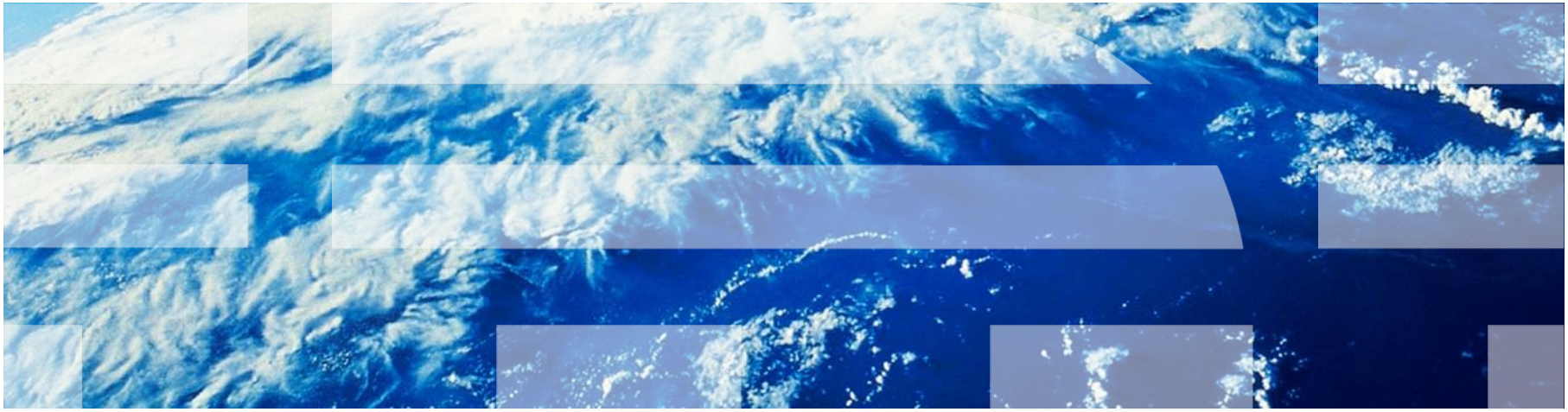
IBM

# Anonymous Credentials on Java Card

Patrik Bichsel, Jan Camenisch, Thomas Groß, Victor Shoup



# Privacy

# Feasibility

# Way Ahead

[Images from iStockPhoto.com]

