

# eID needs Privacy “on”

Jan Camenisch  
IBM Research – Zurich

Leon Feb 10, 2009

Houston, we  
have a problem!



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

*(Robin Wilton, Sun Microsystems)*



# Computers don't forget!



- Storage becomes ever cheaper
- Data mining ever better

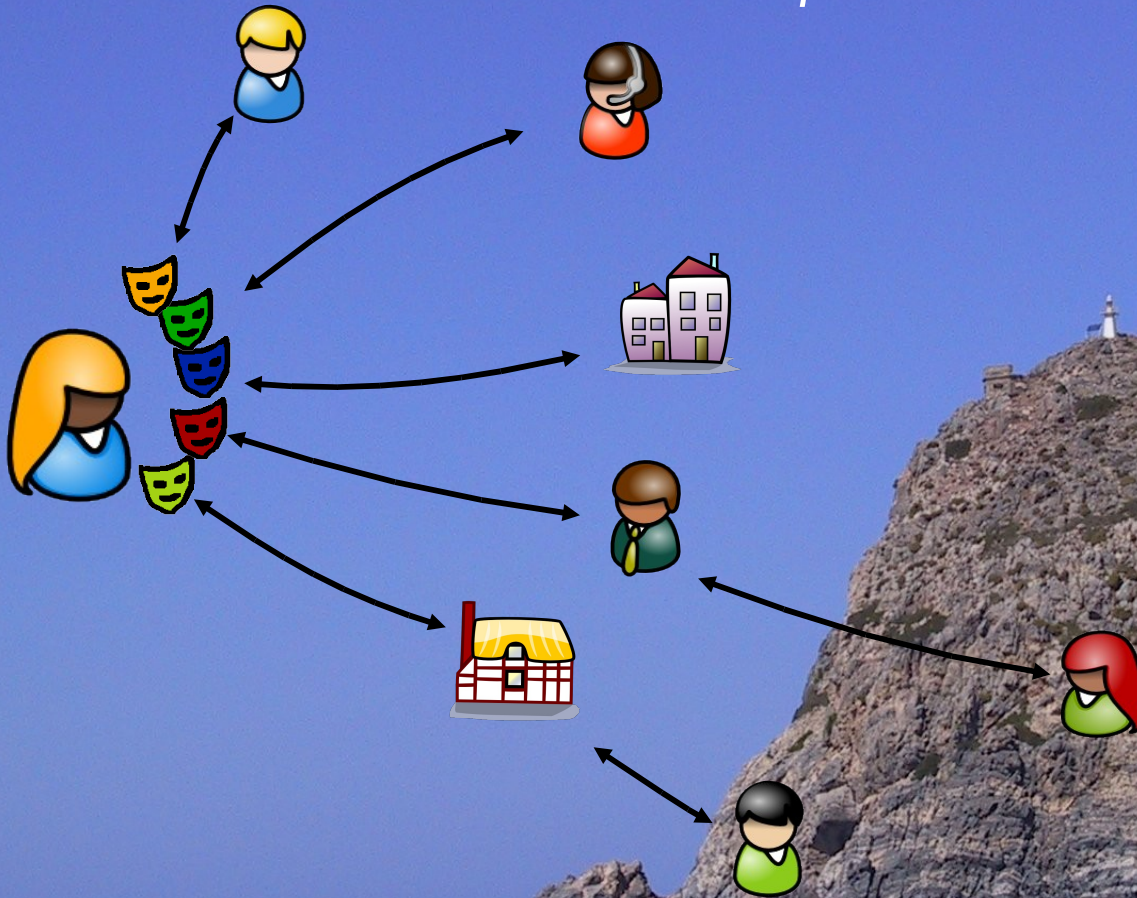



# And we leave traces, lots of traces!



# Our Vision

In the Information Society, *users* can act and interact in a *safe and secure* way while *retaining* control of their private spheres.





