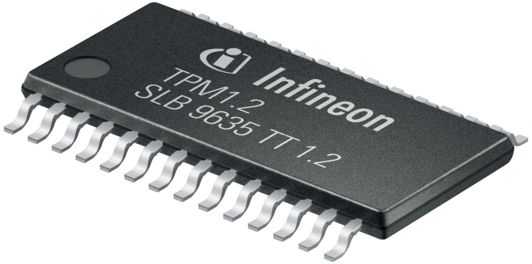
Authentication w/out Identification

Dr. Jan Camenisch

Principle RSM; Member, IBM Academy of Technology
Fellow IEEE, Fellow IACR
IBM Research – Zurich

@JanCamenisch
ibm.biz/jancamenisch



Facts

33% of cyber crimes, including identity theft, take less time than to make a cup of tea.

Facts

10 Years ago, your identity information on the black market was worth $150. Today….

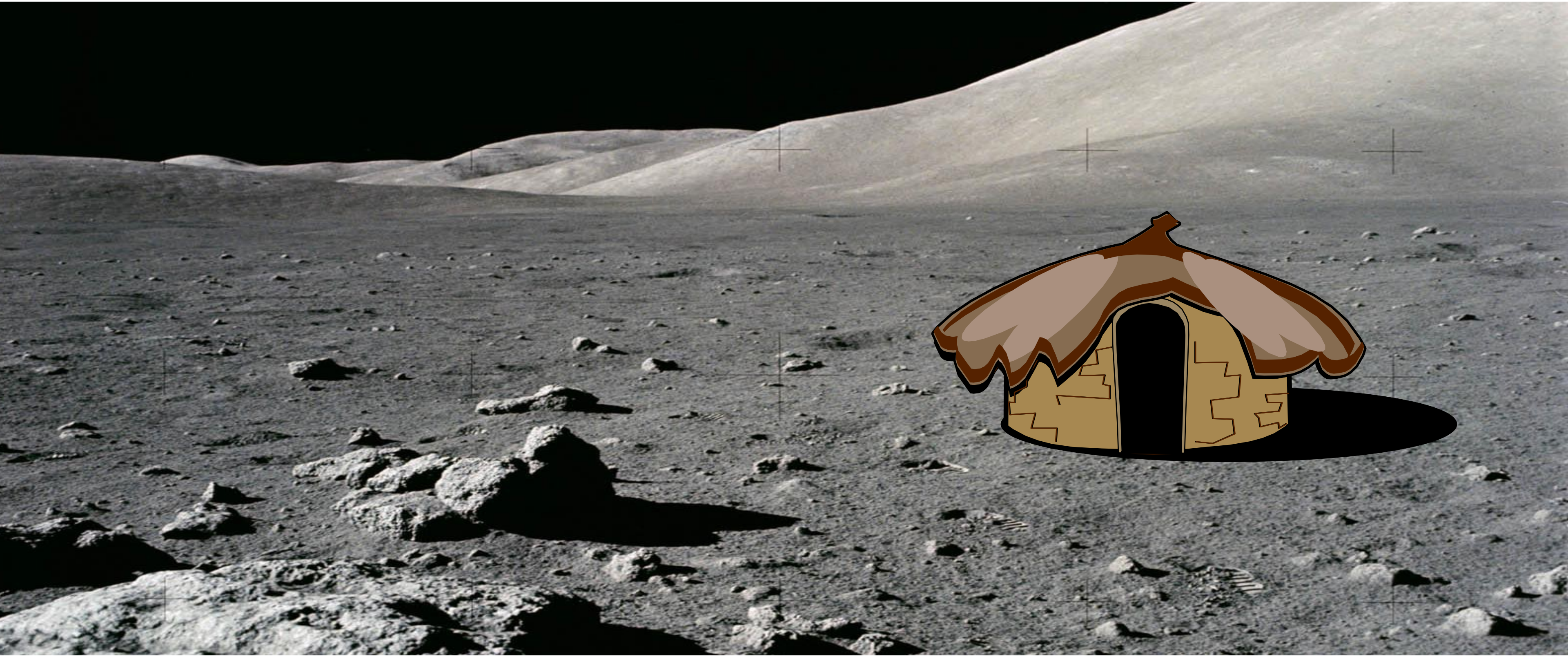
Facts

$15'000'000'000 cost of identity theft worldwide (2015)

