PrimeLife

Privacy & ID Management Cryptographic Challenges

Jan Camenisch

Technical Leader, PrimeLife
Member, IBM Academy of Technology
IBM Research – Zurich

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

Where are we going?

Our world is becoming

INSTRUMENTED

Our world is becoming

INTERCONNECTED

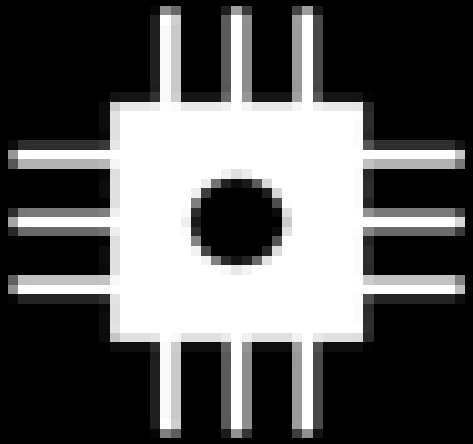
Virtually all things, processes and ways of working are becoming

INTELLIGENT

Social life is becoming highly

INTERACTIVE

Where are we going?



INSTRUMENTED

We now have the ability to measure, sense and see the exact condition of everything.

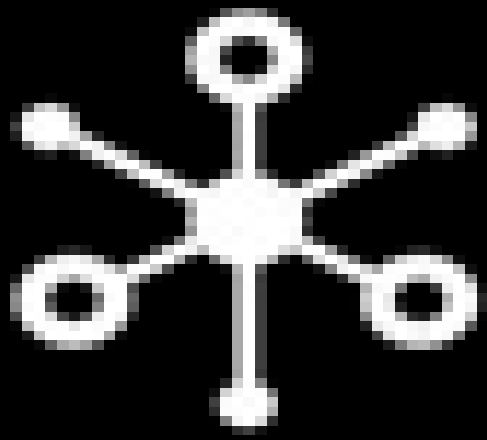
Today, there are 1 billion transistors for each person on the planet.[1]

By 2010, 30 billion RFID tags will be embedded into our world and across entire ecosystems.[1]

Everything will become instrumented: supply chains, healthcare networks, cities and even natural systems like rivers.

[1] Sam Palmisano speech, November 12, 2008

Where are we going?



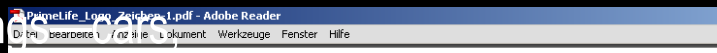
INTERCONNECTED

People, systems and objects can communicate and interact with each other in entirely new ways.

The internet of people is 1 billion strong. Almost one third of the world's population will be on the web by 2011.[1]

There will be nearly 4 billion mobile phone subscribers worldwide by the end of 2008.[1]

The Internet of thin
appliances, cameras
pipeline, pharmaceu
livestock—is headed



Where are we going?

INTELLIGENT

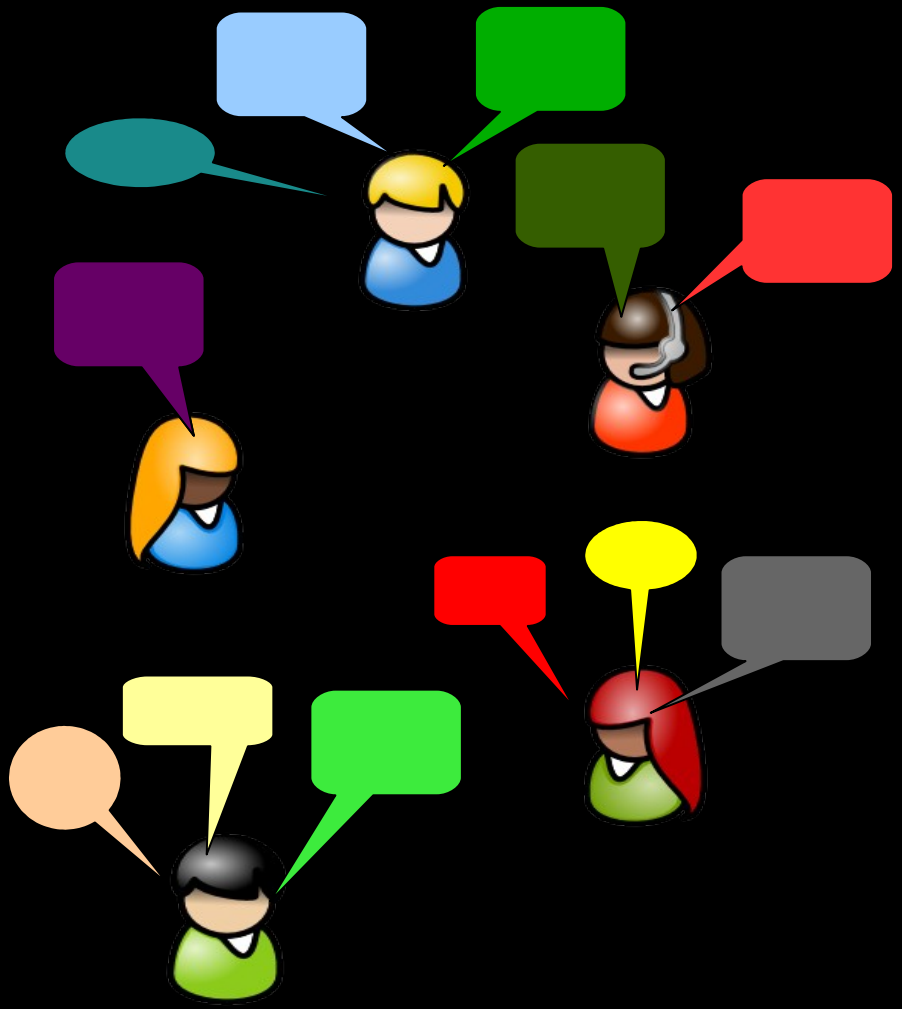
We can respond to changes quickly and accurately, and get better results by predicting and optimizing for future events.

Every day, 15 petabytes of new information are being generated. This is 8x more than the information in all U.S. libraries.[1]

An average company with 1,000 employees spends $5.3 million a year to find information stored on its servers.[1]

New computing models manage the massive amounts of data generated by the proliferation of end-user devices sensors, and actuat advanced analytics, are making us smar

Where are we going?



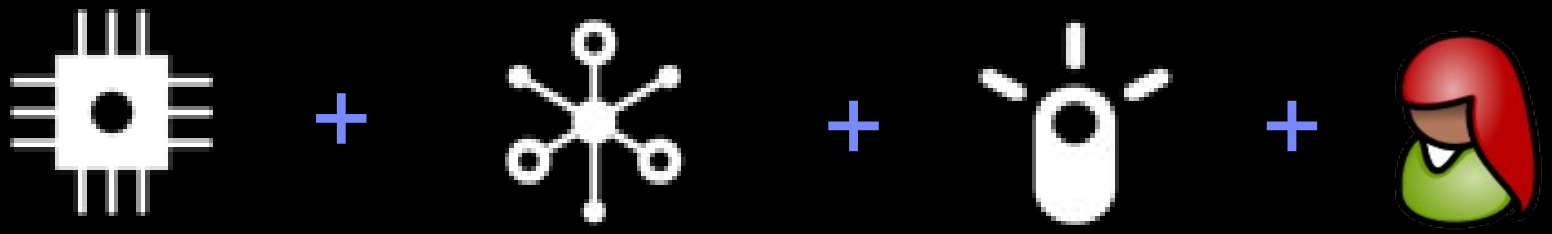
INTERACTIVE

We share information instantly with our friends over the net

Arrange everything last minute & flexible

Rely on our electronic env

Where are we going?