Need to employ  
Private Credentials  
on eID cards

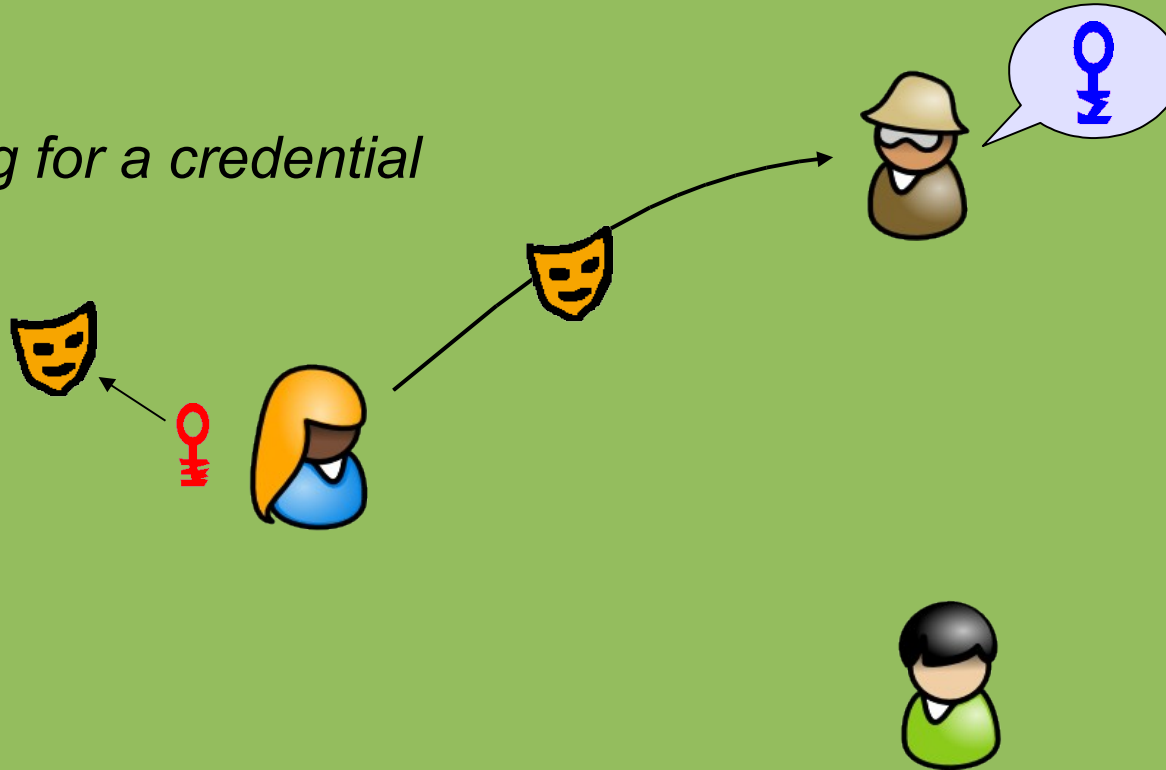
# Private Credentials: how they work

*In the beginning...*



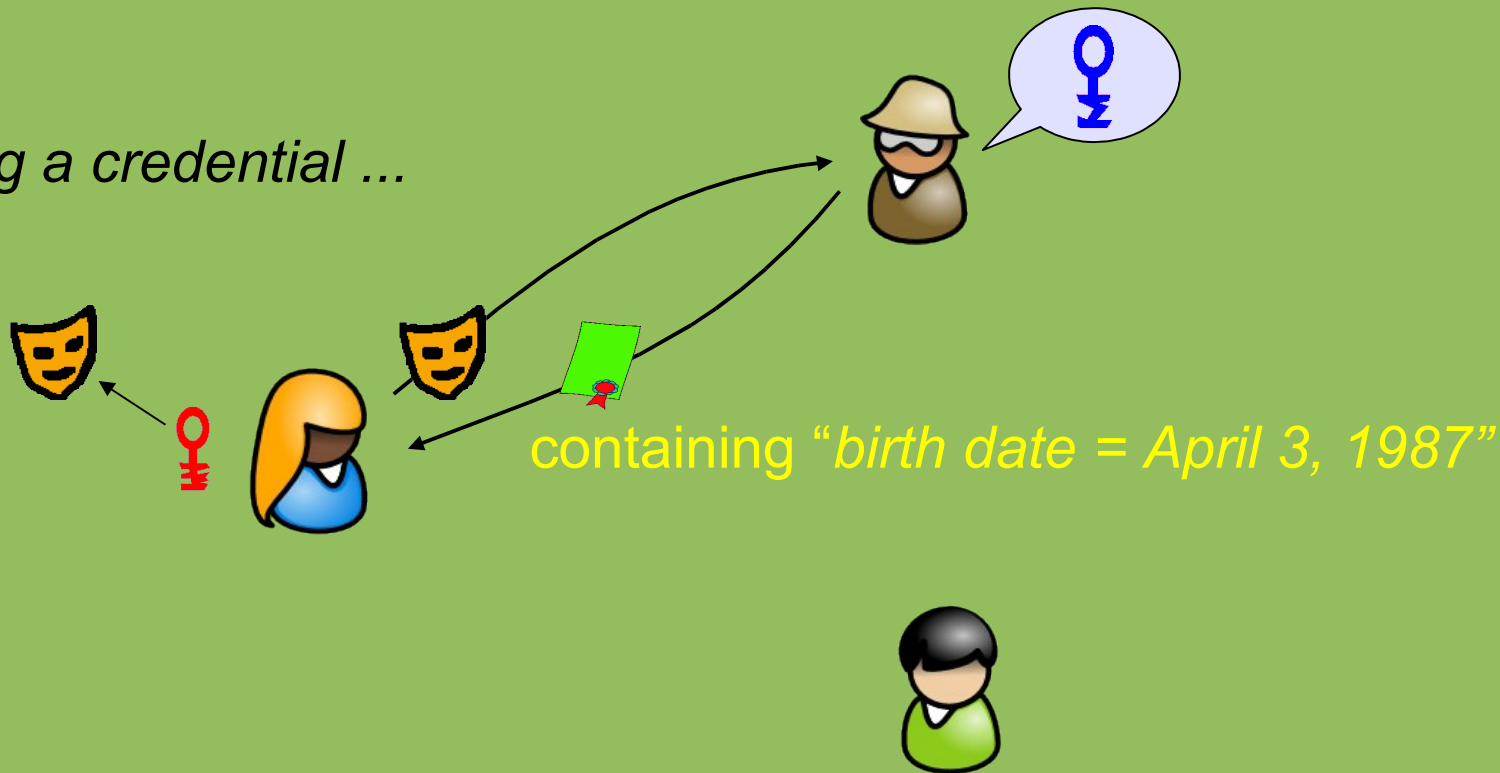
# Private Credentials: how they work

*asking for a credential*



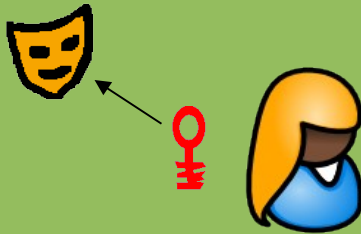
# Private Credentials: how they work

getting a credential ...



# Private Credentials: how they work

*showing a credential ...*



goes off-line



- driver's license
- insurance
- older > 20



# Private Credential are practical!

... work on Smart Cards!

... and offer all features needed:

- Controlled release of attributes
  - Selective disclosure
  - Encrypted for 3<sup>rd</sup> parties
- Revocation of Credentials
- Detection of misuse
- Revocation of “anonymity”