Sitting on top of the world.

Autonomous.

But...

...curiosity killed the cat.

Who cares?

Cats have seven lives, right?

Well yes, but humans don‘t.

This is YOUR...

PrimeLife

PrimeLife

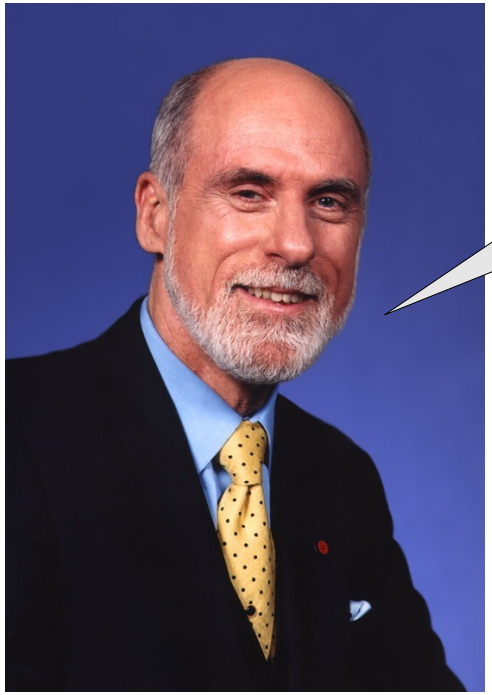
Privacy, Identity, and Trust Management

Jan Camenisch
Technical Leader PrimeLife
IBM Research

A research project funded by the European Commission's 7th Framework Programme

SEVENTH FRAMEWORK PROGRAMME

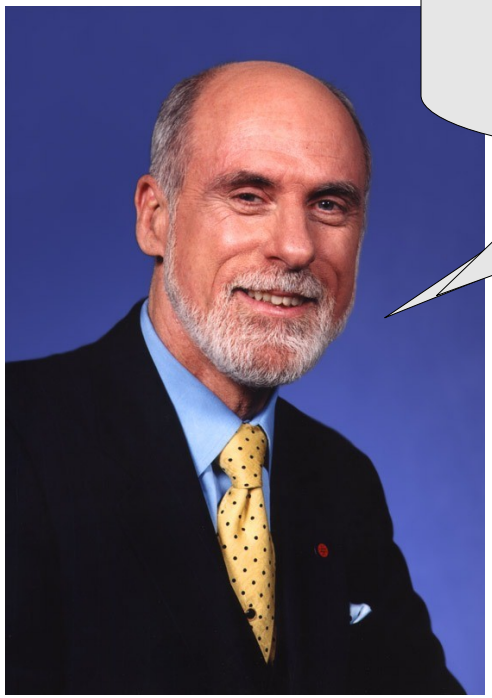
“The Internet will be everywhere, from every mote to interstellar communication”



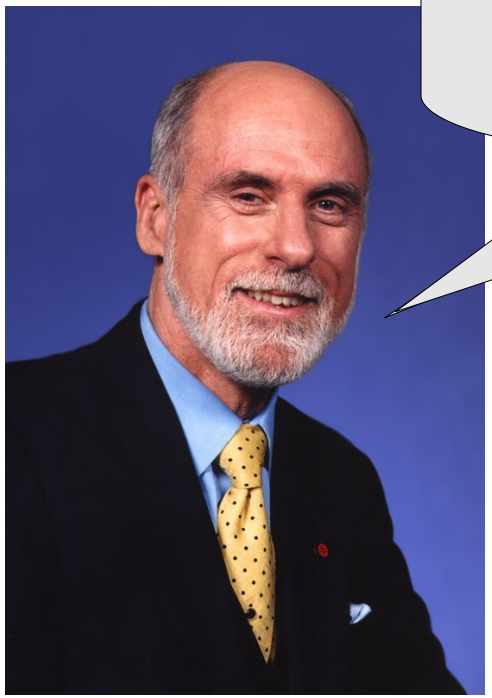
Vint Cerf

“The Internet will be everywhere, from
tellar

“The Internet needs to have an secure identity layer”



Vint Cerf



Vint Cerf

"The Internet will be everywhere, from [illegible]tellar

"The Internet needs to have an

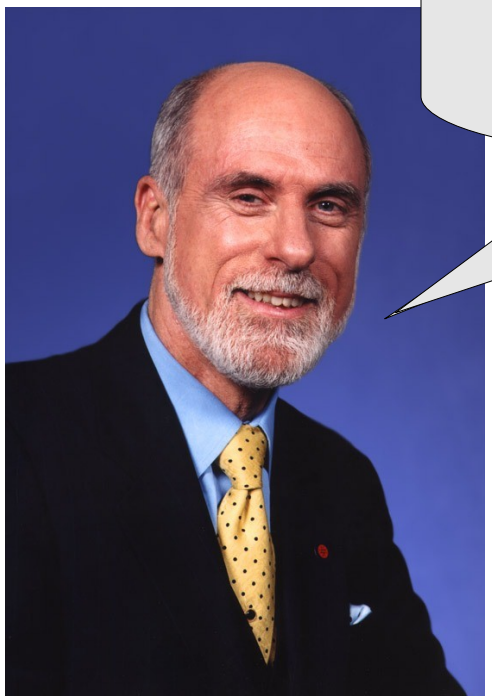
"We need both: sometimes we wanna be anonymous, sometimes we need to be identified"

"The Internet will be everywhere, from

"The Internet needs to have an

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

"...at the *same* time!"



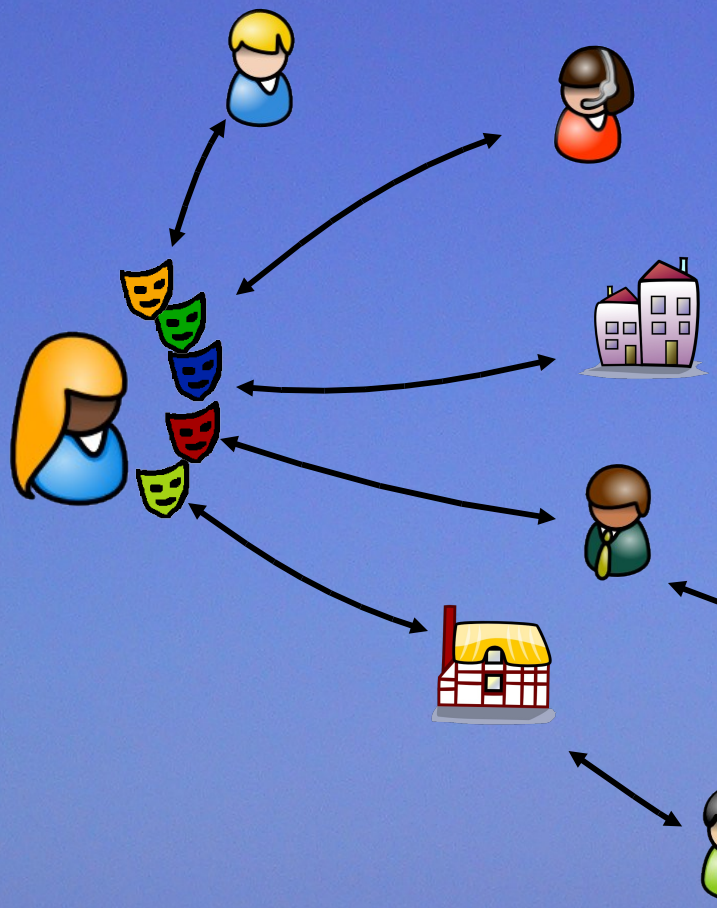
Vint Cerf

A Surfer

It's Not Just the Internet...

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

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.