Smarter planet: Thinking, acting, and interacting in new ways with our systems being more efficient, productive and responsive!

.... but this doesn't come

Where are we going?

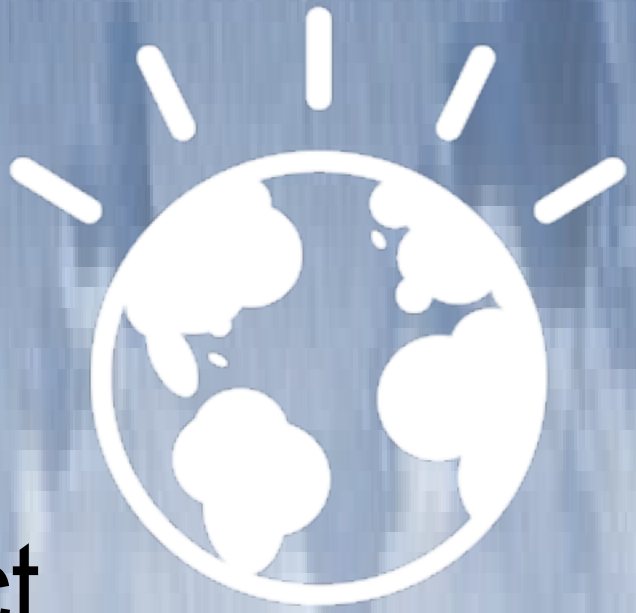
99% OF ALL FINANCIAL ONLINE FRAUD TARGETS THE USA AND EUROPE

INCREASE IN THE NUMBER OF MALICIOUS WEB SITES IN 2008 **50%**

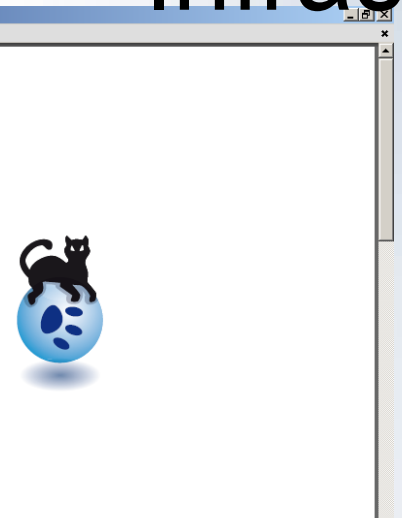
14.5B MESSAGES A DAY ARE CONSIDERED SPAM

IBM Internet Security Systems X-Force® 2008 Trend & Risk Report, http://www.spamlaws.com/spam-stats.html

SECURITY!



Lots of data and
Infrastructure to protect



lots of data & infrastructure to protect

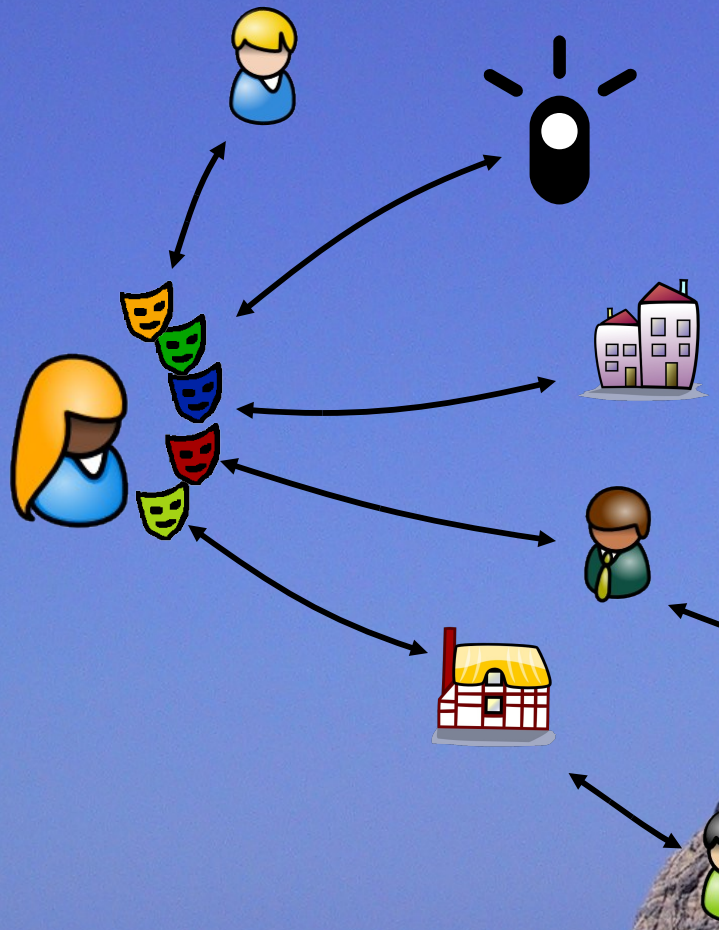
sensor, devices, etc cannot be physically protected!

- authentication of all devices
- authentication of all data

data cannot be controlled!

- minimize (personal) information
- encrypt information
- attach usage policies to each bit

Privacy, Trust and ID Management

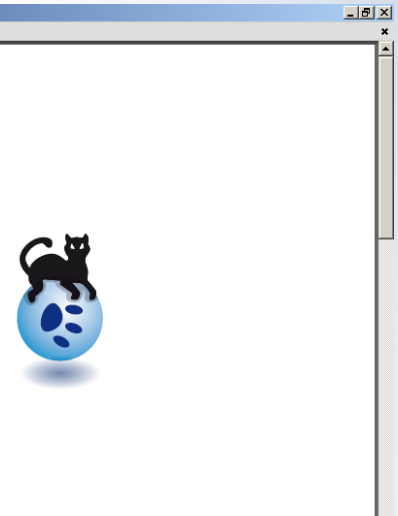


In a smart world, users can act and interact in a safe and secure way while retaining control of their private spheres.

