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

Welcome to PrimeLife's Summerschool

Jan Camenisch
Technical Leader PrimeLife
IBM Research

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

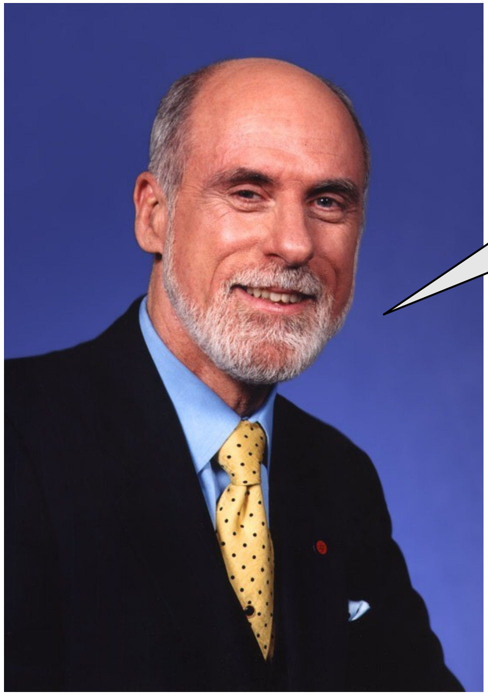
SEVENTH FRAMEWORK PROGRAMME

Part I:
Privacy – What's the Problem

Part II:
PrimeLife's Approach

Part III:
Privacy-Enhancing Cryptography:
Theory & Practice

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

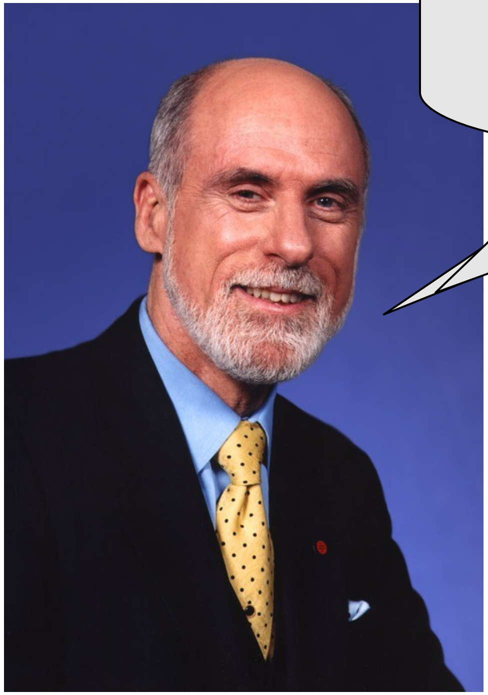


Vint Cerf

“The Internet will be everywhere, from

tellar

“The Internet needs to have an secure identity layer”

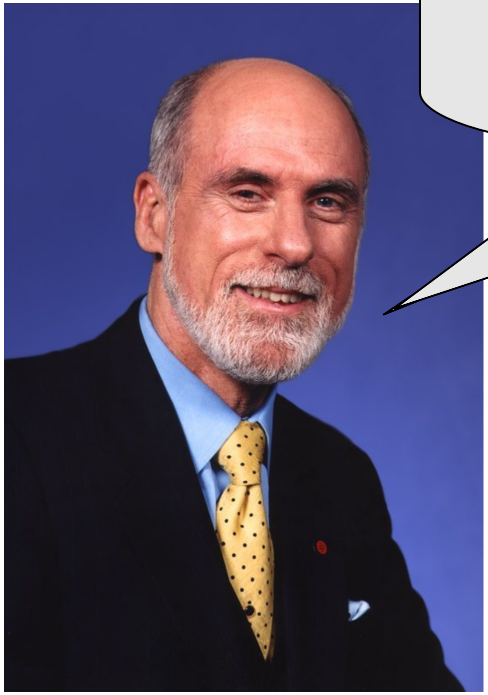


Vint Cerf

“The Internet will be everywhere, from
tellar

“The Internet needs to have an

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

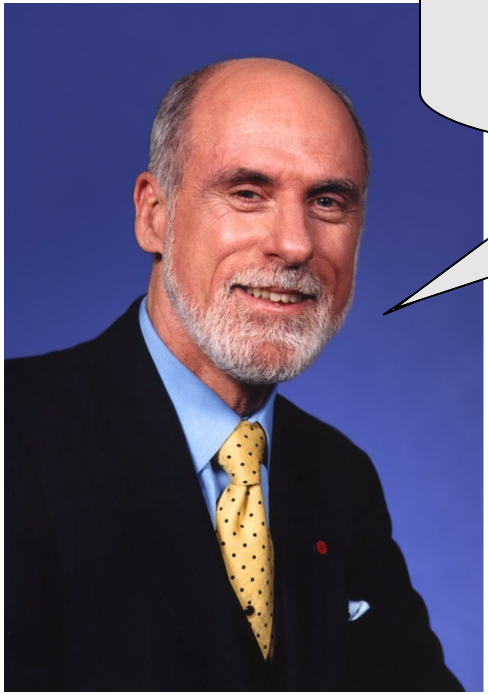


Vint Cerf

“The Internet will be everywhere, from
tellar

“The Internet needs to have an

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



Vint Cerf

“...at the *same* time!”

A Surfer

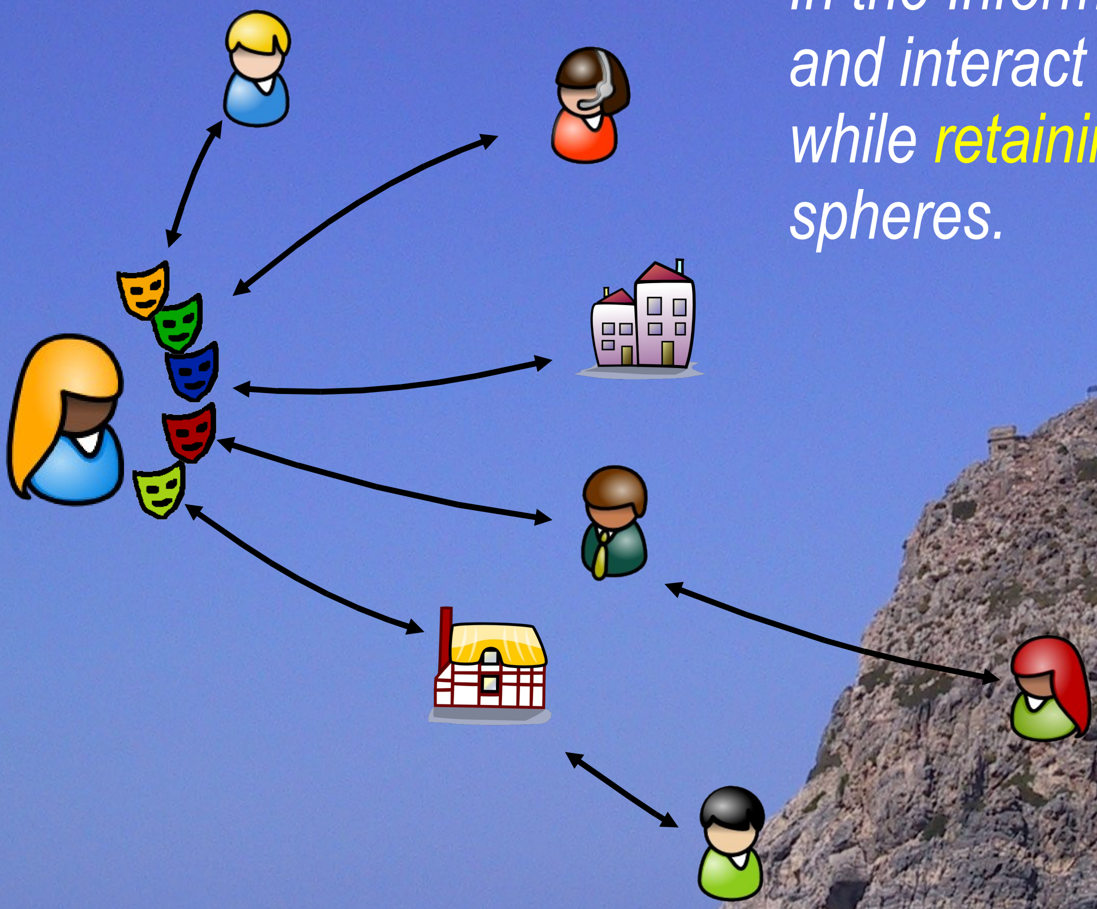
It's Not Just the Internet...

