Cryptography for People

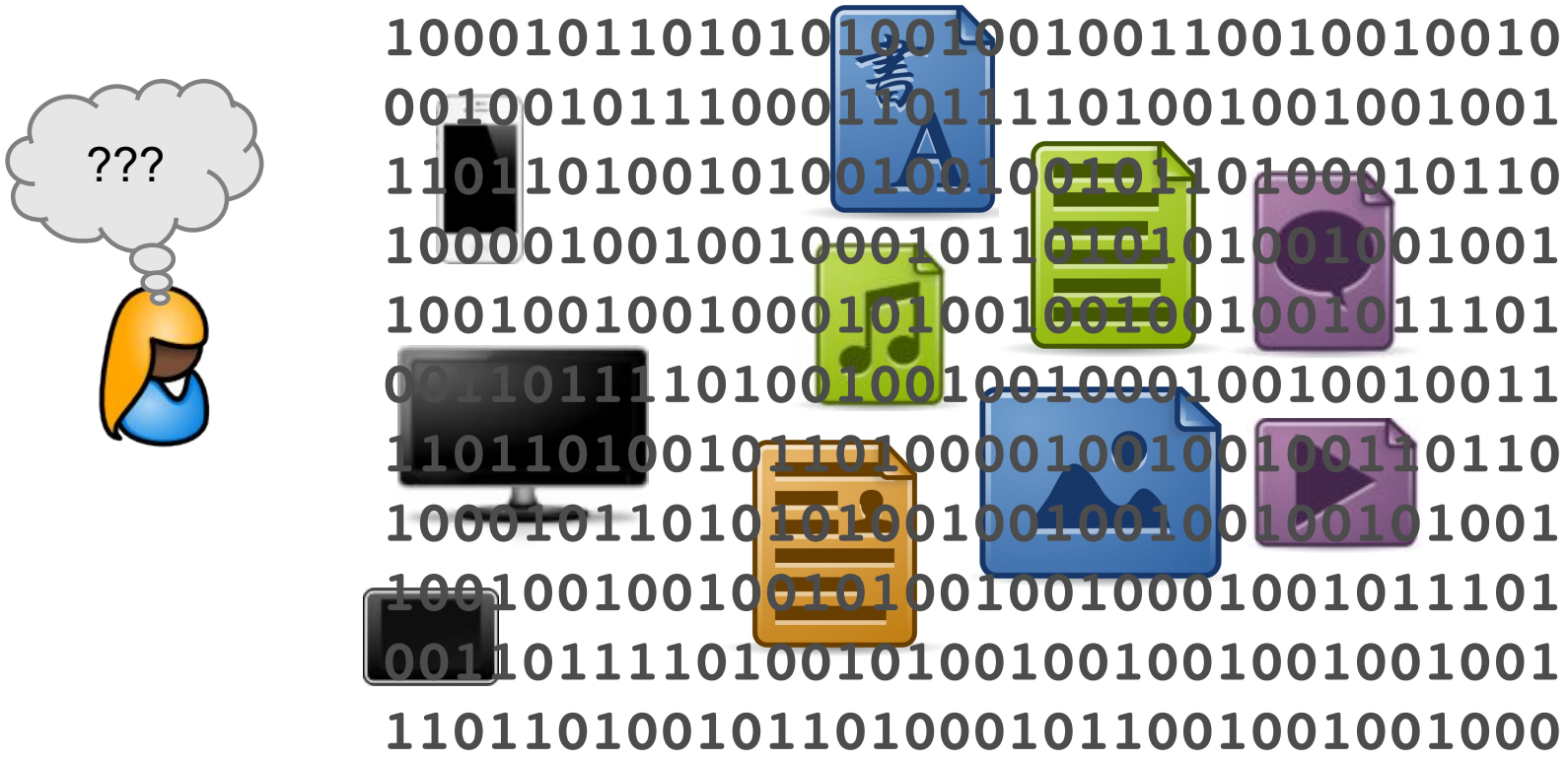
Dr. Jan Camenisch

IBM Research – Zurich
Cryptography & Privacy
Principal Research Staff Member
Member, IBM Academy of Technology

Cryptography for People

Cryptography for People

Cryptography for People

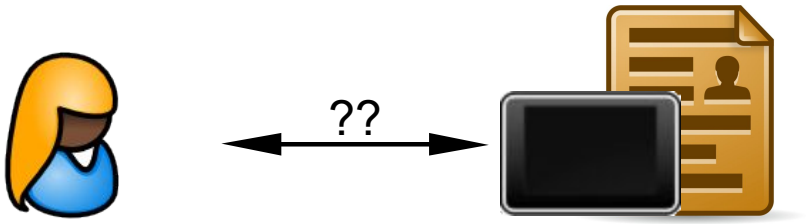


Cryptography for People

Cryptography for People

Cryptography for People

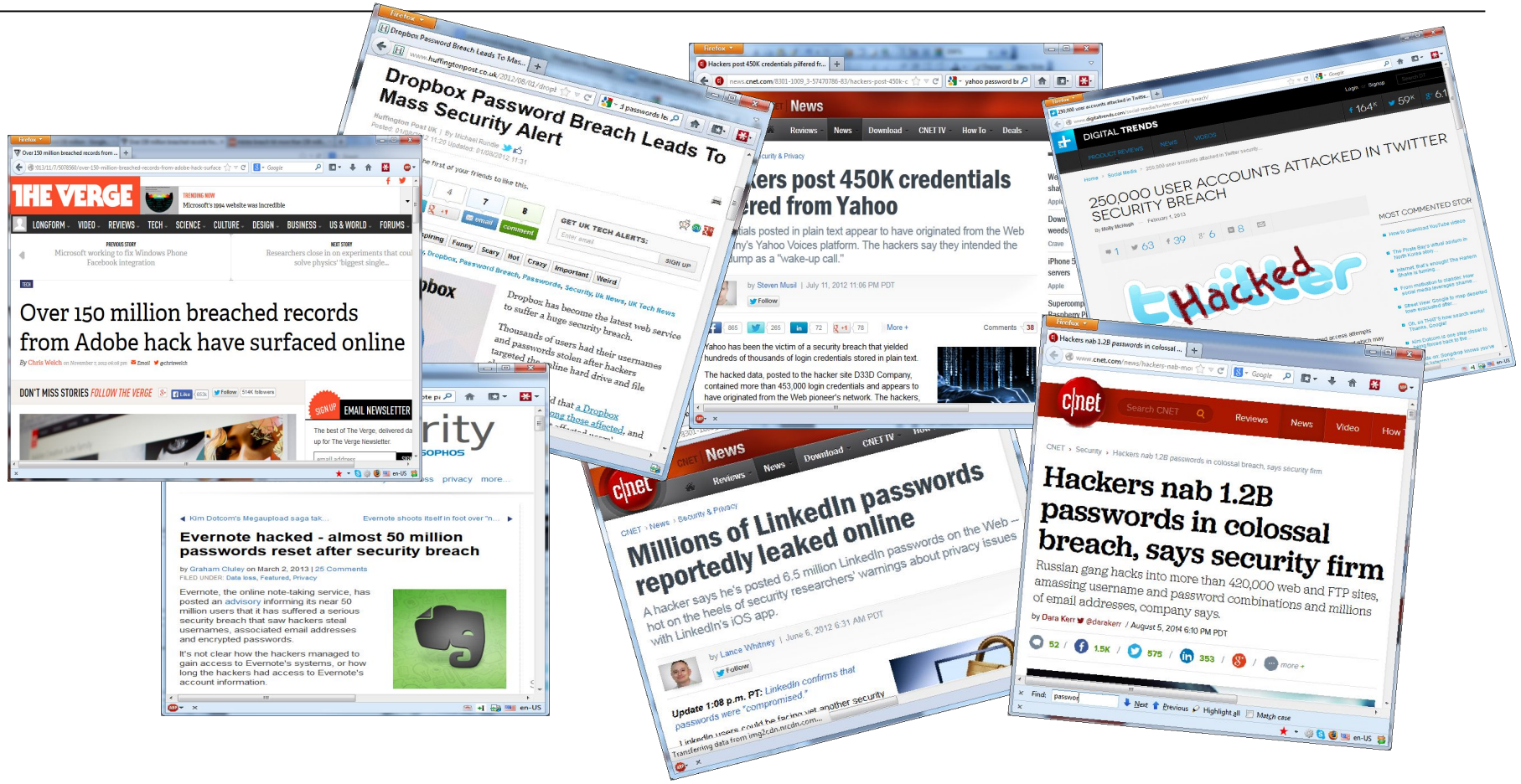
Cryptography for People



How can we bridge the digital gap?

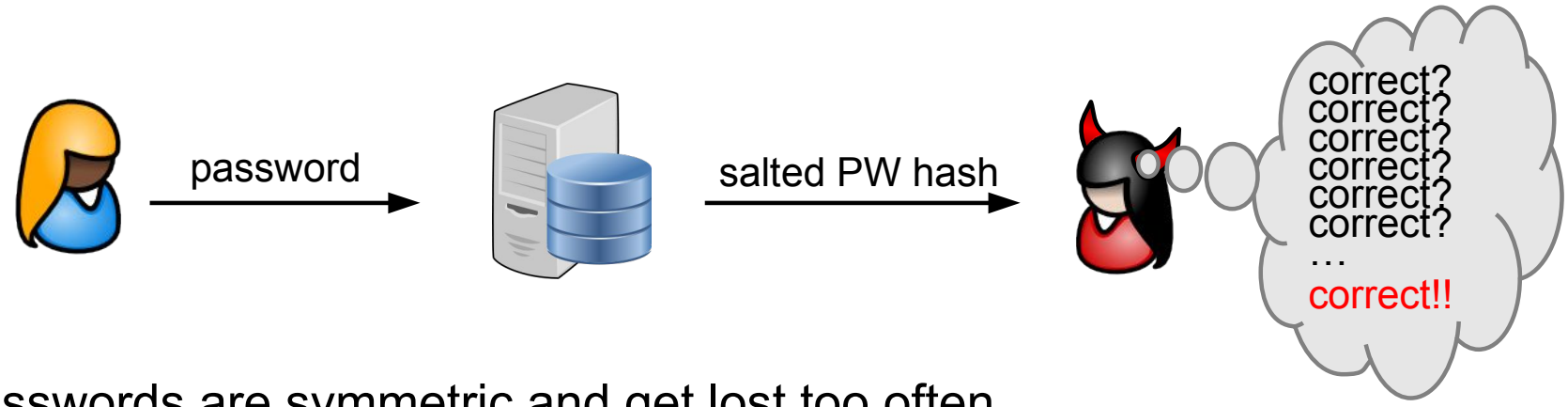
- Passwords?
- Biometrics?
- Watch?
- Implanted Chip?

Password are insecure!?



- Username & password most prominent form of user authentication
- Lots of data breaches resulting in passwords being compromised
- Password are ***not*** insecure – we used them wrongly today!

