

PRIME – Privacy and Identity Management for Europe

Advanced Privacy-Enhancing
Federated Identity Management

Dieter Sommer
dso@zurich.ibm.com
Cryptography Group
IBM Research, Zurich Research Lab

Outline

- Introduction
- PRIME
- Identity Mixer (aka idemix)
- Conclusion

Problem Summary

- IT and data collection gets cheaper and widely deployed
- People are concerned
- Regulations & laws require privacy protection
- Advanced technology is there to some extent
... but hardly used yet

What is privacy?

The right of individuals to determine for themselves when, how and to what extent information about them is communicated to others. [Alan Westin, 1967]

Internationally agreed privacy principles

- No covert / secret collections of personal information
- Informed consent to purpose prior to collection
- Use and retention of PII only according to agreed purpose
- Individual must get access to own data,
can correct, block own data

*US Fair Information Practices (1973)
OECD Guidelines (1980)
EU Privacy Directive (1995) ...*

Outline

- Introduction
- **PRIME**
- Identity Mixer (aka idemix)
- Conclusion

PRIME Privacy and Identity Management for Europe

IBM France, F

IBM Zürich Research Lab, CH 

Unabhängiges Landeszentrum für
Datenschutz, D 

Technische Universität Dresden, D  TECHNISCHE
UNIVERSITÄT
DRESDEN

Katholieke Universiteit Leuven, B  KATHOLIEKE UNIVERSITEIT
LEUVEN

Universiteit van Tilburg, NL  UNIVERSITEIT VAN TILBURG

Hewlett-Packard, UK  **hp**
invent

Karlstads Universitet, S 

JRC / IPSC Ispra, I  EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Università di Milano, I 

Centre National de la Recherche
Scientifique / LAAS, F 


Johann Wolfgang Goethe-Universität
Frankfurt am Main, D 

Chaum LLC, USA

RWTH Aachen, D  RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

Institut EURECOM, F  EURECOM
European University

Erasmus Universiteit Rotterdam, NL  ERASMUS UNIVERSITEIT ROTTERDAM

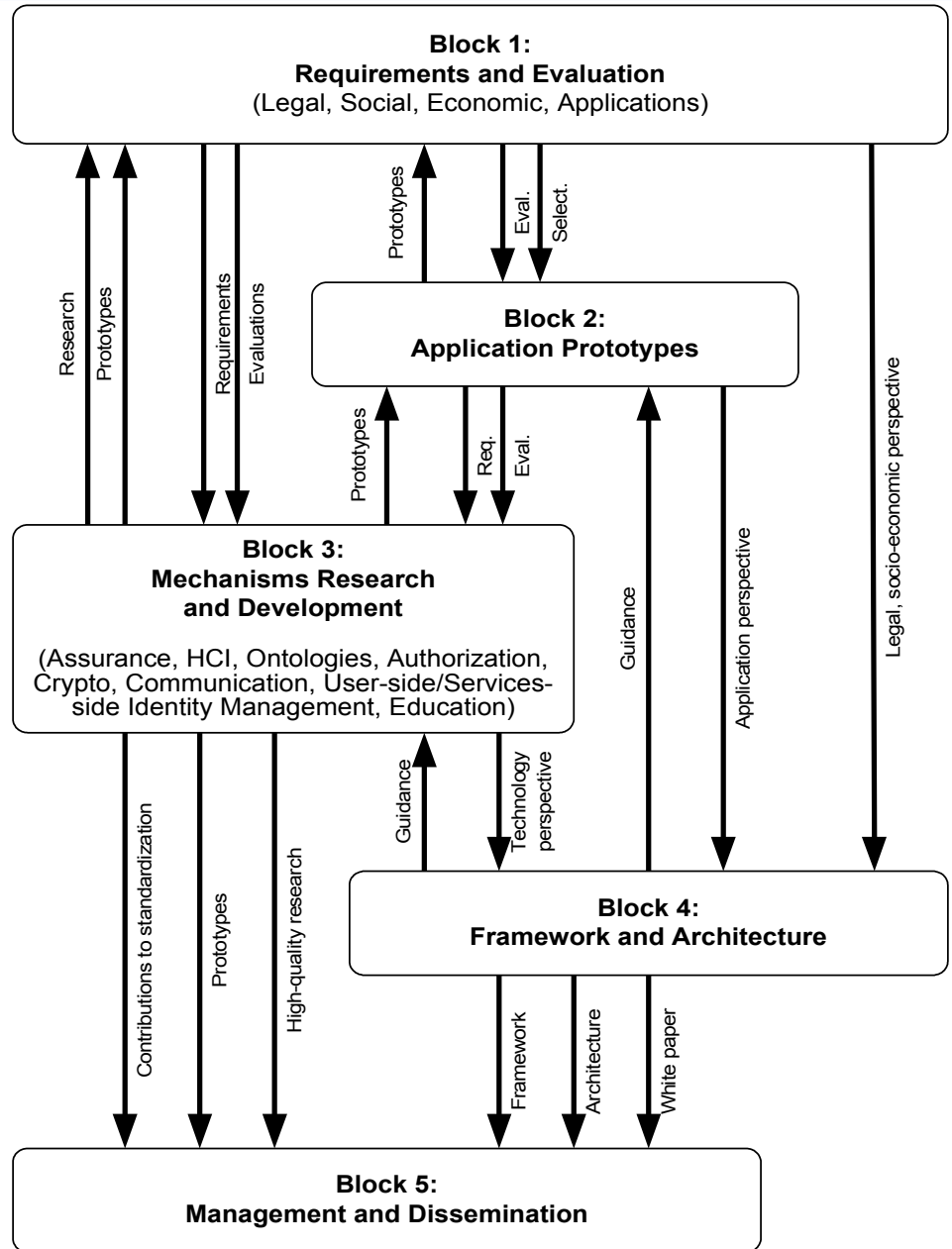
Fondazione Centro San Raffaele
del Monte Tabor, I 