...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
SIGNATURE
DATE OF BIRTH 16-09-84
SERIAL NUMBER ISSUE CENTRE CODE REF
34545 4545676-4555554

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"

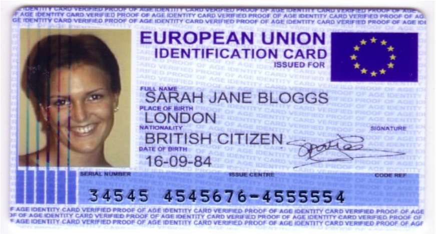
(Robin Wilton, Sun Microsystems)

Photo:cc-nc-by jahdakine

Computers don’t forget

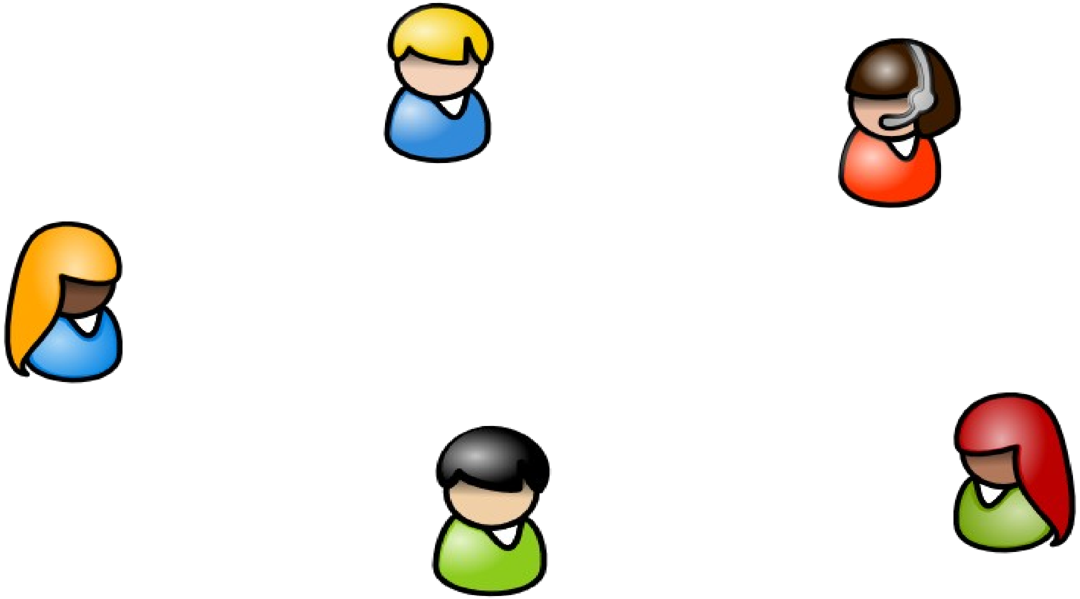
- Storage becomes ever cheaper
- Data mining ever better

Not only the tokens and devices..