The problem with passwords

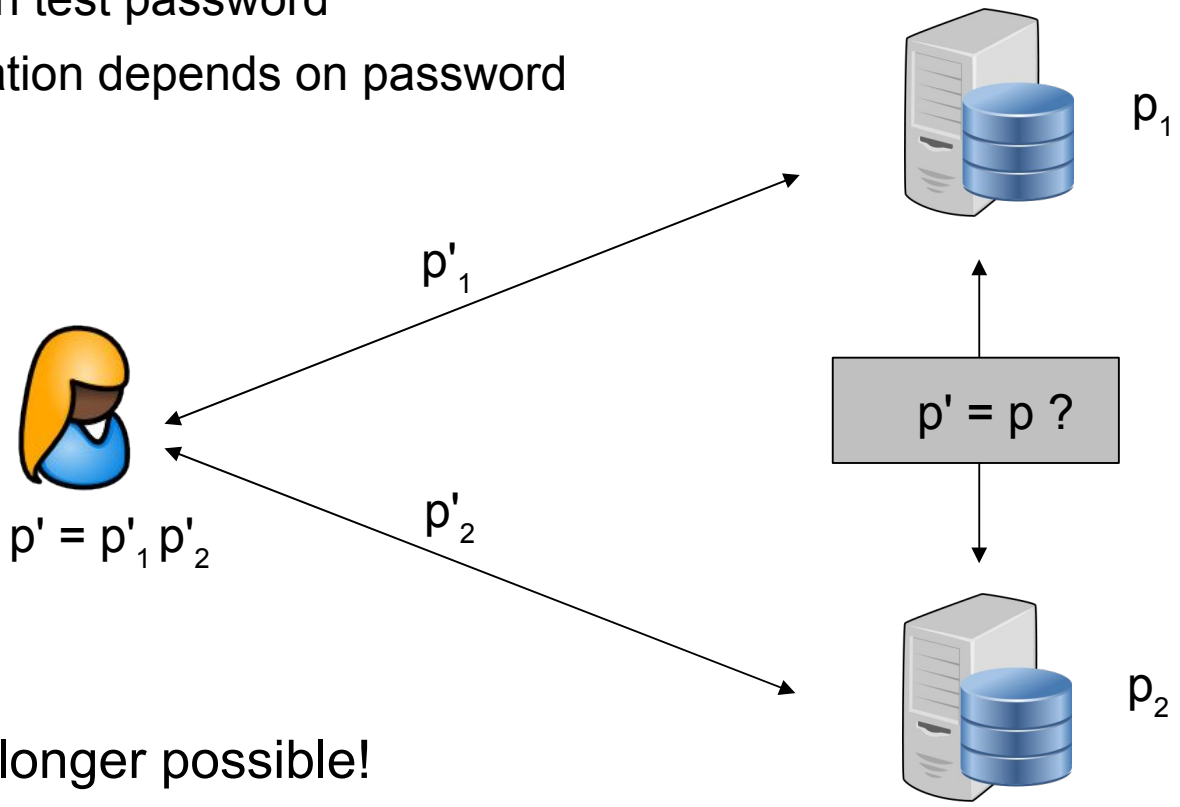


- Passwords are symmetric and get lost too often
- Password (hashes) useless against offline attacks
  - Human-memorizable passwords are inherently weak
  - NIST: 16-character passwords have 30 bits of entropy ≈ 1 billion possibilities
  - Rig of 25 GPUs tests 350 billion possibilities / second, so ≈ 3ms for 16 chars
  - 60% of LinkedIn passwords cracked within 24h
- More expensive hash functions provide very little help only
  - increases verification time as well
  - does not work for short passwords such as pins etc
- Single-server solutions inherently vulnerable to offline attacks
  - Server / administrator / hacker can always guess & test

Solution: distributed password protocols

Basic idea: multi-server password verification protocols

- split password for verification
- no server alone can test password
- no piece of information depends on password



→ Off-line attacks no longer possible!

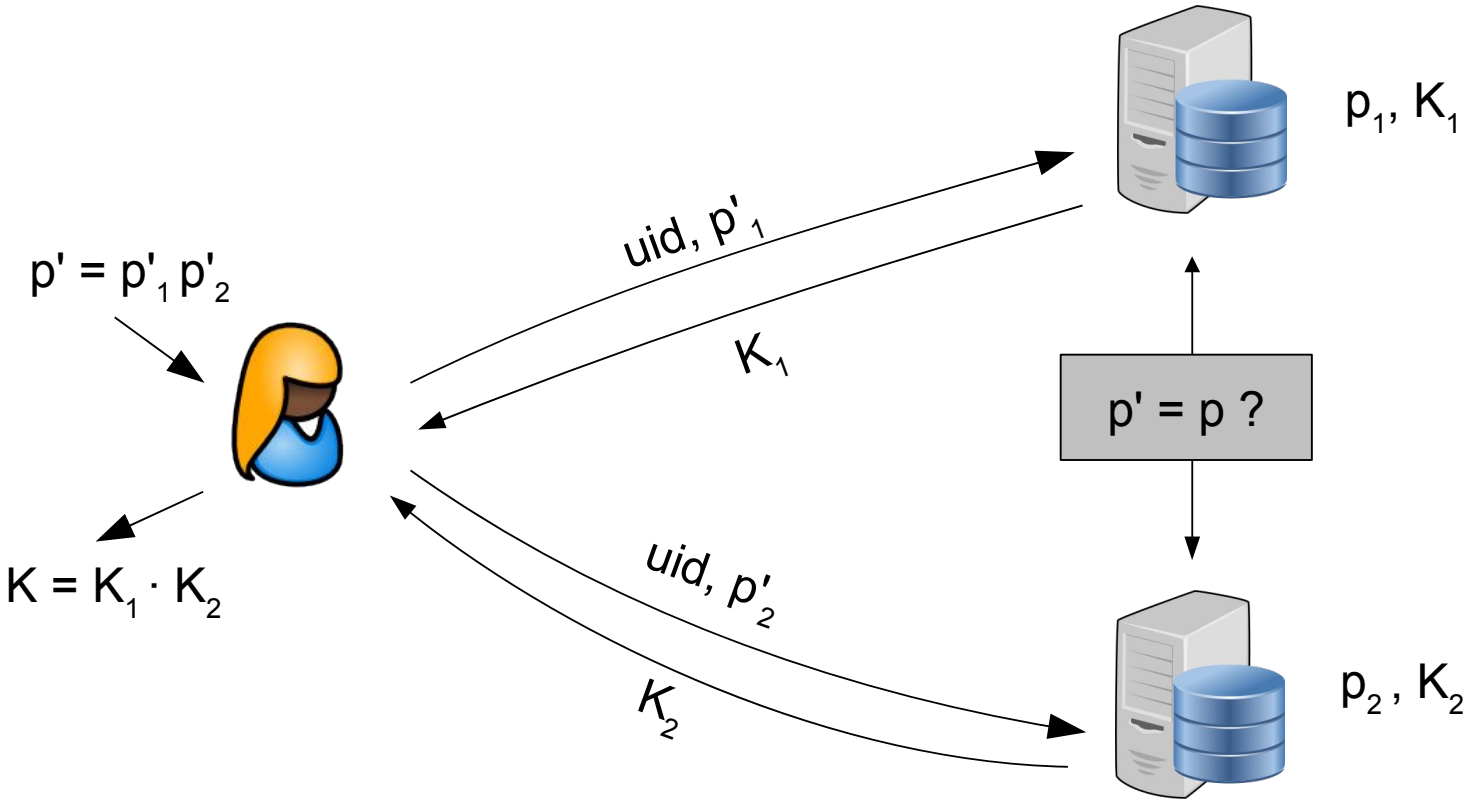
→ On-line attacks detectable and handleable (throttling)

Solution: from passwords to keys – 2PASS

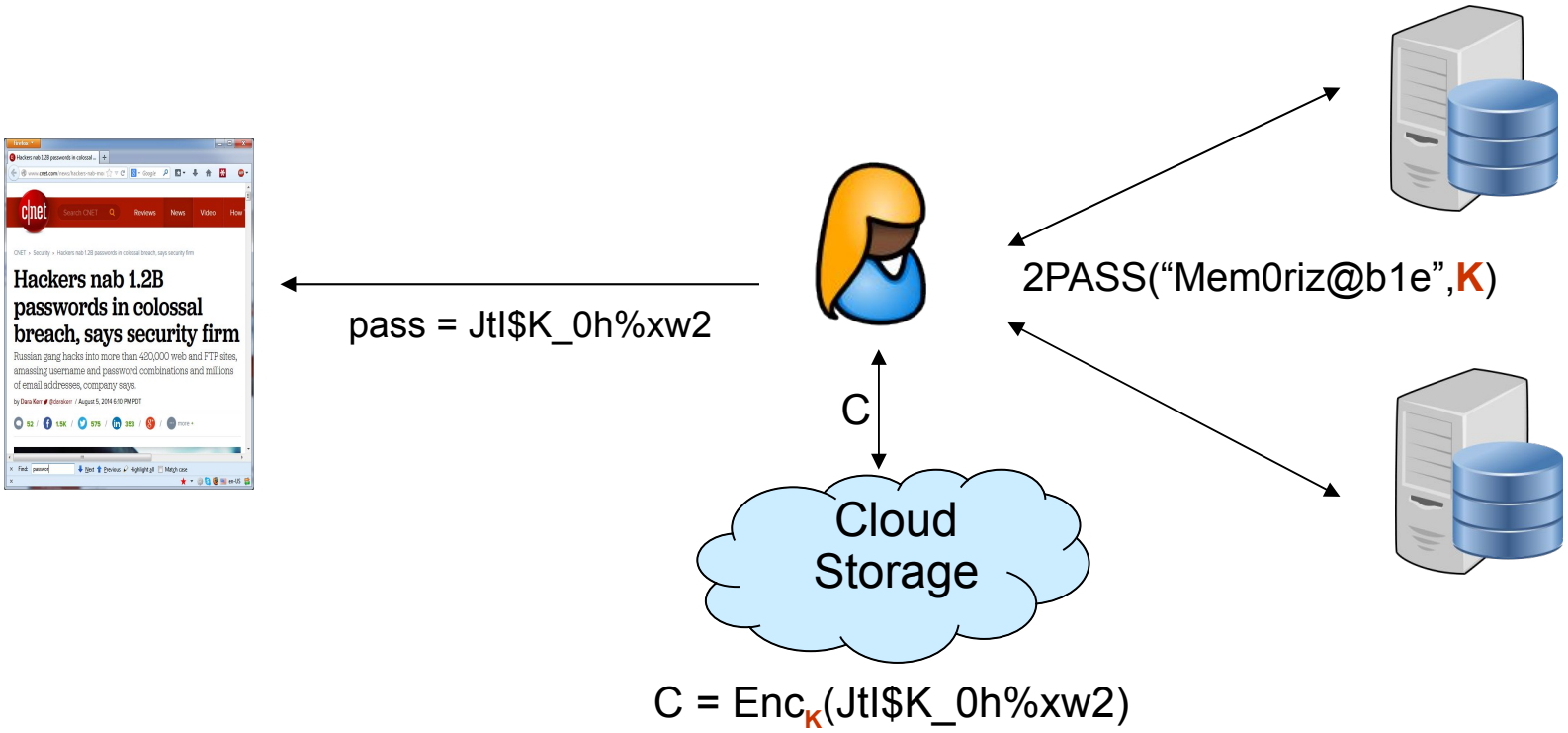
[CLN'12,CLLN'14,CEN'15]

2PASS – Password-authenticated secret sharing

- also secret share a cryptographic key $K = K_1 \cdot K_2$



Example application: secure password manager

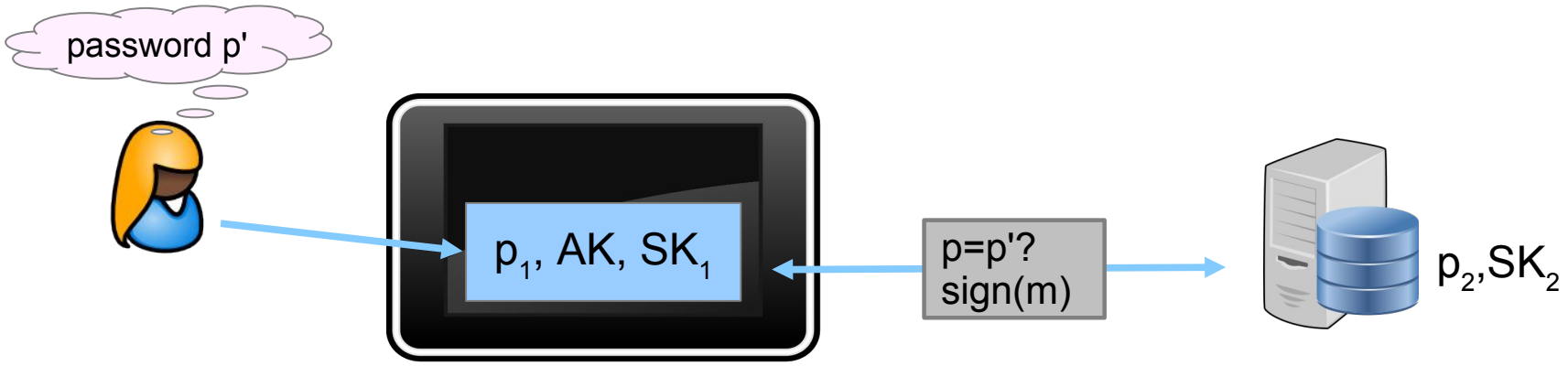


Extension: virtual smart card

[CLNS'15]

