

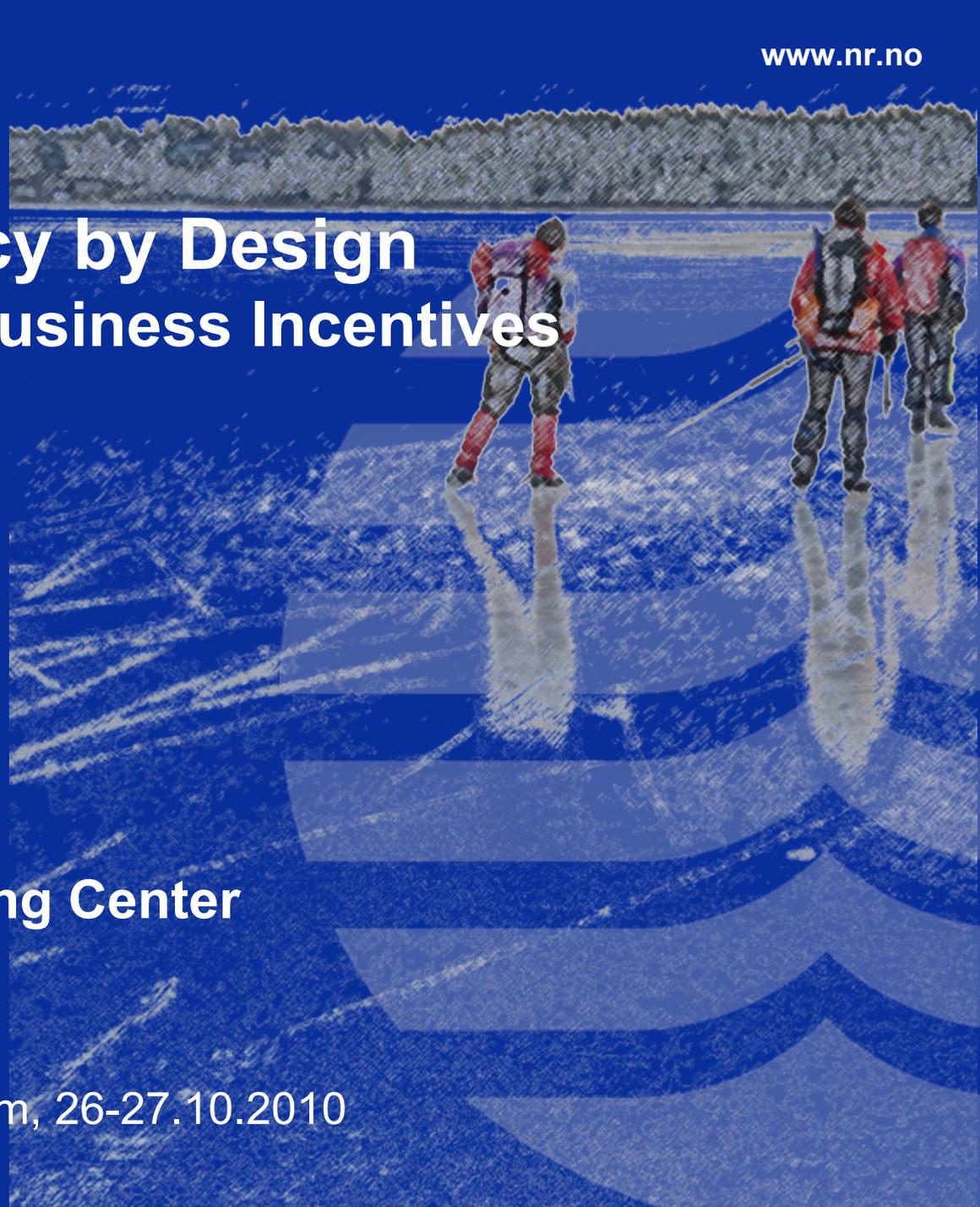
Location Privacy by Design - Technology & Business Incentives

Dr. Lothar Fritsch

**Norsk Regnesentral
Norwegian Computing Center**

Oslo

Internetdargana, Stockholm, 26-27.10.2010



Program

Tis 26
SÄKERHET

Privacy-enhancing technology

[Läs mer](#)

 Plats: **Kongresshall C**

 Datum: **2010-10-26**

 Tid: **11:00-12:30**

In this seminar, the concept of Privacy-enhancing Technologies (PETs) will be presented and examples for basic PET (Mix-nets, anonymous credentials, privacy policies, privacy-enhanced access control, transparency tools) will be given. We will show how, within the scope of the EU PRIME and PrimeLife projects, state of the art and novel PETs have been integrated into a privacy-enhancing identity management architecture, which allows end users to gain better control over their personal spheres.