Deutsche Lufthansa, D  Lufthansa
Konzerndatenschutz 

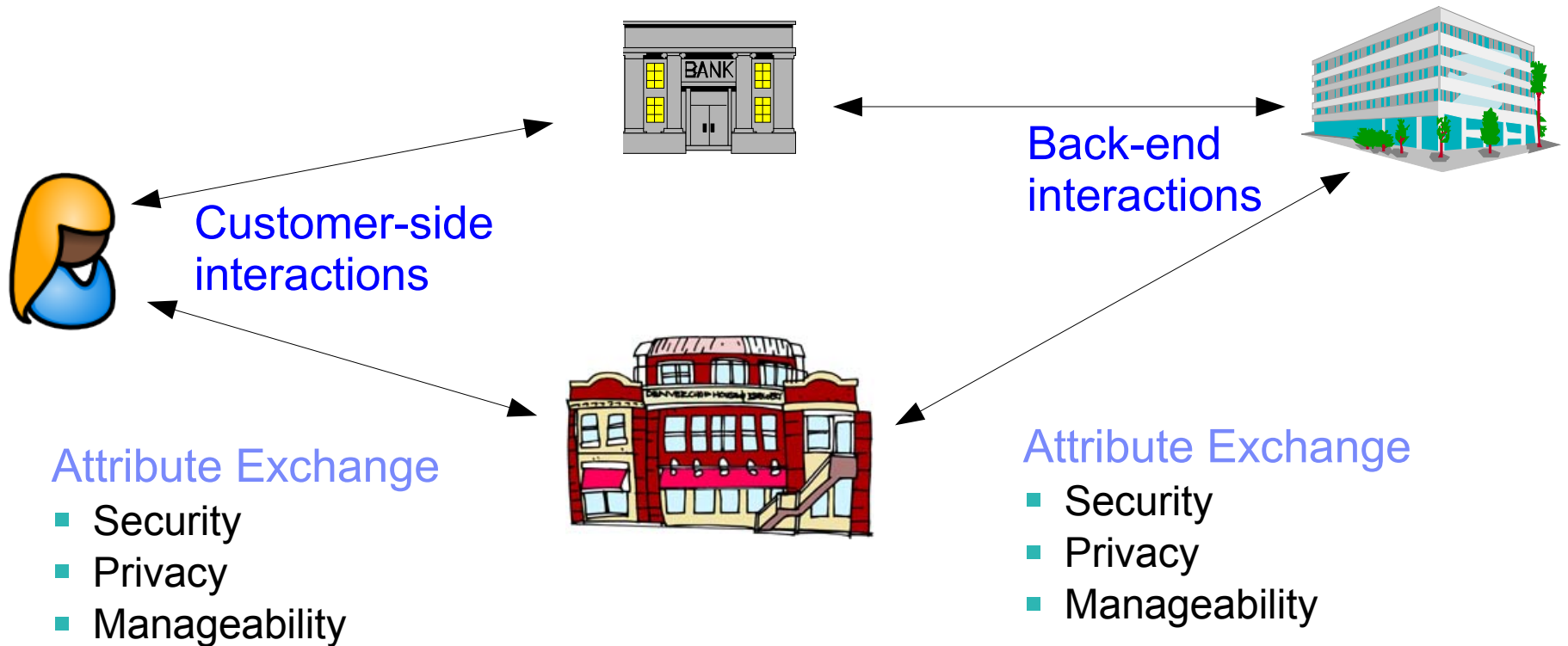
Swisscom, CH  swisscom

T-Mobile, D  T-Mobile

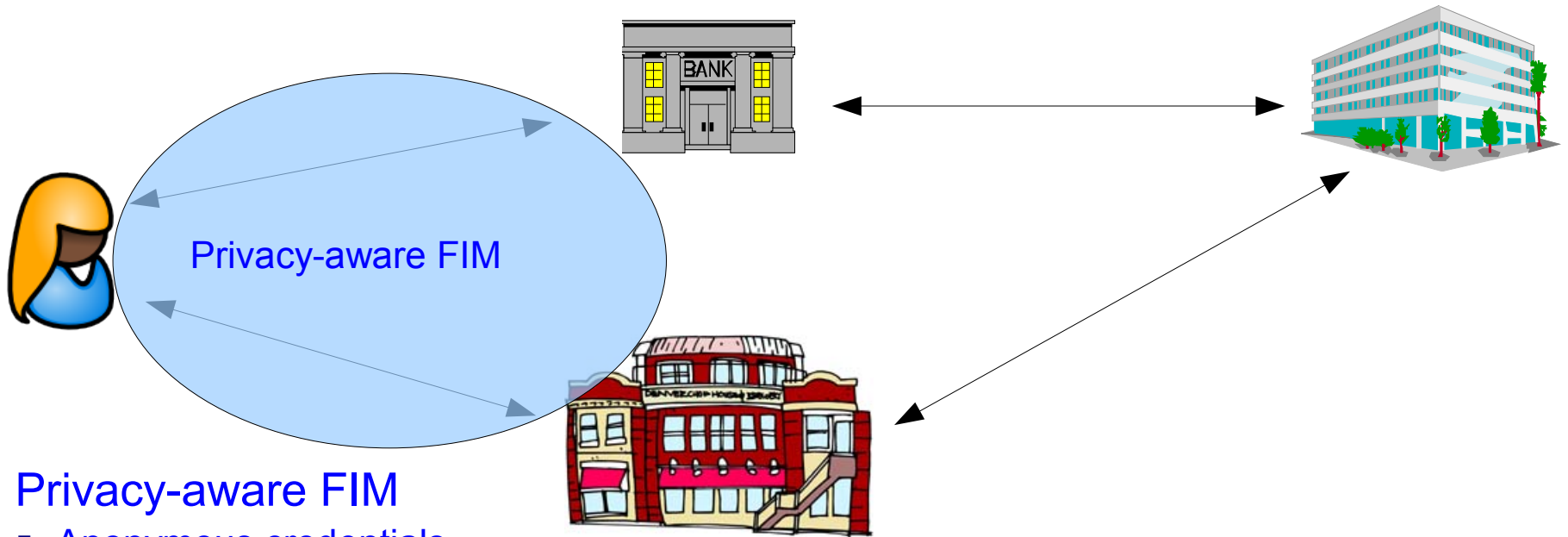
PRIME Project Structure



