Privacy Enhancing Technologies: Privacy by Design

From ID Cards, Cell Phones to the Internet

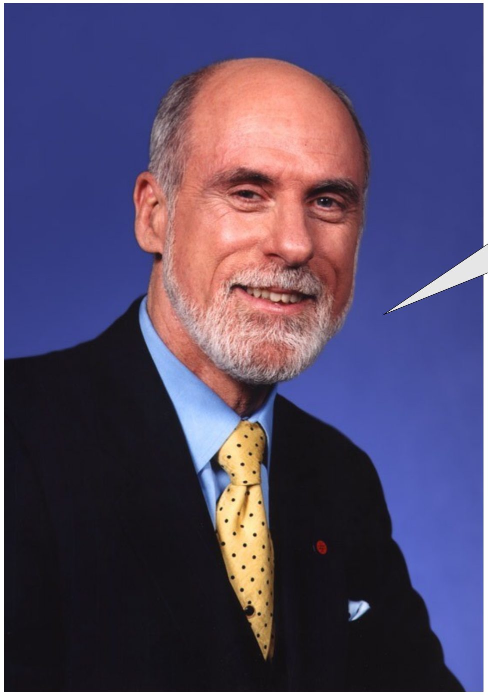
Dr. Jan Camenisch

IBM Research

Technical Leader PrimeLife

May 11th, 2009

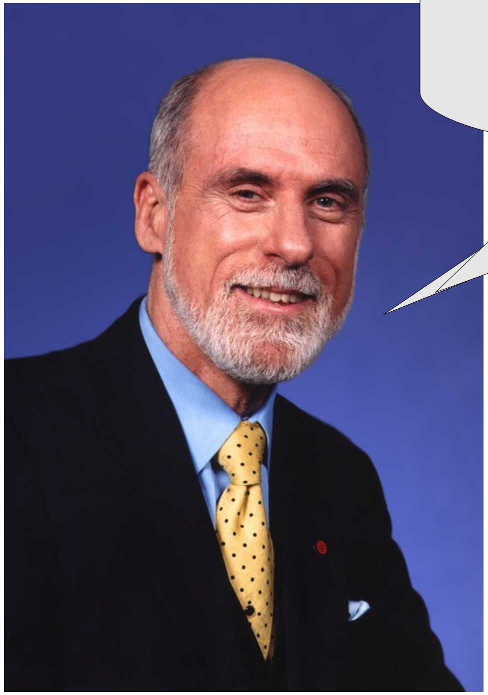
“The Internet will be everywhere, from every mote to interstellar communication”



Vint Cerf

“The Internet will be everywhere, from
stellar

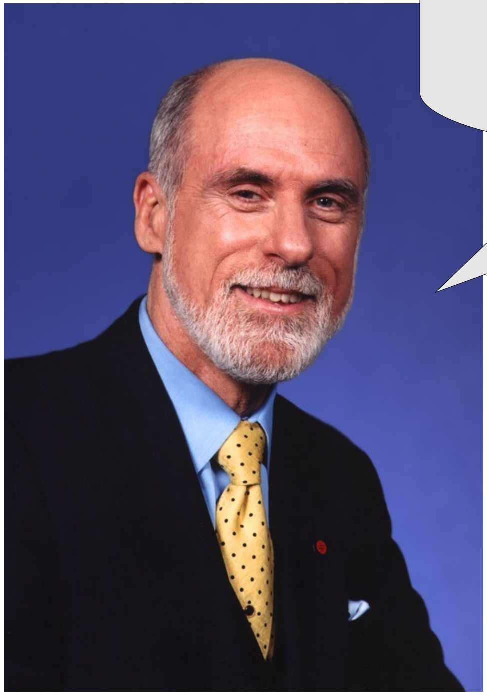
“We need both: sometimes we
wanna be anonymous, sometimes
we need to be identified”



Vint Cerf

“The Internet will be everywhere, from
stellar

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



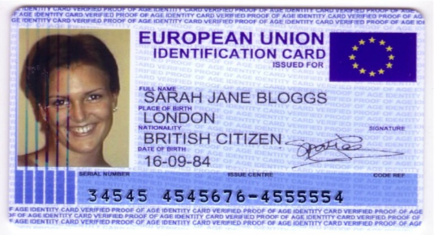
Vint Cerf

“...at the *same* time!”

A Surfer

Not Just the Internet...

...even if it is going to be everywhere ;-)



EUROPEAN UNION
IDENTIFICATION CARD
ISSUED FOR

FULL NAME
SARAH JANE BLOGGS
PLACE OF BIRTH
LONDON
NATIONALITY
BRITISH CITIZEN
DATE OF BIRTH
16-09-84
SIGNATURE

SERIAL NUMBER
ISSUE CENTRE
CODE REF
34545 4545676-4555554

What's the Problem?

“Neil Armstrong’s Footsteps are still there”

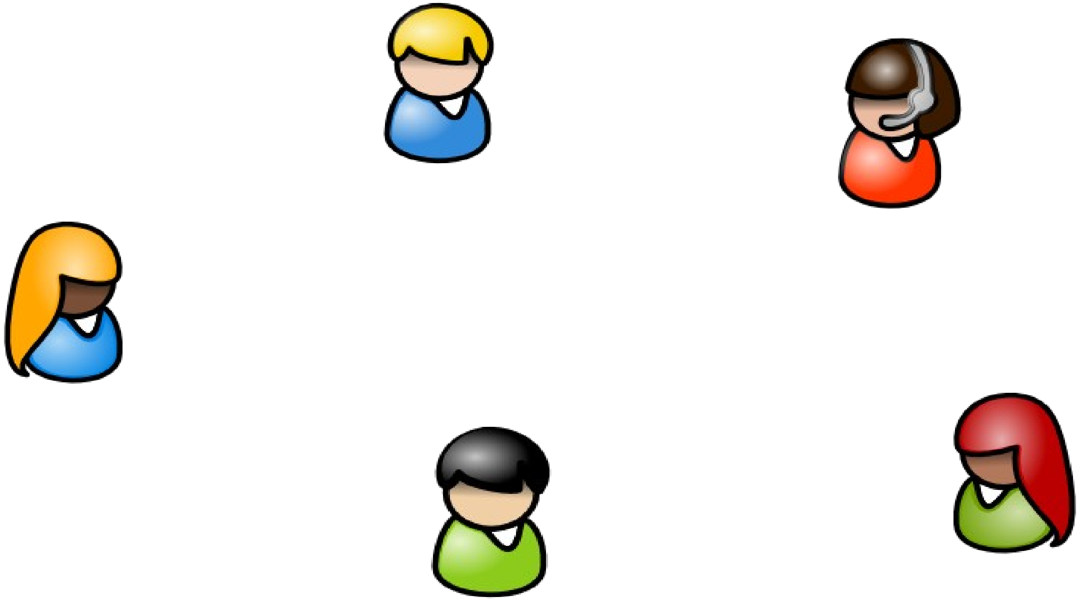
(Robin Wilton)