Talare:

Simone Fischer Hübner, Forskare [Läs mer](#)
Hans Hedbom [Läs mer](#)
Lothar Fritsch, Research Scientist [Läs mer](#)

STÄNG ✕

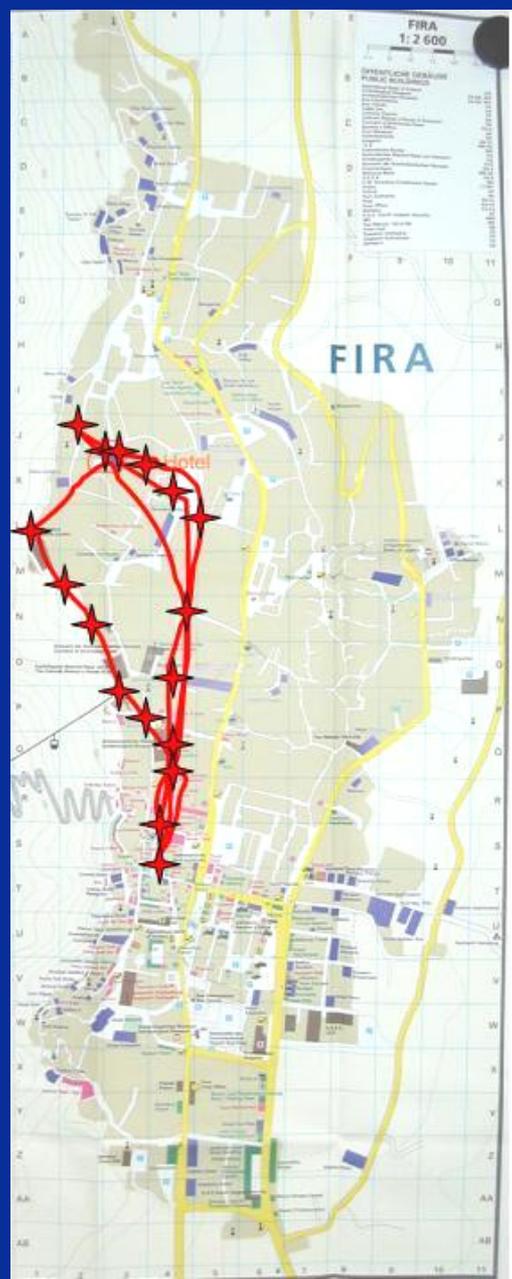
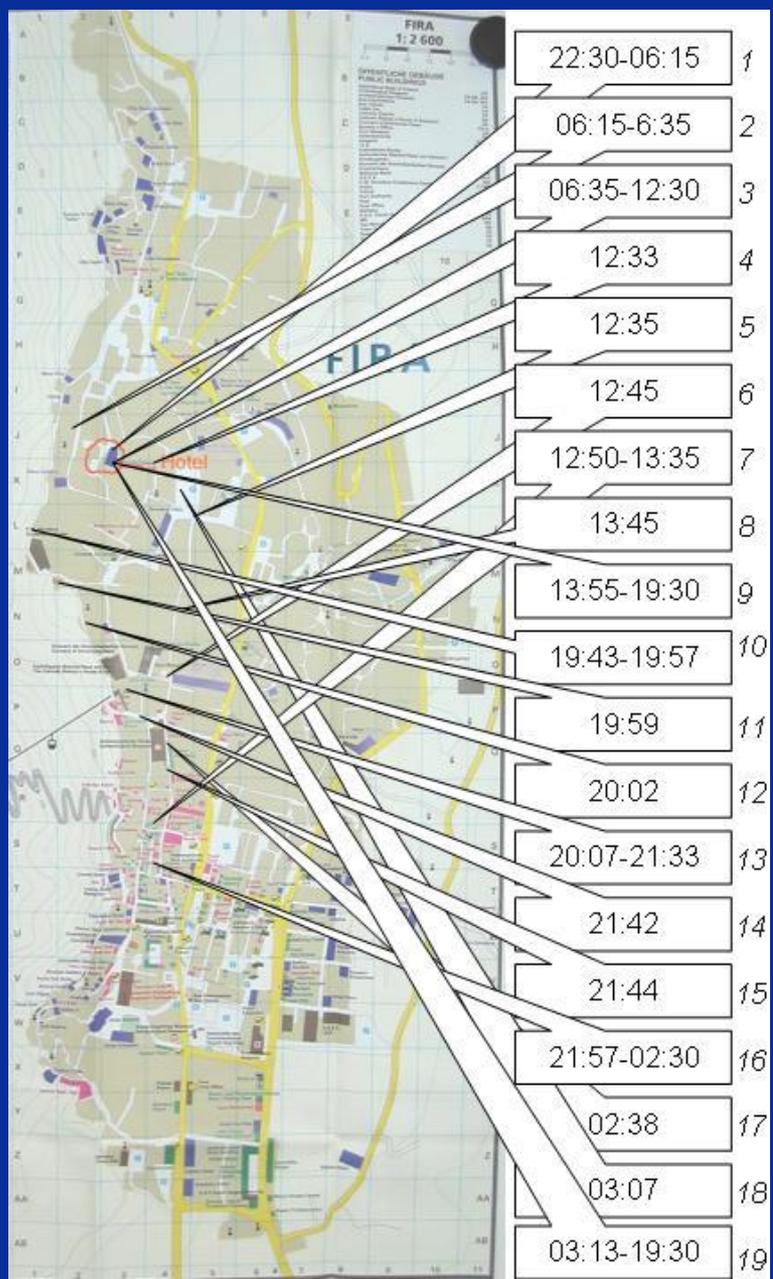
Tid	Rubrik	Talare
09:00-10:30	Keynote dag 1 (LIVESÄNDS)	Jeff Cole
11:00-12:30	When DNS fails	Danny Aer
	Privacy-enhancing technology	Simone Fi
	Sociala medier i valrörelsen 2010 (LIVESÄNDS)	Brit Stakst
	IPv6	Jörgen Eri
	Publiken: Nya aktörer och nya mediavanor	Lena Victo
	Data: Är kartan ritad?	Johanna F
13:40-15:10	DNSSEC developments	Lars-Göra
	Anti-Censorship and Transparency (LIVESÄNDS)	Anne-Mari

