Smarter Identity Cards
with Identity Mixer

Thomas Gross
Computer Science Department
IBM Research, Zurich Lab
Identity: The Trust/Privacy Dilemma

Traditional PKI

- PKI-based authentication
- User uniquely identified

User-centric Identity

- Identity Provider (IDP)
- IDP-certified claim values
- Disclosure of raw identity data

Anonymous Login

- Purely anonymous login
- No trust basis. Accountability?

Privacy?

Service Provider

Tracing

Profiling

Attribute Theft

Account Sharing

Misuse

Trust?
Introducing IDMX Smarter Identity Cards: Design Goals

- **Guarantee strong accountability and privacy at the same time.**
  - Solve the trust/privacy dilemma.

- **Enable sustainable secondary use of identities.**
  - Over the whole identity lifecycle by various partners without trust erosion.
  - Enable prosperous business models in identity usage with network effect.

- **Be a trusted identity basis.**
  - The identity system is autonomous on a secure Javacard and does not trust the terminal.
  - The user’s master key is retained confidential in all transactions.

- **Be future-proof.**
  - Secure key strength.
  - Versatile policies specify transactions and anticipate future business models.

- **Be cost effective.**
  - Standard Javacard used.
  - Reduced issuer workload and operational risk.
Introducing IDMX Smarter Identity Cards: How it works

- **User** interacts/consents to policy
  - **Browser**
    - **Identity Wallet**
    - **Smarter ID Card Identity Mixer**
      - Maintains master key and certificates confidential
      - Secure JavaCard
      - Key Point: Transforms certificates in privacy-preserving identity proof statements
    - **Identity Mixer Validation**
      - Validates proofs with issuer's public key
  - **Backend (Server)**
    - request: policy/response: proof
- **User PC**
  - inserts/owns
Questions?

Thomas Gross (tgr@zurich.ibm.com)
+41 44 724 8307

Smarter Identity Cards with Identity Mixer

www.zurich.ibm.com/security/idemix
identity@zurich.ibm.com