Photo:cc-nc-by jahdakine

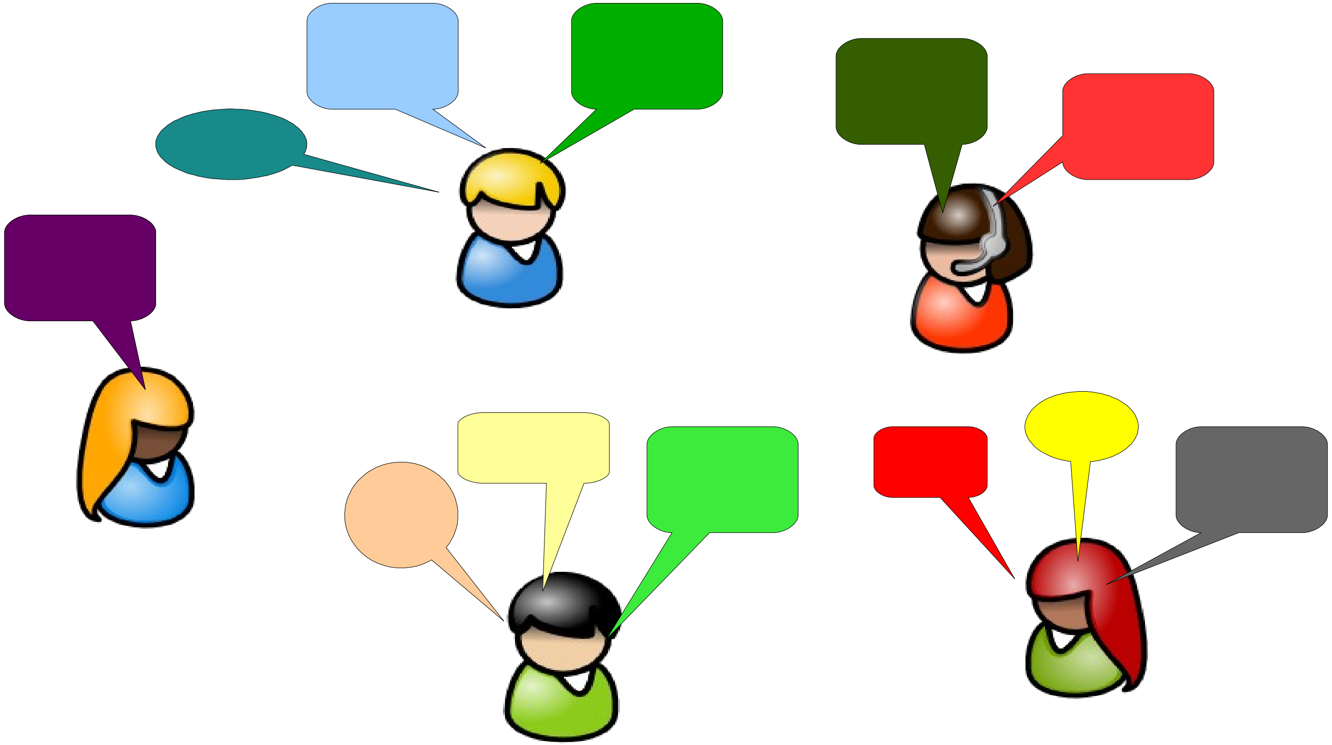
Computers don't forget

- Storage becomes ever cheaper
- Data mining ever better

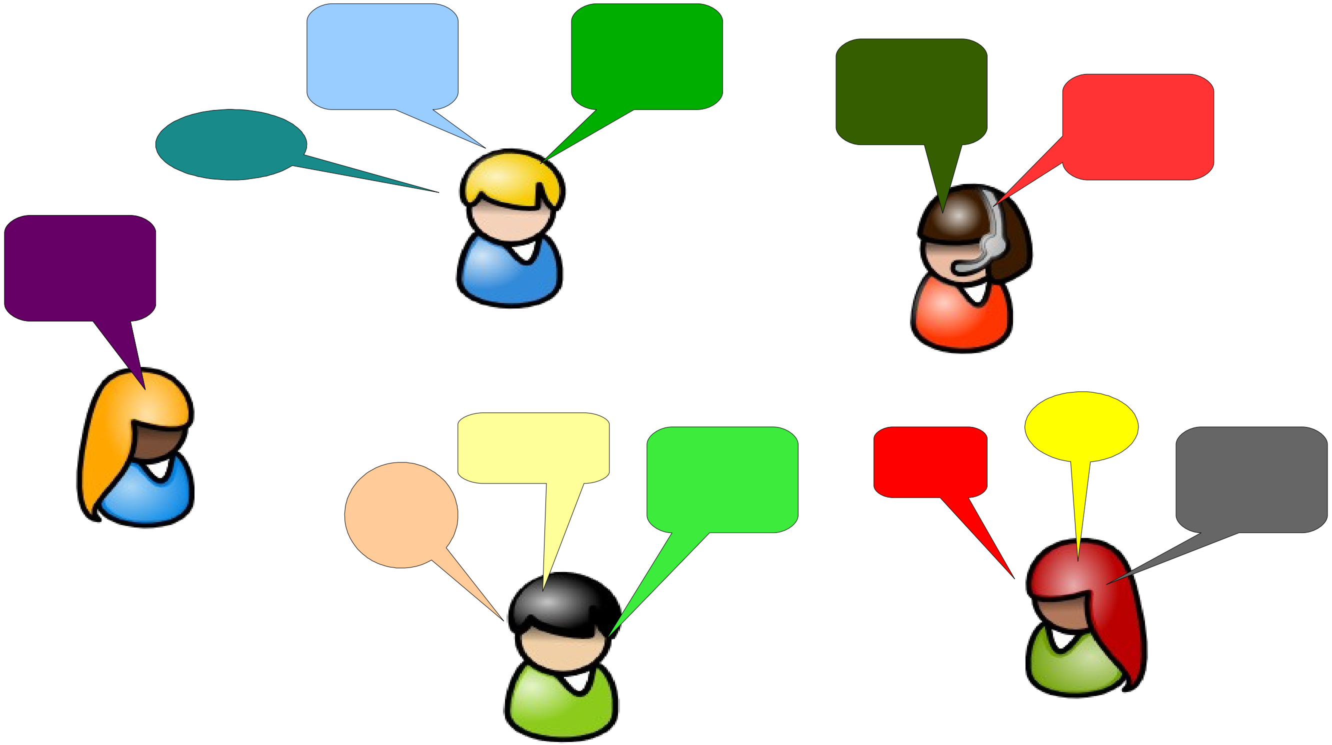
People



People Who Like to Talk



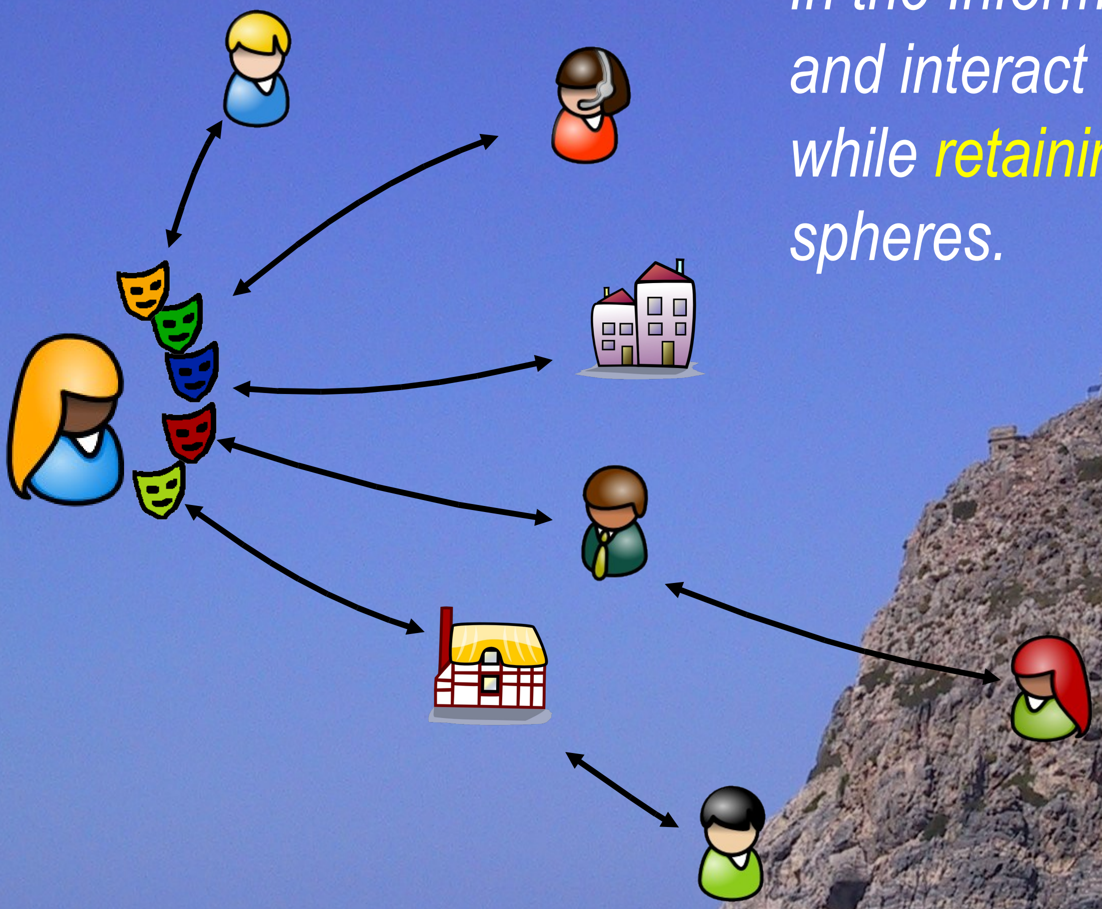
People Who Like to Talk



- Distributing Information is easier
- Controlling it much harder
- Establish trust and security even harder

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.



Privacy By Design!

- Network Layer
  - Anonymity as default
- Identity Layer (Access Control & Authorization)
  - Data minimization
- Application Layer
  - Control of Data: Policies and UI
  - Social Networks, etc,...
- Specific Applications
  - Voting, Auctions....

Privacy By Design!

- Network Layer
  - Anonymity as default

Technology exists (Tor, ...)
Change infrastructure
Internet 2, GSM, ...

- Identity Layer (Access Control & Autho
  - Data minimization

Technology Ready
Needs to Applied
eID, ...

- Application Layer
  - Control of Data: Policies and UI
  - Social Networks, etc,...

Policies Understood
User Interfaces & Easy Design
Still needs research....

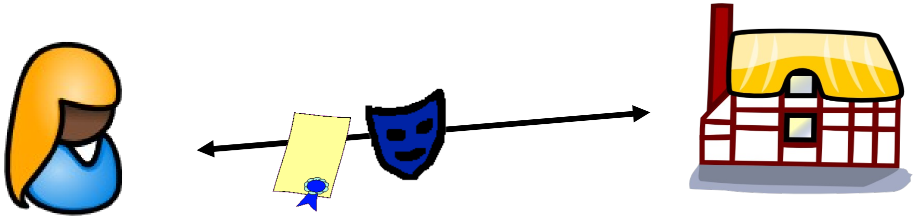
- Specific Applications
  - Voting, Auctions....