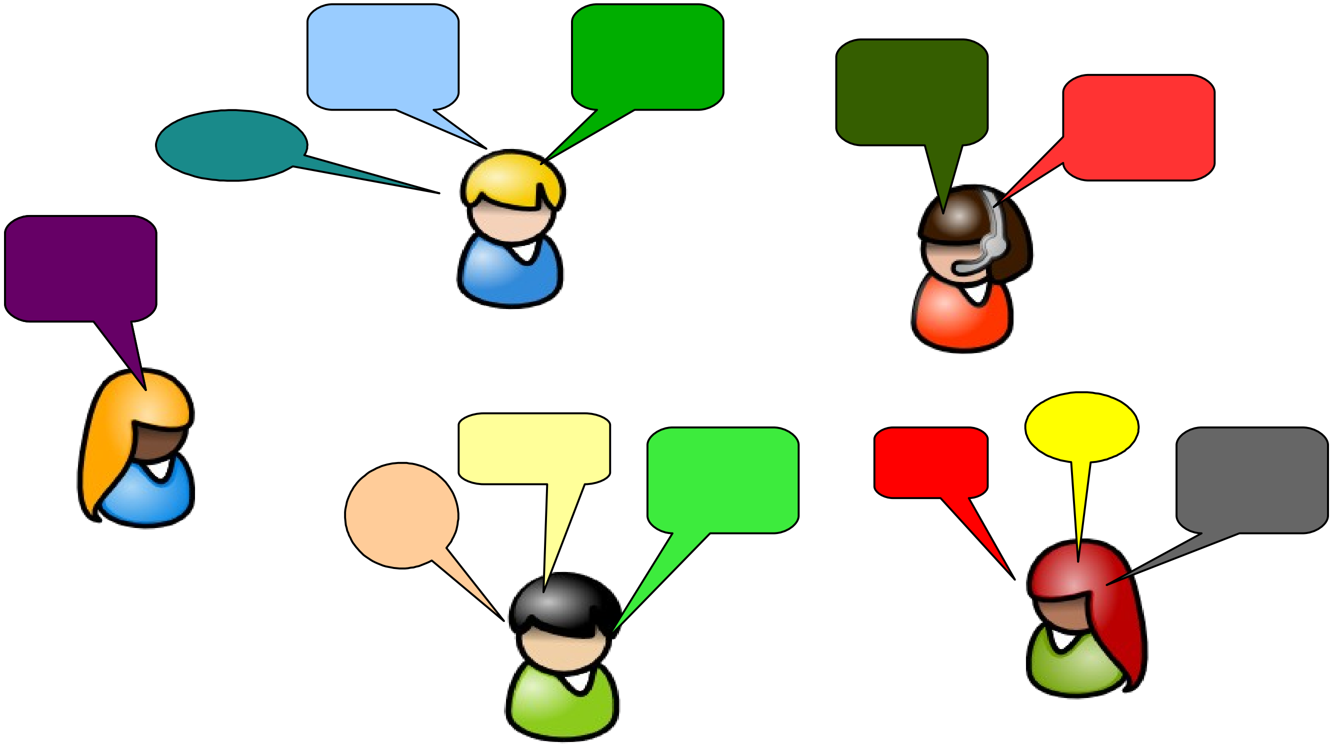


EUROPEAN UNION
IDENTIFICATION CARD
ISSUED FOR
FULL NAME SARAH JANE BLOGGS
PLACE OF BIRTH LONDON
NATIONALITY BRITISH CITIZEN
SIGNATURE
DATE OF BIRTH 16-09-84
SERIAL NUMBER ISSUE CENTRE CODE REF
34545 4545676-4555554