The Big Picture: Privacy & Identity Management



PRIME's Activities



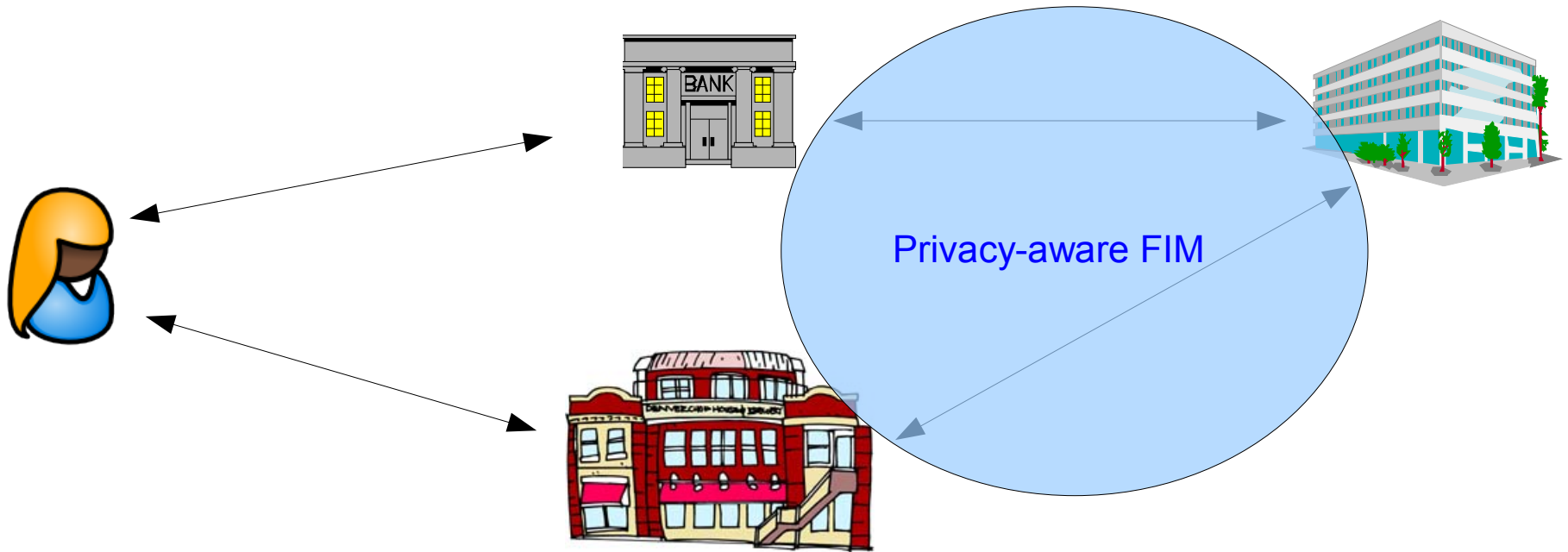
Privacy-aware FIM

- Anonymous credentials
- Privacy policies
- Access control policies
