Privacy
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
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

Data Subject

Collection
- Surveillance
- Interrogation

Invasions
- Intrusion
- Decisional interference

Data Holders

Processing
- Aggregation
- Identification
- Insecurity
- Secondary Use
- Exclusion

Dissemination
- Confidentiality breach
- Disclosure
- Exposure
- Increased accessibility
- Blackmail
- Appropriation
- Distortion

From Daniel J. Solove, Understanding Privacy
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

- Mechanisms
- HCI
- Policies
- Infrastructures
- Privacy In Life
- Privacy Live!
Scenario
PrimeLife's approach
PrimeLife's approach

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

(Anonymous Communication)
PrimeLife's approach

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

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

(Anonymous Communication)
PrimeLife's Approach

User

Server

1. Request for resource
2. Applicable policy
3. Proof, p-descr., data
4. Authorization decision

- Credentials
- User Interface, Heuristics
- Proof generation

- Policies
- Resources

- Description verification
- Proof verification
- Data storage
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"

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.
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
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
Trusted 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

Key Point
Transforms certificates in privacy-preserving identity proof statements

User

interacts/consents to policy

User PC

Browser

Identity Wallet

request: policy/response: proof

Identity Mixer Validation

$pk_i$

Validates proofs with issuer’s public key

$sk_U$

Maintains master key and certificates confidential

Smarter ID Card

Secure Javacard

certificates

request: policy/response: proof

Backend (Server)
Sustainable identity & privacy 'for life'

Privacy

PrimeLife

Technology

Important & complex challenge

Crypto to rescue: efficient on any device

Privacy PrimeLife Technology
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

http://idemix.wordpress.com/