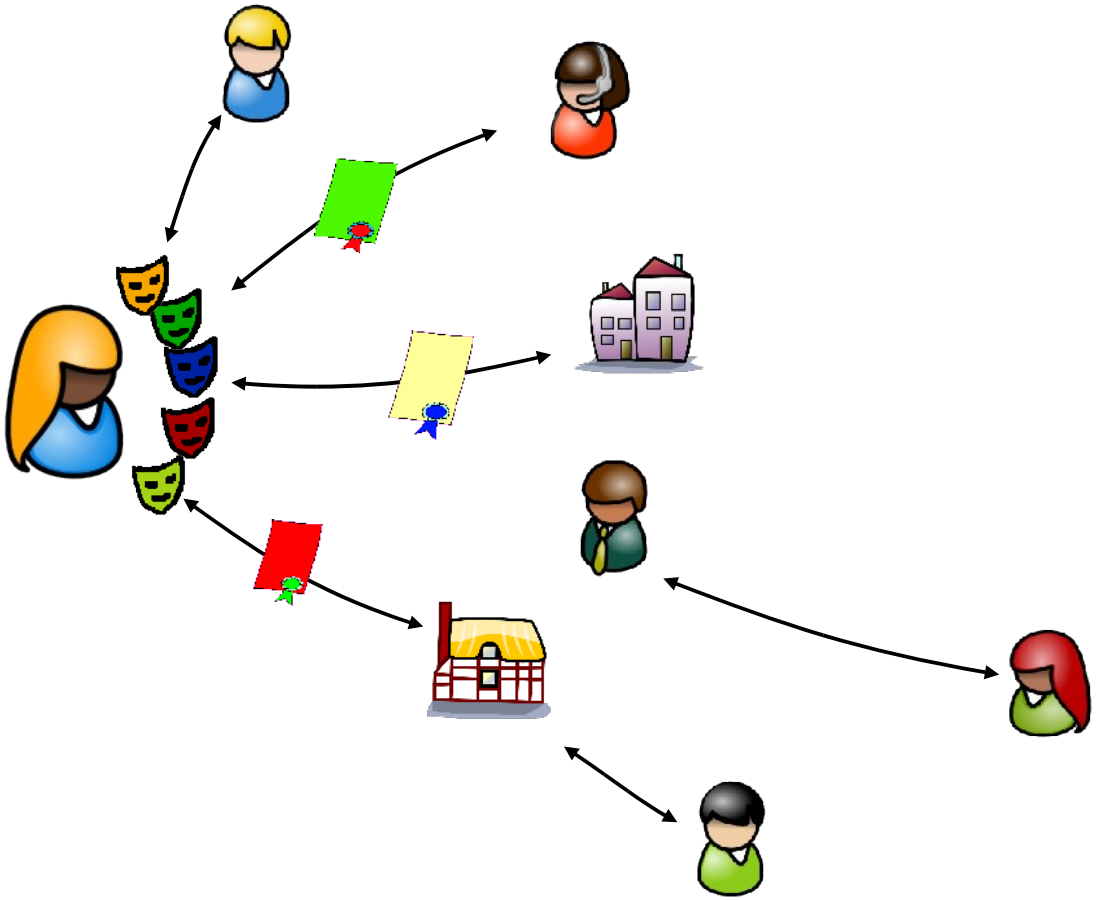
Privacy

Feasibility

Way Ahead

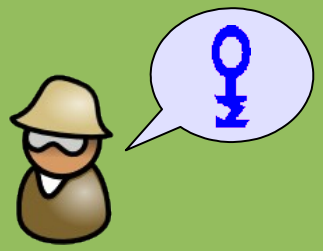

*“Neil Armstrong’s Footsteps are still there”*
(Robin Wilton, Sun Microsystems)
2

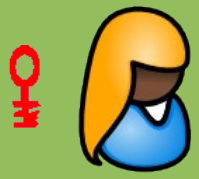
# Anonymous Credentials:
## Attribute-based Access w/ Strong Security & Privacy



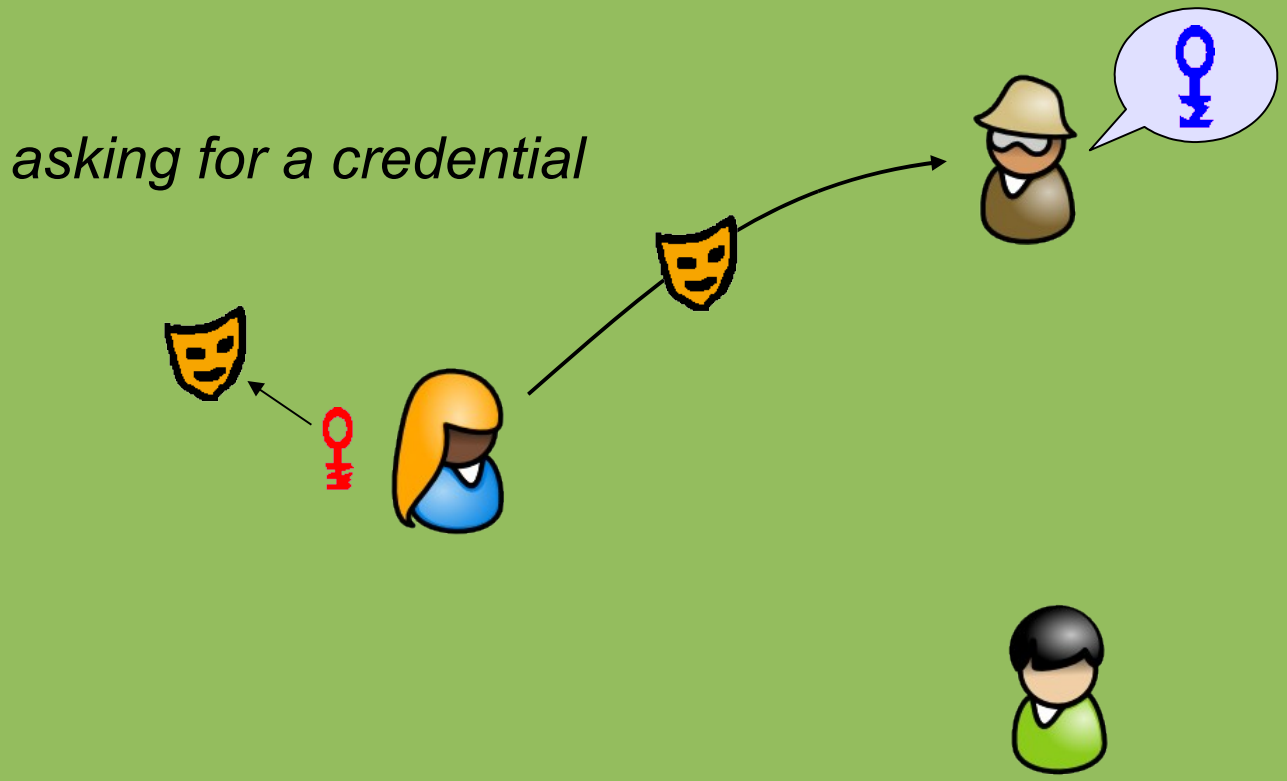
# Private Credentials: How to Build Them