- Assurance
- ...

Emerging IDM tools

- Higgins
- MS InfoCard

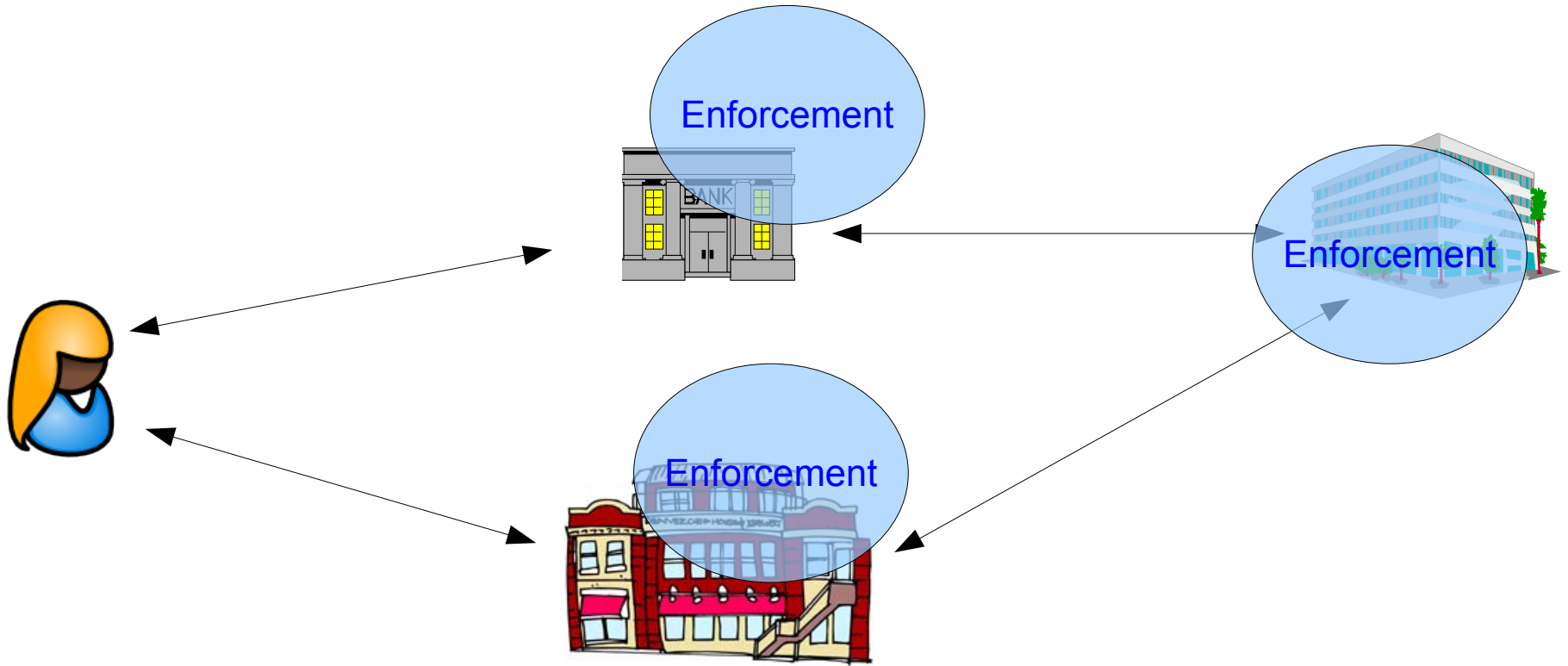
PRIME's Activities



Privacy-aware FIM

- Privacy policies
- Access control policies
- Assurance
- ...