We can also do cryptographic operations, e.g., signing

- User with device: device can be one of the password checking servers
- Device & user authenticate towards server: two factor authentication
- After authentication, device and server run distributed signing protocol



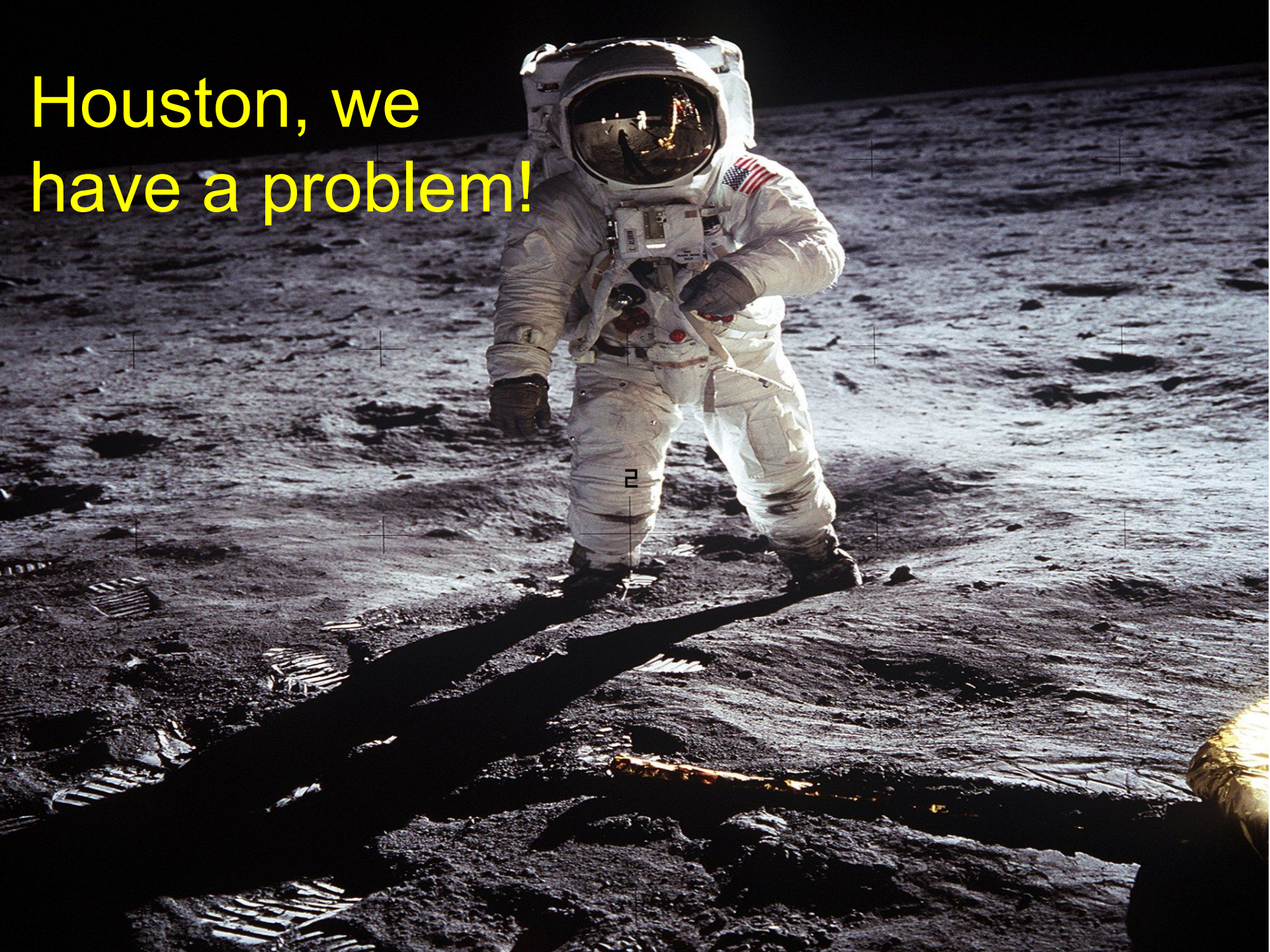
- Security equivalent to real smart card
  (-) Hard to protect against malware on device (smart card fares better here)
  (+) Virtual smart card can be revoked if lost.
- Virtual smart cards much more convenient (roll out, different devices, ...)

So are we happy?

… we know how we can protect our data :-)

… but only as long as it's under our control :-(

→ How can we use the Internet with our data being protected?


Houston, we
have a problem!


Houston, we have a problem!
“Neil Armstrong's footprints are still up there”

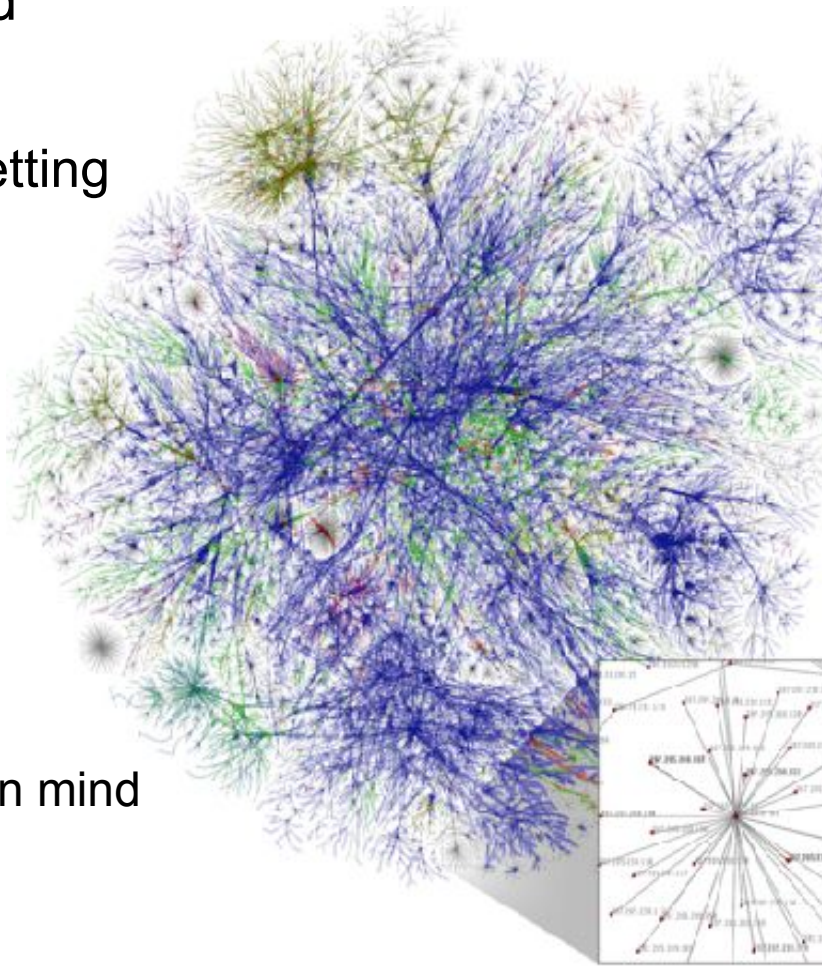
Computers don't forget

- Data storage ever cheaper → “store by default”
  - e.g., surveillance cameras, Google Street View with wireless traffic, Apple location history,...
- Data mining ever better
  - self-training algorithms cleverer than their designers
  - not just trend detection, even prediction, e.g., flu pandemics, ad clicks, purchases,…
  - what about health insurance, criminal behavior?
  - correlation with illegal criteria, e.g., race, religion
  - spying and sabotage by intelligence agencies

Where's all my data?

The ways of data are hard to understand

- Devices, operating systems, & apps are getting more complex and intertwined
  - Mashups, Ad networks
  - Not visible to users, and experts
  - Data processing changes constantly
- Networks and systems badly protected
  - Systems are being built with “paper world” in mind
  - Feature creep, security comes last, if at all
  - Everyone can do apps and sell them



→ It is far too easy to lose data and to collect data

You have no privacy, get over it .....?!?

- Huge security problem!
  - Millions of hacked passwords (100'000 followers $115 - 2013)
  - Lost credit card numbers ($5 - 2013)
  - Stolen identities ($150 - 2005, $15 - 2009, $5 – 2013)
  - Lots of not reported issues (industrial espionage, etc)

- Difficult to put figures down
  - Credit card fraud
  - Spam & marketing
  - Manipulating stock ratings, etc..

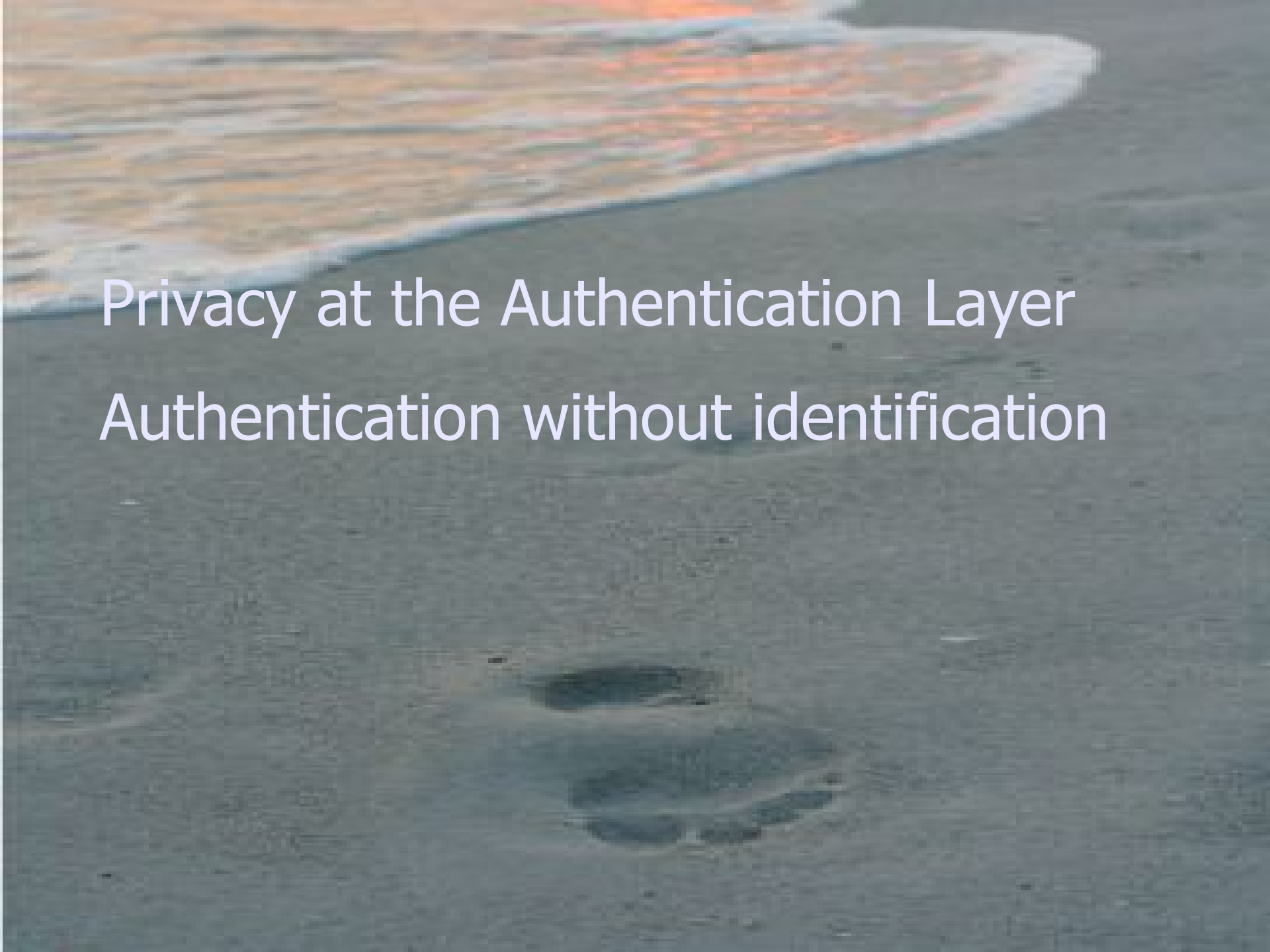
- We know secret services can do it easily, but they are not the only ones
  - but this is not about homeland security
  - and there are limits to the degree of protection that one can achieve