Some are implemented
A lot can be done :-)

Privacy @ ID Layer

A Closer Look & Solutions

The ID Layer

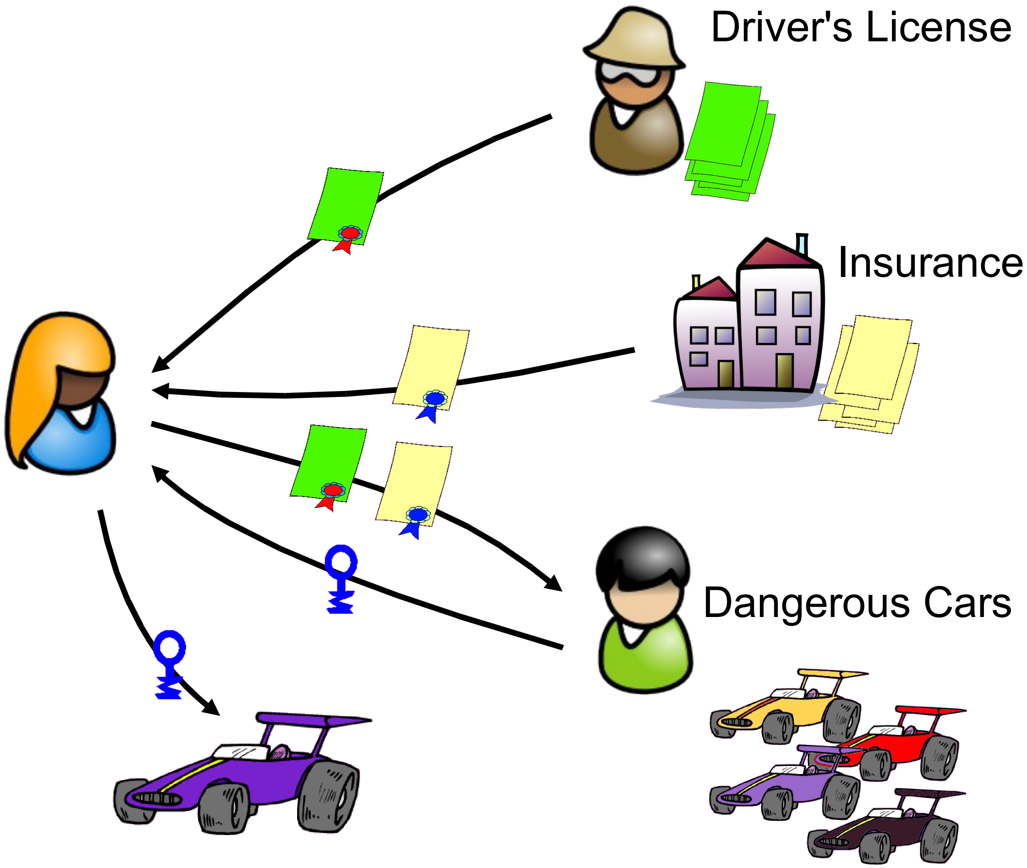


User needs to send Personal Information to Service Provider

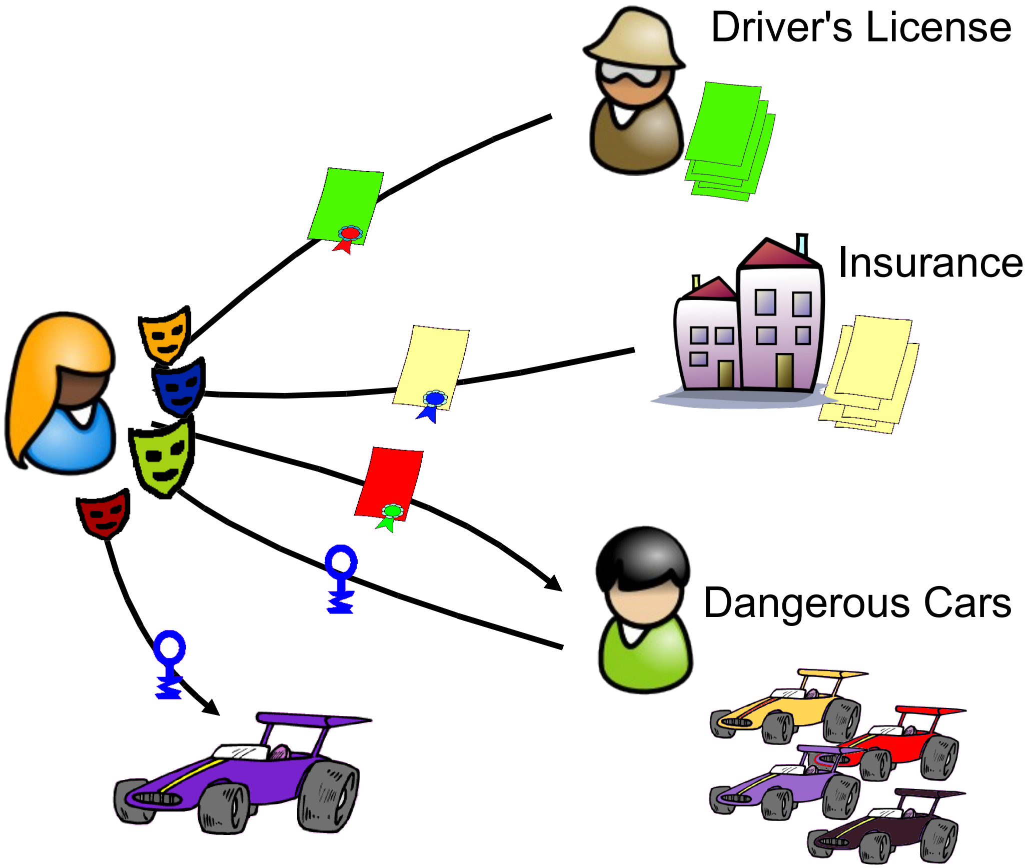
1. Agree on which information to exchange: Policy Language
2. User needs token certifying this information: Credentials
3. User needs to picks which credential to show: Digital Wallet

Design Principle: Minimize Information Exchanged!