PRIME's Activities



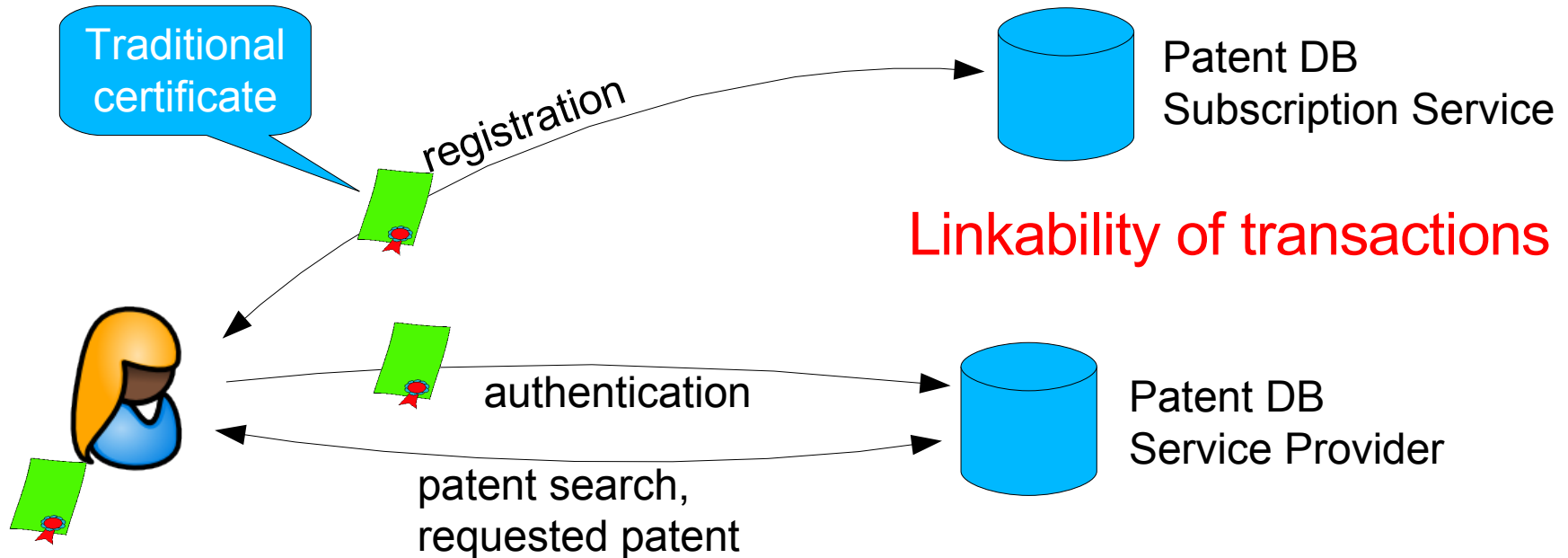
PRIME's Activities



Outline

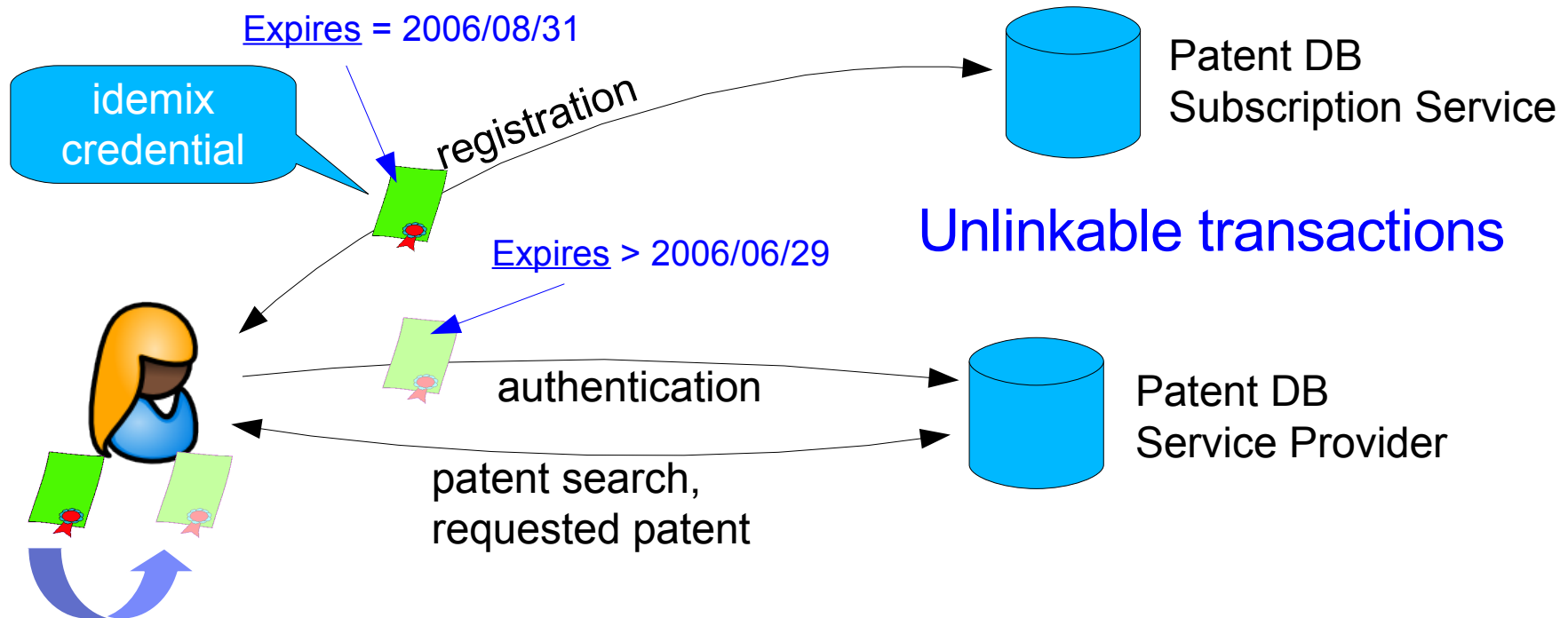
- Introduction
- PRIME
- Identity Mixer (aka idemix)
- Conclusion

Privacy Problem: Access to Patent Database