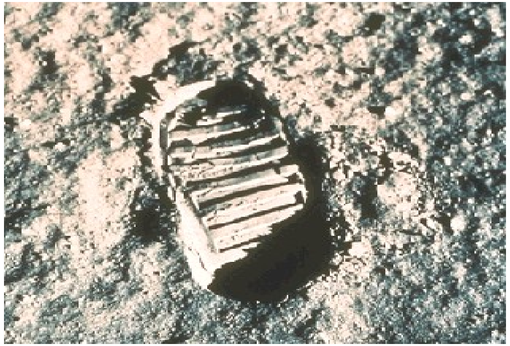
Attackers hide easily in the vast of cyberspace

Houston, we have a problem!

The problem is this…



…computers never forget



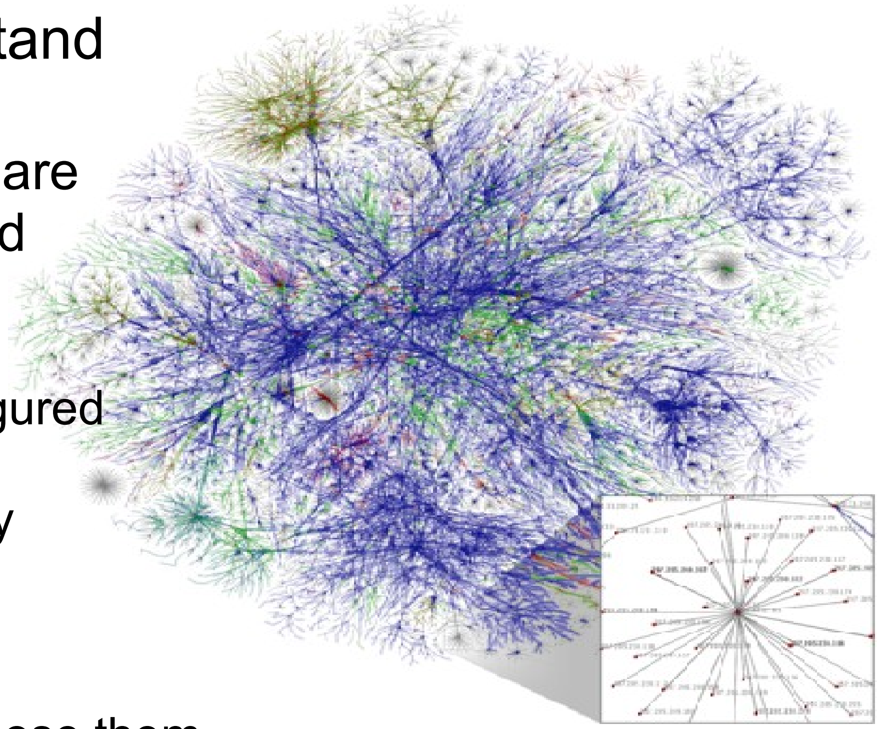
- Data is stored by default
- Data mining gets ever better
- Apps built to use & generate (too much) data
- New (ways of) businesses using personal data

- Humans forget most things too quickly
- Paper collects dust in drawers
- But that’s how we design and build applications!

Where's all my data?