Contents

- ▶ **Location Privacy**
 - Concepts
 - Technology

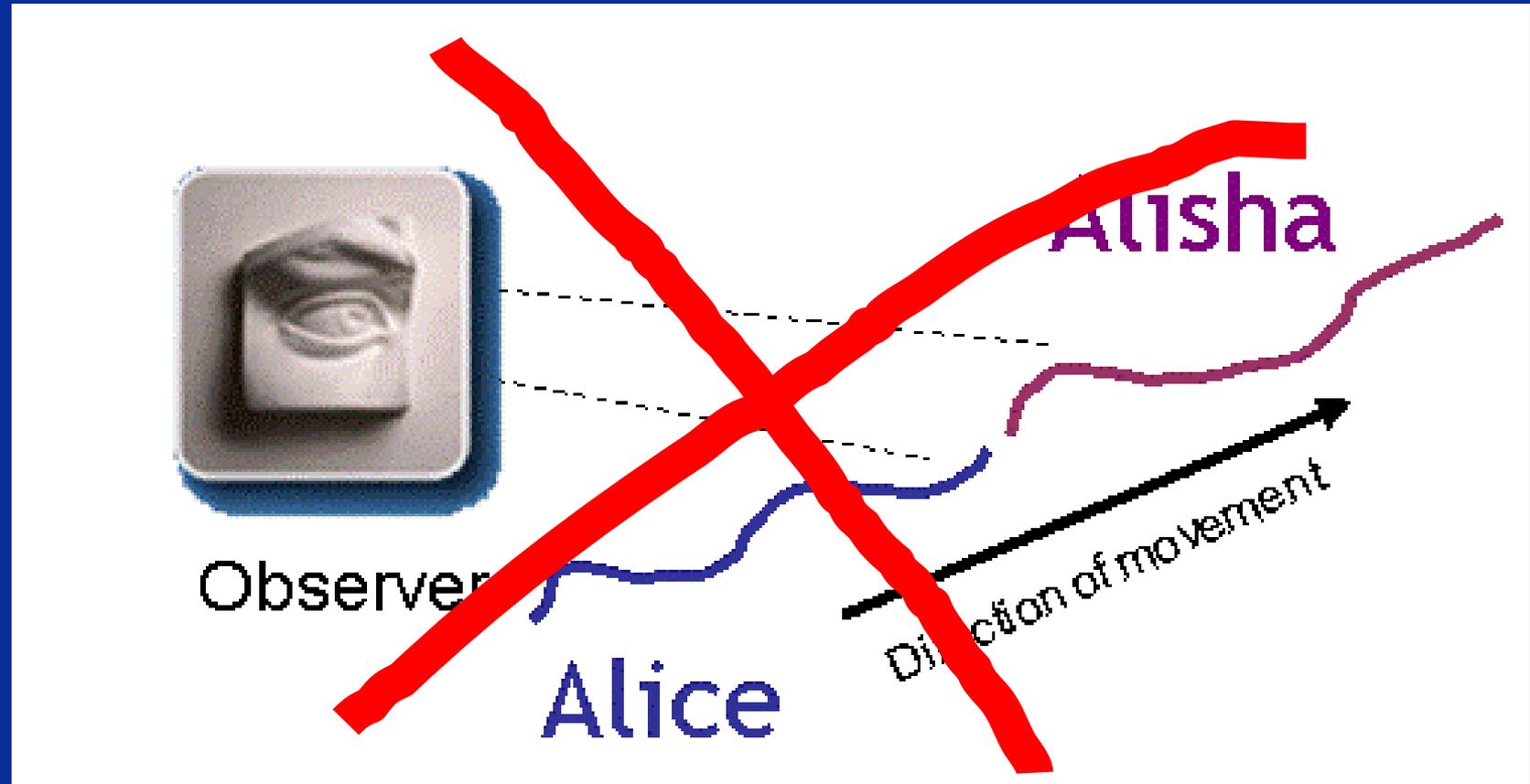
- ▶ **Privacy by Design**
 - Planning vs. Patching
 - Design Process