- … and we have not event discussed social issues such as democracy etc

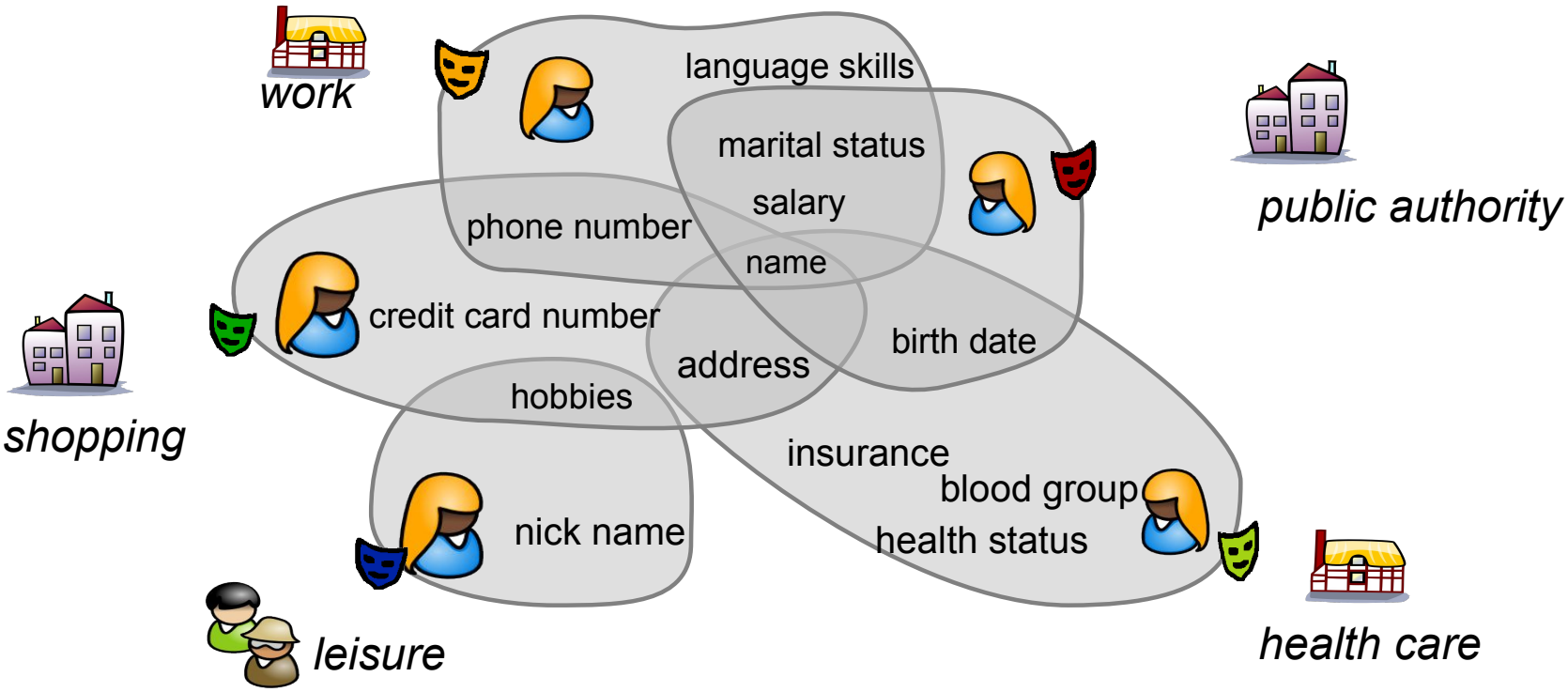
- last but not least: data are the new money, so they need to be protected!

Privacy by design

- Communication layer
  - TOR, JAP, etc
- Authentication layer
  - privacy-preserving attribute-based credentials
- Application layer
  - eVoting, ePolls, ...
  - all apps should be done as “privacy by design”


Privacy at the Authentication Layer
Authentication without identification

Identity, Identity Management, & Authentication

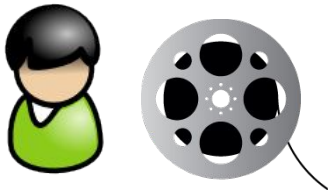


- ID:
  - (dynamic) set of attributes shared w/ someone
  - different with different entities
- ID Management: two things to make identities useful
  - authentication means: strong e-authentication
  - means to transport attributes between parties: certified attributes


Let's see a scenario

Alice wants to watch a movie at Movie Streaming Service

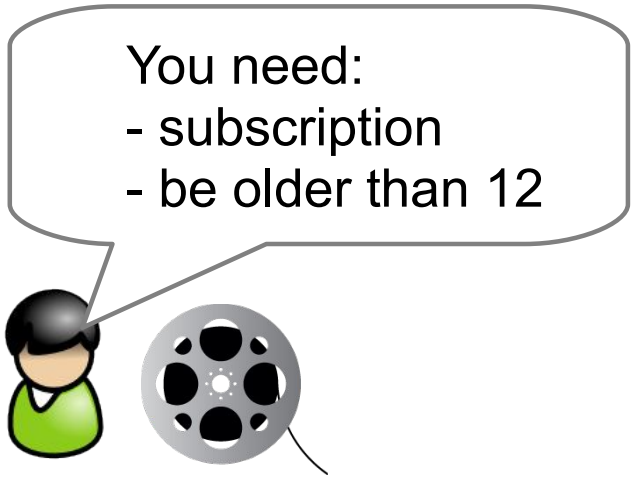
Alice



Movie Streaming Service

Alice wants to watch a movie at Movie Streaming Service

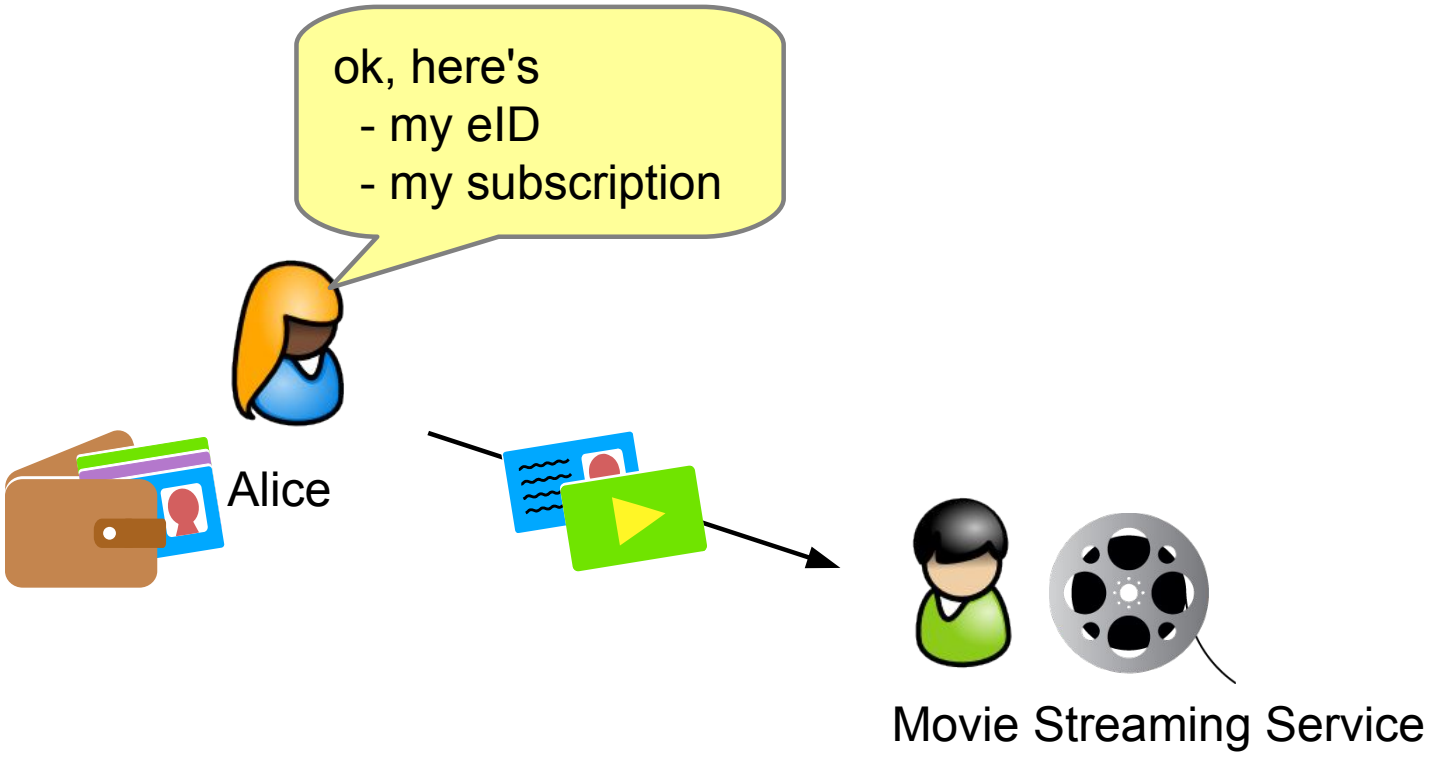
Alice



Movie Streaming Service

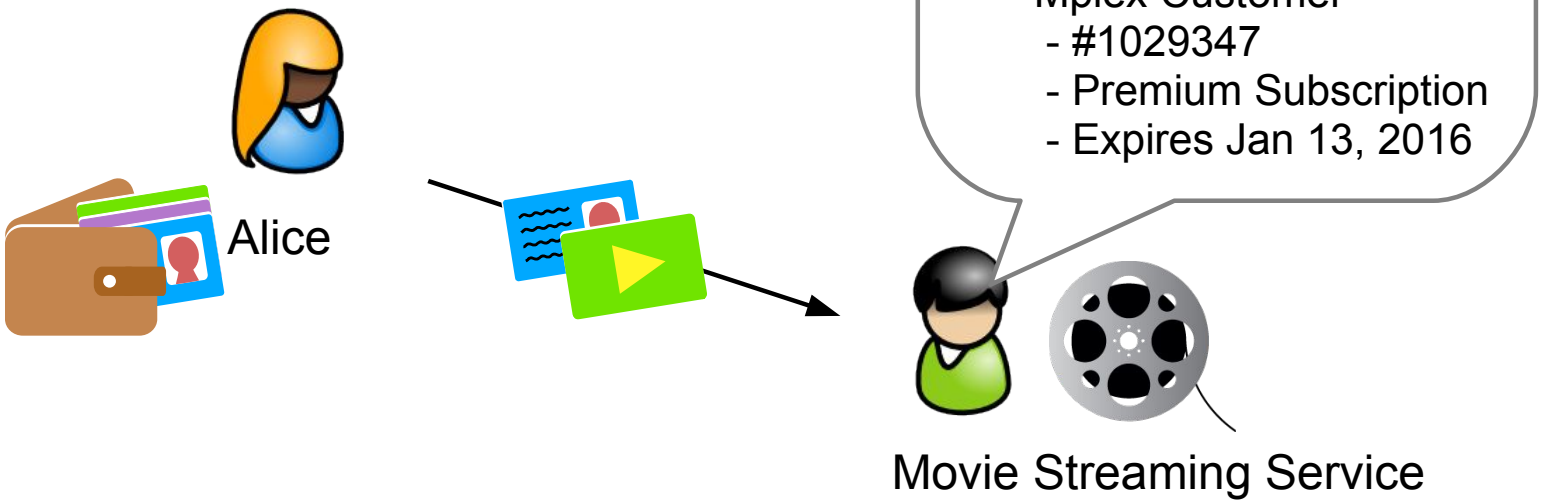
Watching the movie with the traditional solution