*In the beginning...*

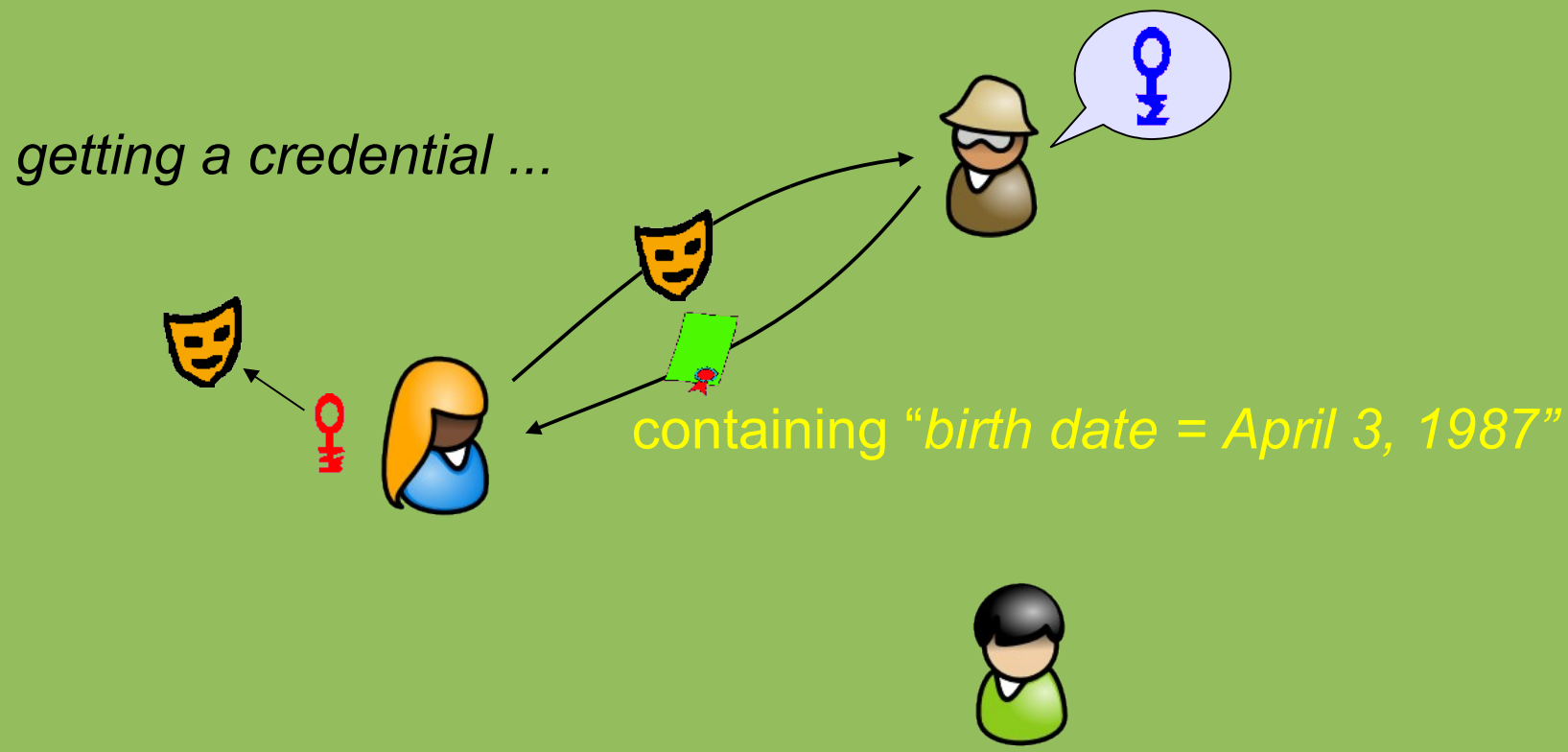




# State of the Art: How to Build Them

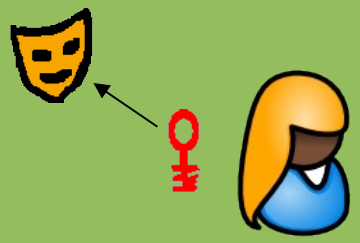


# State of the Art: How to Build Them

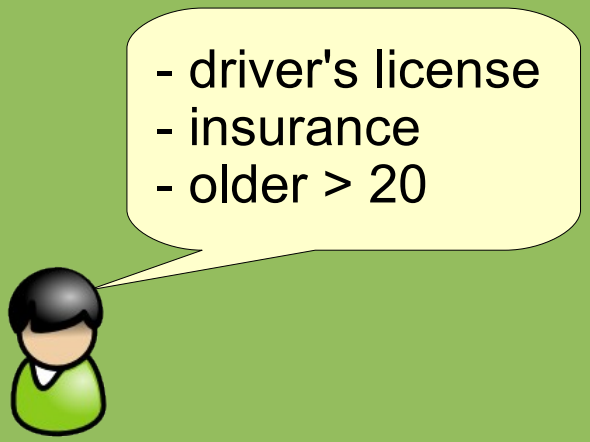


# State of the Art: How to Build Them

*showing a credential ...*

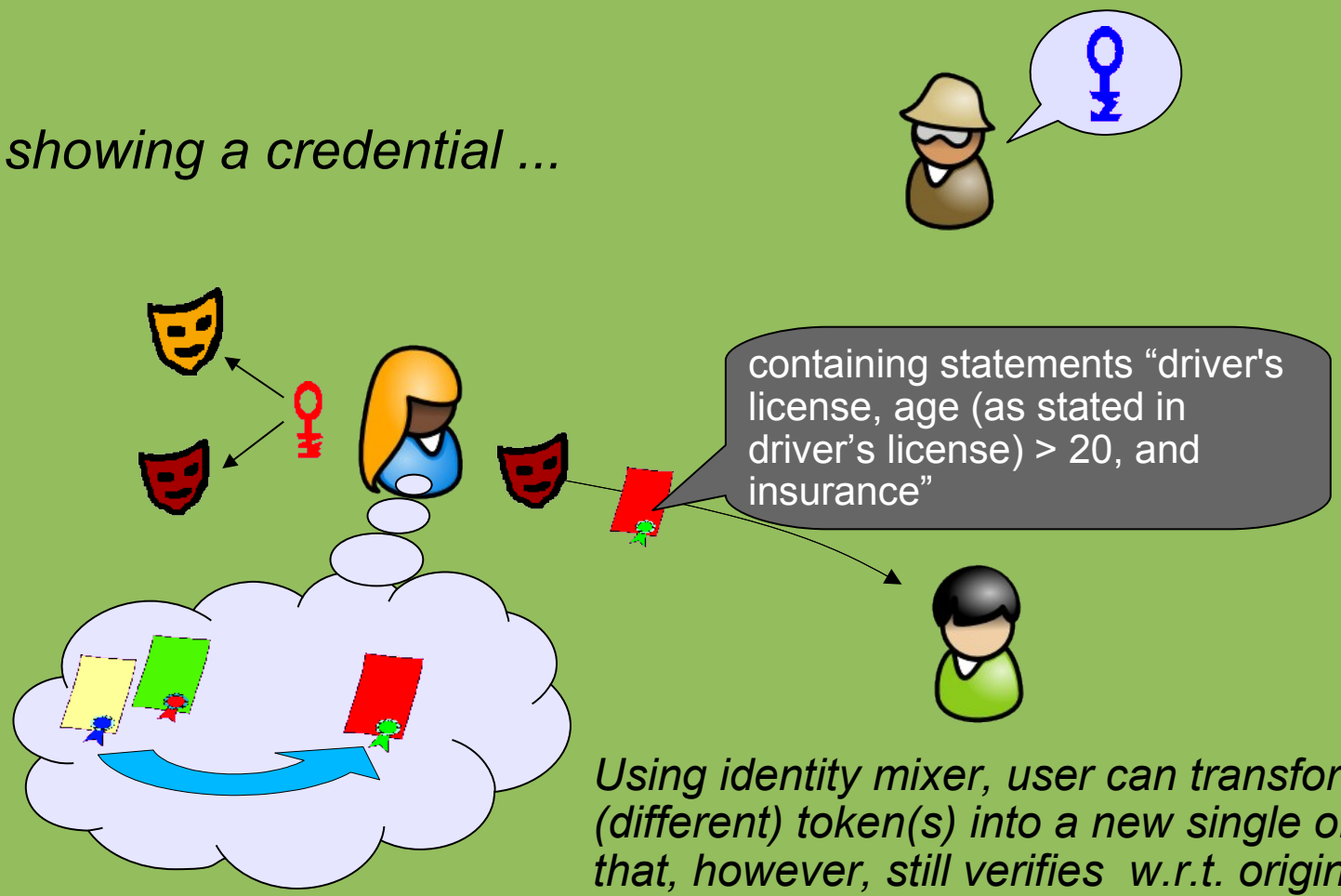


goes off-line



# 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.*

# Signature Scheme based on SRSA [CL01]

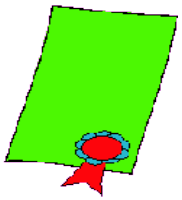
Public key of signer: RSA modulus $n$ and $a_i, b, d \in QR_n$

Secret key: factors of $n$

To sign $k$ messages $m1, \ldots, mk \in \{0,1\}^{\ell}$ :

- choose random prime $e > 2^{\ell}$ and integer $s \approx n$
- compute $c$ such that

$$d = a_1^{m1} \cdot \ldots \cdot a_k^{mk} \; b^s \; c^e \mod n$$



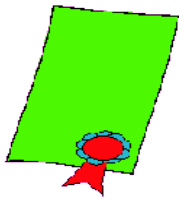
- signature is $(c,e,s)$

[SRSA CL-signature system introduced in Camenisch and Lysyanskaya '01. There exist alternative systems in elliptic curve settings, for instance with BBS-alike signatures.]