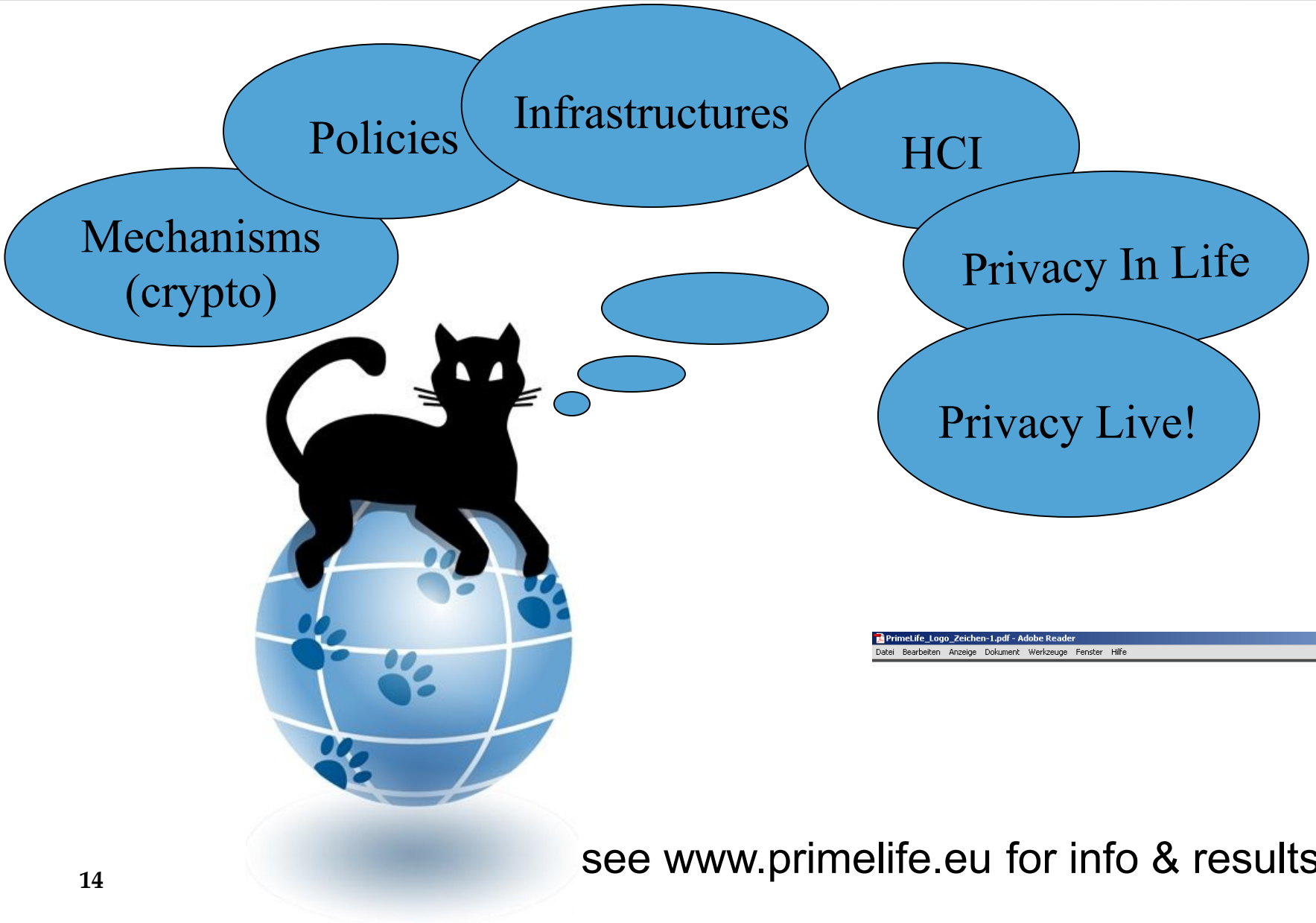
Privacy, Identity & Trust Mgmt Built-In Everywhere!

- Communication Layer Anonymity
  - … in mobile phone networks
  - … in the Future Internet as currently discussed
  - … access points for ID cards
  - … all the sensors etc (depending where they are)
- Identification Layer
  - Access control & authorization to apps and devices etc.
- Application Layer
  - “Standard” e-Commerce
  - Specific Apps, e.g., eVoting, ...
  - Web 2.0, e.g., Facebook & Wikis