Using digital equivalent of paper world, e.g., with X.509 Certificates



Watching the movie with the traditional solution

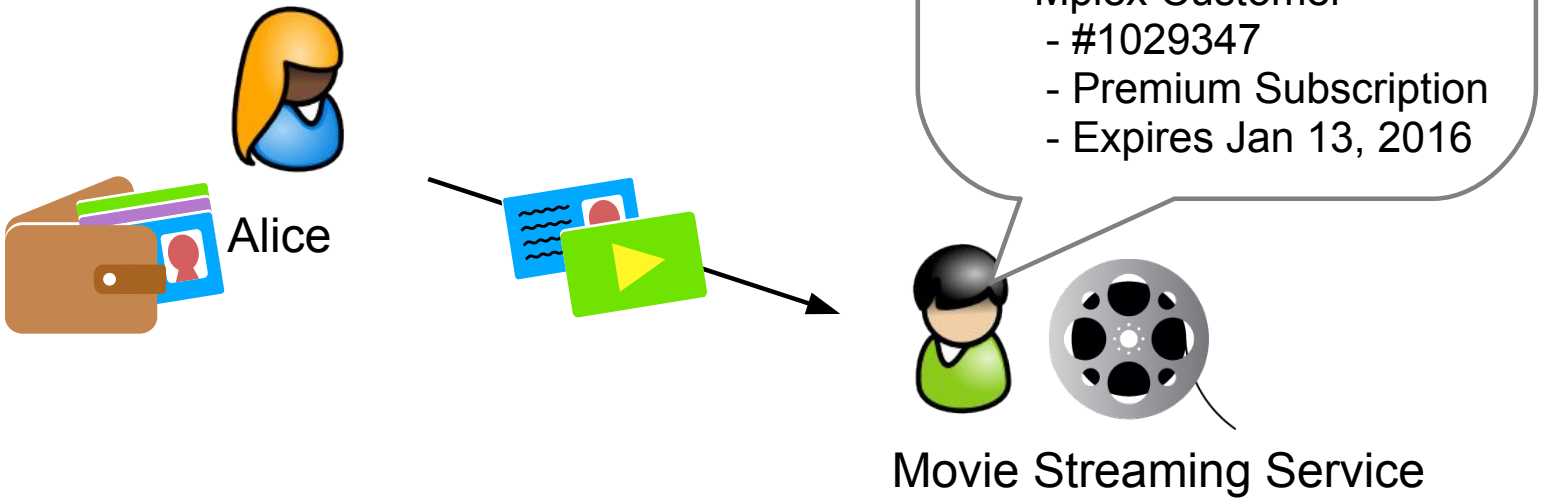
...with X.509 Certificates



Watching the movie with the traditional solution

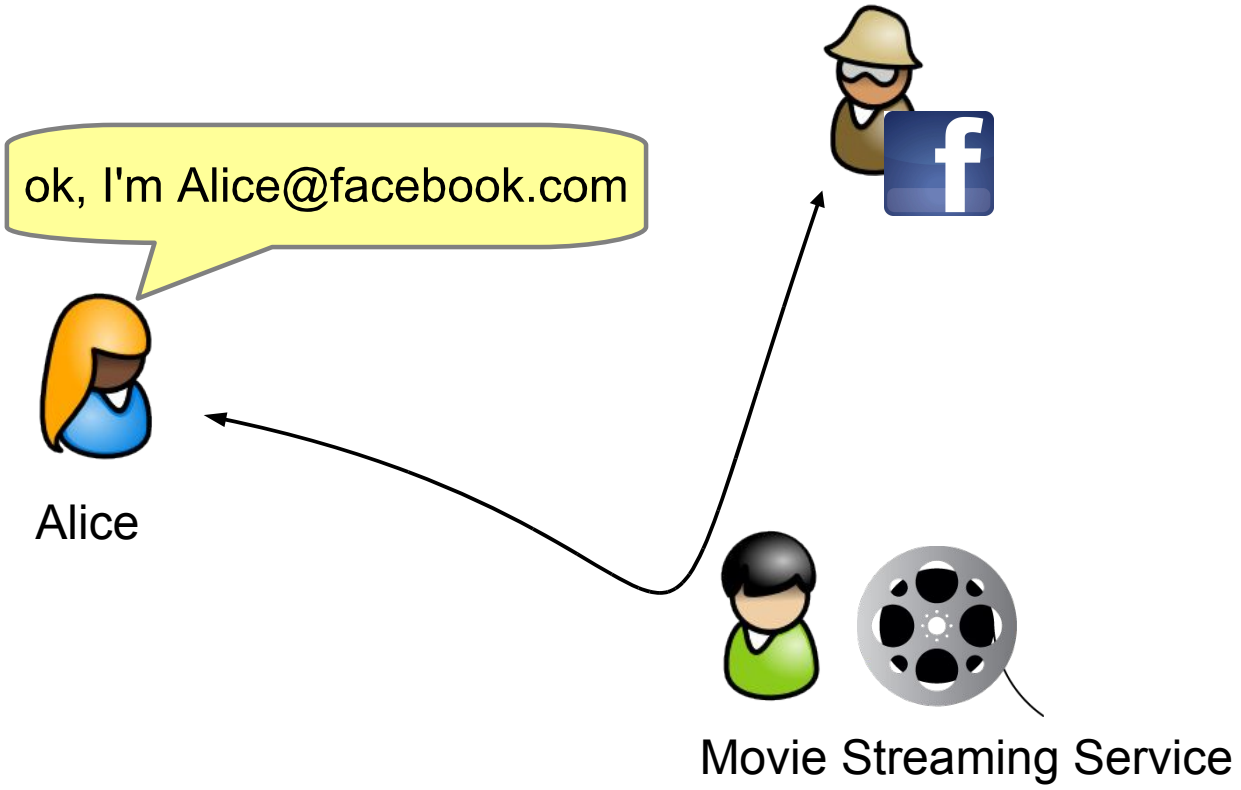
This is a privacy and security problem!

- identity theft
- profiling
- discrimination



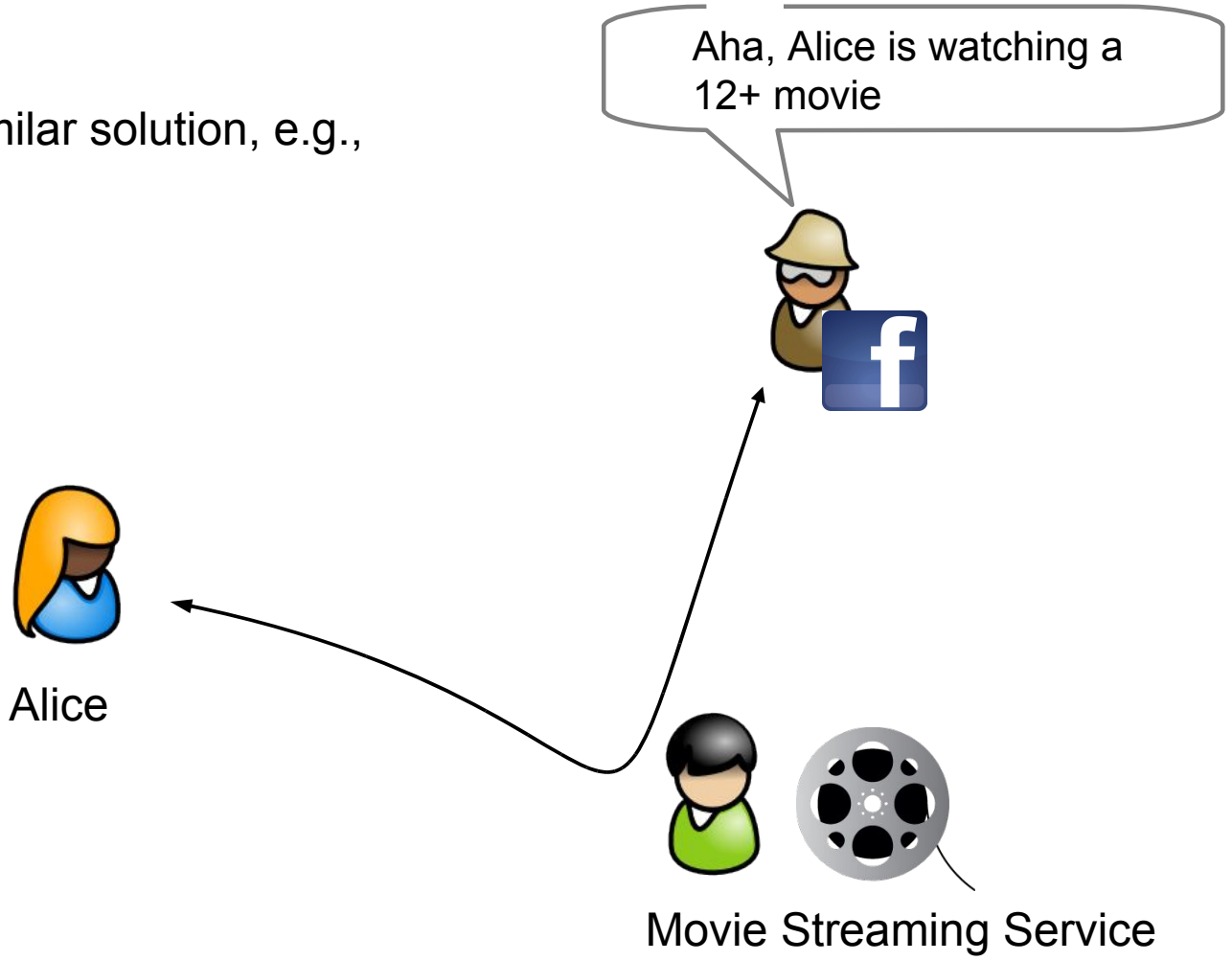
Watching the movie with the traditional solution

With OpenID and similar solution, e.g.,
log-in with Facebook



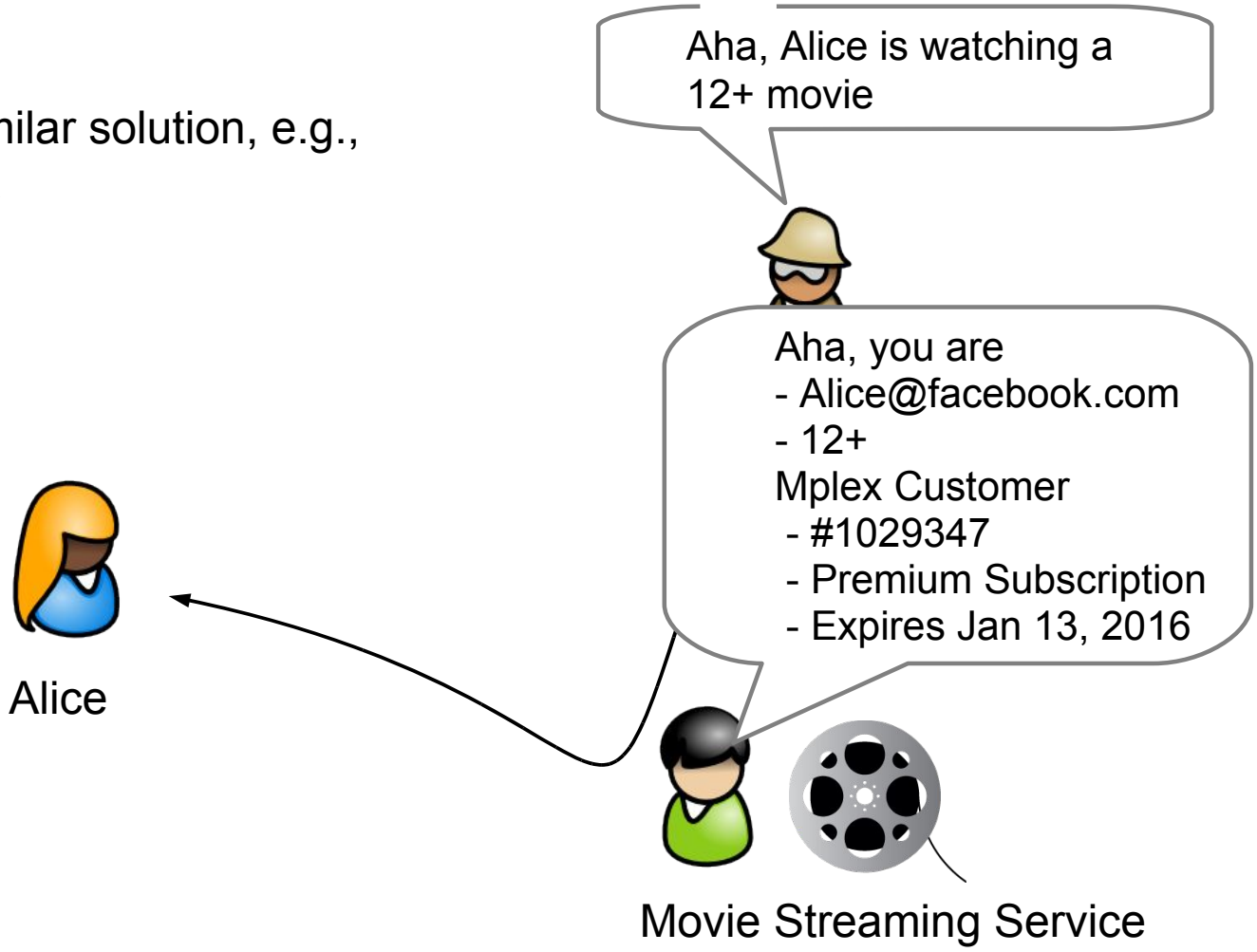
Watching the movie with the traditional solution

With OpenID and similar solution, e.g., log-in with Facebook



Watching the movie with the traditional solution

With OpenID and similar solution, e.g., log-in with Facebook



Identity Mixer (Privacy ABCs) solve this.