What's the Problem?

"Neil Armstrong's Footsteps are still there"

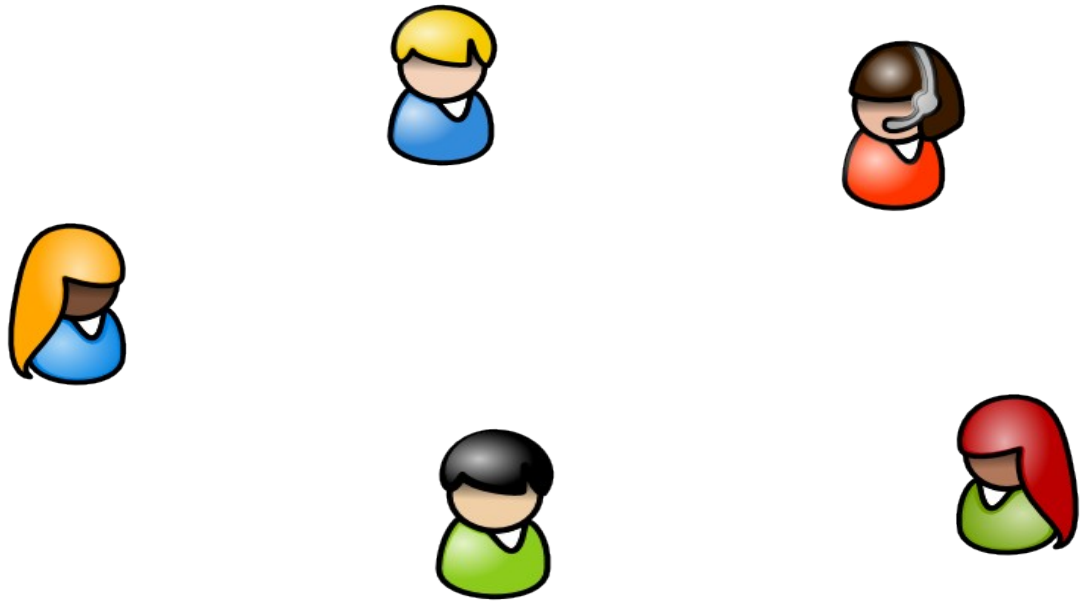
(Robin Wilton, Sun Microsystems)

Computers don't forget

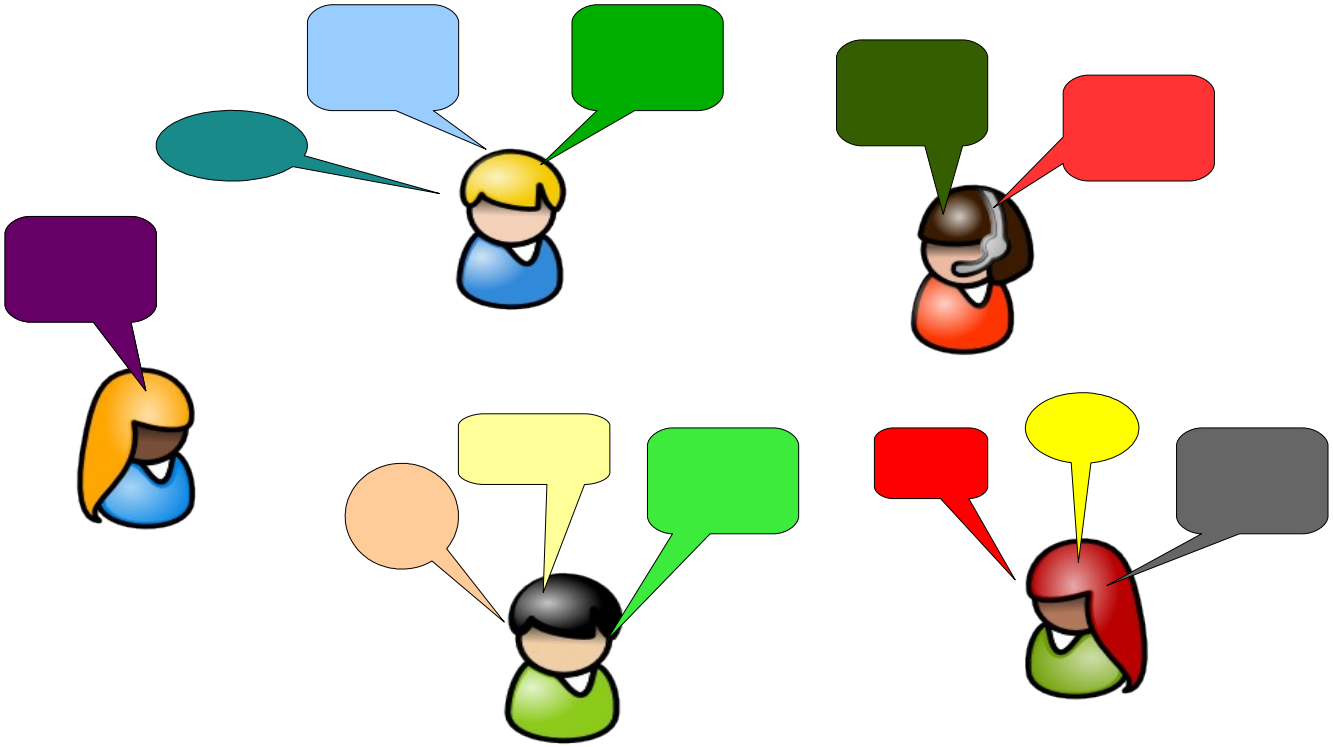
- Storage becomes ever cheaper
- Data mining ever better

Not only the tokens and devices..