PrimeLife's Research and Solution



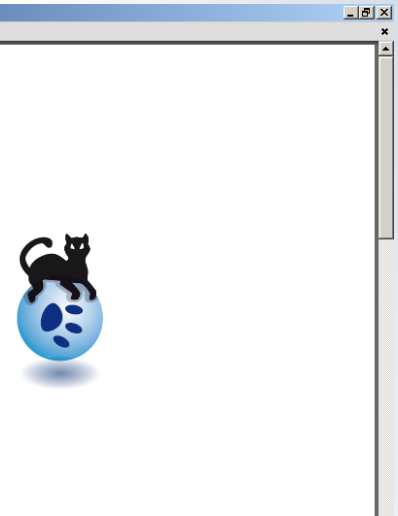
PrimeLife's 6 Activities



see www.primelife.eu for info & results

Privacy & Identity Management

Cryptographic Challenges



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

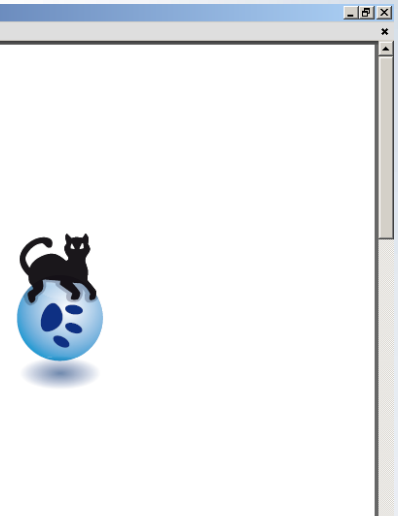
Private information retrieval

Secret Handshakes

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

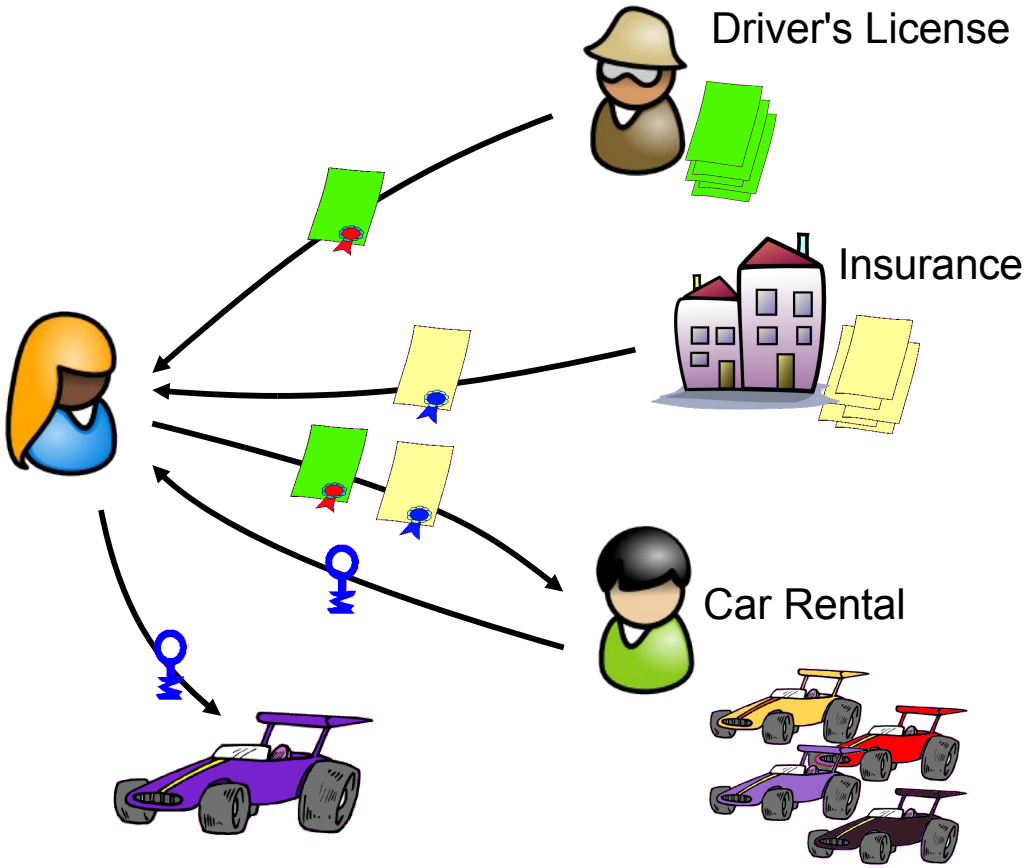
What Crypto Can Do

The Identification Layer



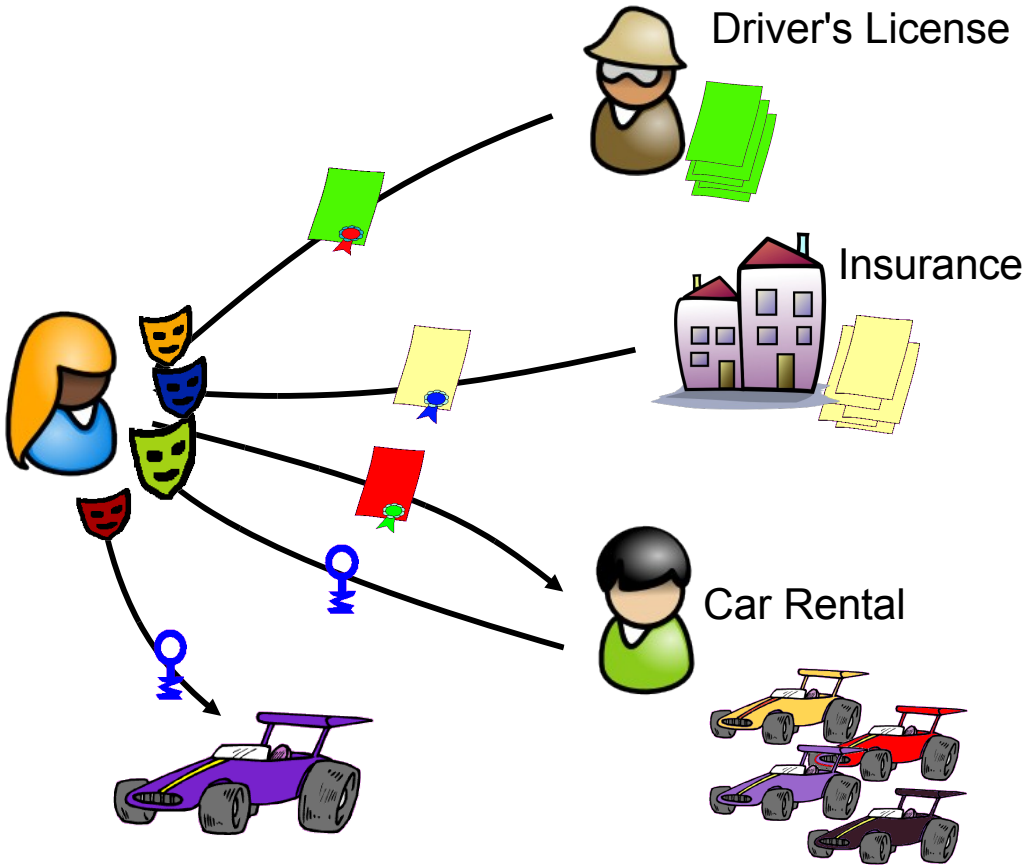
Digital Credentials

... or transmitting certified information



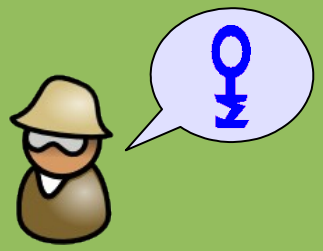
Solution: Private Digital Credentials

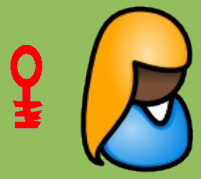
[Chaum, Damgaard, Brands, CL,....]



Private Credentials: How to Build Them

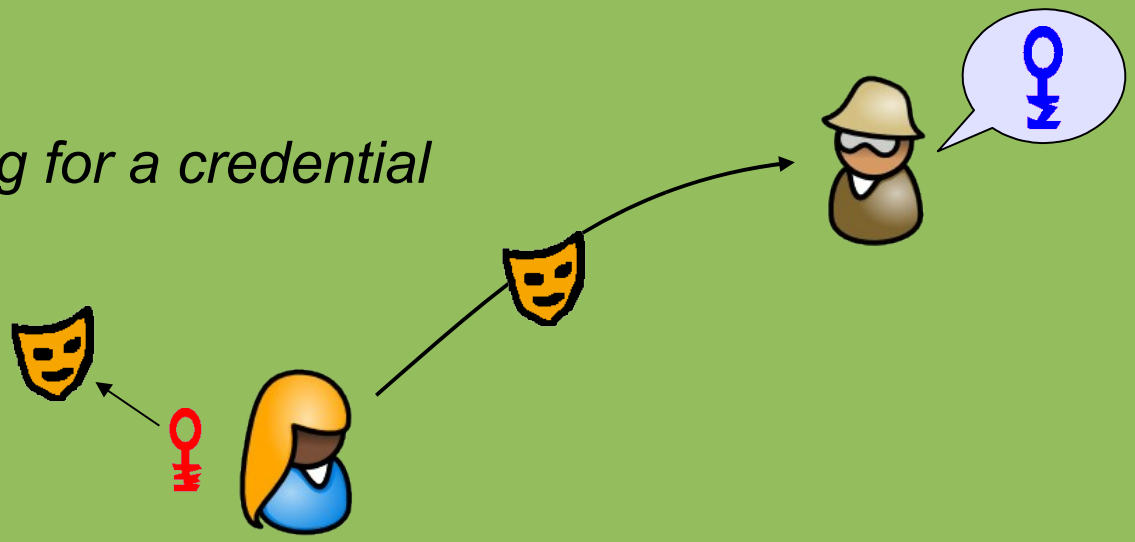
In the beginning...