When Alice authenticates to the Movie Streaming Service with Identity Mixer, all the services learns is that Alice

has a subscription

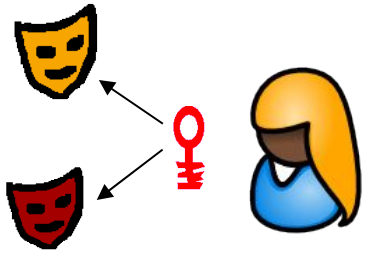
is older than 12

and no more!

Privacy-protecting authentication with Privacy ABCs

Like PKI, but better:

- One secret Identity (secret key)
- Many Public Pseudonyms (public keys)

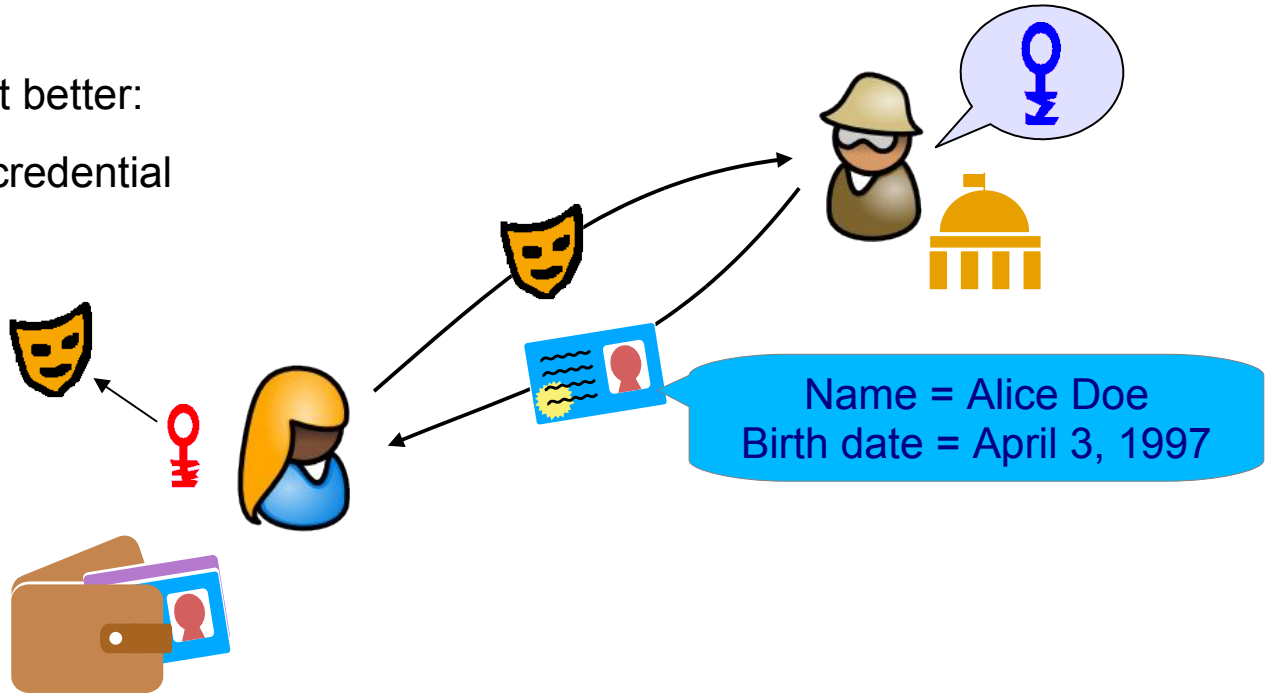


Concepts: Key binding & Pseudonyms

Privacy-protecting authentication with Privacy ABCs

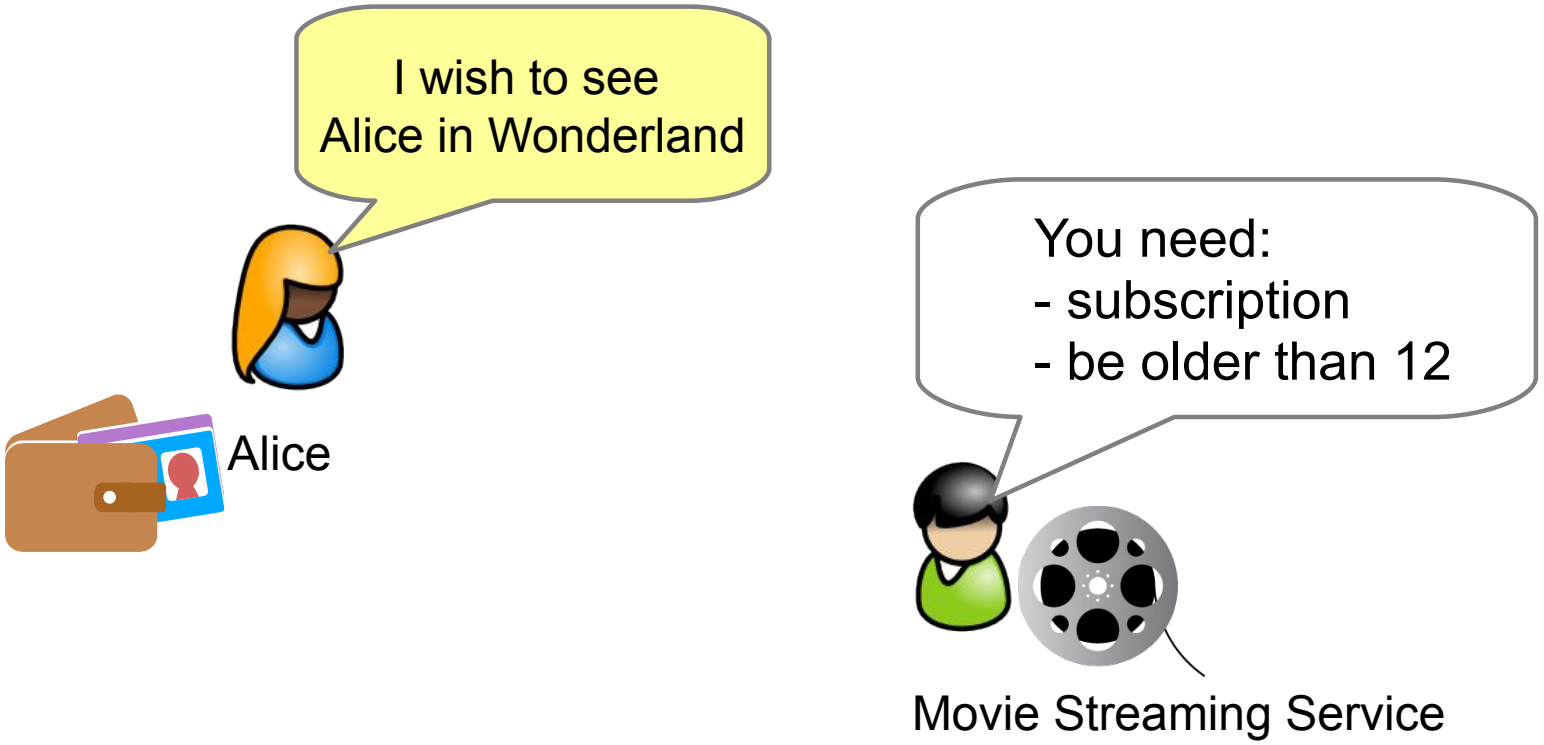
Like PKI, but better:

- Issuing a credential

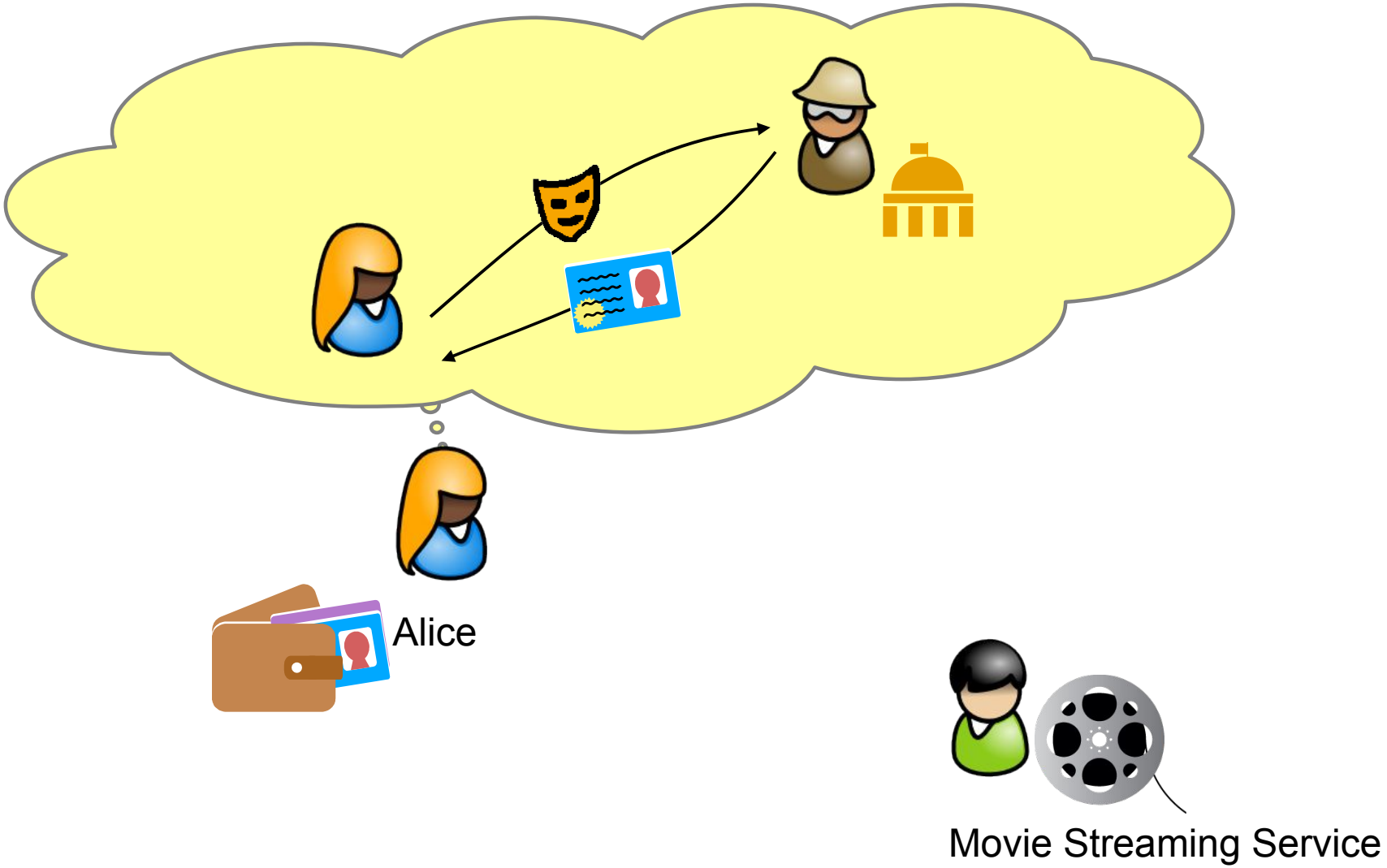


Concept: credentials

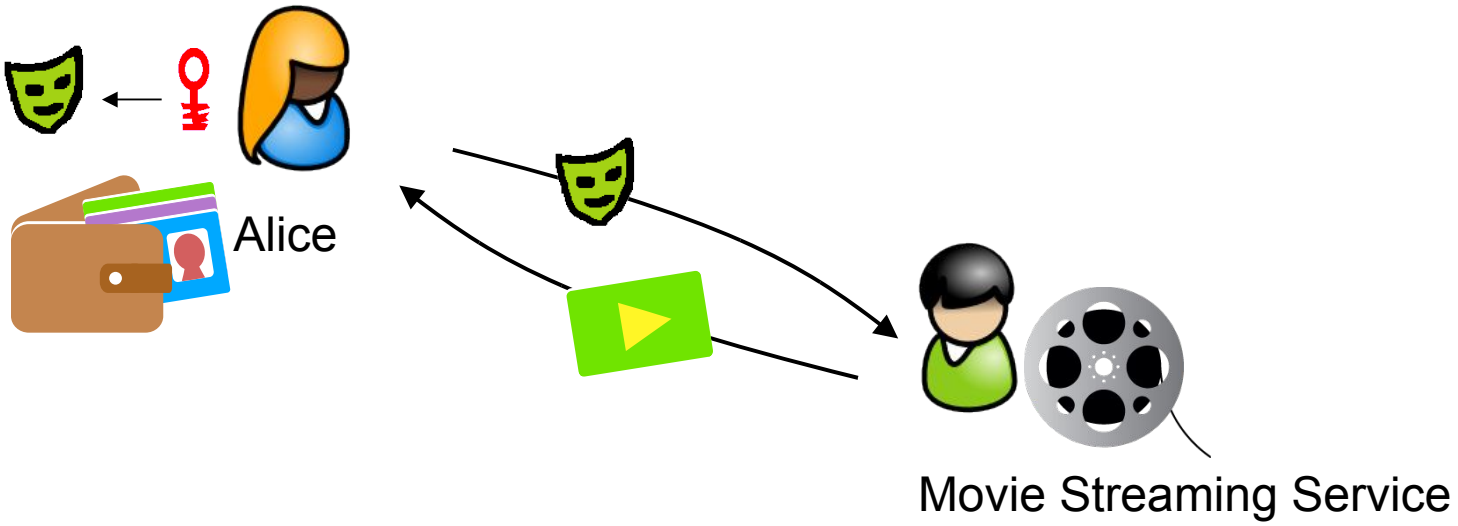
Privacy-protecting authentication with Privacy ABCs



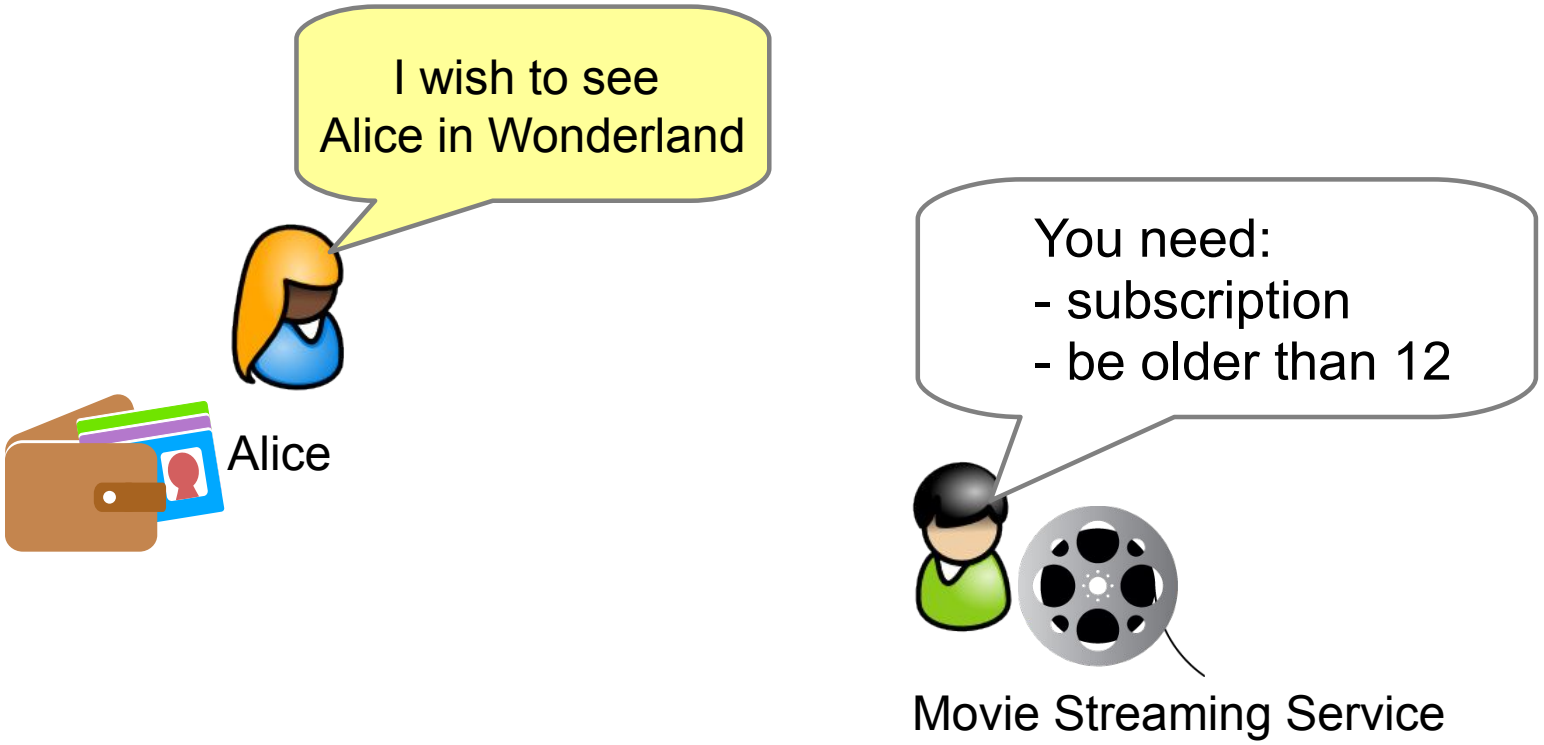
Privacy-protecting authentication with Privacy ABCs



