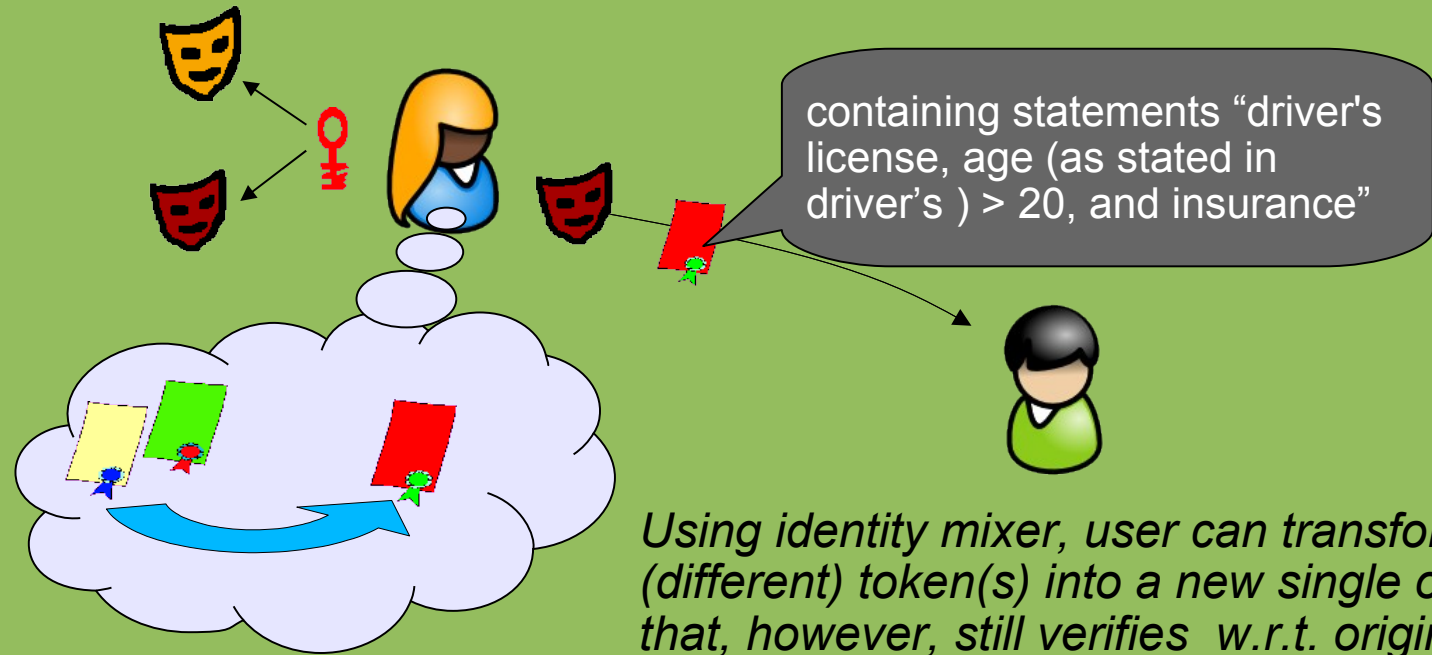
goes off-line

- driver's license
- insurance
- older > 20



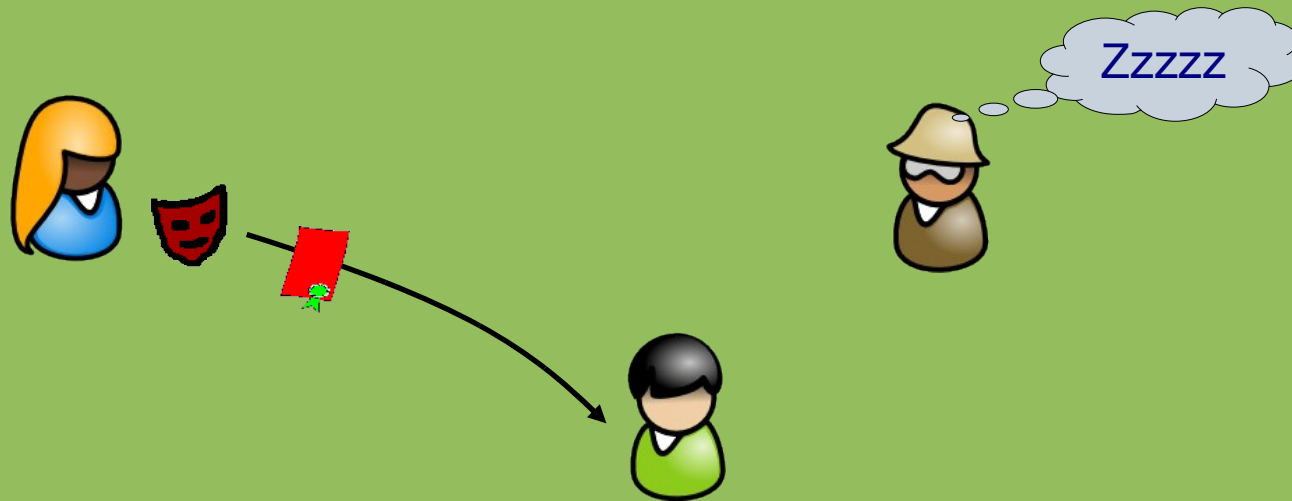
# State of the Art: How to Build Them

*showing a credential ...*



*Using identity mixer, user can transform (different) token(s) into a new single one that, however, still verifies w.r.t. original signers' public keys.*