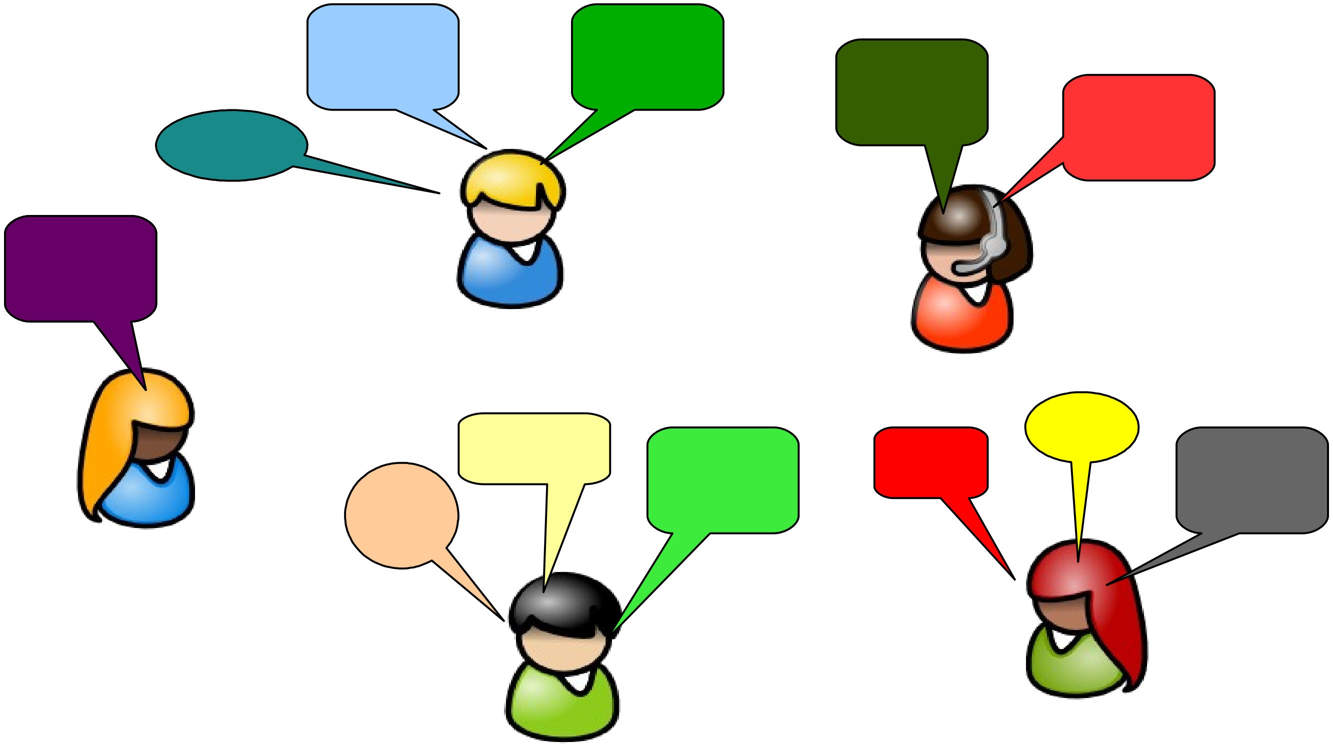
People



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

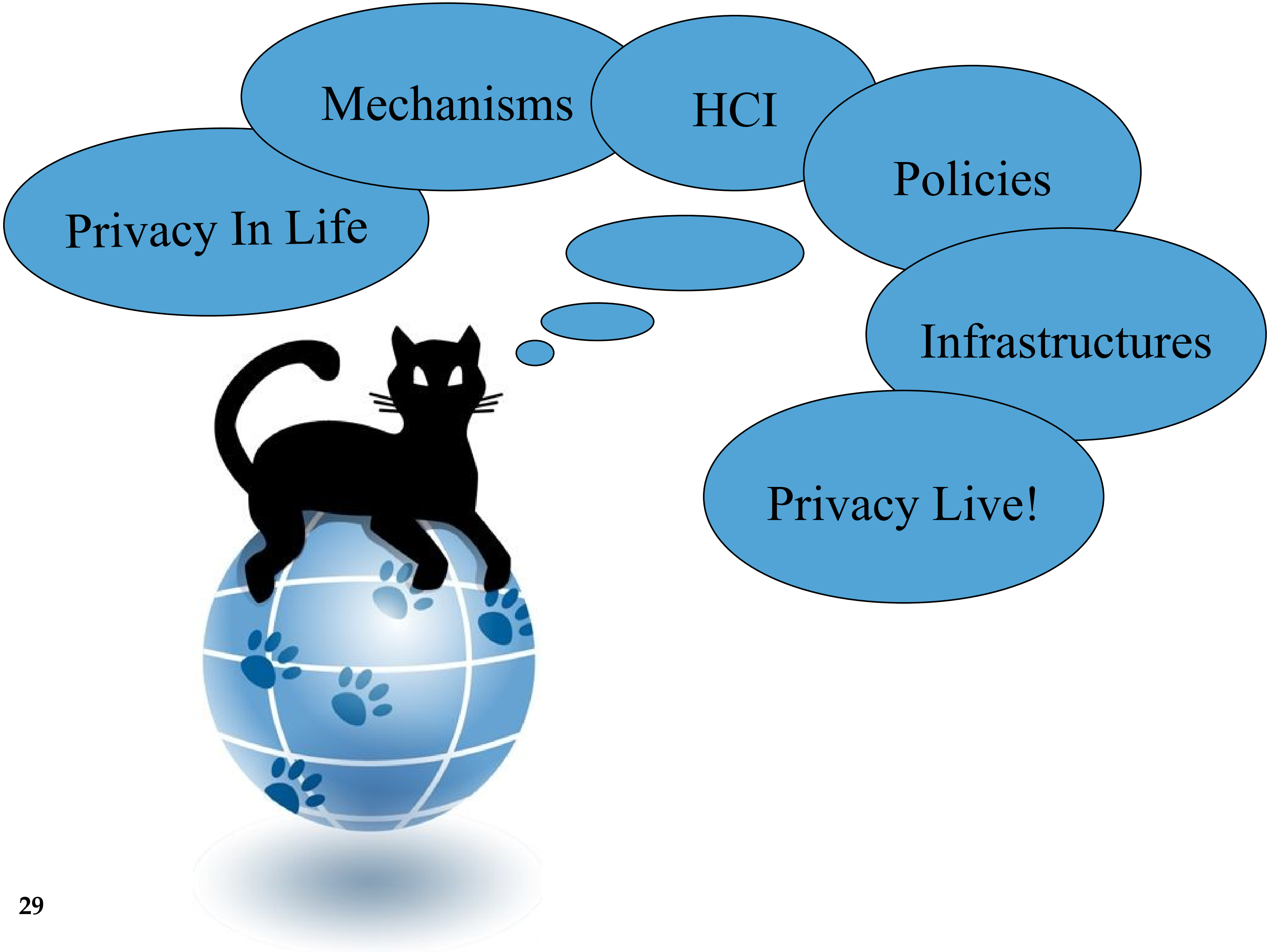
Part II
PrimeLife's Approach

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.**

Part III
Privacy-Enhancing Cryptography
Theory & Practice

What Can Crypto Do For Us?

David, please help!?

Oblivious Transfer

Mix Networks

Onion Routing

Confirmer signatures

Anonymous Credentials

Pseudonym Systems

OT with Access Control

Group signatures

e-voting

Priced OT

Blind signatures

Private information retrieval

Secret Handshakes

Disclaimer: there's too many researchers and paper to call for help to cite them all.....

PETs Can Help! - A More Structured Approach

Privacy, Identity, and Trust Mgmt Built-In Everywhere!

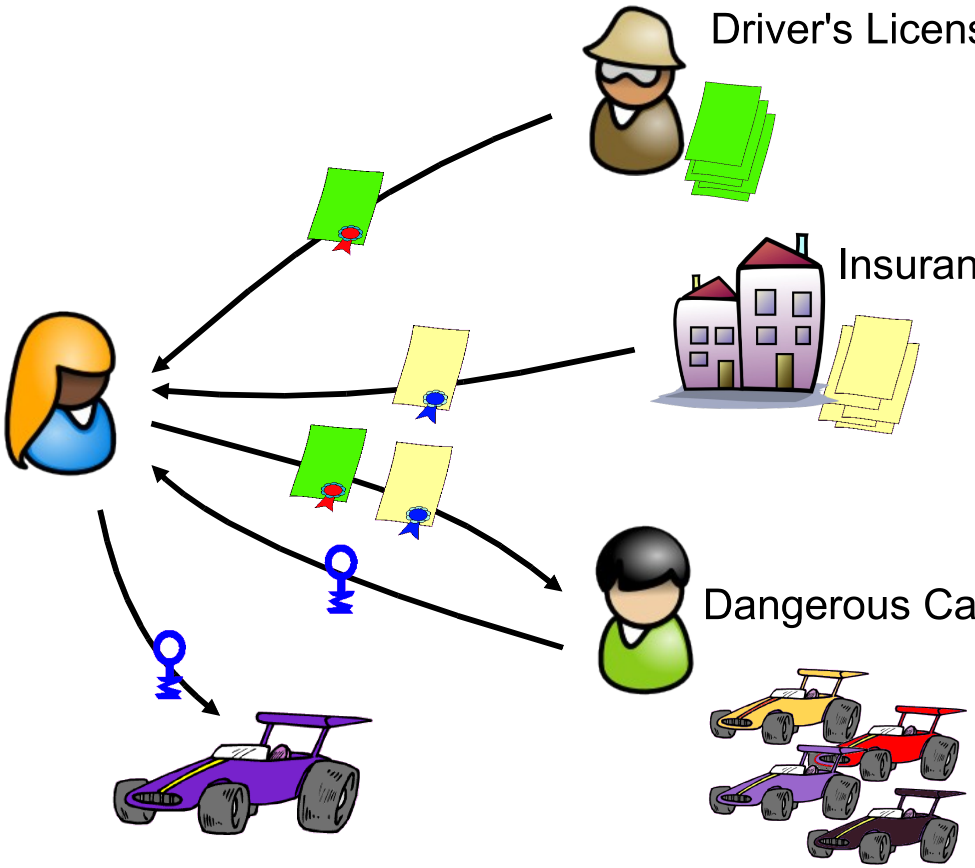
- Network Layer Anonymity
  - ... in mobile phone networks
  - ... in the Future Internet as currently discussed
  - ... access points for ID cards
- Identification Layer
  - Access control & authorization
- Application Layer
  - “Standard” e-Commerce
  - Specific Apps, e.g., eVoting, OT, PIR, ...
 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

What PETs Can Do

The Identification Layer

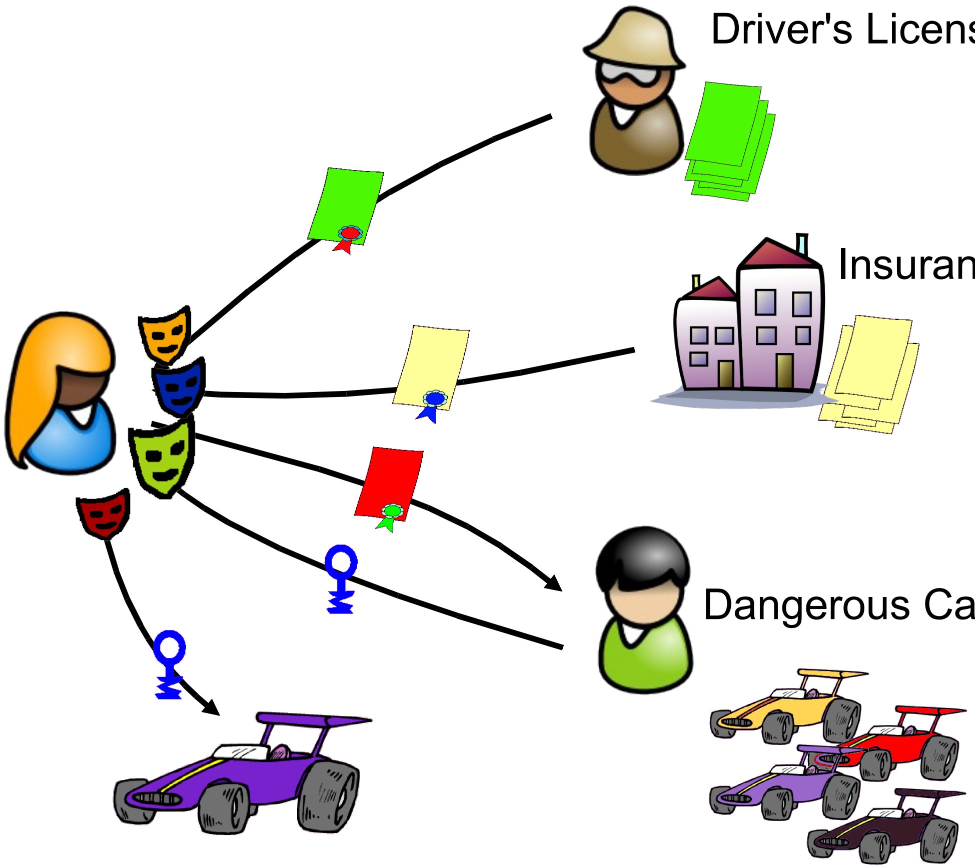
Digital Credentials

... or transmitting certified information



Solution: Private Digital Credentials

[Chaum, Damgaard, Brands,....]