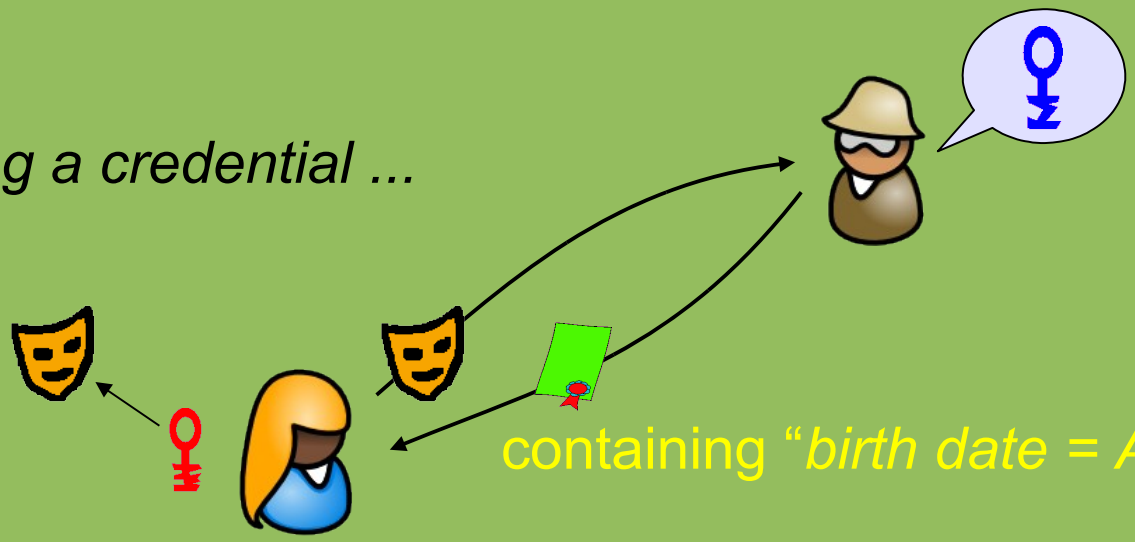
State of the Art: How to Build Them

asking for a credential



State of the Art: How to Build Them

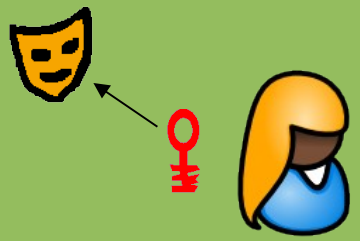
getting a credential ...

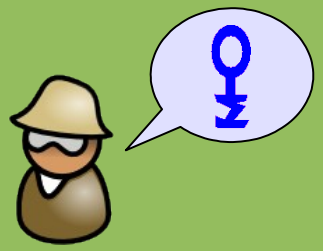


containing "*birth date = April 3, 1987*"

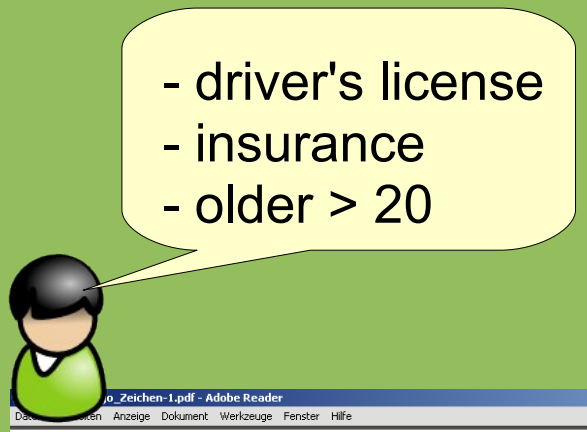
State of the Art: How to Build Them

showing a credential ...