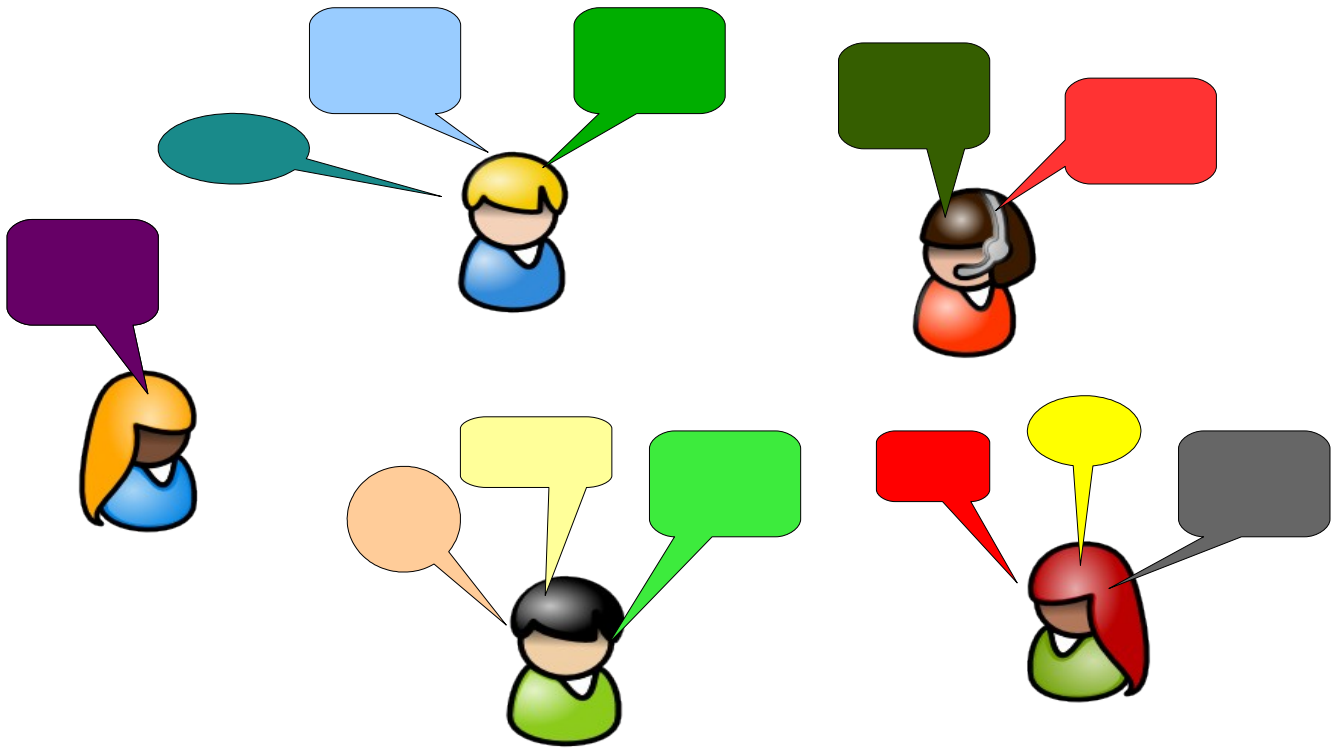
People



People Who Like to Talk



People Who Like to Talk



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

So what do we need?

Privacy, Identity and Trust Mgmt Built-In Everywhere!

- Network Layer Anonymity
  - ... in mobile phone networks
  - ... in the Future Internet as currently discussed
  - ... access points for ID cards
- Identification Layer
  - Access control & authorization
- Application Layer
  - “Standard” e-Commerce
  - Specific Apps, e.g., eVoting, ...
  - Web 2.0, e.g., Facebook & Wikis

State of the Art

Results of predecessor **PRIME**:

- Privacy-enhancing IDM is viable today
- Enable use of PRIME within legal, social and economic environment
- Raise awareness among stakeholders

However:

- Transactional view...
- Still not usuable...

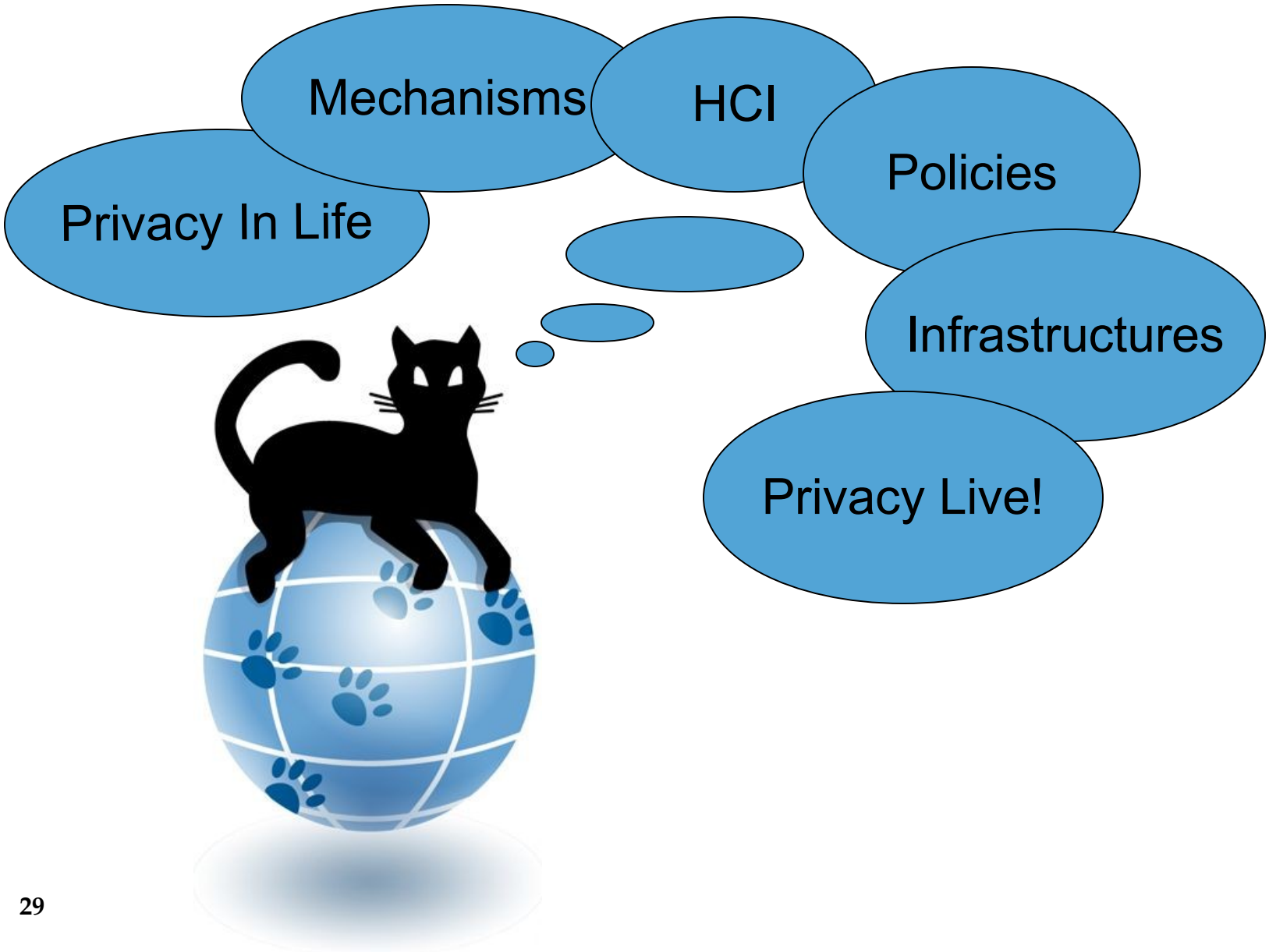
Going Further
PrimeLife's Approach

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



1. Privacy in Life:

Trusted Contents, Selective Access Control in Social Networks, PII-management in Real Life.

- How to bring privacy to real **social life?**
- How can privacy, identity, and trust be managed throughout one's **whole life?**
- **Formative evaluations** of demonstrators will both validate research results and generate new ones as well as assure quality of the demonstrators.

2. Policies

Requirements, Research on Next Gen Policies, Development of Next Gen Policies.

- Policies are the **central mechanism** for enabling privacy, identity and trust management.
- Policies **must govern such a system end-to-end** and throughout different applications.
- Will gather the requirements from Activities 1-3 and to
- **specify the languages** that are required by these activities.

3. Mechanisms:

Crypto, Measures, Privacy of Data, AC for user generated data.

- **Basic mechanisms** for privacy-enhancing identity management and trust establishment to advance the state of the art.
- Implementation of **prototypes**

4. Usability

UIs for PE-IDM, Trust and Assurance HCI, UIs for Policies.

- Researching **mental models** and **metaphors**
- Developing **intuitive, trustworthy** and **legally compliant interfaces**
- implemented in the **prototype studies** in Activity 1

→ **Synchronization** of efforts.

→ **Providing guidance**, help, and formative analysis for the development of all user interfaces.

5. Infrastructures

Service Architecture, Trusted Infrastructure Elements, Service Composition.

- **Study infrastructures** for privacy, identity and trust management, e.g., **SOAs**
- Cooperation with Activities 1-3 to gather the requirements of such an infrastructure,
- Develops a **road-map**

6. Privacy Live

PR & Cooperation, Education, Open Source, Standards.