# Other Properties: Offline Usage



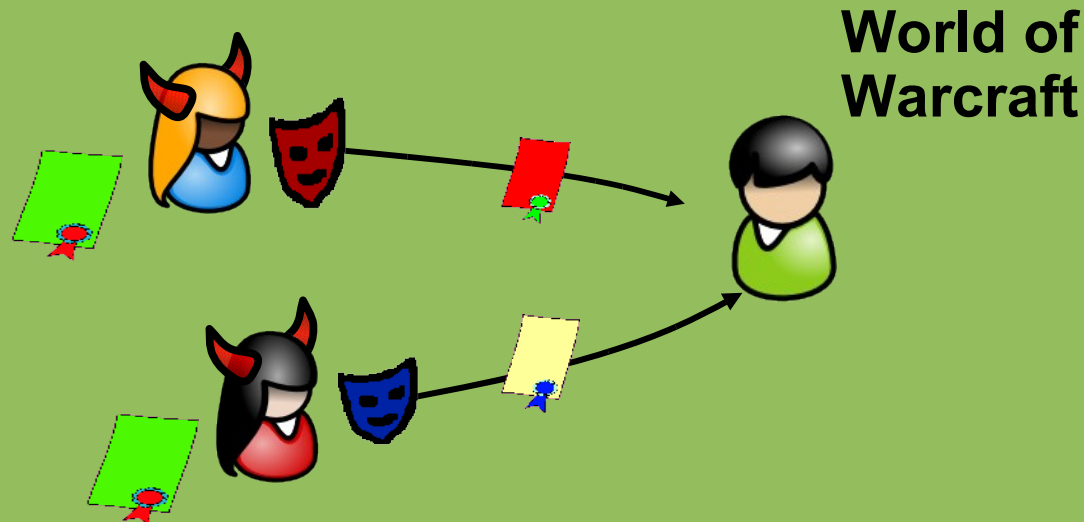
ID providers (issuers) need sleep, too!

- Sometimes it is too expensive to have connectivity
- Or a security risk (e.g., ID cards)

Certs can be used as many times as needed!

- cf. Revocation; can be done w/ signer's secrets offline

# Other Properties: Cheating Prevention



Limits of anonymity possible (*optional*):

- If Alice and Eve are on-line together they are caught!
- Use Limitation – anonymous until:
  - If Alice used certs  $> 100$  times total...
  - ... or  $> 10'000$  times with Bob
- Alice's cert can be bound to hardware token (e.g., TPM)

# Privacy Preserving Access Control

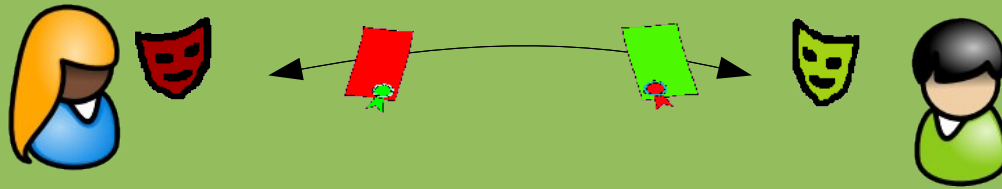


Simple case: DB learns not who accesses DB

Better: Oblivious Access to Database (OT with AC)

- Server must not learn *who* accesses
- *which* record
- Still, Alice can access only records she is *authorized* for

# Secret Handshakes



- Alice and Bob both define some predicate  $PA$  and  $PB$
- Alice learns whether Bob satisfies  $PA$  if she satisfies  $PB$