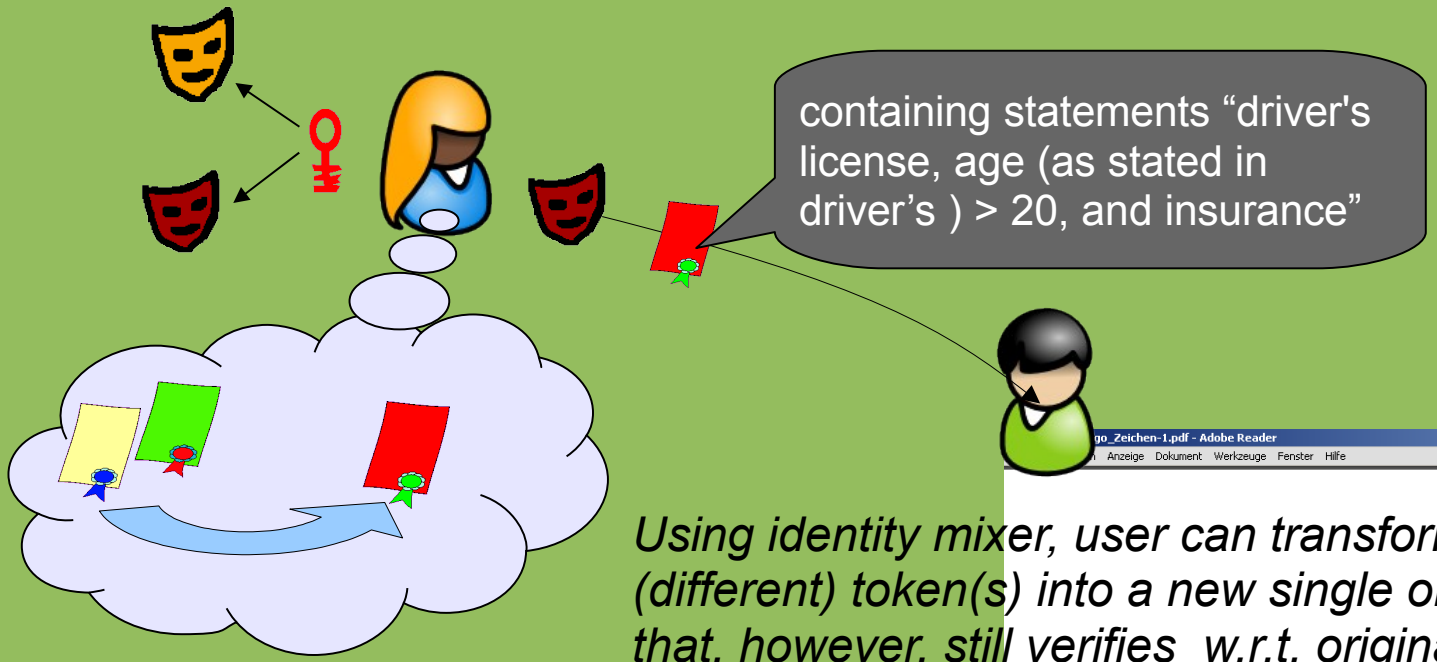


goes off-line



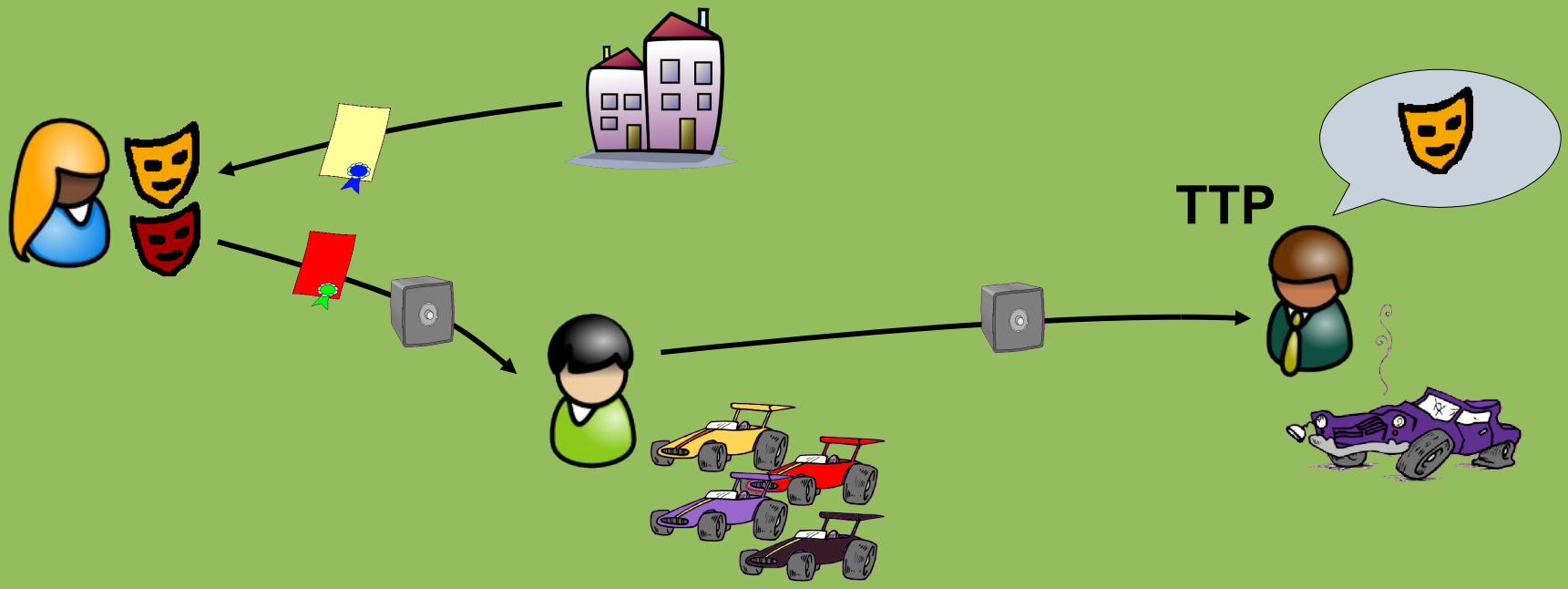
State of the Art: How to Build Them

showing a credential ...



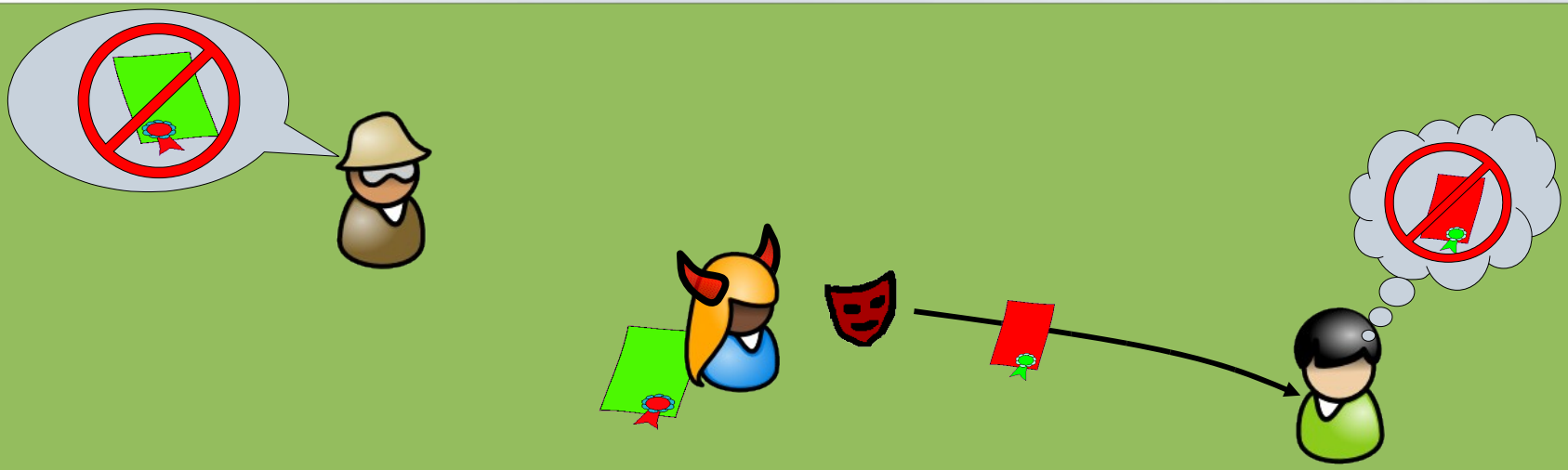
Using identity mixer, user can transform (different) token(s) into a new single one that, however, still verifies w.r.t. original signers' public keys.

Other Properties: Attribute Escrow (Opt-In)

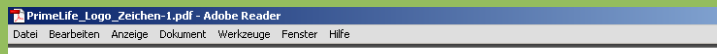


- If car is broken: ID with insurance needs be retrieved
- Can verifiably encrypt any certified attribute *(optional)*
- TTP is off-line & can be distributed to lessen trust

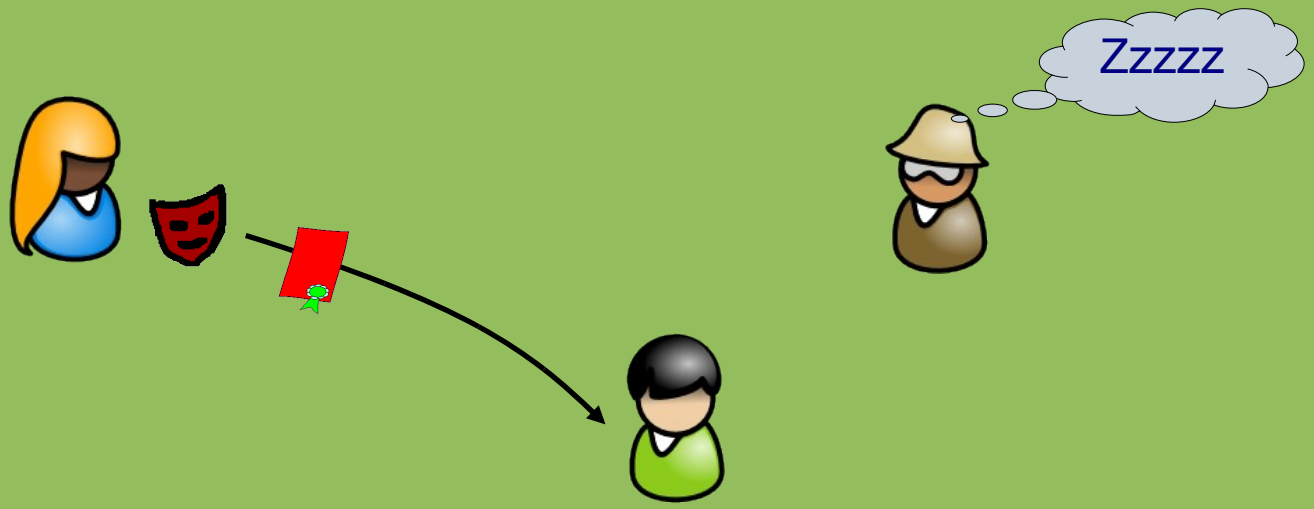
Other Properties: Revocation



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

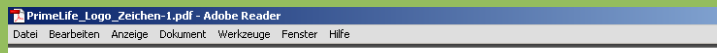


Other Properties: Offline Usage



ID providers (issuers) need sleep, too!