# Signature Scheme based on SRSA [CL01]

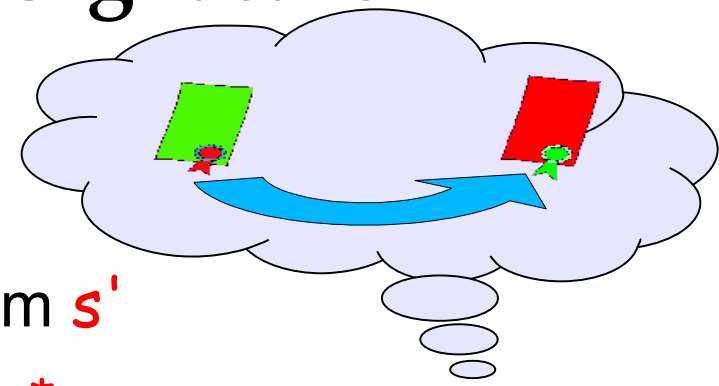
A signature $(c,e,s)$ on messages $m1, \ldots, mk$ is valid iff:

- $m1, \ldots, mk \in \{0,1\}^{\ell}$:
- $e > 2^{\ell}$
- $d = a_1^{m1} \cdot \ldots \cdot a_k^{mk} \; b^s \; c^e \mod n$



Theorem: *Signature scheme is secure against adaptively chosen message attacks under Strong RSA assumption.*

# Proof of Knowledge of a CL Signature



Solution randomize $c$ :

- Let $c' = c\, b^{s'} \bmod n$ with random $s'$
- then $d = c'^{e}\, a_1^{m1} \cdot \ldots \cdot a_k^{mk}\, b^{s^*} \pmod n$ holds,

  i.e., $(c', e, s^*)$ is a also a valid signature!

Therefore, to prove knowledge of signature on hidden msgs:

- provide $c'$
- $PK\{(e, m1, \ldots, mk, s) : \quad d = c'^{e}\, a_1^{m1} \cdot \ldots \cdot a_k^{mk}\, b^{s}$

$$\wedge\ mi \in \{0,1\}^{\ell} \quad \wedge\ e \in 2^{\ell+1} \pm \{0,1\}^{\ell} \quad \}$$

Privacy

Feasibility

Way Ahead

# Vision: Smart Identity Card

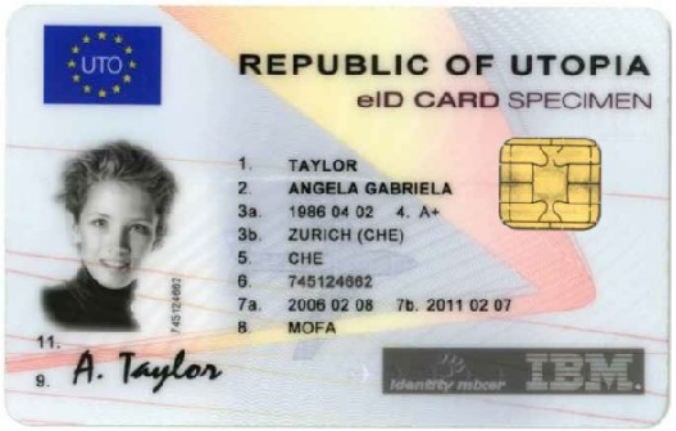
**Strong accountability and privacy**

**Sustainable secondary use**

**Trusted identity basis**

**Cost effective**

**Future-proof**




[Card picture is an artists conception: the chip of the actual JCOP 41/v.2.2 Java Card used for the feasibility study is on the backside.]

# Feasibility Problem

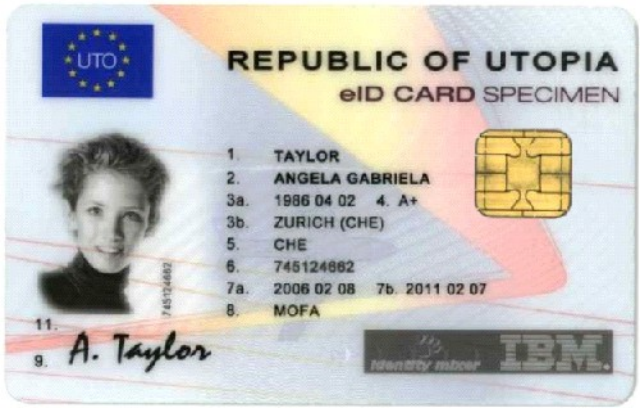
[**Independent proof point:**
Sterckx, Gierlichs, Preneel, Verbauwhede '09]