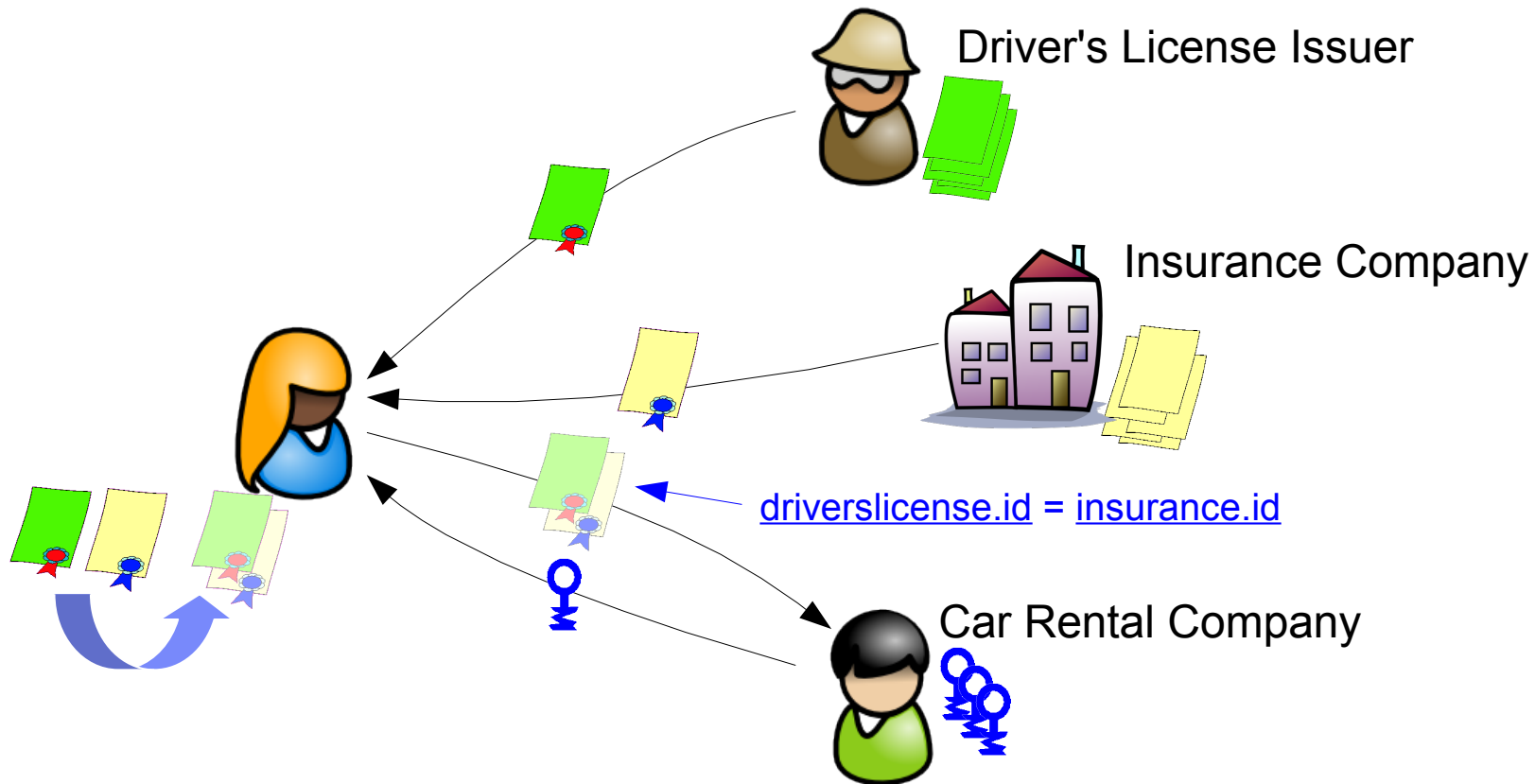
- **Security:** Access restricted to registered users
- **Privacy:** Linkability
 - Substantial information leakage
 - Allows for industrial espionage, profiling, ...