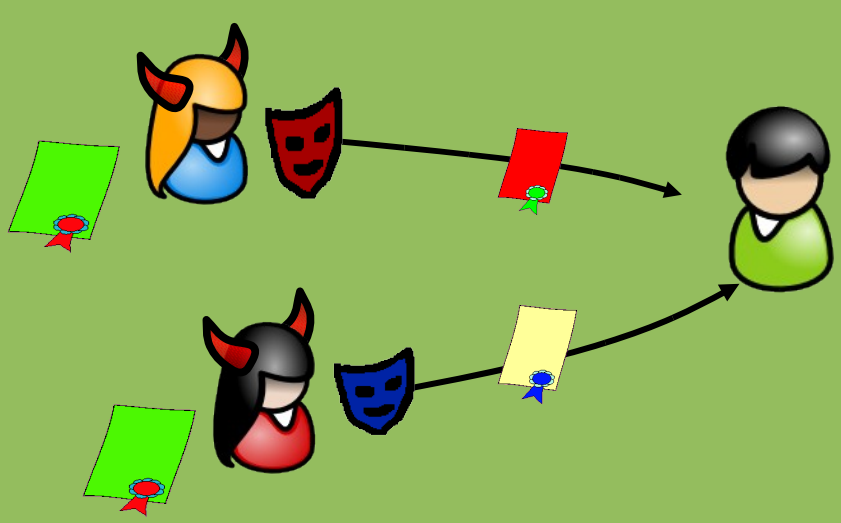
- Sometimes it is too expensive to have connectivity
- Or a security risk (e.g., ID cards)



Certs can be used as many times as needed!

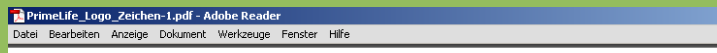
- cf. Revocation; can be done w/ signer's secrets offline

Other Properties: Cheating Prevention

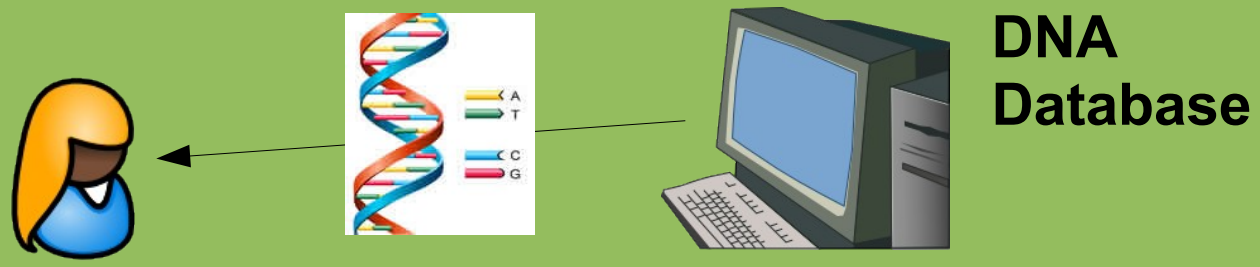


Limits of anonymity possible *(optional)*:

- 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

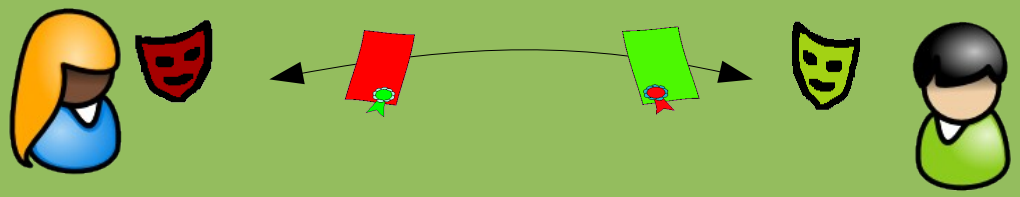


DNA Database

Oblivious Access to Database

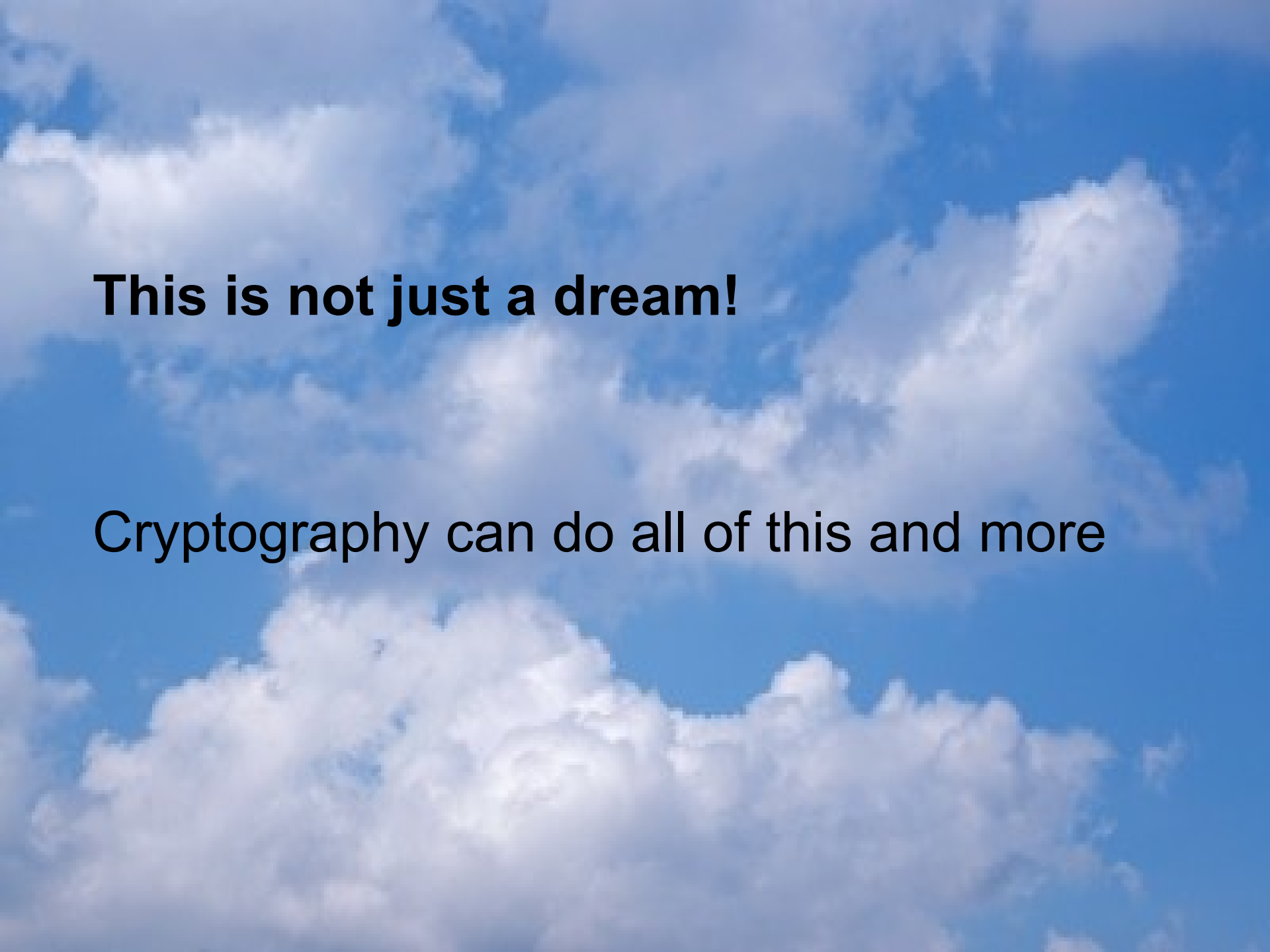
- Server must not learn *who* accesses …
- … *which* record
- Still, Alice can access only records she is *authorized* for