**Run anonymous credential system autonomously and securely on a standard off-the-shelf Java Card.**

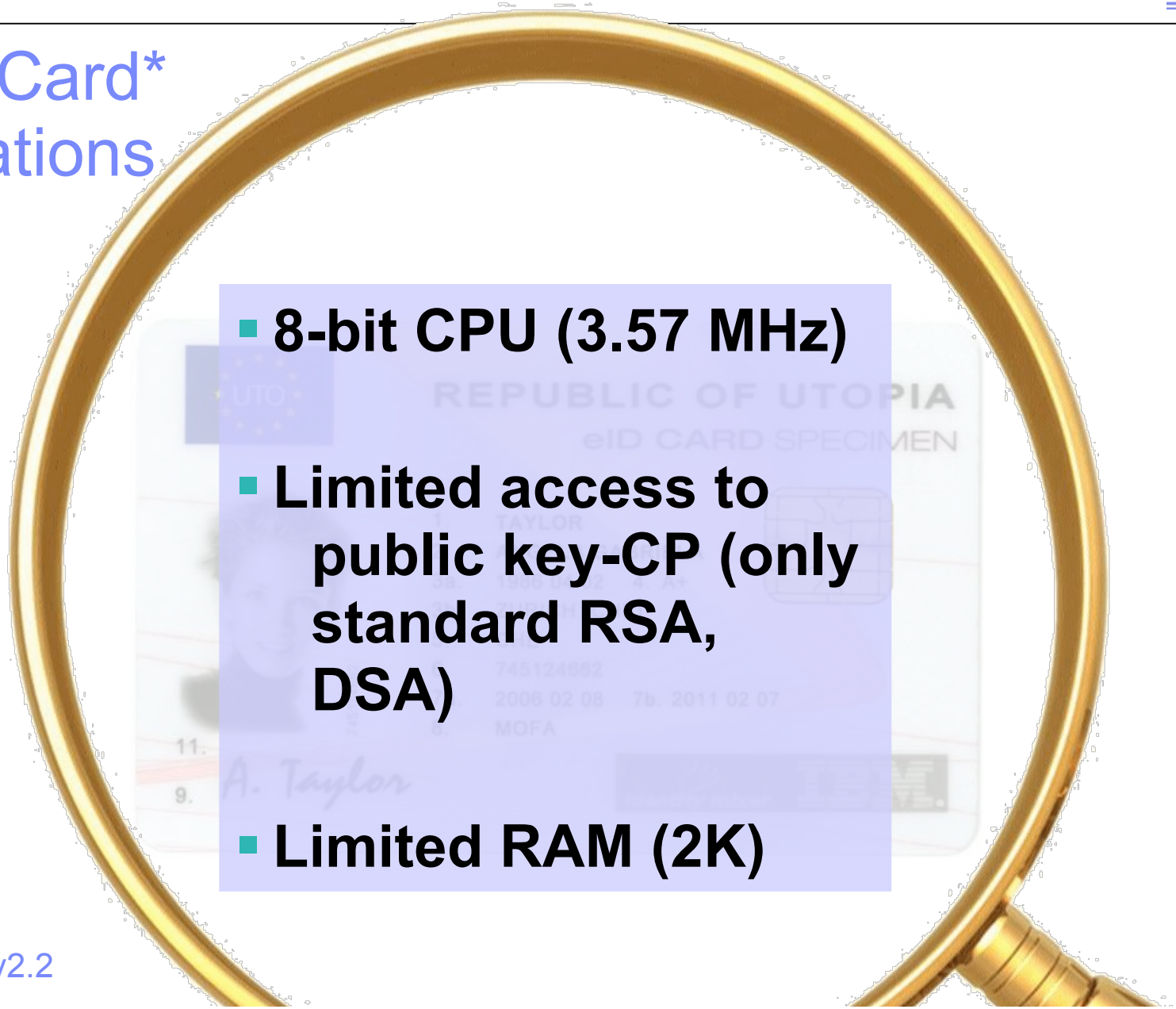
**Autonomy**
**All data on card**
**Malicious terminal**