Driver's License

Insurance

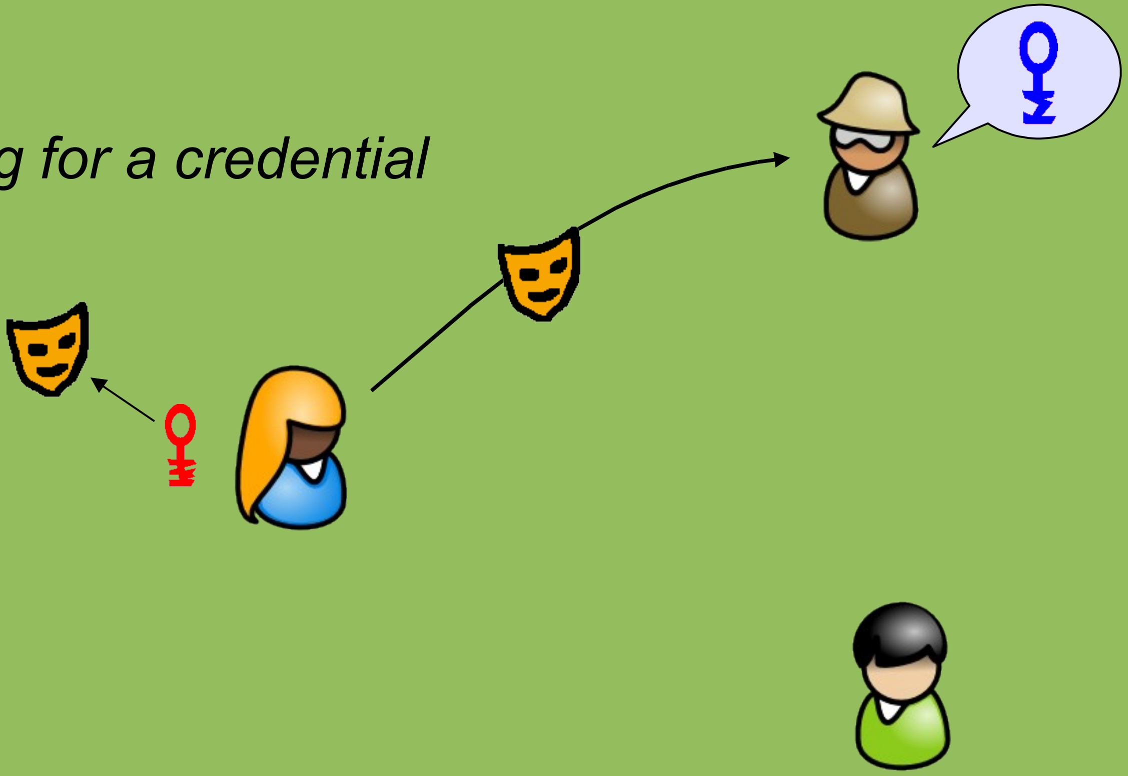
Dangerous Cars

Private Credentials: How to Build Them

In the beginning...

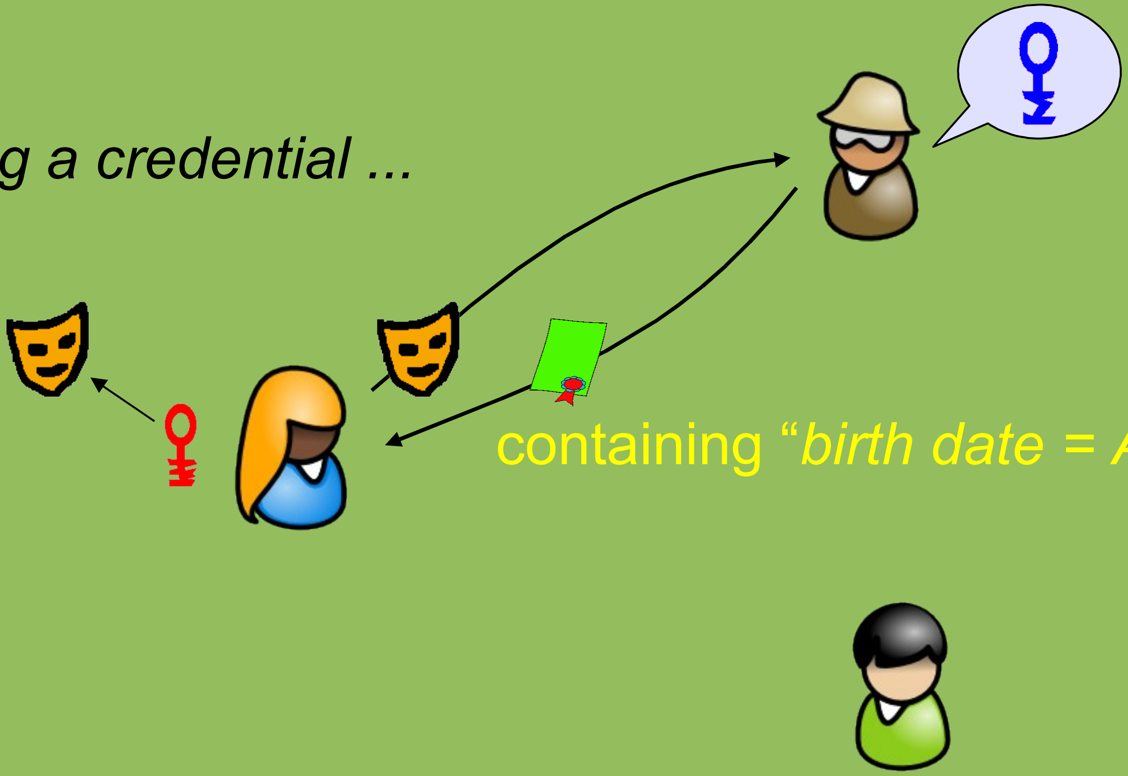
State of the Art: How to Build Them

asking for a credential



State of the Art: How to Build Them

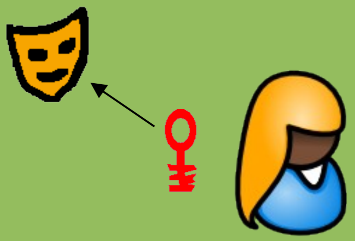
getting a credential ...