Digital Credentials



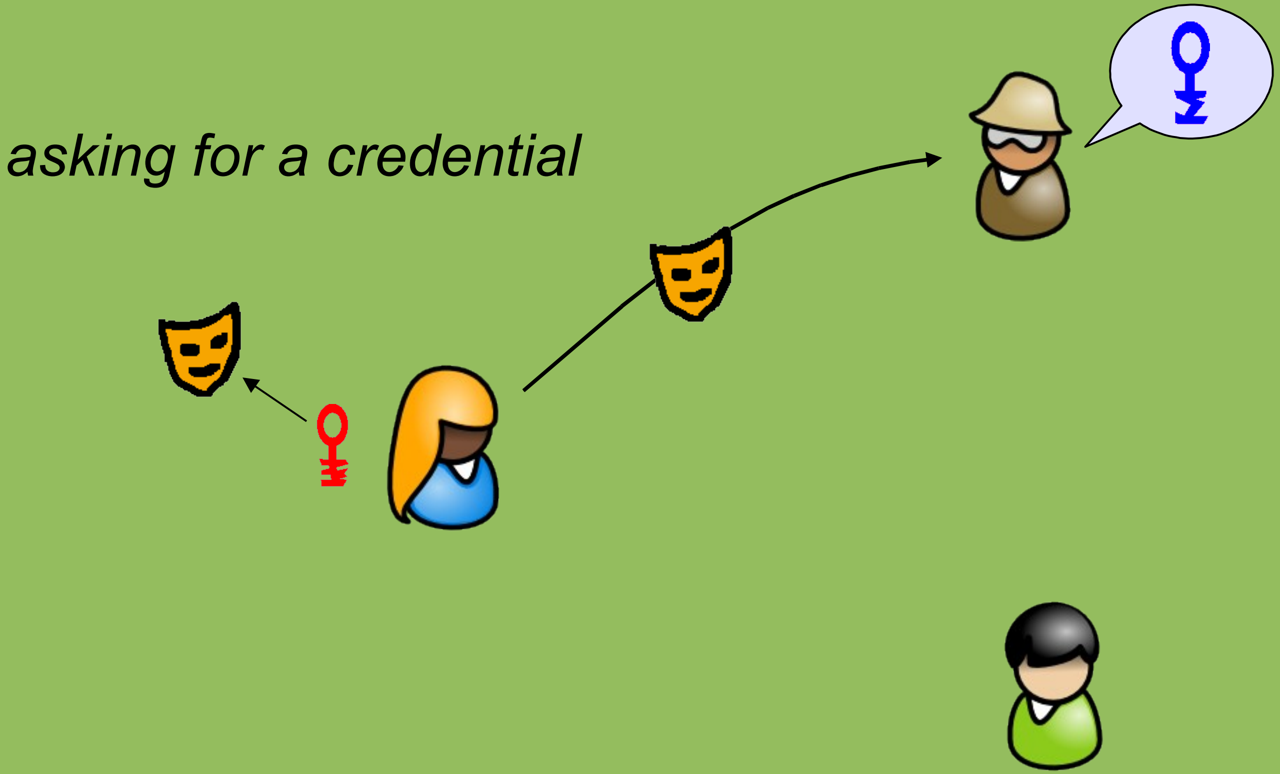
Solution: Private Digital Credentials



Private Credentials: How to Build Them

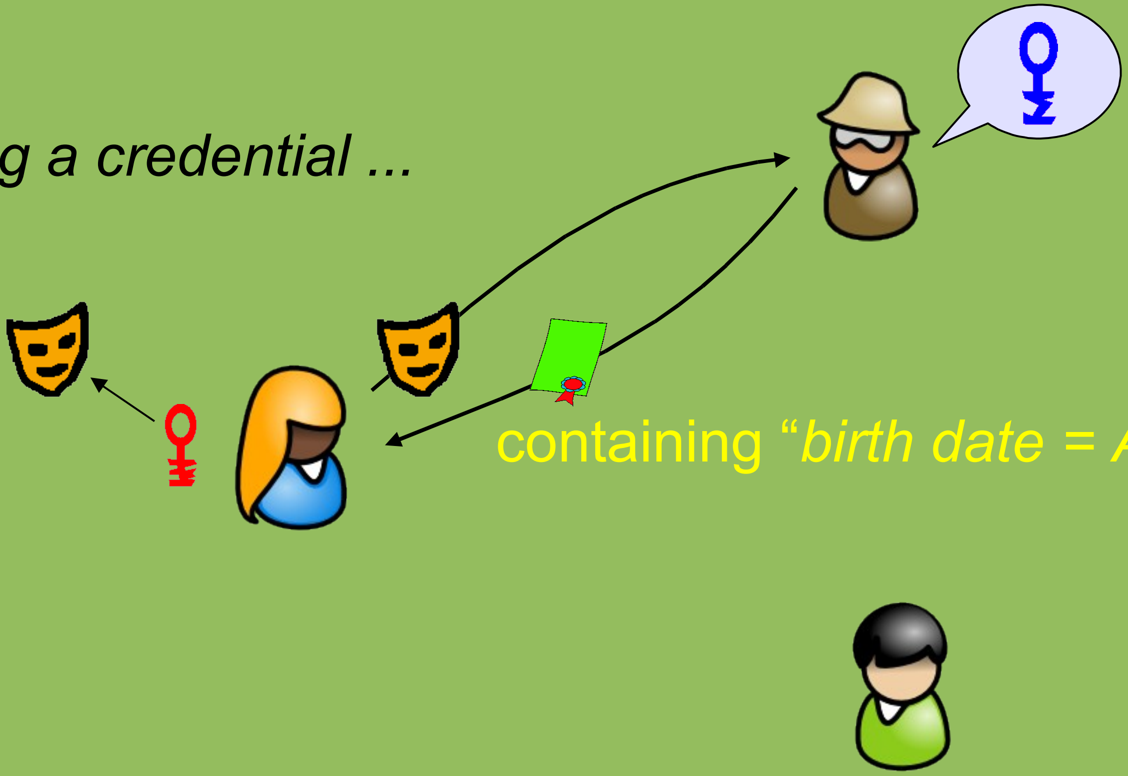
In the beginning...

State of the Art: How to Build Them



State of the Art: How to Build Them

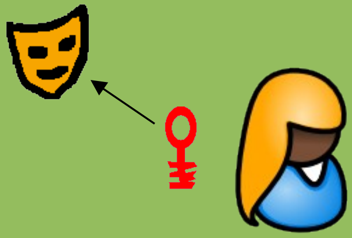
getting a credential ...

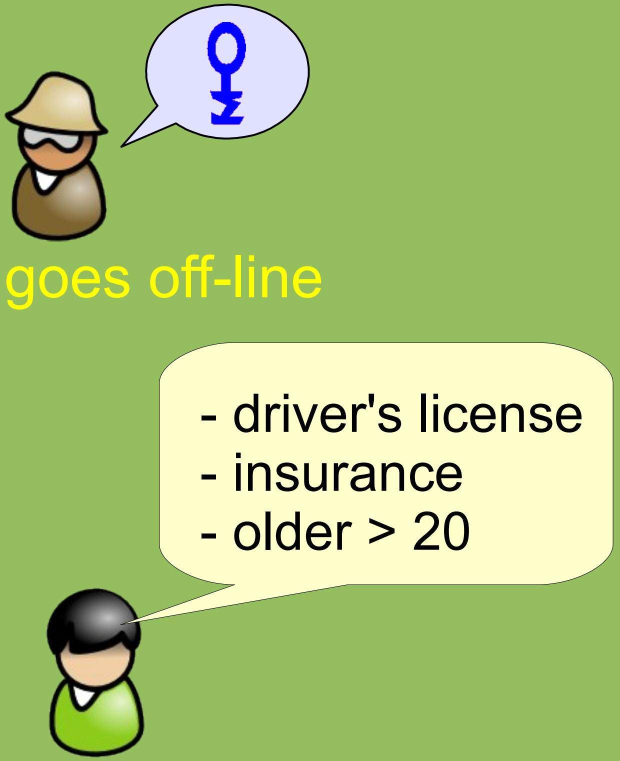


containing “*birth date = April 3, 1987*”

State of the Art: How to Build Them

showing a credential ...