- Making available privacy-enhancing mechanisms as **Open Source**
- **Interaction with the community** and other **EU projects**
- Organizes **workshops, summer schools**
- contributes to **standardization bodies**,
- and provides **dissemination material.**

Web 2.0

Towards Solutions

Web 2.0: Wikis and Social Networks

Trusted Content

- Is what we see true?
- Contributions by many people we don't know...
- Approach
  - Signing & tagging & rating
  - Reputation (hierarchical & P2P)
  - Incentives for reviewing & rating

Web 2.0: Wikis and Social Networks

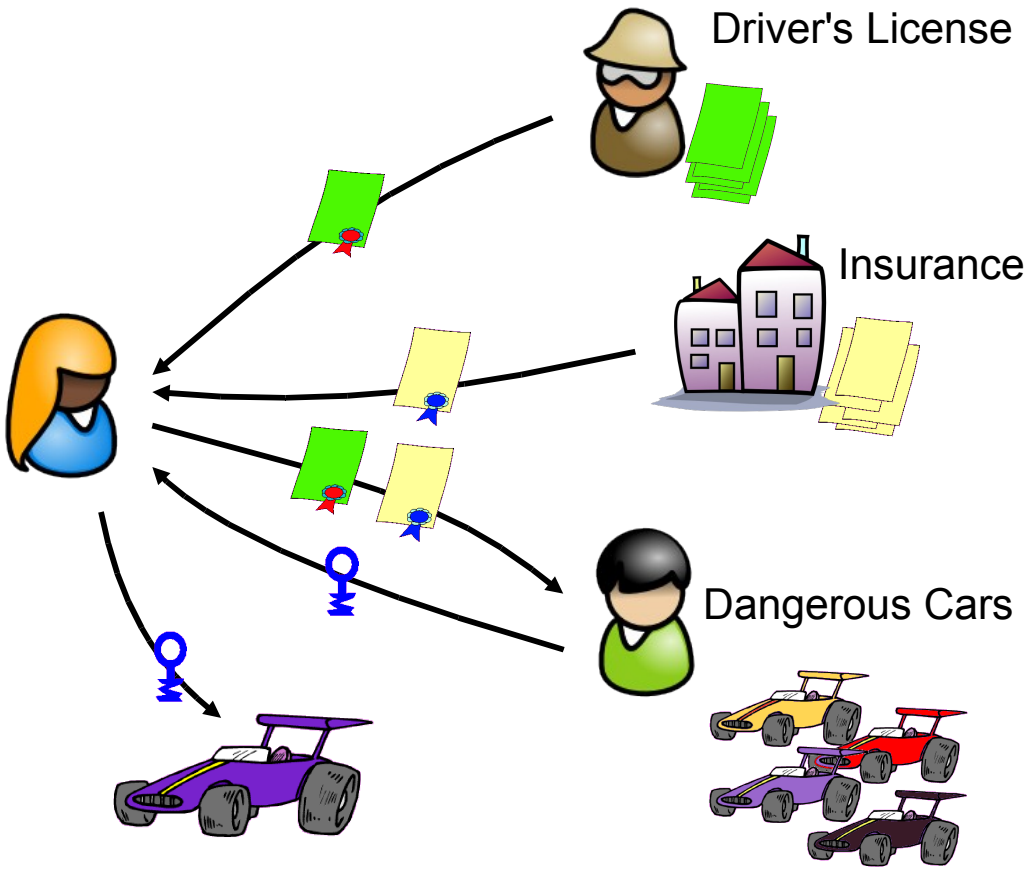
Social Networks

- Who should be able to see what?
- How should they treat that information?
- Basic Solution: Access control
  - How to set policies?
  - Maybe: grouping users & data
  - How to enforce it?
    - Encryption
    - P2P