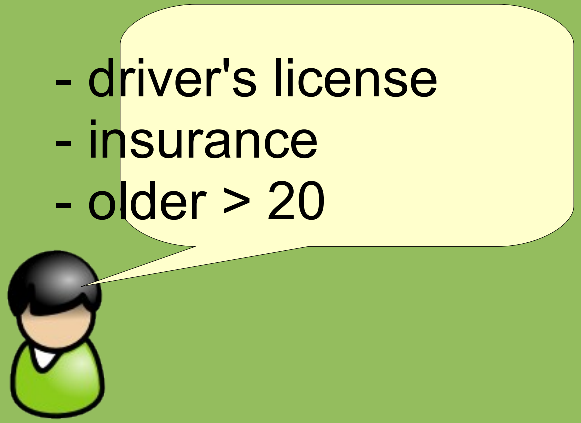
containing “*birth date = April 3, 1987*”

State of the Art: How to Build Them

showing a credential ...



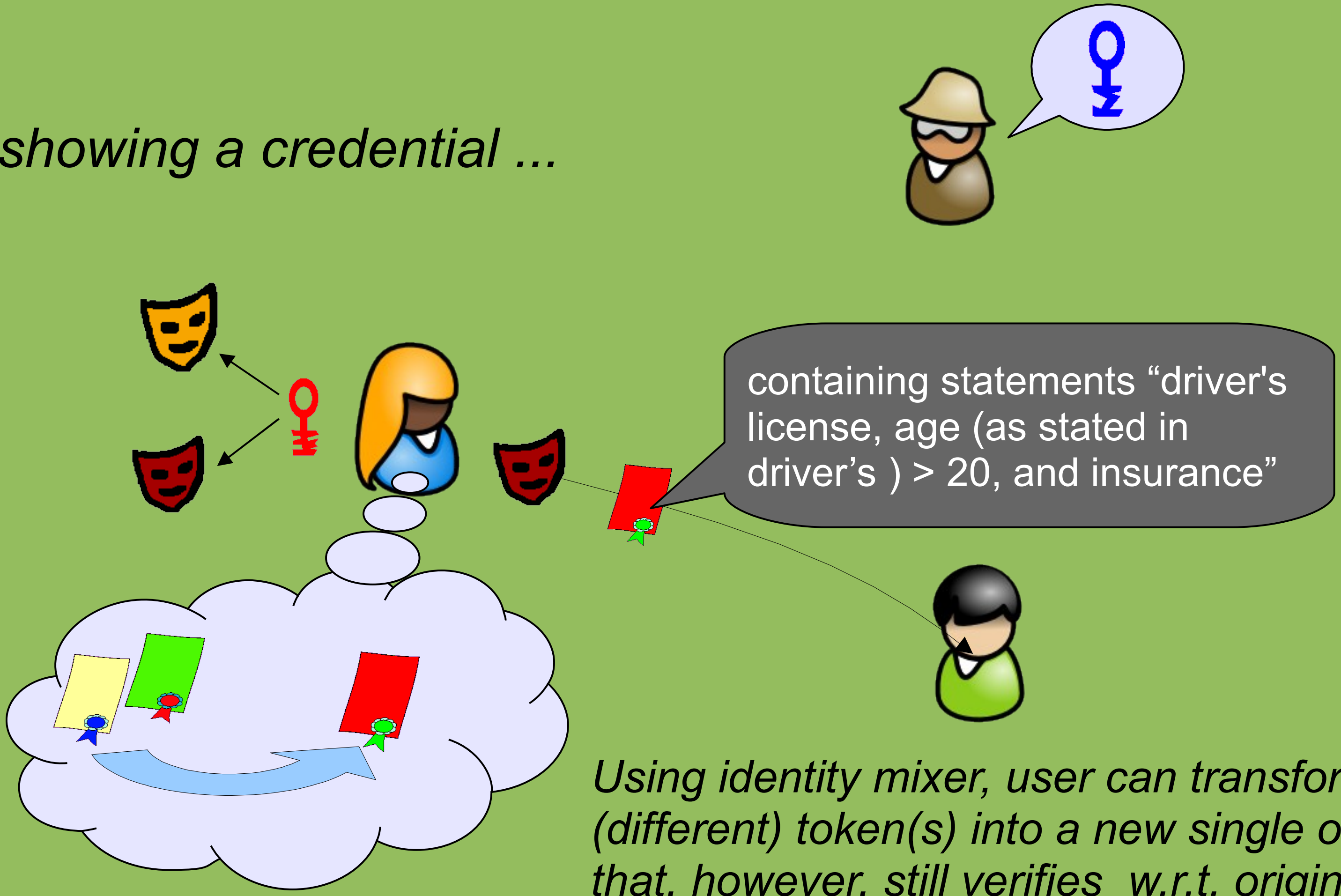
goes off-line



- driver's license
- insurance
- older > 20

State of the Art: How to Build Them

showing a credential ...

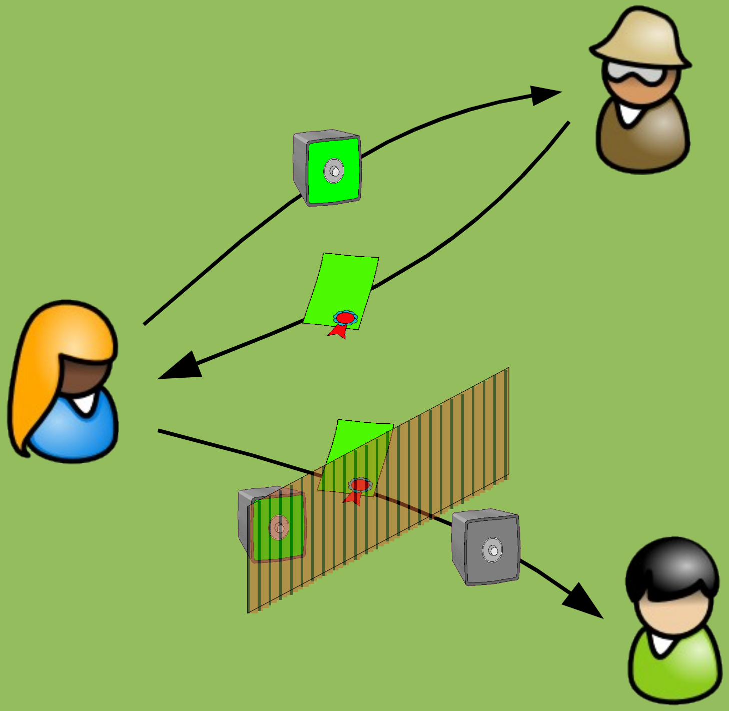


containing statements "driver's license, age (as stated in driver's) > 20, and insurance"

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.