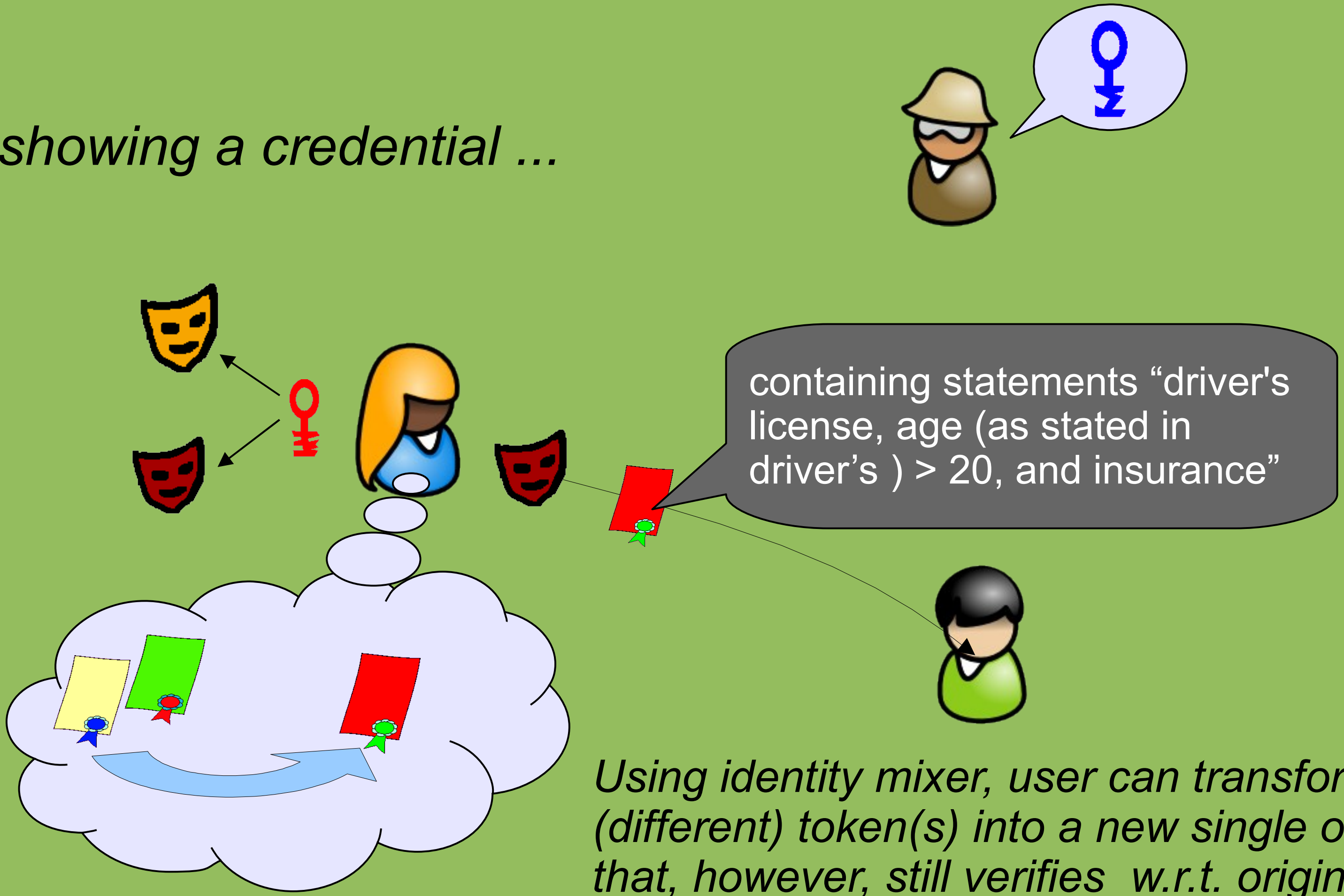


goes off-line

- driver's license
- insurance
- older > 20

State of the Art: How to Build Them

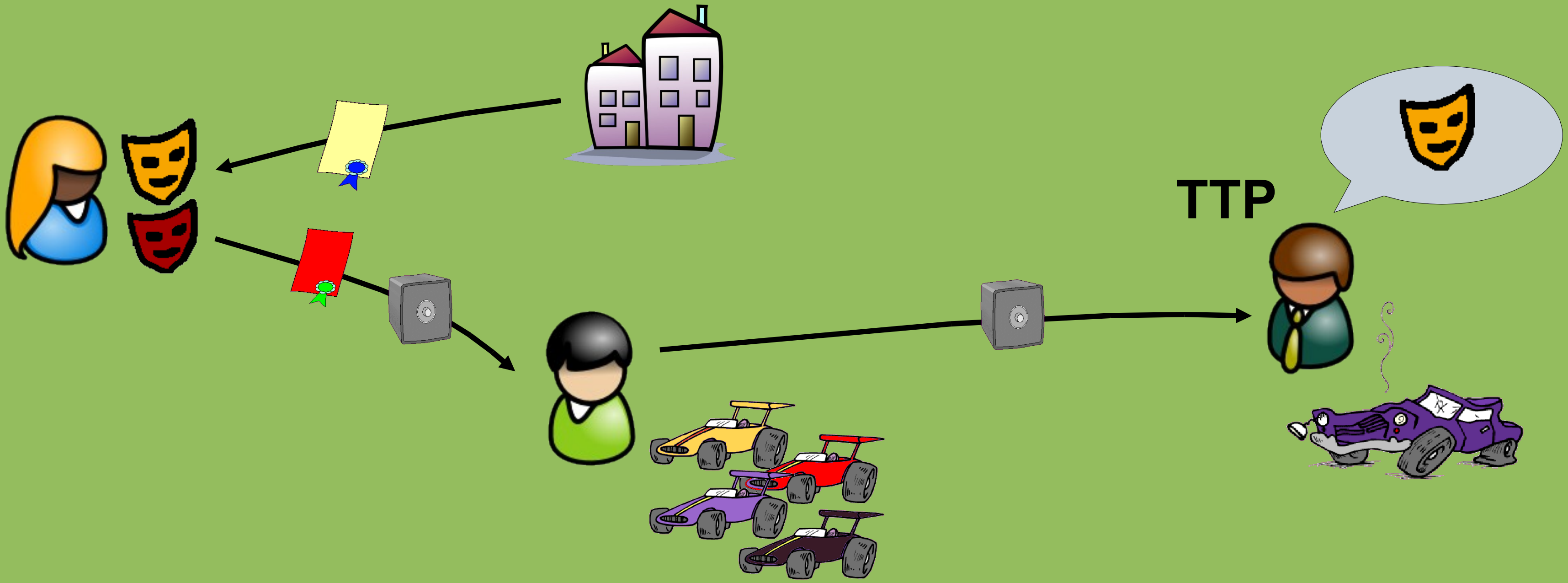
showing a credential ...