**Security**
**CL-Signatures**
**Realistic keys**

**Efficiency**
**Proof in seconds**



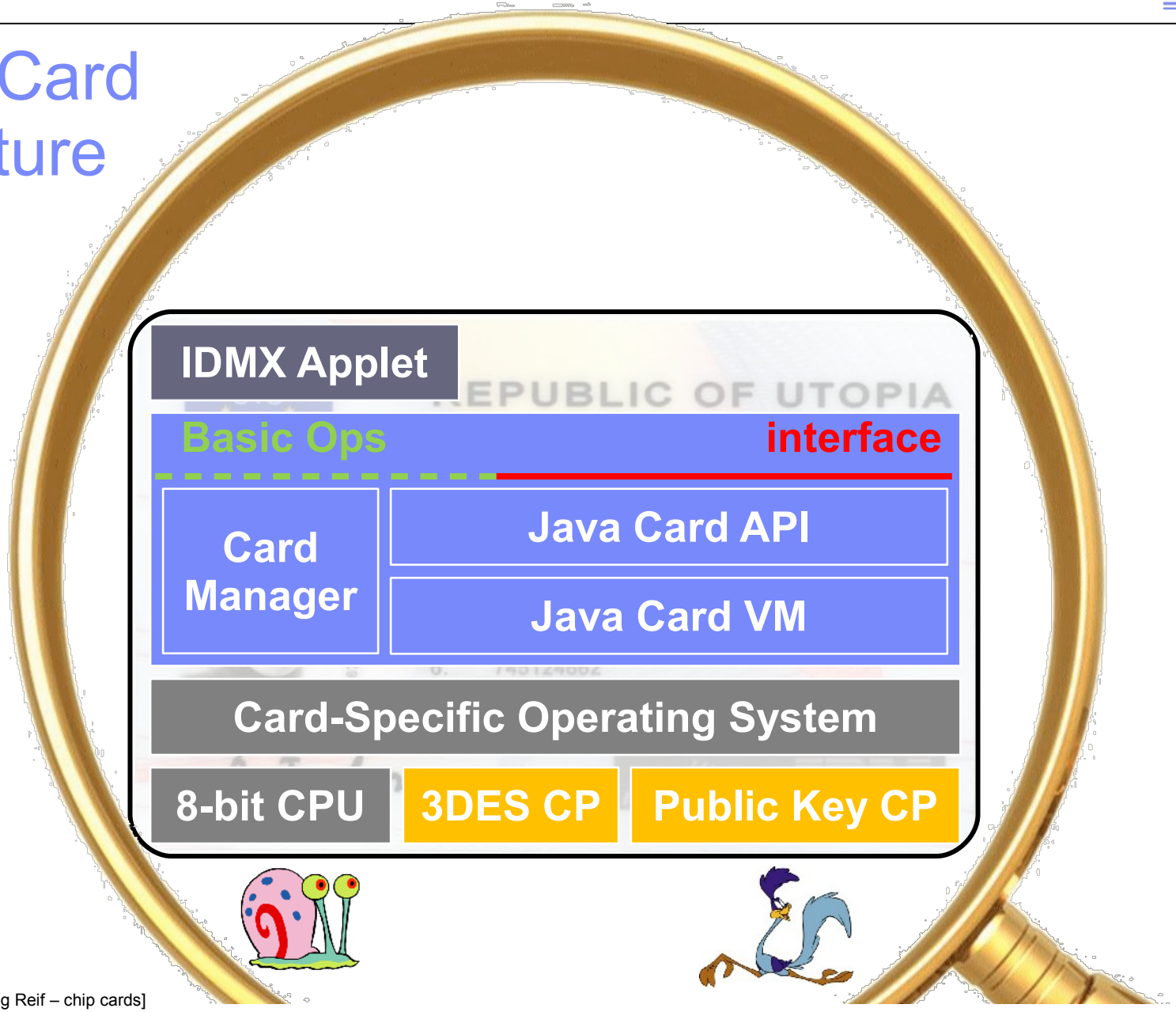
# Java Card* Limitations



- 8-bit CPU (3.57 MHz)
- Limited access to public key-CP (only standard RSA, DSA)
- Limited RAM (2K)