The ways of data are hard to understand

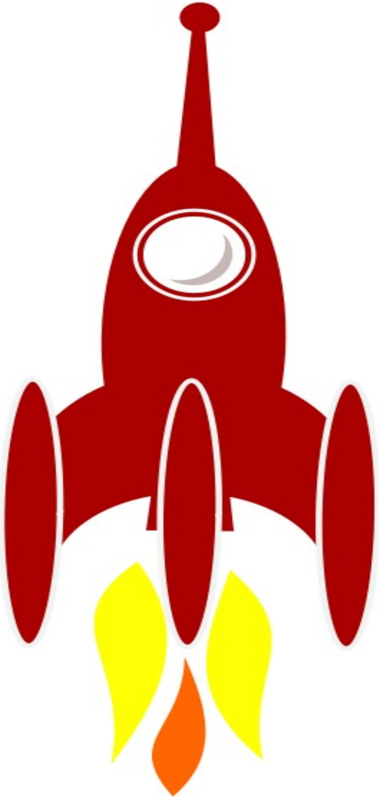
- Devices, operating systems, & apps are getting more complex and intertwined
  - Mashups, Ad networks
  - Machines virtual and realtime configured
  - Not visible to users, and experts
  - Data processing changes constantly



→ No control over data and far too easy to loose them

Security & Privacy is not a lost cause!

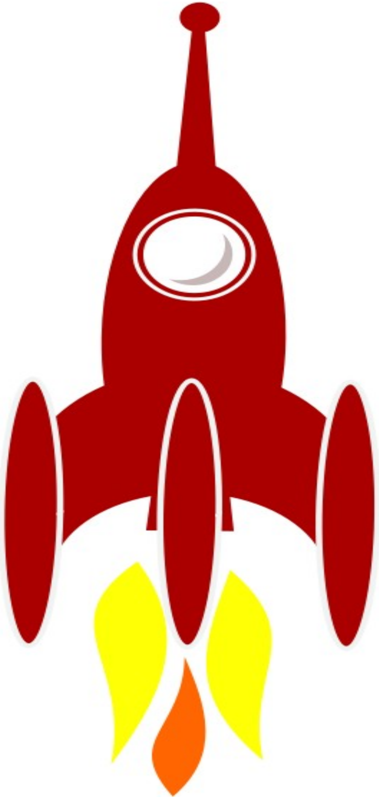
We need paradigm shift &
build stuff for the moon
rather than the sandy beach!



That means:

- Reveal only minimal data necessary
- Encrypt every bit
- Attach usage policies to each bit

Cryptography can do that!



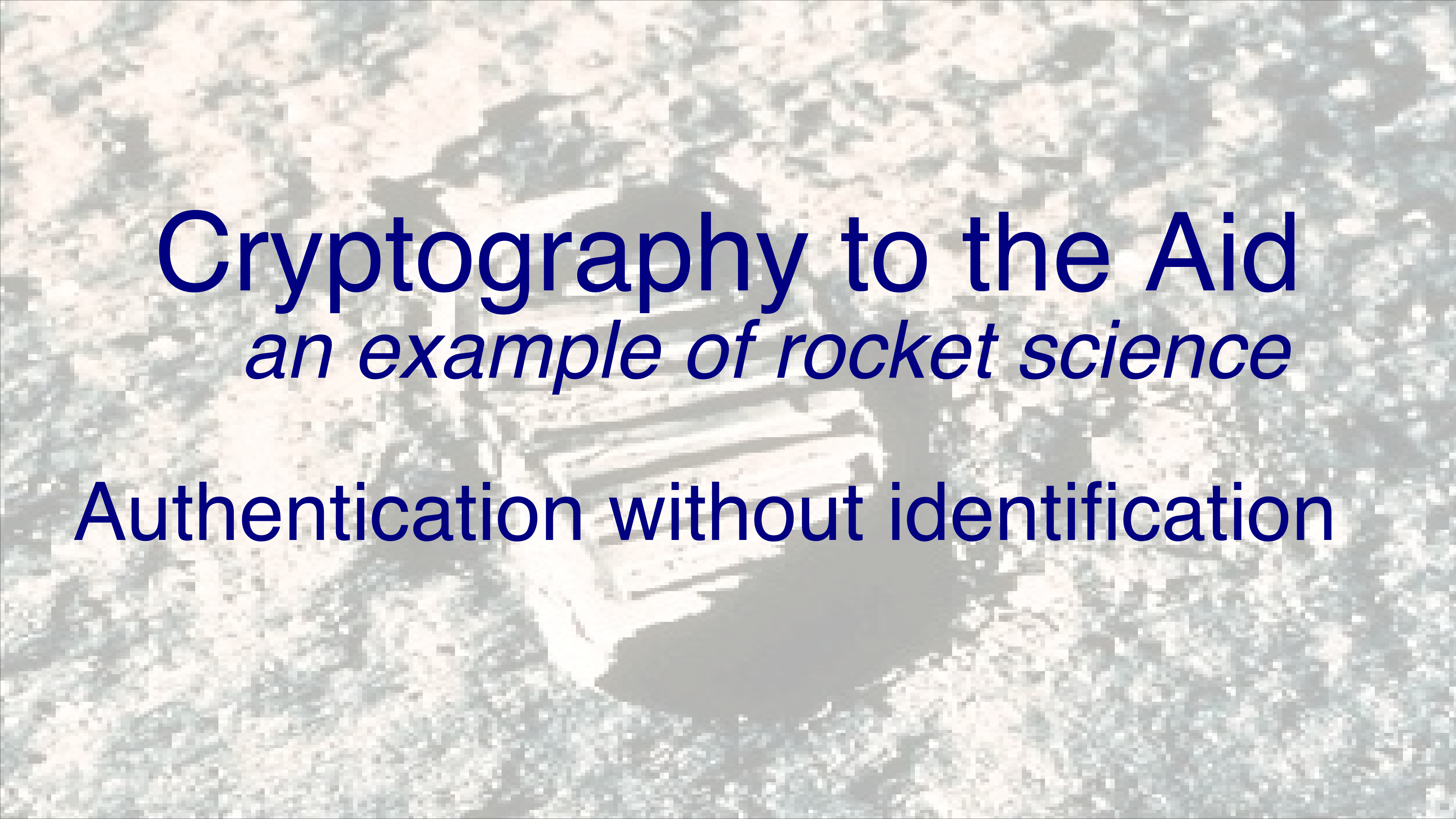
What does that mean?