containing statements “driver's license, age (as stated in driver’s) > 20, and insurance”

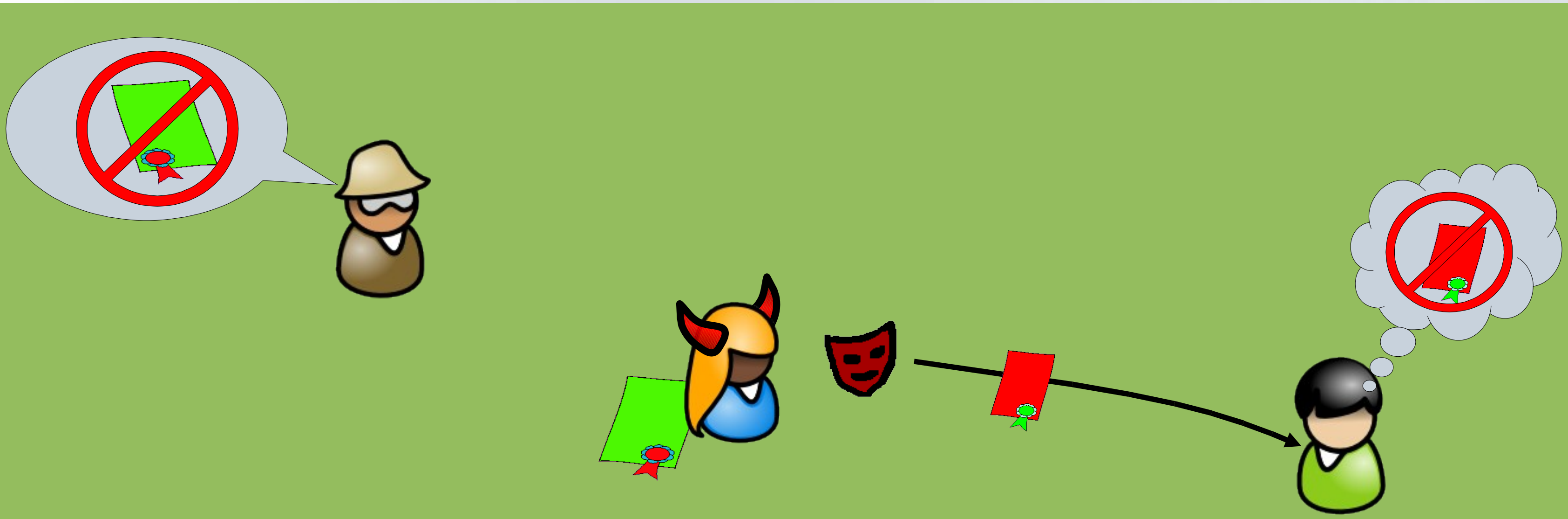
Using identity mixer, user can transform (different) token(s) into a new single one that, however, still verifies w.r.t. original signers' public keys.

Other Properties: Attribute Escrow (Opt-In)



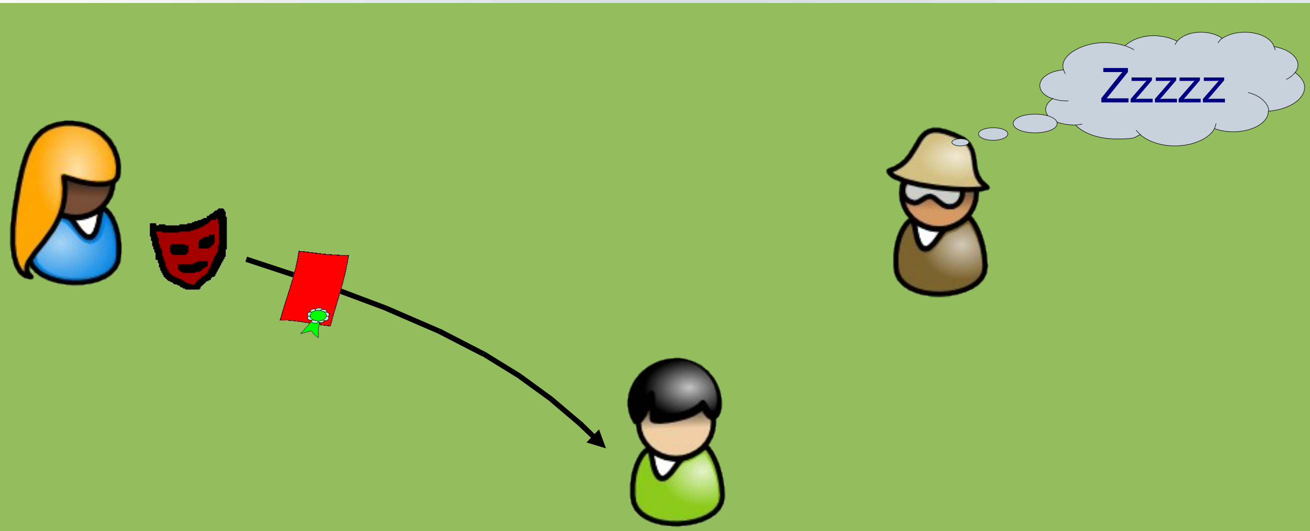
- If car is broken: ID with insurance needs be retrieved
- Can verifiably encrypt any certified attribute *(optional)*
- TTP is off-line & can be distributed to lessen trust

