Privacy and ID Management for Life

From ID Cards, Cell Phones to the Internet

Dr. Jan Camenisch
IBM Research
Technical Leader PrimeLife

November 27th, 2008
“The Internet will be everywhere, from every mote to interstellar communication”
“The Internet will be everywhere, from mote to interstellar communication.”

“We need both: sometimes we wanna be anonymous, sometimes we need to be identified.”

Vint Cerf
“The Internet will be everywhere, from mote to interstellar...at the same time!”

“We need both: sometimes we wanna be anonymous, sometimes we need to be identified”

“...at the same time!”
Not Just the Internet...

...even if it is going to be everywhere ;-)
Vision: *Privacy, Trust and ID Management*

In the Information Society, users can act and interact in a *safe and secure* way while *retaining* control of their private spheres.
What's the Problem?
“Neil Armstrong’s Footsteps are still there”

(Robin Wilton, Sun Microsystems)
Computers don’t forget

- Storage becomes ever cheaper
- Data mining ever better
So what do we need?

Privacy Built-In Everywhere!

- Network Layer Anonymity
  - ... in mobile phone networks
  - ... in the Future Internet as currently discussed
  - ... access points for ID cards

- Identification Layer
  - Access control & authorization

- Application Layer
  - “Standard” e-Commerce
  - Specific Apps, e.g., eVoting, ...
  - Web 2.0, e.g., Facebook & Wikis
So what do we need?

Privacy Built-In Everywhere!
- Network Layer Anonymity
  - ... in mobile phone networks
  - ... in the Future Internet as currently discussed
  - ... access points for ID cards
- Identification Layer
  - Access control & authorization
- Application Layer
  - "Standard" e-Commerce
  - Specific Apps, e.g., eVoting, ...
  - Web 2.0, e.g., Facebook & Wikis
Privacy @ ID Layer
A Closer Look & Solutions
Digital Credentials

Driver's License
Insurance
Dangerous Cars
Solution: Private Digital Credentials
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.

containing statements “driver's license, age (as stated in driver's ) > 20, and insurance”
Other Properties: Attribute Escrow (Opt-In)

- If car is broken: ID with insurance needs be retrieved
- Can verifiably encrypt any certified attribute *(optional)*
- TTP is off-line & can be distributed to lessen trust
Other Properties: Revocation

• If Alice was speeding, license needs to be revoked!
• There are many different use cases and many solutions
  • Variants of CRL work (using crypto to maintain anonymity)
  • Limited validity – certs need to be updated
  • ... For proving age, a revoked driver's license still works
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)
This is not just a dream!
This is not just a dream!

Cryptography can do all of this and more
This is not just a dream!

Cryptography can do all of this and more

.... efficiently
This is not just a dream!

Cryptography can do all of this and more

.... efficiently

.... even on a smart card  :-(
What Else's Left to Do?

Prime Life
Realizing Privacy

Make privacy-enhancing identity management widely available:
- Infrastructures, Open Source, and Standards
- Cooperation with other Projects (Master, PICOS, TAS3, SWIFT, ... ),
- Education (summer schools, educational materials, ...)

Research focus on main remaining issues:
- HCI, Policies, and Infrastructures (and some mechanisms)

Basic Research: Beyond data minimization:
- Address data-intensive scenarios and user-generated content (Web 2.0, virtual communities such as FaceBook, SecondLife)
- Trust building and Enforceable data protection (end-to-end policies)
- Real life privacy (and throughout life)
Let's Make it Real!

info@primelife.eu
www.primelife.eu
(www.prime-project.eu)