Two Approaches

ZK Proofs

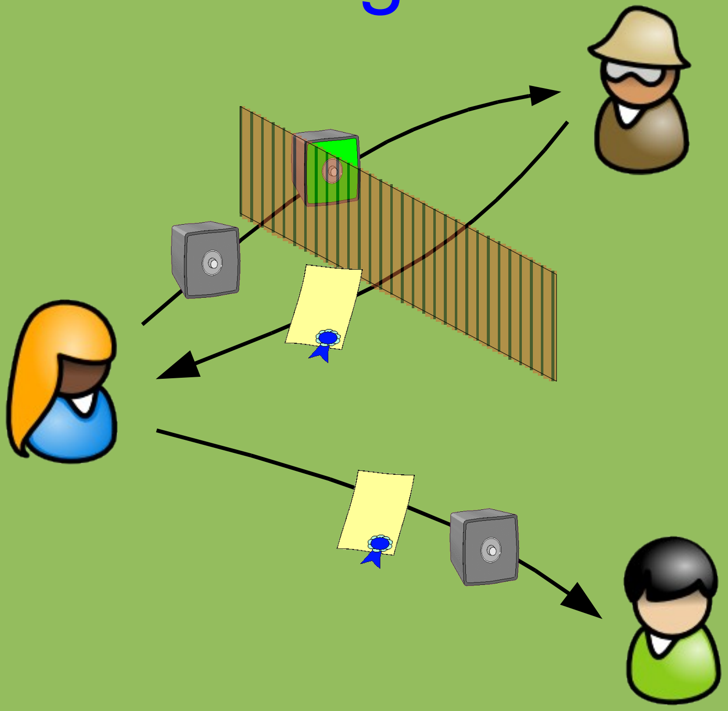


can be used multiple times

Damgaard,Camenisch&Lysyanskaya

Strong RSA, DL-ECC,..

Blind Signatures

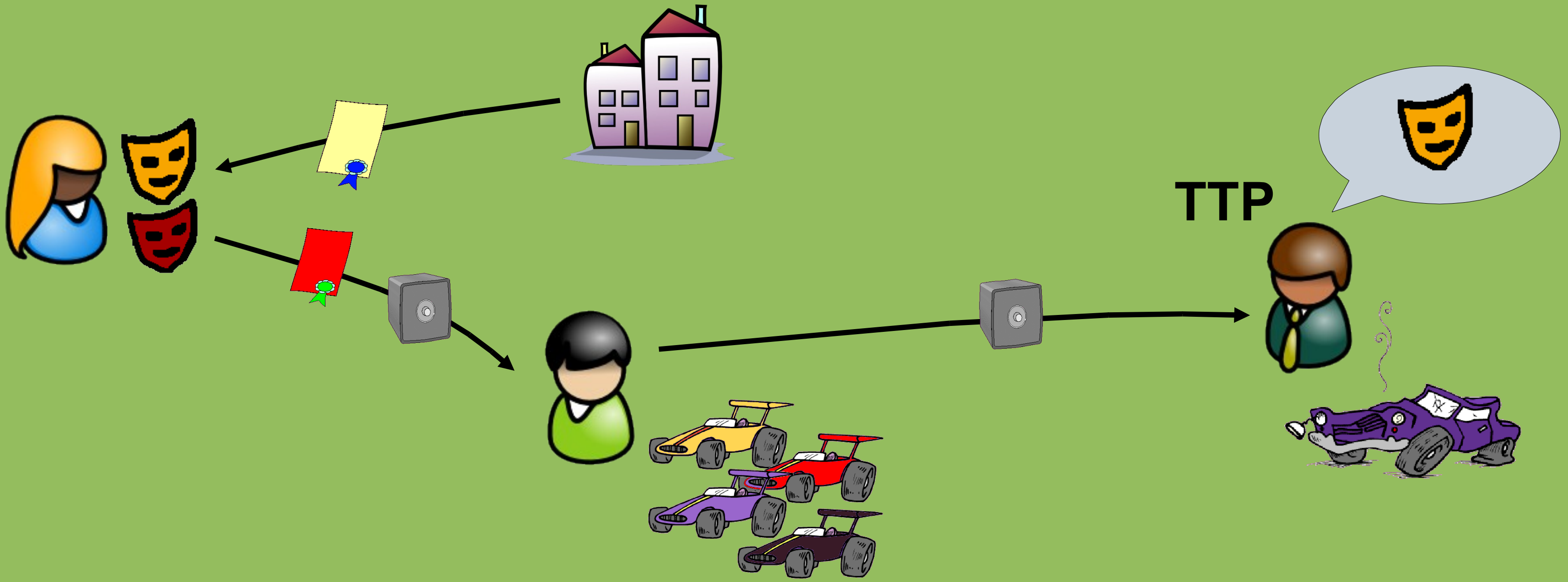


can be used only once

Chaum, Brands, et al.

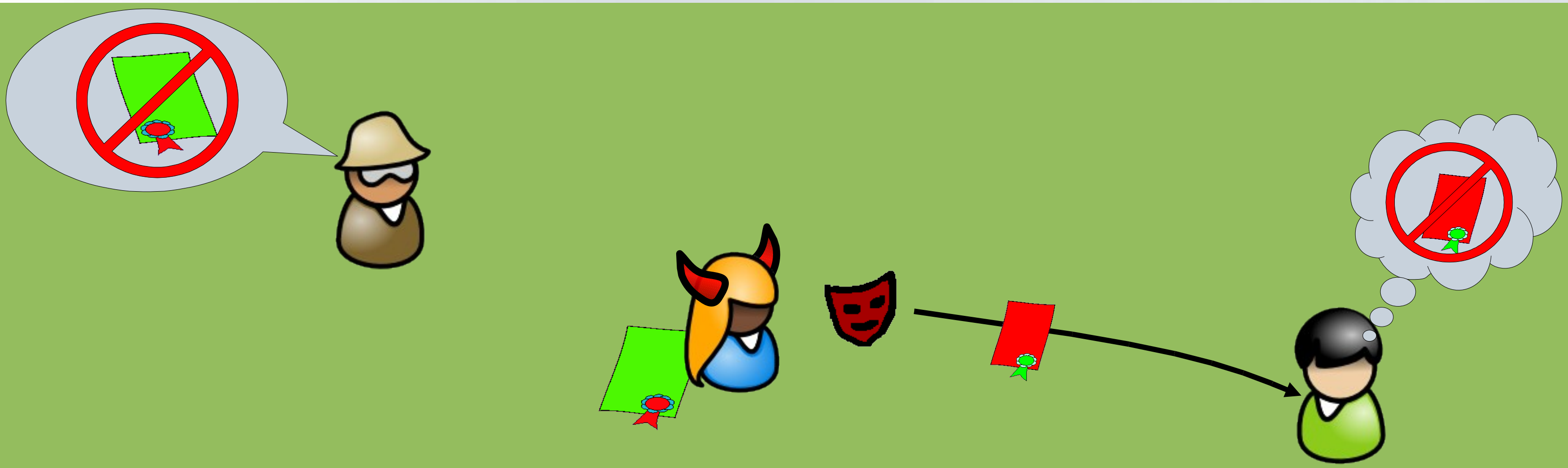
Discrete Logs, RSA,..