We do have the (fancy) cryptography, but it is hardly used

- Deemed too expensive
- Too hard to manage all the keys, fear of loosing keys
- Protecting data is considered futile
- Often required by law, but these are w/out teeth
- Debate about legality of encryption V2.0

On the positive side

- Importance of security and privacy increasingly recognized
- Laws are getting better in protecting privacy (cf. EU GDPR)



Cryptography to the Aid

an example of rocket science

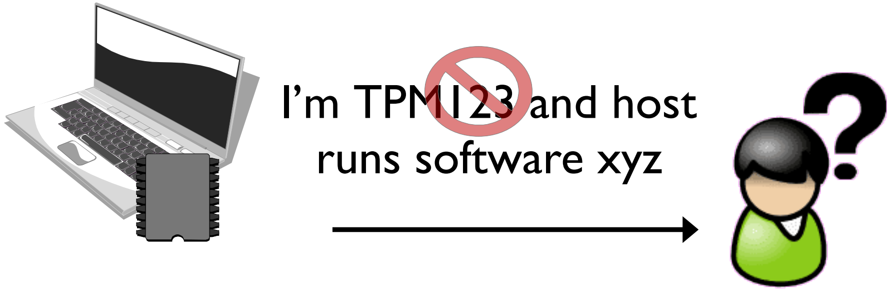
Authentication without identification

Use case: Attestation

Direct Anonymous Attestation:

- Protocol standardized by TCG (trusted computing group) in 2004
- Attestation of computer state by TPM (root of trust)
- TPM measures boot sequence
- TPM attest boot sequence to third party
- Attestation based on cryptographic keys