Privacy-Enhanced Access to Patent Database

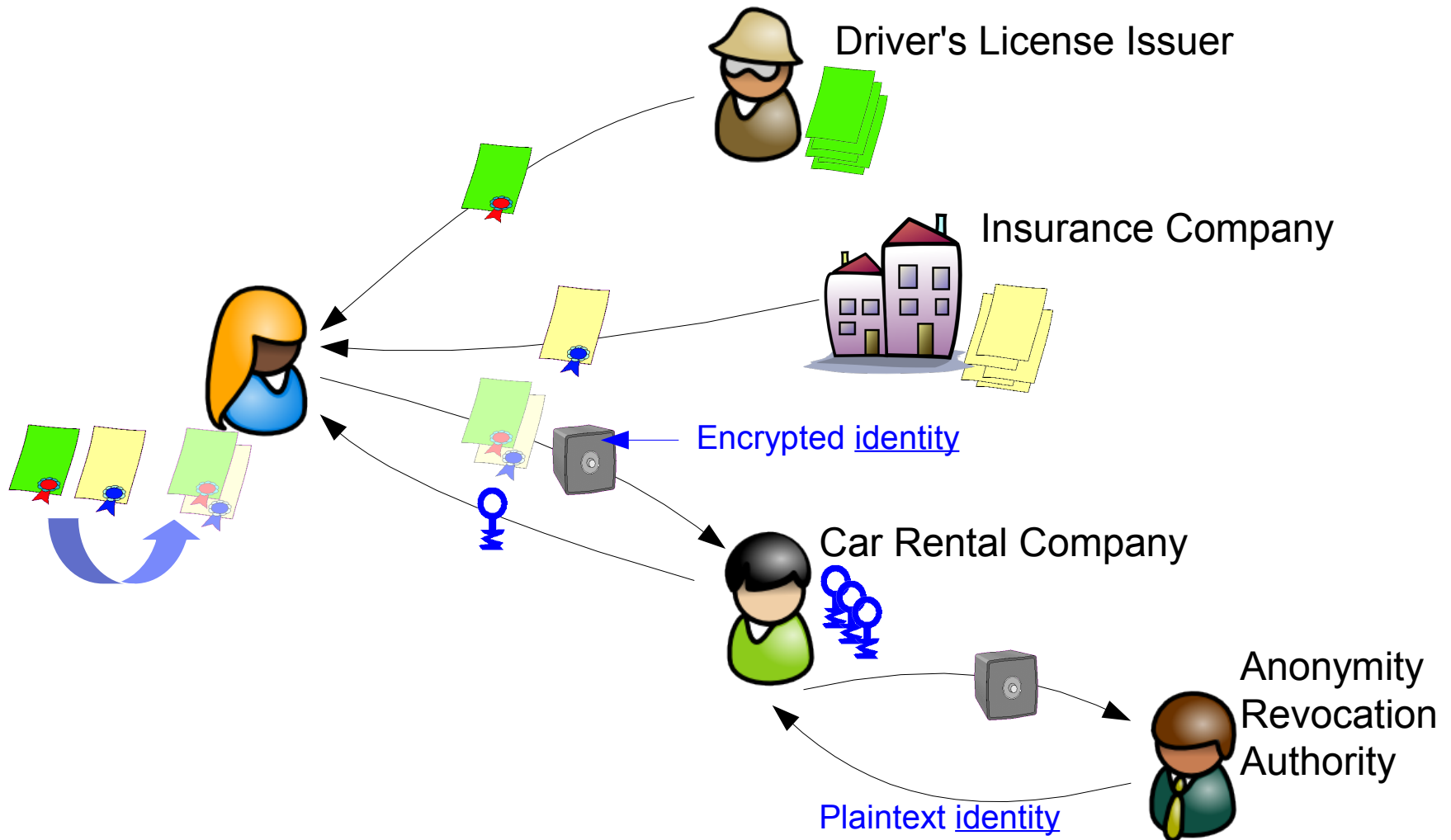


- **Security:** Access restricted to registered users
- **Privacy:** Requests can be anonymous
 - Neither linkable to registration transaction,
 - nor to any other requests (no profiling, data mining)

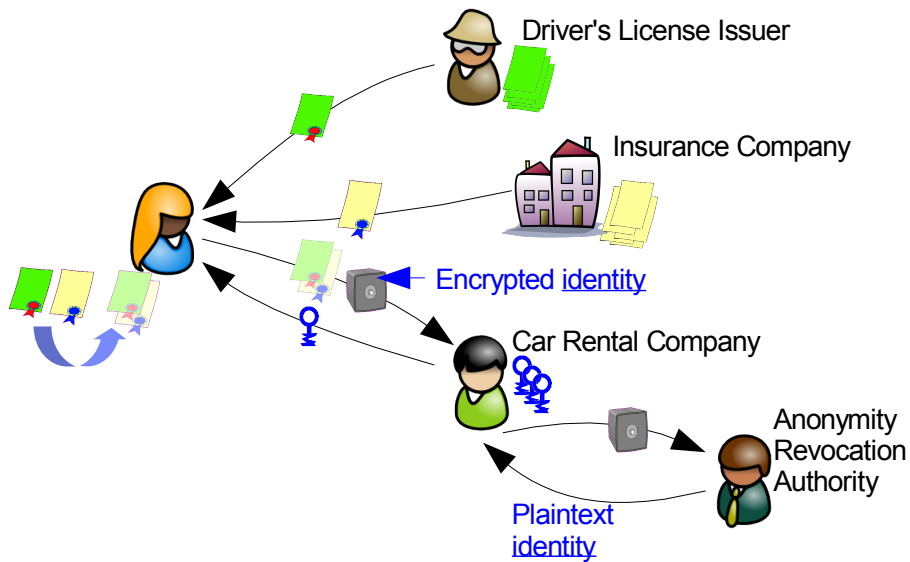
Multiple Credentials: More Evolved Example

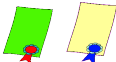

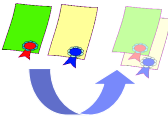



Accountability: Even More Evolved Example



Idemix – Key Features Summarized



- **Security** 
 - As secure as certificates
- **Accountability**
 - Verifiable encryption 
- **Privacy** 
 - Unlinkability 
 - Partial attribute release
- **Identity Providers**
 - Can be off-line
- **Multi-use credentials**
 - Reduction of amortized cost
- **Additional features**
 - Possibility of revocation, k-show credentials, ...

New Business Model for Established Industries

- Telcos, banks
 - Possess securely established identities for large customer bases
 - Can act as identity providers (credential issuers) for their customers
 - Leverage existing assets
 - High convenience for customers (no separate registration)
 - Bootstrap open identity federations

Outline

- Introduction
- PRIME
- Identity Mixer (aka idemix)
- Conclusion

Conclusion

- PRIME
 - Provides strong privacy solutions
- DAIDALOS
 - Is concerned about privacy: Profiling, pseudonymity ...
 - Efforts of PRIME apply to DAIDALOS
 - Privacy policies
 - Enforcement
 - Trust negotiation
 - Assurance
 - *Idemix*, in particular, can improve on the current situation
 - Authentication
 - Pseudonymity
 - Secure, privacy preserving, yet accountable transactions

Zurich Research Laboratory

Dieter Sommer
dso@zurich.ibm.com
Cryptography Group
IBM Research, Zurich Research Lab

www.prime-project.eu
www.zurich.ibm.com/security/idemix