Privacy-protecting authentication with Privacy ABCs



Privacy-protecting authentication with Privacy ABCs

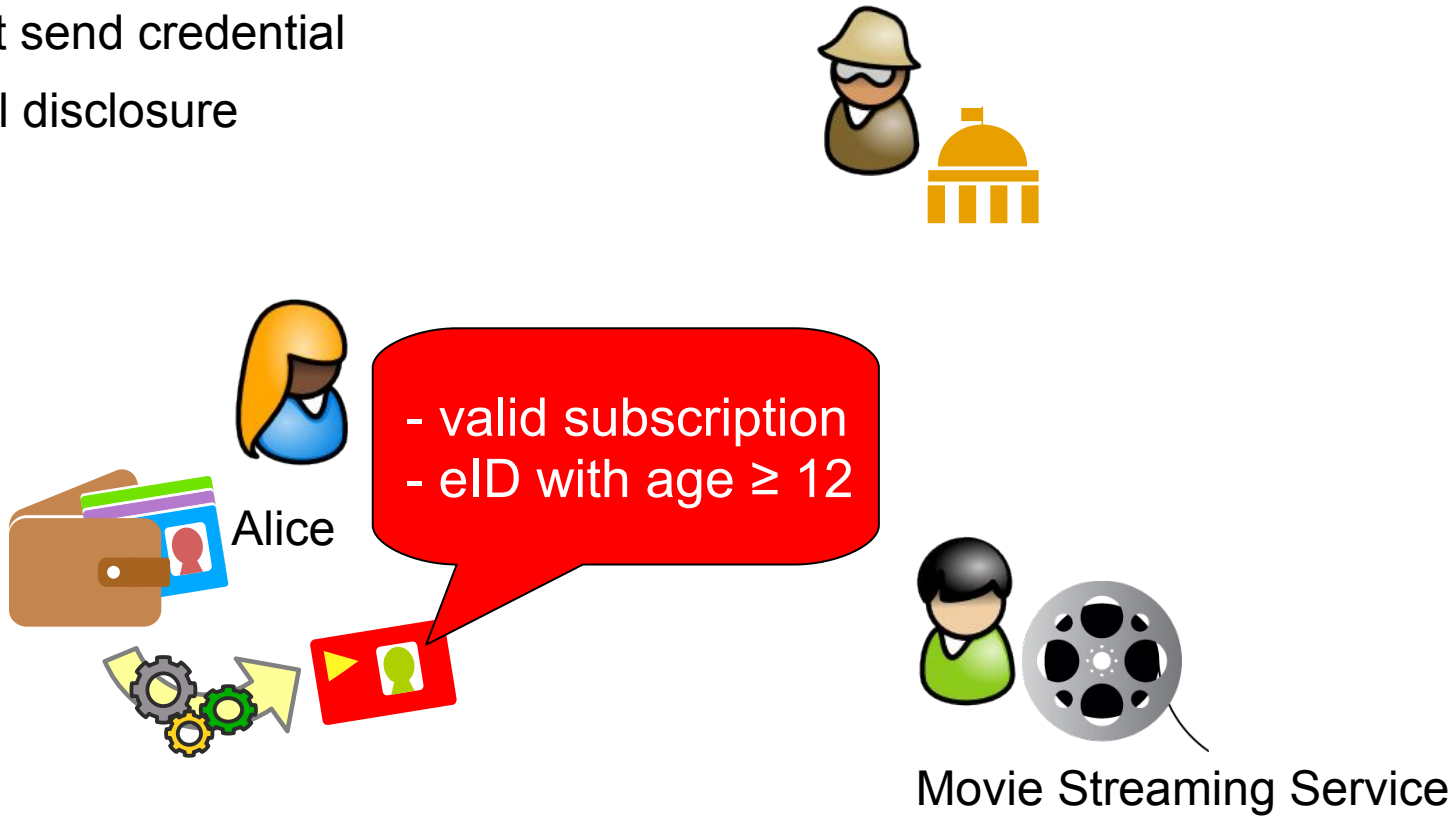


Concept: presentation policy

Privacy-protecting authentication with Privacy ABCs

Like PKI

- but does not send credential
- only minimal disclosure

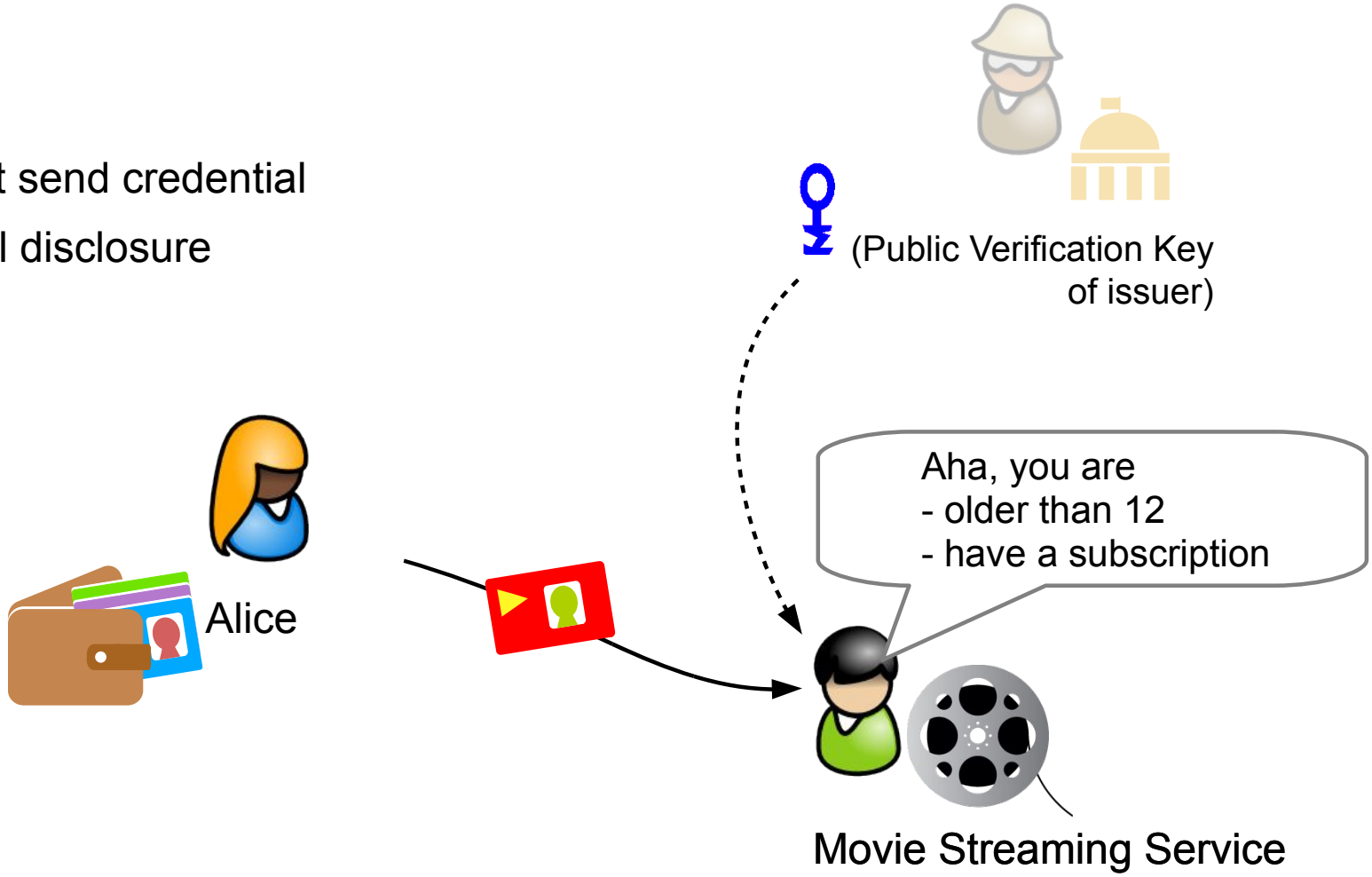


Concept: presentations token

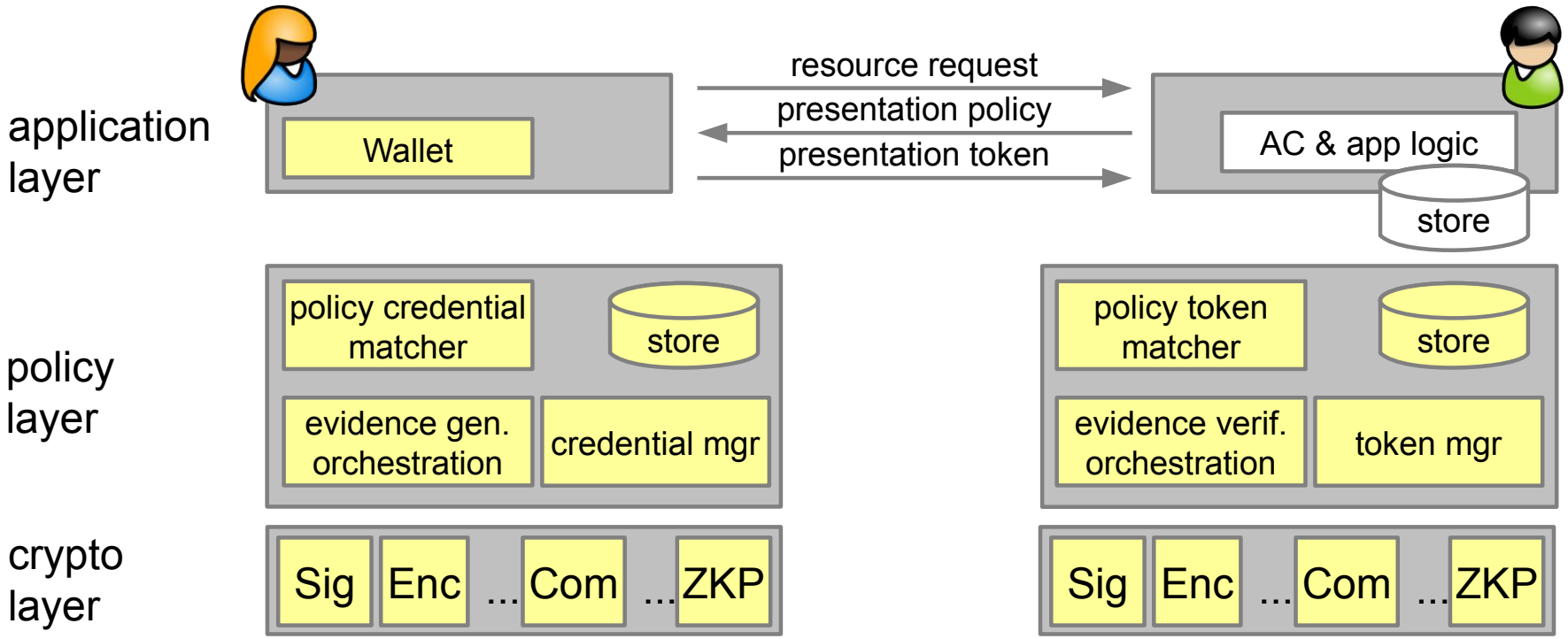
Privacy-protecting authentication with IBM Identity Mixer

Like PKI

- but does not send credential
- only minimal disclosure

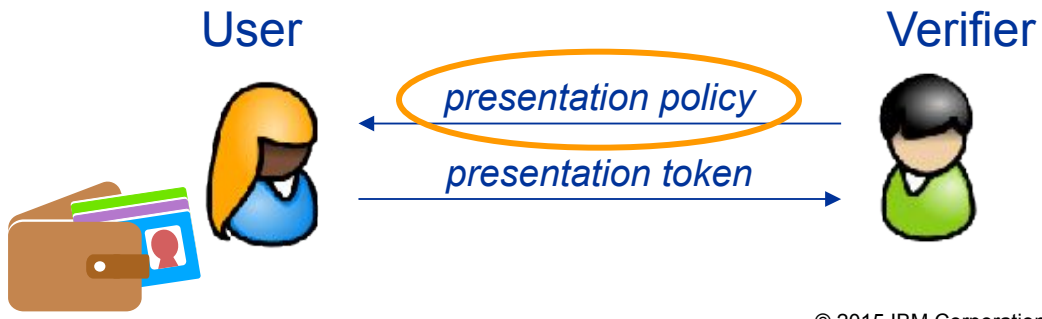


An Software Stack View on Identity Mixer

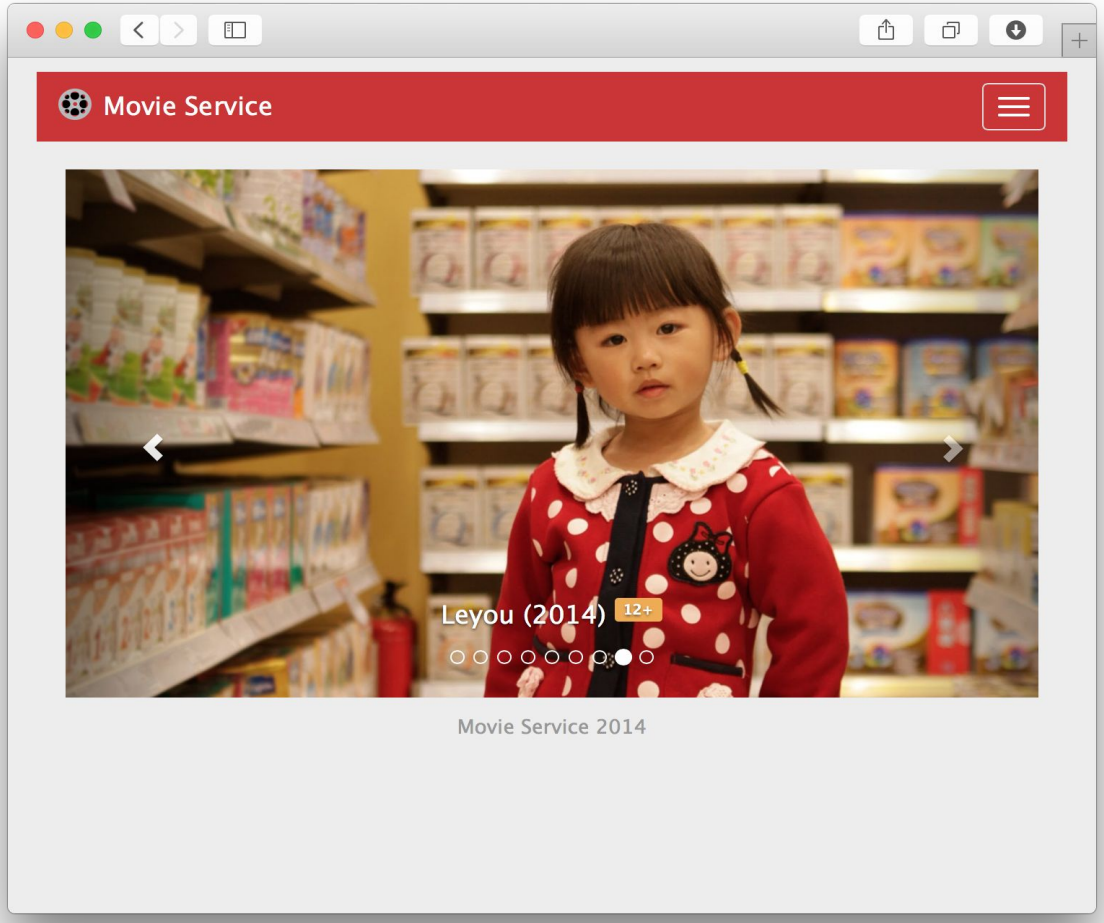


The Policy Layer – An Example: Presentation policy

```
<abc:PresentationPolicy PolicyUID="https://movies...com/presentationpolicies/movie1">

  <abc:Message>
   <abc:ApplicationData>  Terms and Conditions </abc:ApplicationData>
  </abc:Message>

  <abc:Credential Alias="#voucher">
   <abc:CredentialSpecAlternatives>
    <abc:CredentialSpecUID>https://movies.....com/specifications/voucher</abc:CredentialSpecUID>
   </abc:CredentialSpecAlternatives>
   <abc:IssuerAlternatives>
    <abc:IssuerParametersUID>https://movies....com/parameters/voucher</abc:IssuerParametersUID>
   </abc:IssuerAlternatives>
  </abc:Credential>

  <abc:AttributePredicate Function="urn:oasis:names:tc:xacml:1.0:function:dateTime-geq">
   <abc:Attribute CredentialAlias="#voucher" AttributeType="Expires" />
   <abc:ConstantValue>2014-06-17T14:06:00Z</abc:ConstantValue>
  </abc:AttributePredicate>

</abc:PresentationPolicy>
```



So, let's watch a movie!



idemixdemo.zurich.ibm.com
idemixdemo.mybluemix.net

Conclusions

- Idemix available for use
  - pilots done
  - code at github, also in IBM Bluemix as a service late spring
- Using IT *securely* still hard
  - Much of the technology exists, needs to get used and made usable
- Roadmap
  - Explain possibilities to engineers, policy makers, and end-user
  - Laws with teeth (encourage investment in privacy)
- Challenges
  - Internet services get paid with personal data (inverse incentive)
  - End users are not able to handle their data (user interfaces..)
  - Security technology typically invisible and hard to sell
- Towards a secure information society
  - Society changes quickly and gets shaped by technology
  - Consequences are hard to grasp yet (time will show...)
  - We must inform and engage in a dialog

Thank you!

- eMail: identity@zurich.ibm.com
- Links:
  - www.abc4trust.eu
  - www.futureID.eu
  - www.au2eu.eu
  - www.PrimeLife.eu
  - www.zurich.ibm.com/idemix
  - idemixdemo.zurich.ibm.com
- Code
  - github.com/p2abcengine & abc4trust.eu/idemix