Other Properties: Attribute Escrow (Opt-In)



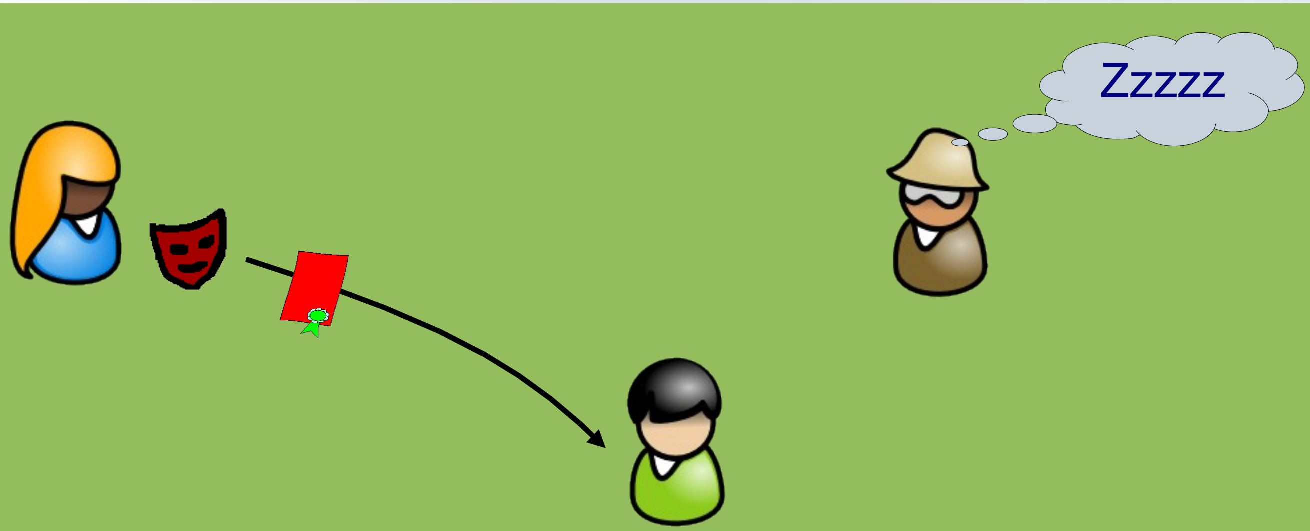
- If car is broken: ID with insurance needs be retrieved
- Can verifiably encrypt any certified attribute *(optional)*
- TTP is off-line & can be distributed to lessen trust

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)
    - Accumulators
    - Signing entries & Proof, ...
  - Limited validity – certs need to be updated
  - ... For proving age, a revoked driver's license still works

Other Properties: Offline Usage



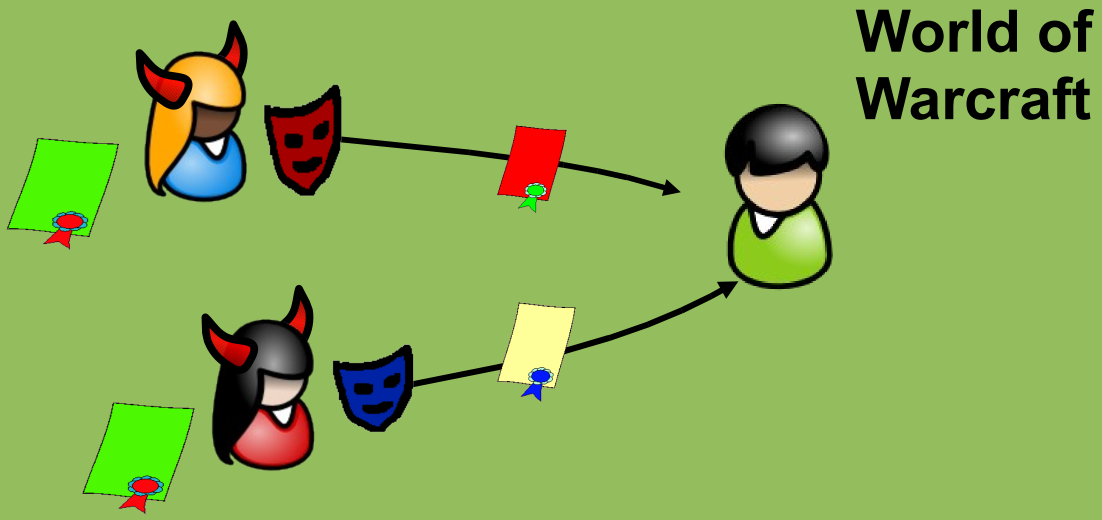
ID providers (issuers) need sleep, too!

- 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

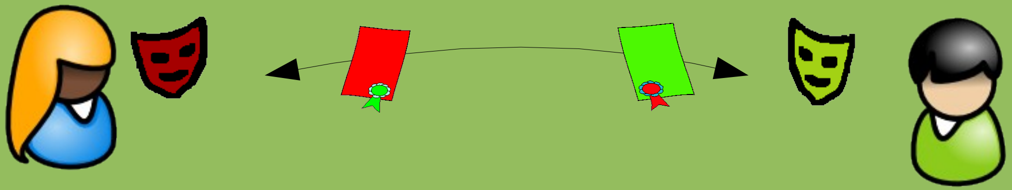
DNA Database

Simple case: DB learns not who accesses DB

Better: Oblivious Access to Database (OT with AC)

- Server must not learn *who* accesses
- *which* record
- Still, Alice can access only records she is *authorized* for

Secret Handshakes



- Alice and Bob both define some predicate PA and PB
- Alice learns whether Bob satisfies PA if she satisfies PB

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   :-)

And in Practice?

- Awareness is raising, still! :-)
- “Products”
  - Anonymous Communication
    - TOR,
    - JAP, ...
  - Private Authentication (Credentials)
    - Direct Anonymous Attestation (2004)
    - Microsoft's U-Prove (soon in CardSpace); IBM Identity Mixer (available for free)
  - Other than that?
    - A few prototypes
      - auctions,...
    - A few things w/out crypto
      - Polices and TTPs

What's Left to Do?

Next Steps Towards Practice and Research

- Lots of technologies are ready – but need to be made usable
  - Standards
    - User interfaces
    - Policies
    - Infrastructure
  - Need to change Applications & Business processes
  - Do it better for Internet 2 :-)
- Research
  - User interfaces, User interfaces, User interfaces
  - Policies
  - Key & ID Management (Infrastructure, back-ups...)
  - and of course crypto ....

...and Still Lots of New Crypto Needed

- More efficient primitives
  - Smaller footprints as to fit into all the sensors, cars, ...
  - Faster generation & verification of signatures, ...
  - Maybe using combination of HW security and crypto

- New primitives & PET solutions for applications
  - Location based services
  - Social networks

- Lots of Remaining Hard Problems
  - Revocation of Credentials
  - Finding the right security model and meeting it (UC Framework?)

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