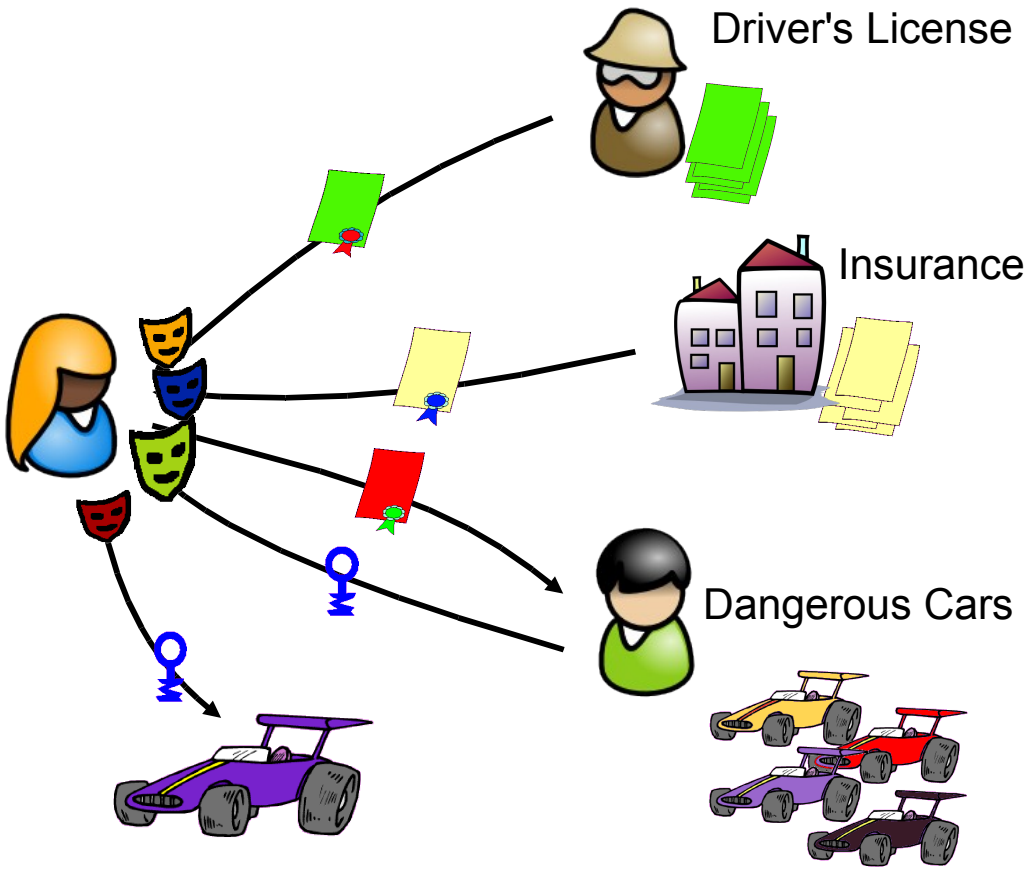
Privacy @ ID Layer

A Closer Look & Solutions

Digital Credentials

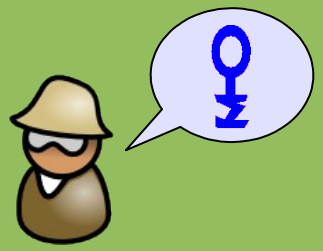


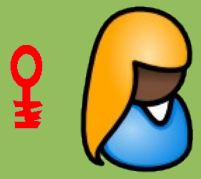
Solution: Private Digital Credentials



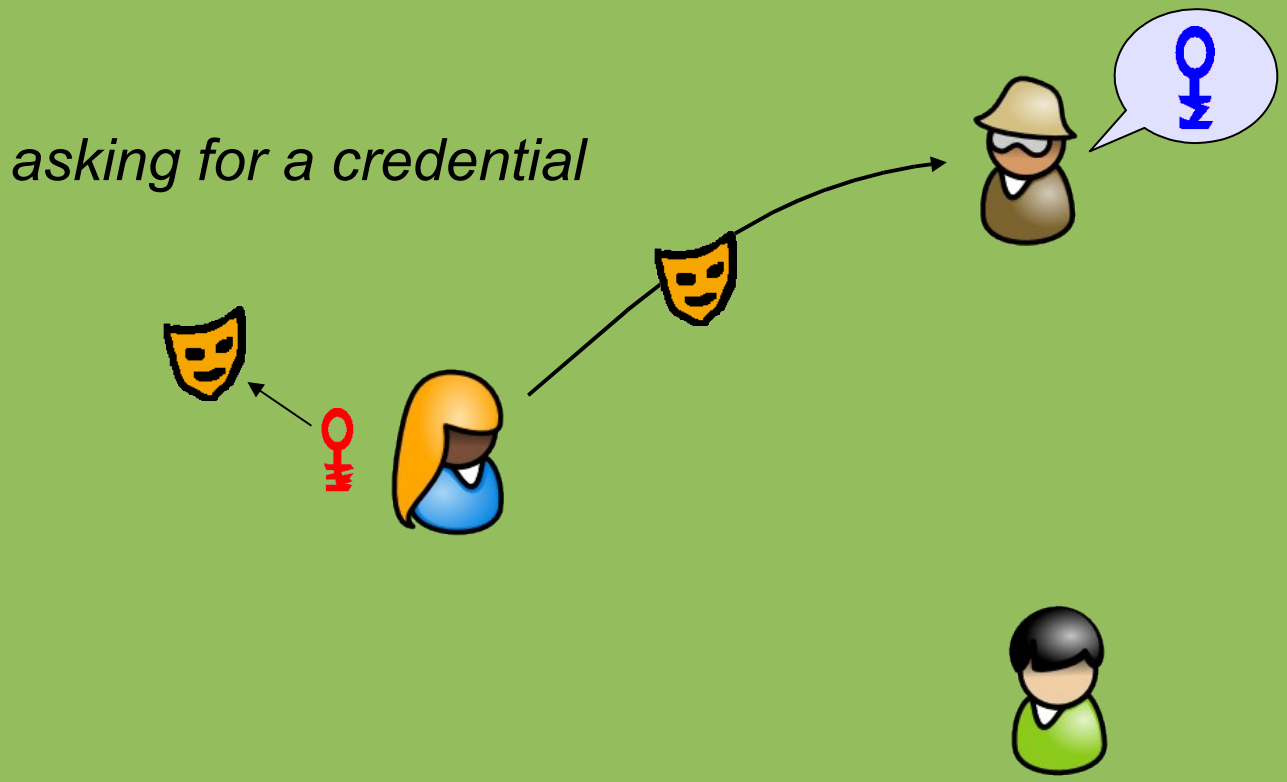
Private Credentials: How to Build Them

In the beginning...

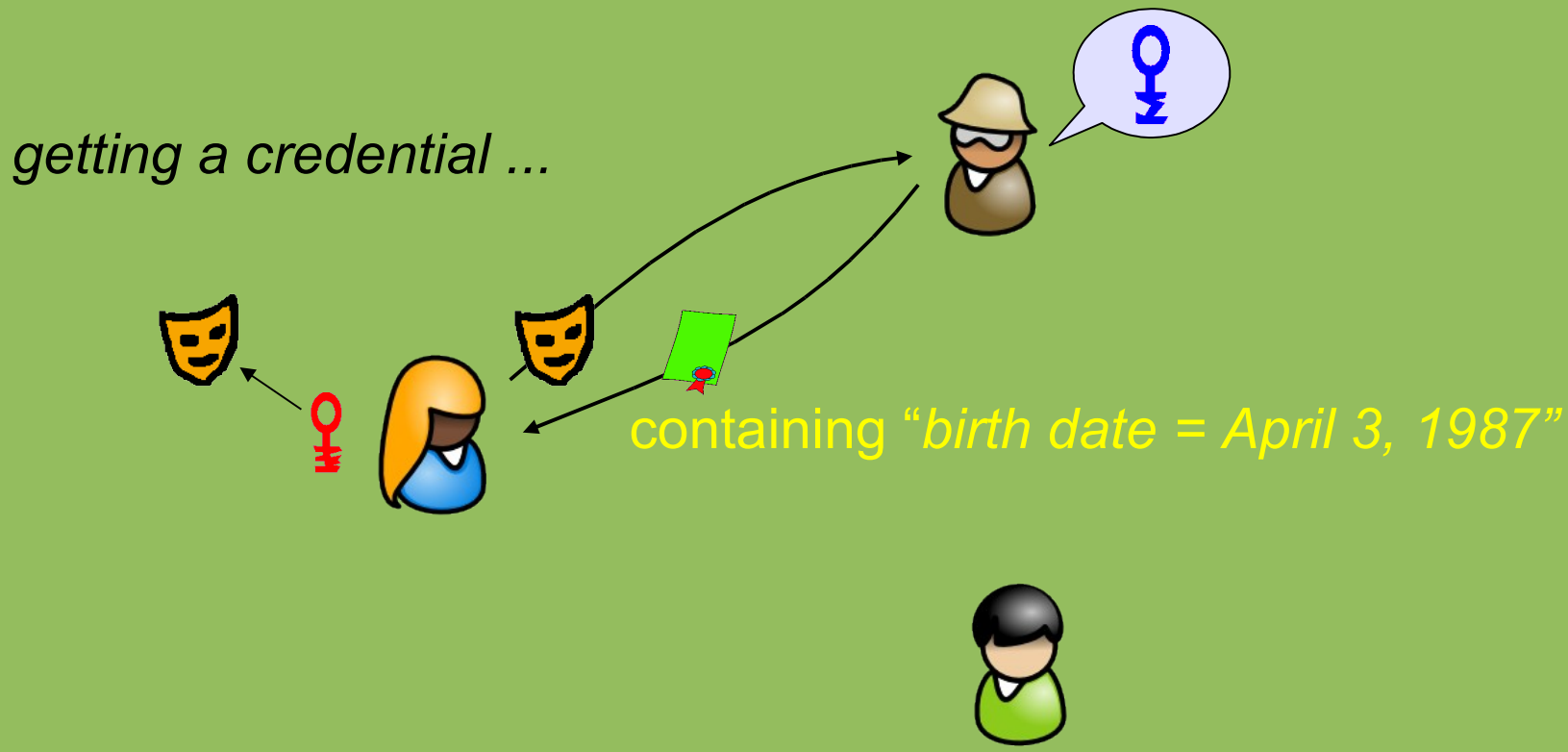




State of the Art: How to Build Them

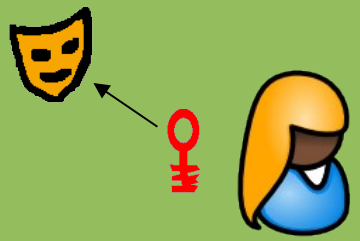


State of the Art: How to Build Them

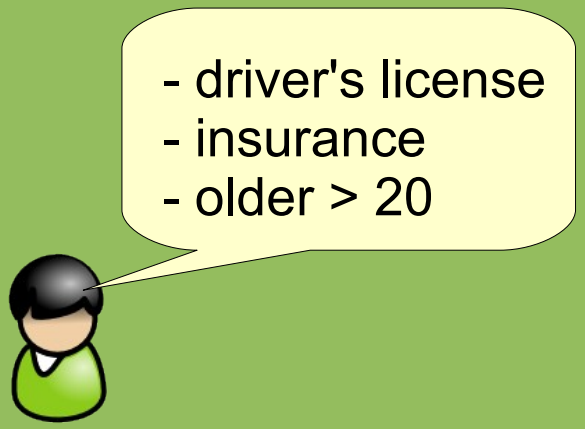


State of the Art: How to Build Them

showing a credential ...