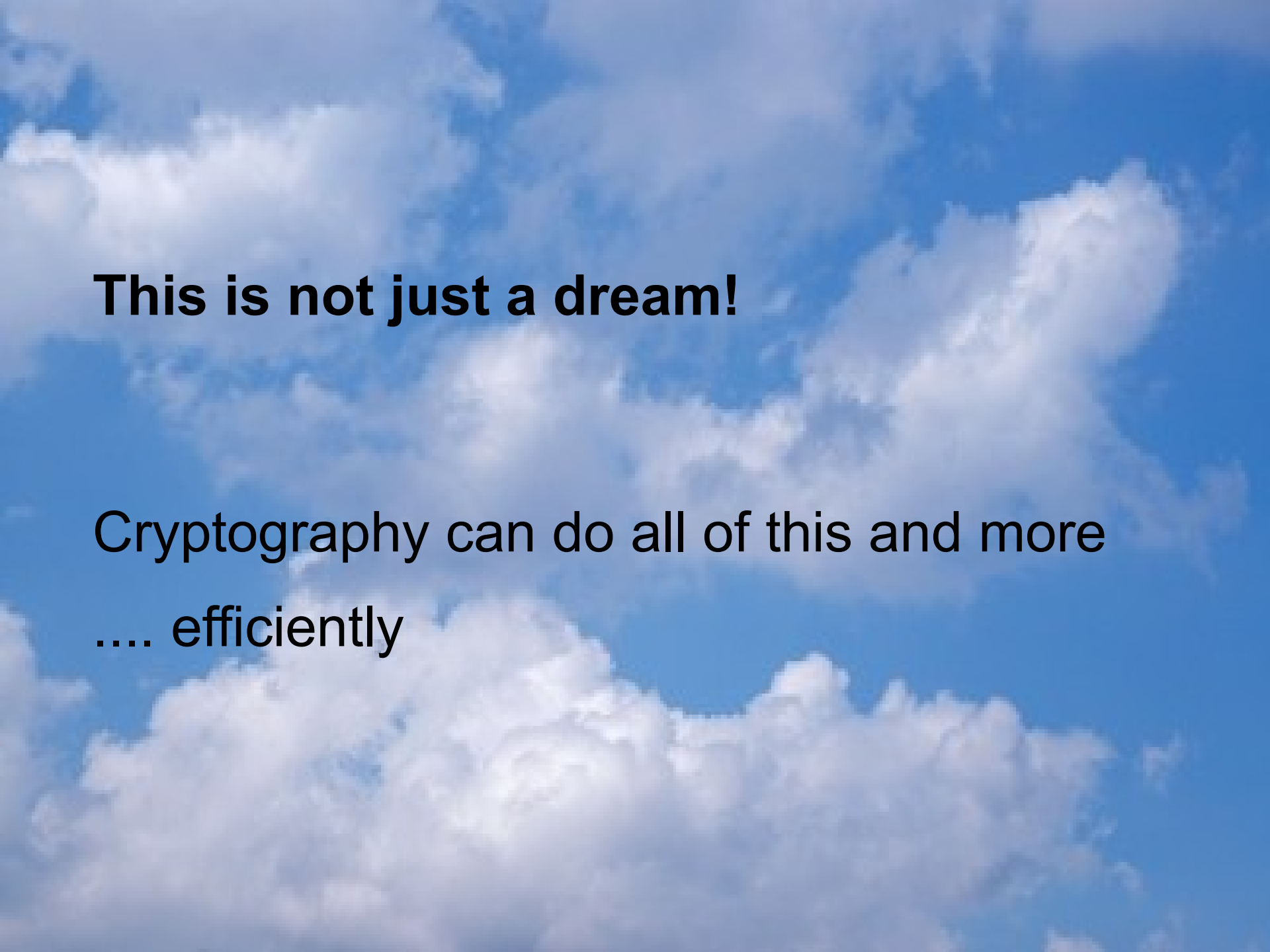
Secret Handshakes



- Alice and Bob both define some predicate P_A and P_B
- Alice learns whether Bob satisfies P_A iff she satisfies P_B


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!

Cryptogra… …more

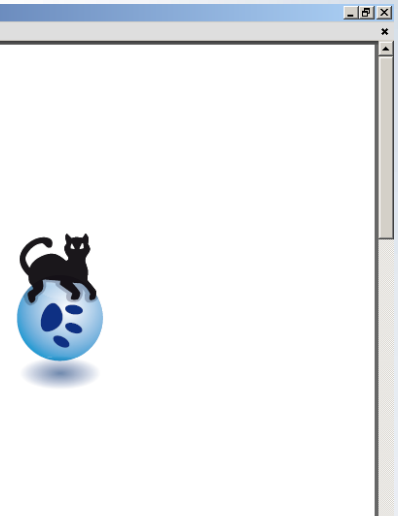
…. effici…

…. even on a … card :-)

Crypto 4 Privacy Short Course

Later This Week :-)

And Here Come the Challenges!



Non-Crypto Challenges for Cryptographers

- Explain what can be done so that people want it & employ it
- 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 The Future Internet!
- 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

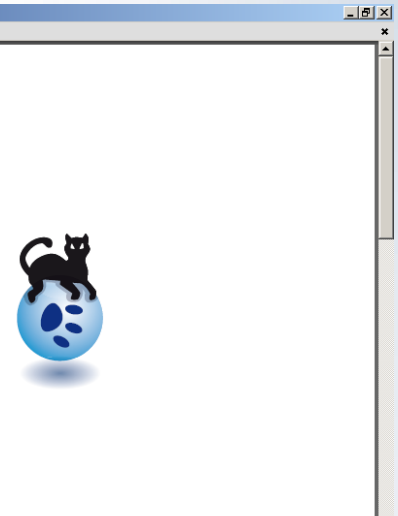
More efficient primitives
- Smaller footprints as to fit into all the sensors, cars, …
- Faster generation & verification of signatures, …
- … maybe using combination of HW security and crypto

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

The really hard problems

- Finding the right security model and meeting it (UC Framework!!)
- Protection against bad guys with Quantum Computers

Summary



Summary

- Privacy, Identity and Trust Mgmt More Important Than Ever
- Achieving & Maintaining Security & Privacy is Challenging
  - Difficult to build in afterwards!
  - ICT is spreading and provides new ways to use electronic media
  - Lots of open research questions here
- Lots of crypto tools are ready – but need to be used
  - Policies
  - Infrastructure
  - User interfaces, User interfaces, User interfaces, User interfaces
  - Need to change Applications & Business processes

Let's Make it Real!

info@primelife.eu
www.primelife.eu
(www.prime-project.eu)
www.zurich.ibm.com/idemix

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.**