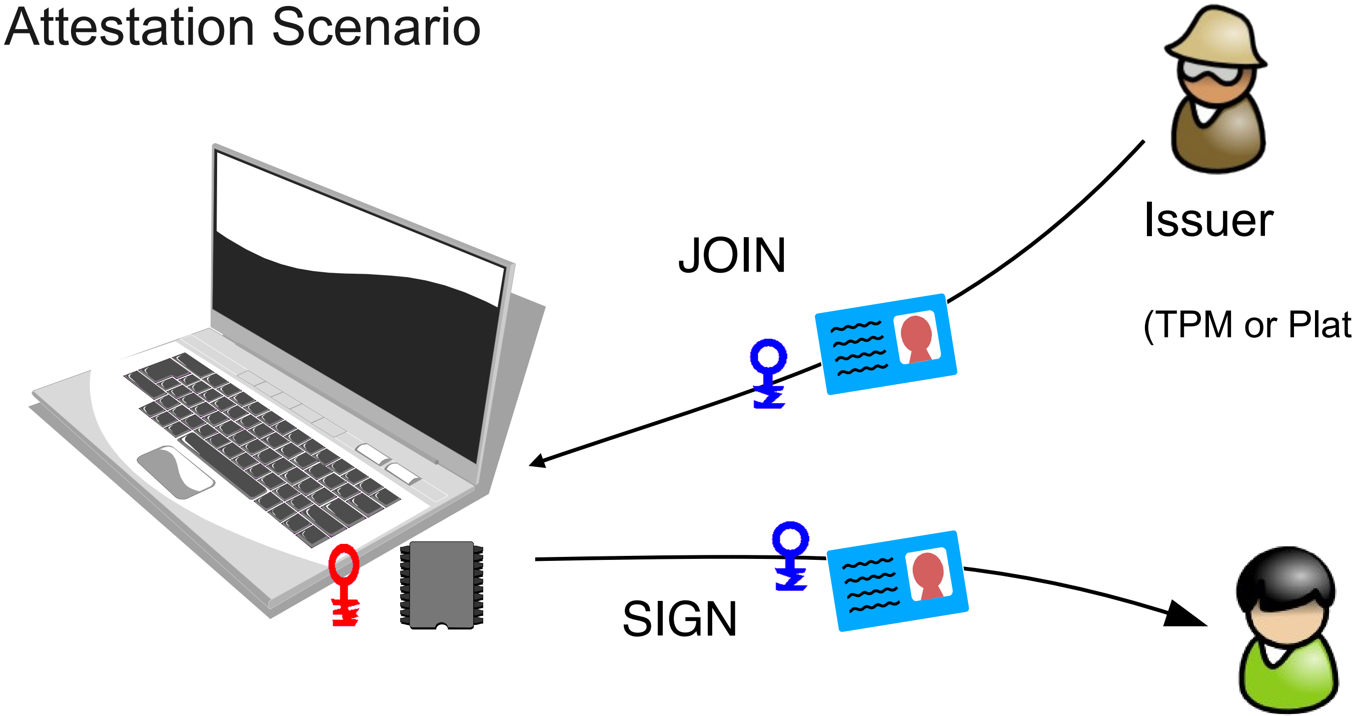
→ Strong authentication of TPM with *privacy*



Other use cases of this crypto (hardware root of trust):

- secure access to networks, services, any resources of devices (IoT, V2X, Industry 4.0, etc)
- can be extended to user of device (trusted execution environment) – cf. FIDO

Attestation Scenario



JOIN

SIGN

Issuer

(TPM or Platform Manufacturer)

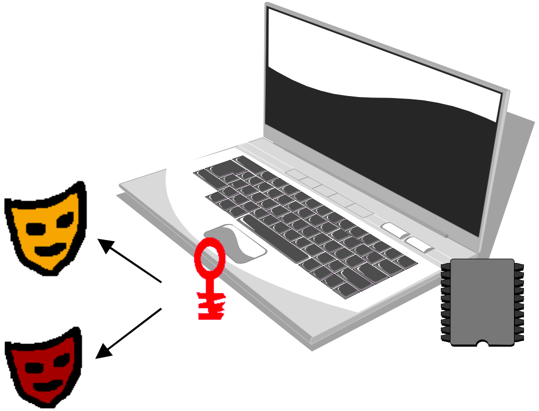
Verifier

(Bank, eShop, Tax authority, …)

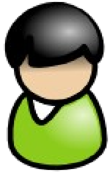
Problem: using traditional certificates, all transactions of the same platform become linkable :-(

Not Rocket Science!