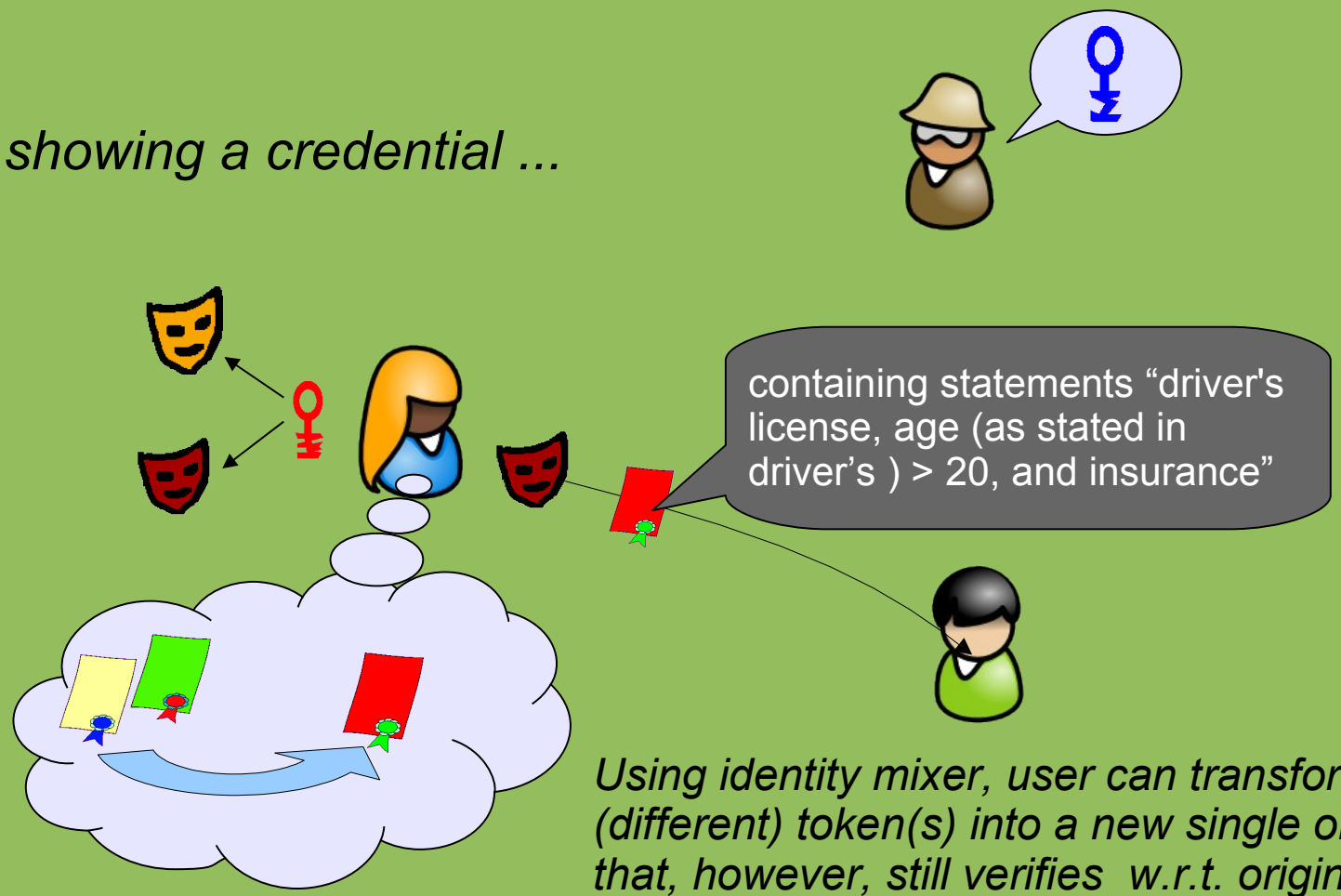


goes off-line



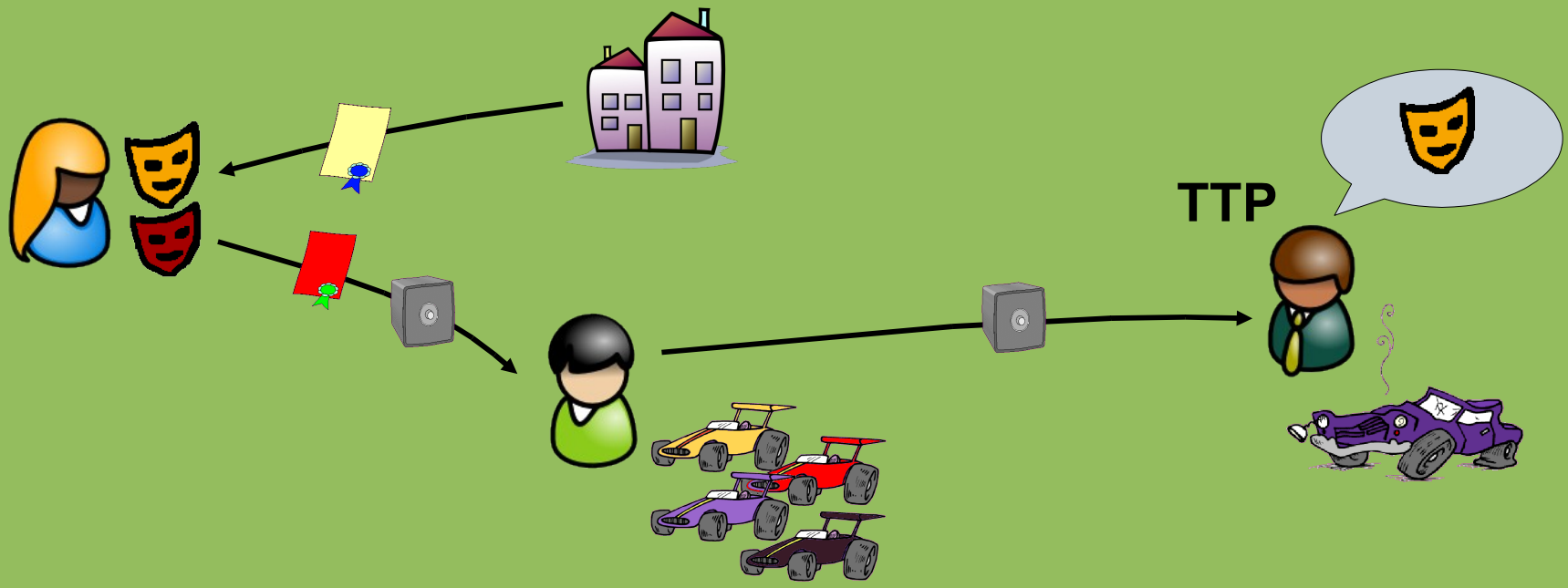
State of the Art: How to Build Them

showing a credential ...