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

Other Properties: Offline Usage



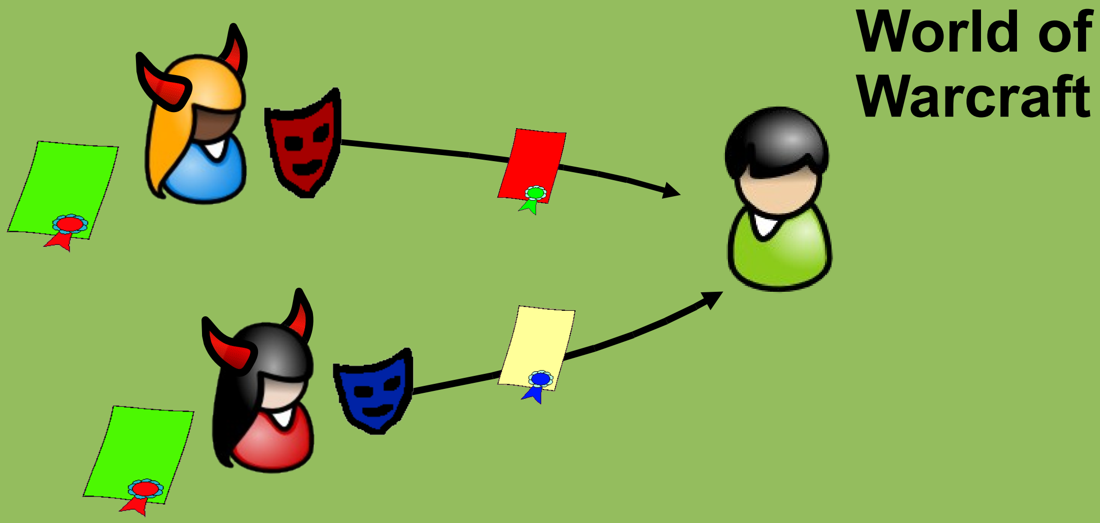
ID providers (issuers) need sleep, too!

- 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

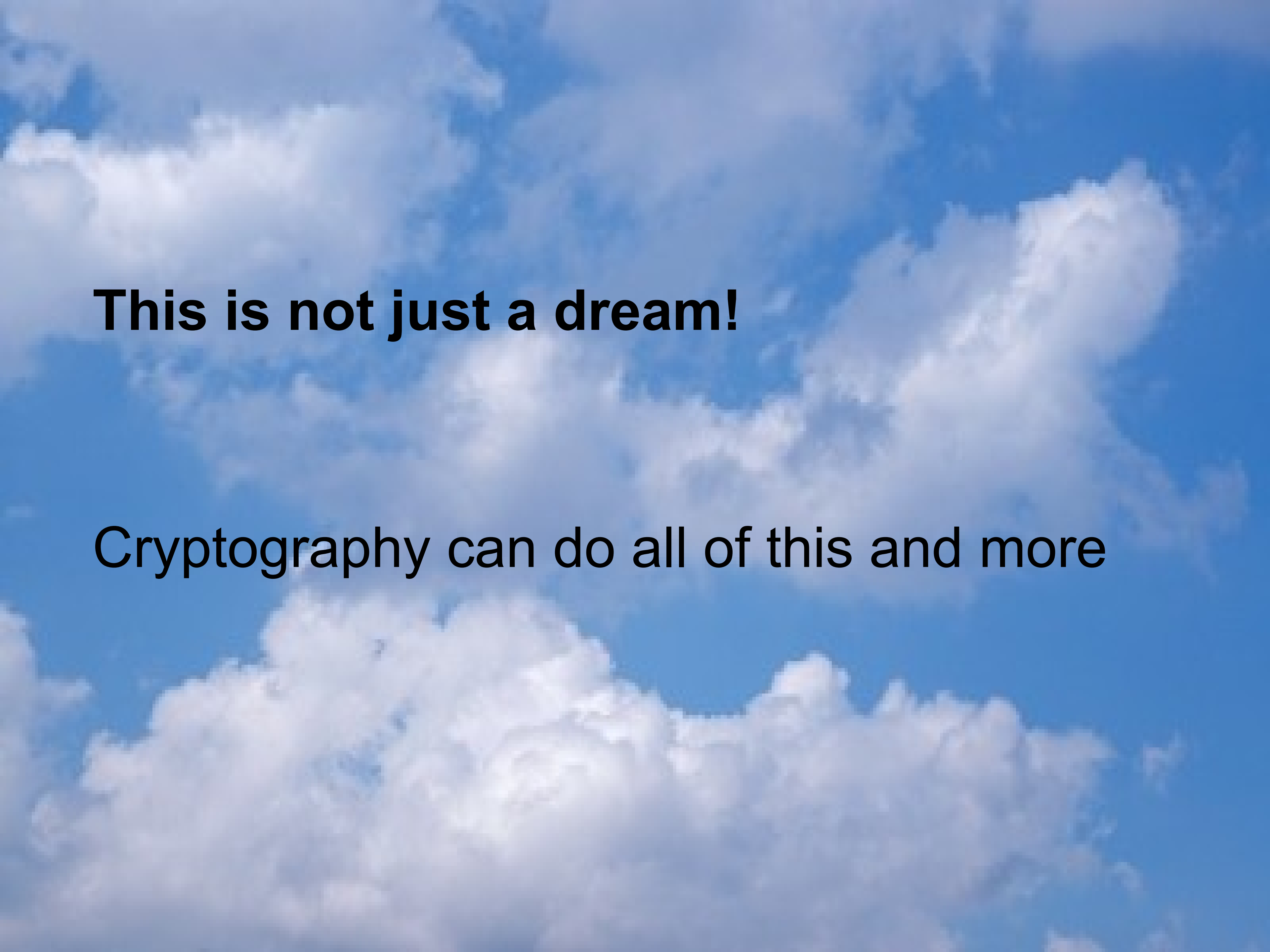
Other Properties: Cheating Prevention



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 :-)

This is not just a dream!

Cryptography can do all of this and more

.... efficiently

.... even on a smart card   :-)

.... and is for free: prime.inf.tu-dresen.de/idemix

Let's Make it Real!

jca@zurich.ibm.com
www.zurich.ibm.com/idemix

info@primelife.eu
www.primelife.eu