# Smart Identity Card: Design Goals

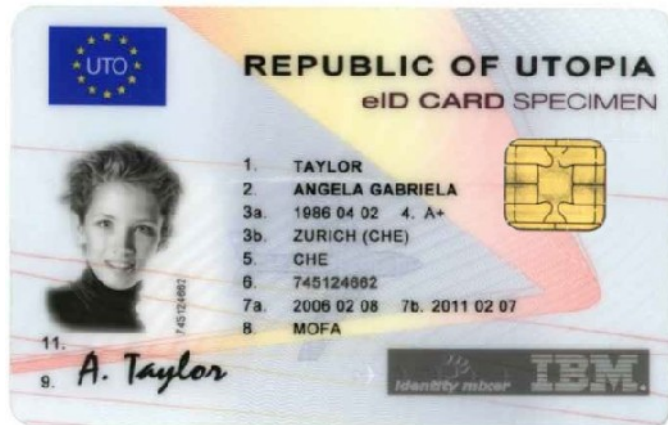
**Strong accountability and privacy**

**Sustainable secondary use**

**sted identity basis**

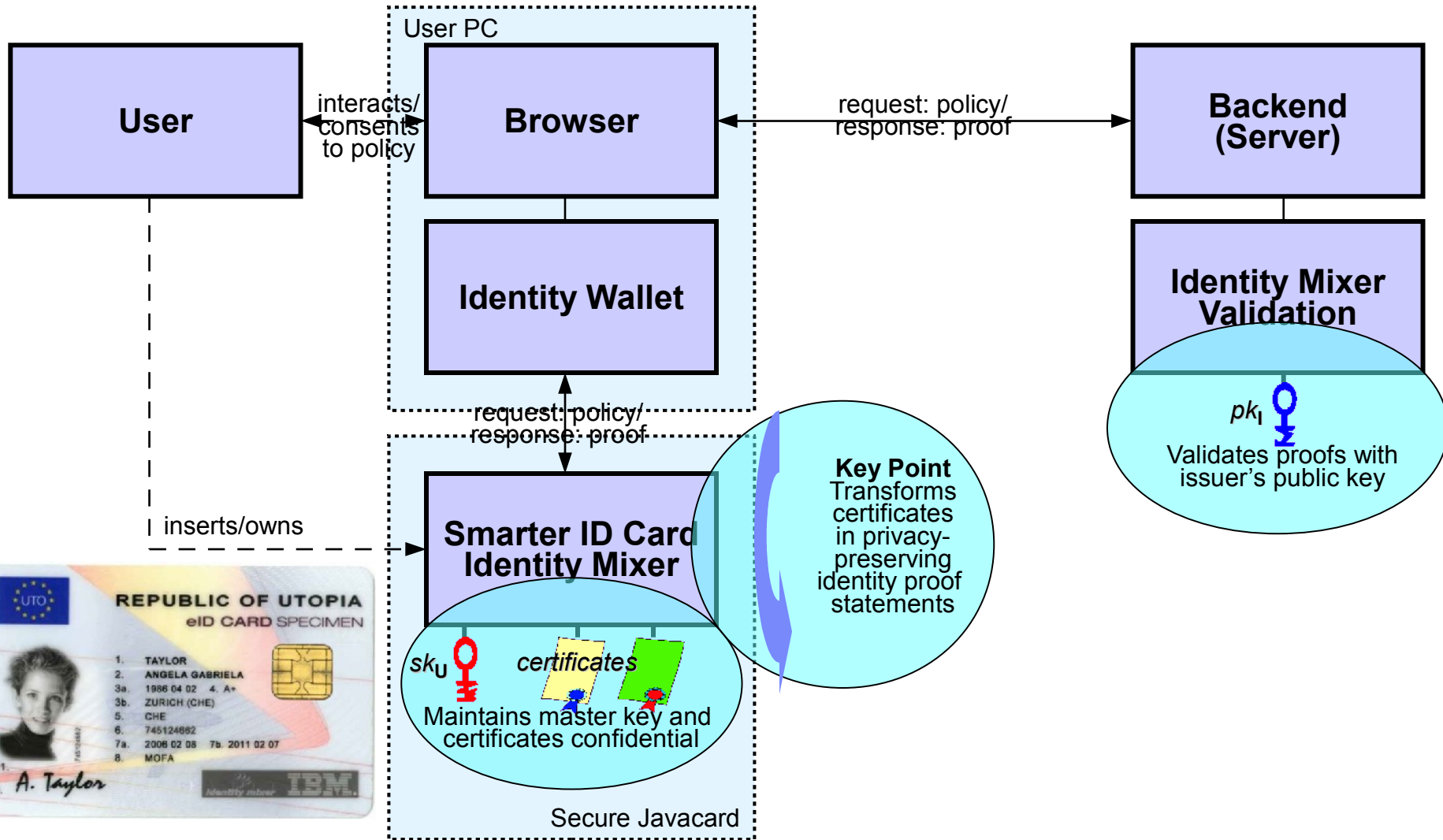
**Future-proof**

**Cost effective**



Won the Innovation Award 2009 of the Society for Computer Science (GI, comparable to the ACM in Germany)

# Smart Identity Card



# Privacy



**Important &  
complex  
challenge**

# PrimeLife



**Sustainable  
identity &  
privacy  
'for life'**

# Technology



**Crypto to  
rescue:  
efficient on  
any device**

Thank you!



## Contributors:

Björn Assmann, Endre Bangerter, Patrik Bichsel, Carl Binding, Anthony Bussani, Jan Camenisch, Thomas Gross, Susan Hohenberger, Phil Janson, Gregory Neven, Franz-Stefan Preiss, Dieter Sommer, Abhi Shelat, Victor Shoup, Michael Waidner, Roger Zimmermann, & innumerous interns