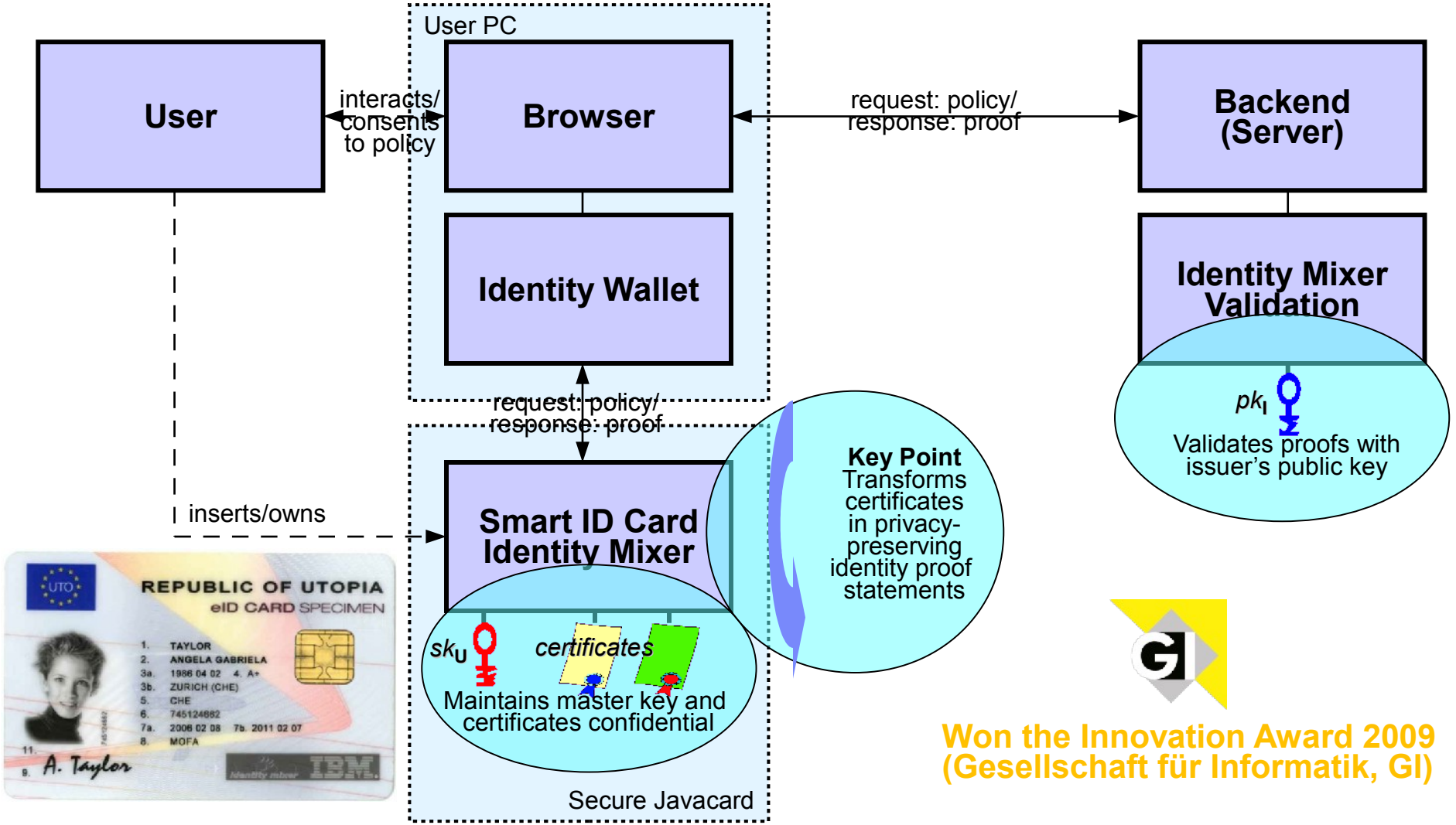
*: JCOP 41/v2.2

# Java Card Structure




[Source: Prof. Wolfgang Reif – chip cards]

# System Overview




**Won the Innovation Award 2009 (Gesellschaft für Informatik, GI)**

# Execution Times for a Full Proof (incl. Communication)

| Modulus | 1280 bit | 1536 bit | 1984 bit |
|---|---|---|---|
| **Precomputation** | **5203 ms** | **7828 ms** | **13250 ms** |
| Compute A’ | 2125 ms | 2906 ms | 5000 ms |
| Compute T1 | 3078 ms | 4922 ms | 8250 ms |
| | | | |
| **Policy-dependent** | **2234 ms** | **2625 ms** | **3298 ms** |
| Compute 1 response | 562 ms | 656 ms | 828 ms |
| | | | |
| **Total** | **7437 ms** | **10453 ms** | **16548 ms** |

[Avg. performance measurements with 100 experiments on JCOP 41/v2.2. A': credential blinding, T1: first stage of Sigma-proof commitment, response: Sigma-proof response]

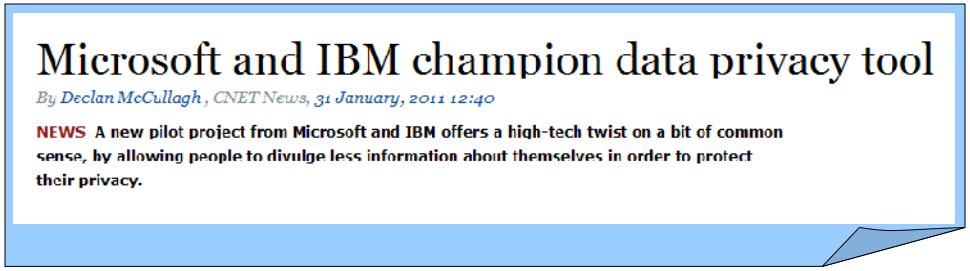
Privacy

Technology

Way Ahead

# Just Launched ABC4Trust Project

- EU FP 7 research project
- 13.5 Million EUR, 4 years


Microsoft and IBM champion data privacy tool

By Declan McCullagh, CNET News, 31 January, 2011 12:40

NEWS A new pilot project from Microsoft and IBM offers a high-tech twist on a bit of common sense, by allowing people to divulge less information about themselves in order to protect their privacy.

- **12 partners**
  - •Goethe University Frankfurt
  - •Alexandra Institute
  - •Research Academic Computer Technology Institute
  - •IBM Research
  - •Lenio
  - •Nokia Siemens Networks
  - •Unabhängiges Landeszentrum für Datenschutz
  - •Eurodocs
  - •CryptoExperts (SmartCards)
  - •Microsoft R&D France
  - •Municipality of Söderhamn
  - •Technische Universität Darmstadt

# ABC4Trust Goals

**Achieve paradigm shift and interoperability in trustworthy infrastructures**

- Establish abstraction and unification of different crypto algorithms.
- Create interaction flows, architecture & data formats as well as policies.
- Realize reference implementation.
- Validate concepts by real-world pilots in the eID space.

- Establish NG smart card implementation of anonymous credentials.
  - Realization by CryptoExperts, lead by Pascal Paillier.
  - Native SmartCard, direct access to crypto co-processor.

## Privacy

Anonymous credentials: future-proof solution to minimal disclosure and attribute authentication

## Feasibility

Technology feasible and practical: efficiently realizable on smart cards

## Way Ahead

Anonymous credential systems to be harmonized, integrated into identity management systems

# Resources

- This talk is based on P. Bichsel, J. Camenisch, T. Gross, V. Shoup. Anonymous Credentials on a Standard Java Card. ACM CCS 2009. Prof. V. Shoup is affiliated with the New York University and contributed to this work during a sabbatical at IBM Research – Zurich.

- **Identity Mixer Community: idemix.wordpress.com**
  - Download Identity Mixer Library 2.3.2
  - Read Identity Mixer Specification 2.3.2
  - http://prime.inf.tu-dresden.de/idemix/

- **PrimeLife:** www.primelife.eu
- **ABC4Trust:** www.abc4trust.de

- **Email Jan or Thomas:** {jca, tgr}[at]zurich.ibm.com