- ▶ **Business Incentives for Privacy**
 - Customer damage is business damage
 - Businesses want privacy, too!



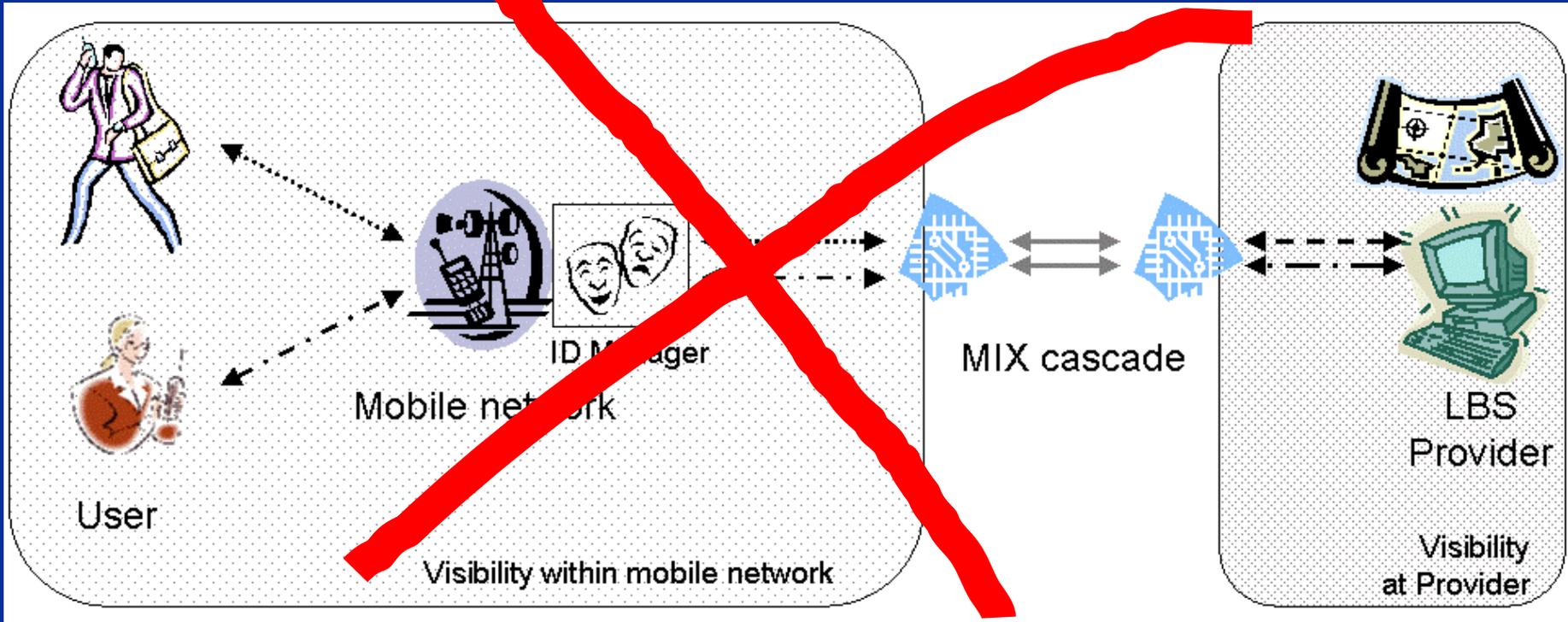
[1]

Simple change of pseudonym?