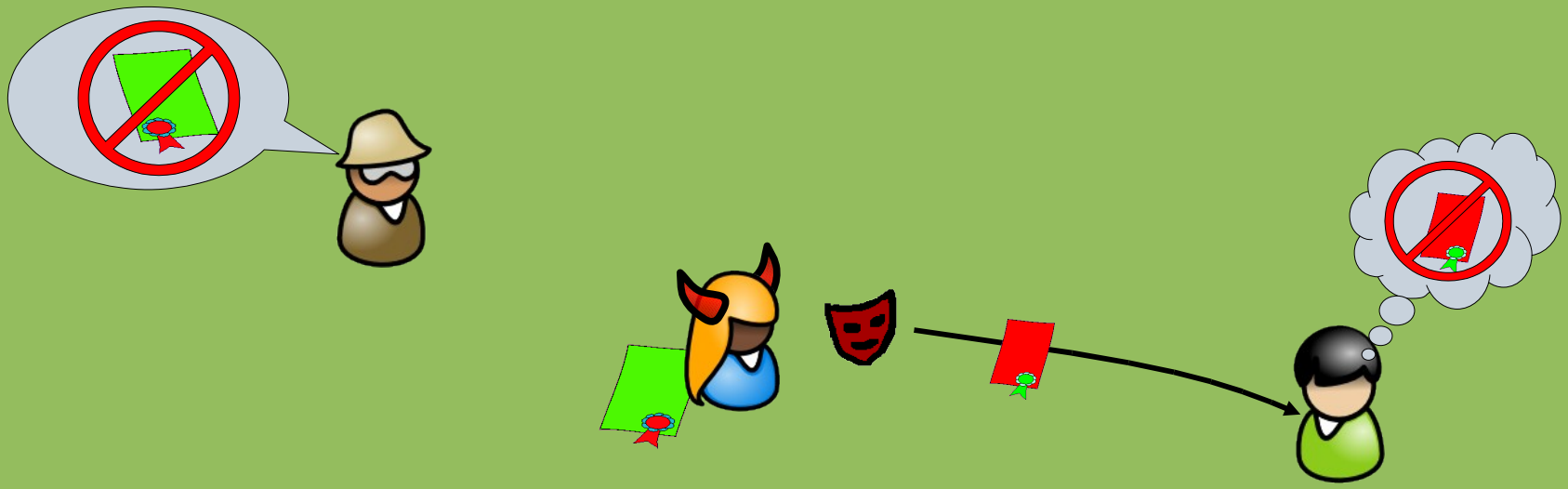
Using identity mixer, user can transform (different) token(s) into a new single one that, however, still verifies w.r.t. original signers' public keys.

Other Properties: Attribute Escrow (Opt-In)



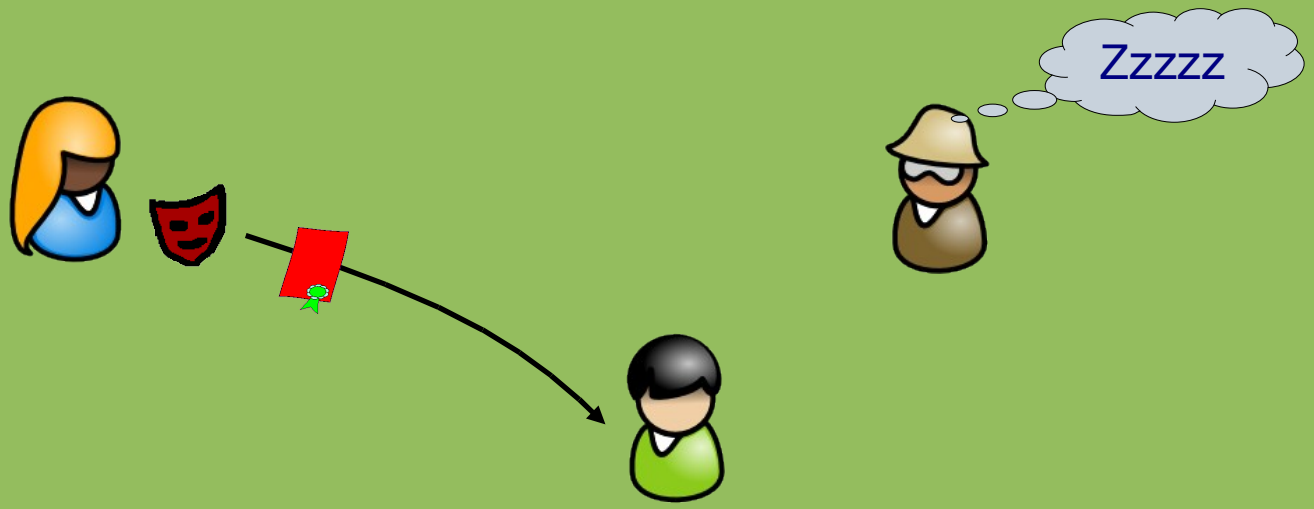
- If car is broken: ID with insurance needs be retrieved
- Can verifiably encrypt any certified attribute *(optional)*
- TTP is off-line & can be distributed to lessen trust

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



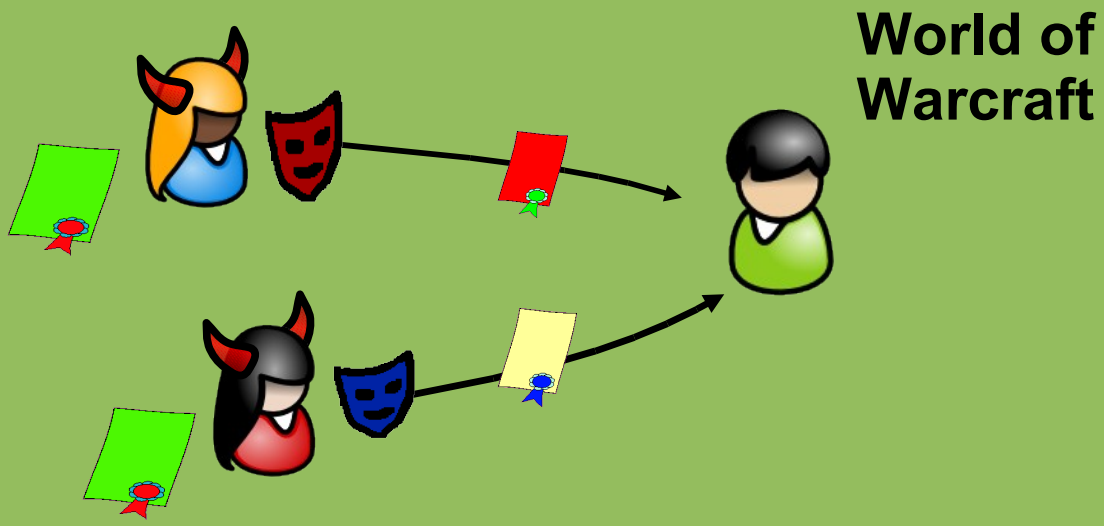
ID providers (issuers) need sleep, too!

- 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)*:

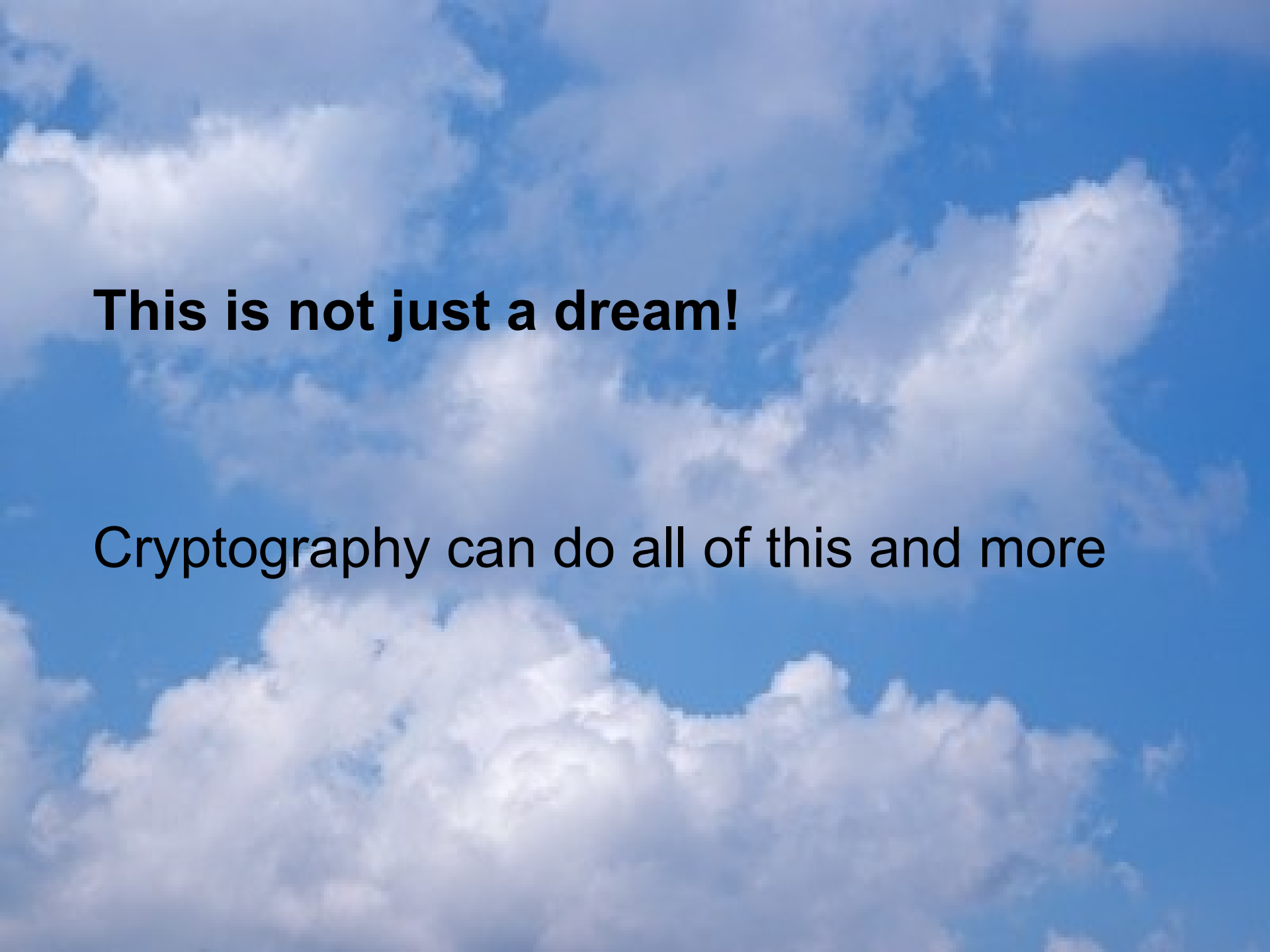
- If Alice and Eve are on-line together they are caught!
- Use Limitation – anonymous until:
  - If Alice used certs > 100 times total...
  - ... or > 10'000 times with Bob
- Alice's cert can be bound to hardware token (e.g., TPM)

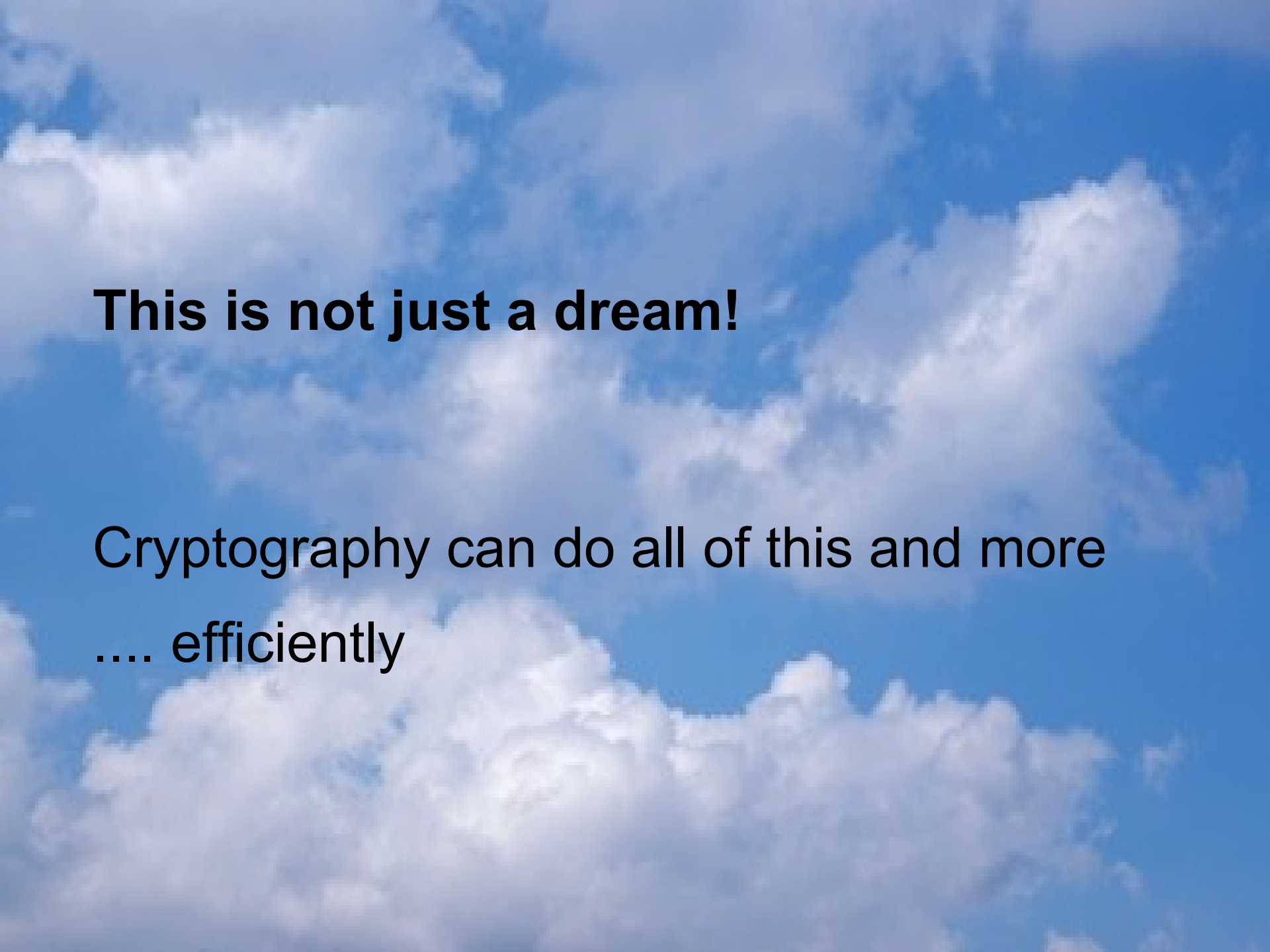
Privacy Preserving Access Control

Oblivious Access to Database

- Server must not learn which record Alice accesses
- Actually, server shall not learn who access a record
- Still, Alice can access only allowed records


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 :-)

Summary

- Privacy, Identity and Trust Mgmt More Important Than Ever
- Achieving & Maintaining Privacy is Challenging
  - Difficult to build in!
  - New ways to use electronic media – new ways to address privacy
  - Lots of open research questions here
- Lots of Technologies are ready – but need to be used
  - User interfaces, User interfaces, User interfaces, User interfaces
  - Policies
  - Infrastructure
  - Need to change Applications & Business processes
  - Do it better for Internet 2 :-)


Let's Make it Real!

info@primelife.eu

www.primelife.eu

(www.prime-project.eu)

www.zurich.ibm.com/idemix



iNetSec 2009

Open Research Problems in Network Security

23-24 April 2009

IBM Research Labs, Zurich, Switzerland

http://www.zurich.ibm.com/inetsec2009/