Direct Anonymous Attestation (Brickell, Camenisch, Chen - 2003)



Issuer

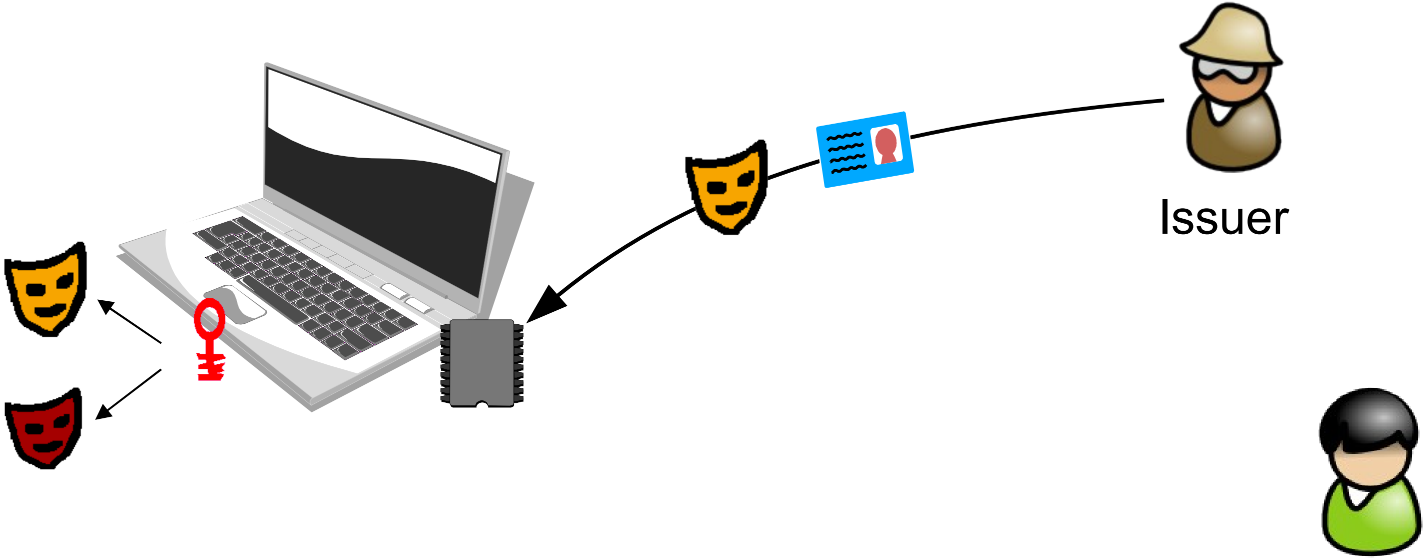


Verifier

Two crucial differences:

1. One secret key - several public keys

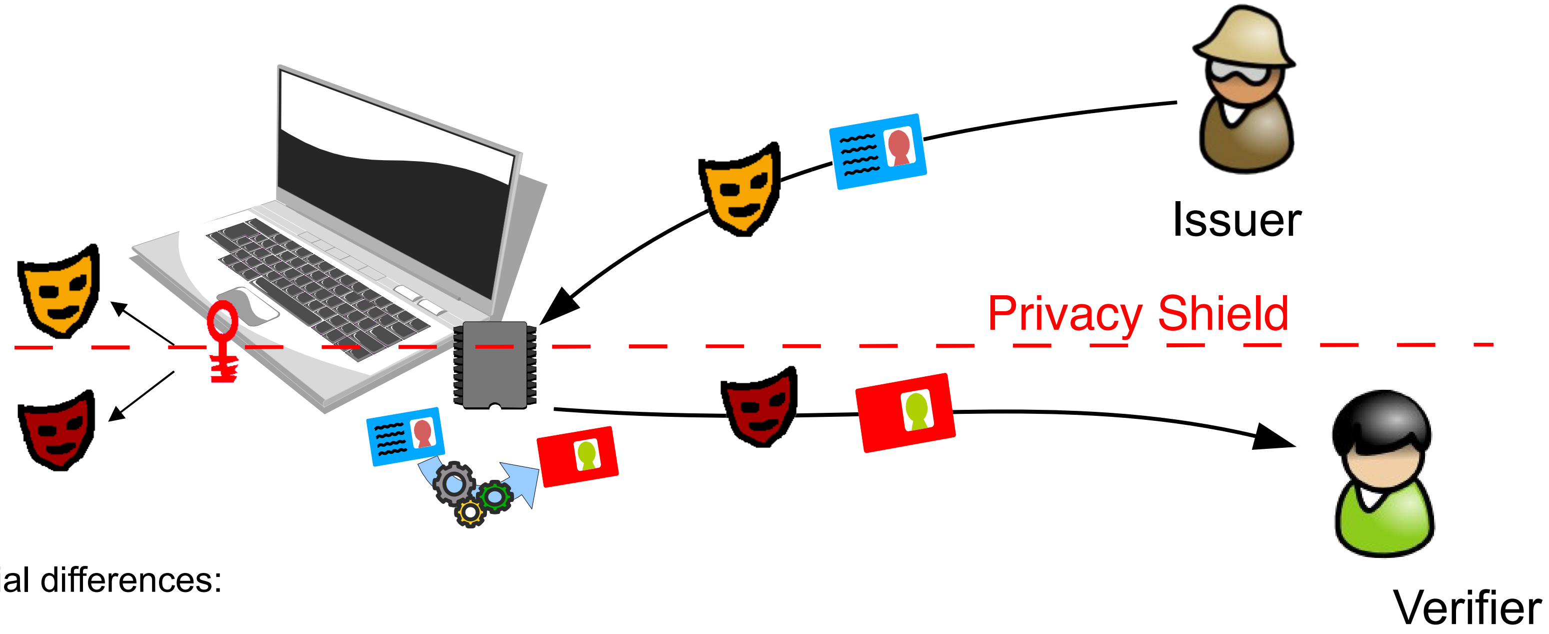
Direct Anonymous Attestation (Brickell, Camenisch, Chen - 2003)



Two crucial differences:

1. One secret key - several public keys

Direct Anonymous Attestation (Brickell, Camenisch, Chen - 2003)



Two crucial differences:

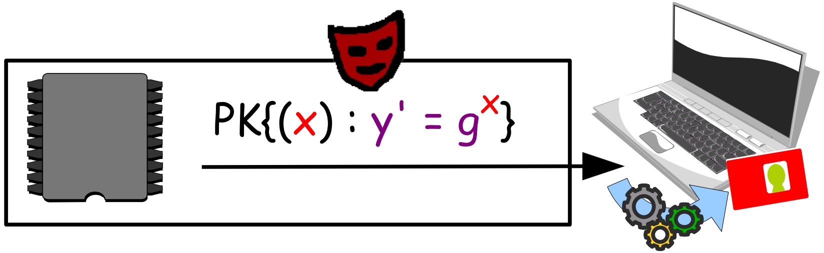
1. One secret key - several public keys
2. Randomizable credentials: original credential into new credentials that “looks like” a fresh credential

   → different randomize credentials cannot be linked (anonymity)

   → still credentials are unforgeable

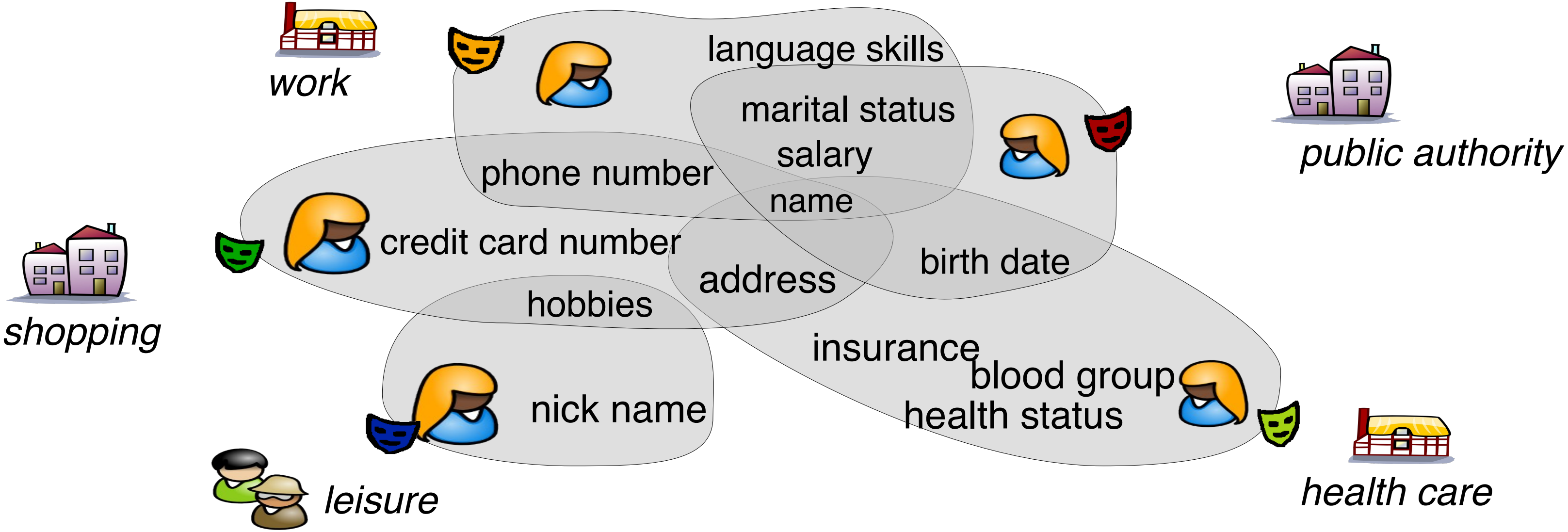
Status DAA 2017

- RSA-based scheme standardized by TCG in 2004, later also in ISO
- Replaced by ECC-based scheme in 2015 (both TCG and ISO)
- DAA is split in TPM and host part, ECC-based scheme only defined for TPM



- Supports multiple DAA protocols (q-SDH, LRSW based etc)
- Scheme is really efficient: TPM computes single exponentiation
- Some security issues identified, fixed in latest TPM spec
- See our paper at IEEE S&P 2017 with full scheme and security proof

Privacy-preserving identities on-line – authentication w/out Identification



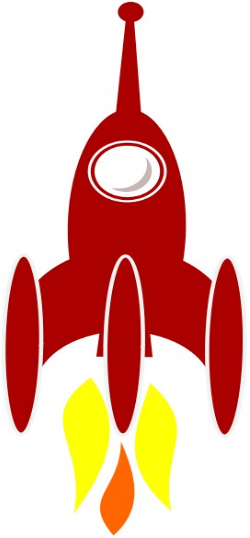
ID:

- (dynamic) set of attributes shared w/ someone
- different with different entities

Privacy Preserving Identity Management – identity mixer or DAA extended

- authentication means: strong e-authentication, using strong cryptography
- means to transport attributes between parties: certified attributes without linking identities

Conclusions



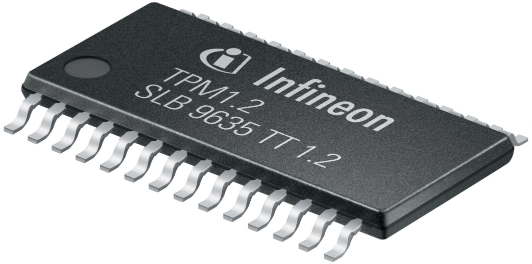
- Device authentication more relevant than ever
- Data parsimony is the key to security
- Fancy crypto can realize this, today
- More public awareness and discussion needed

Let’s do some rocket science together!

Thank you!

For information:

- www.zurich.ibm.com/idemix
- idemixdemo.mybluemix.net



jca@zurich.ibm.com

@JanCamenisch