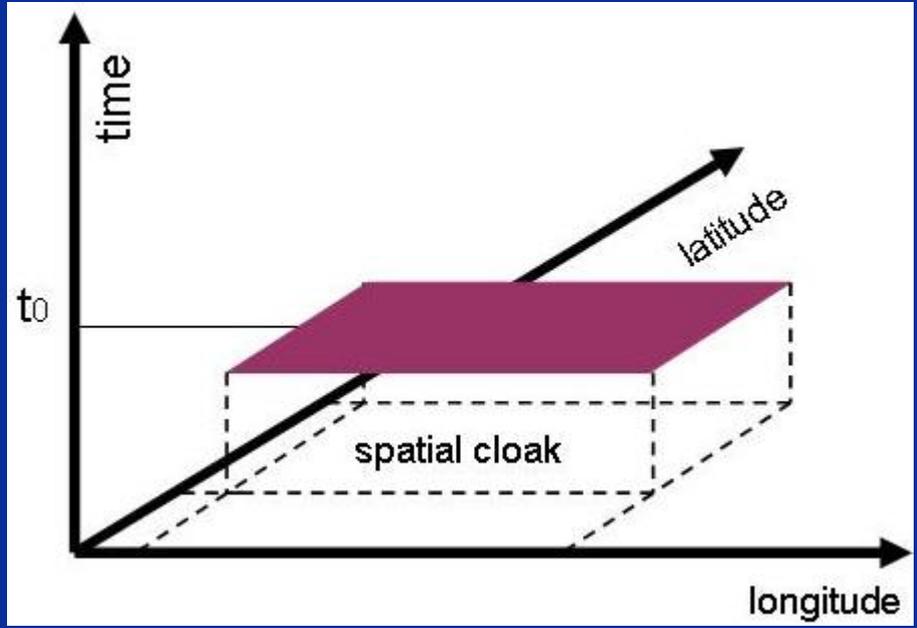
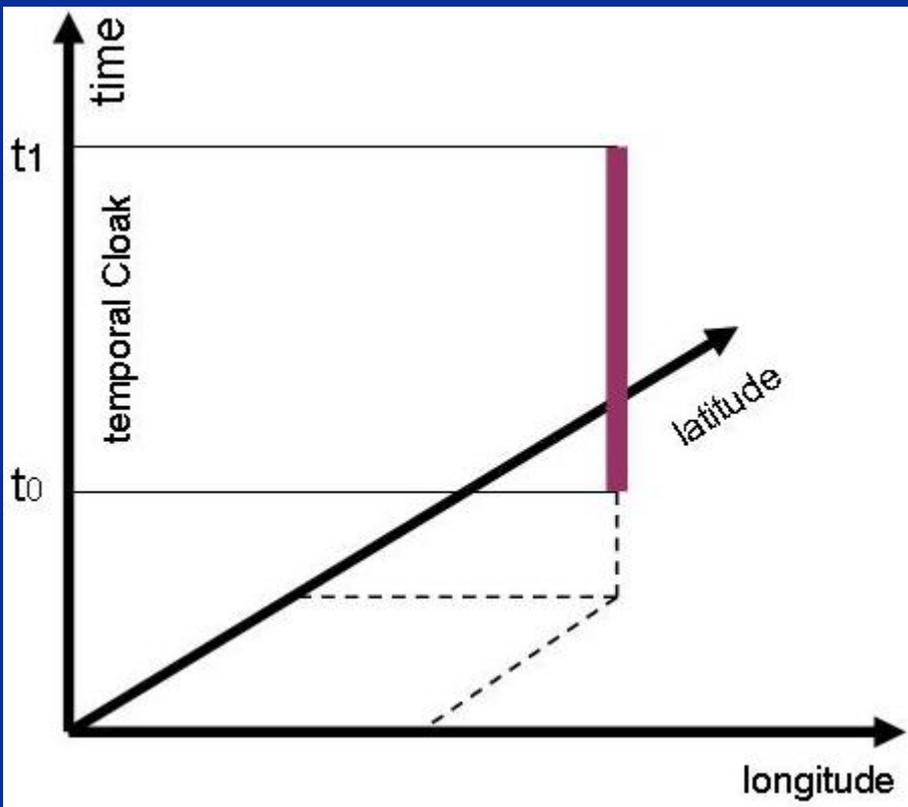
[1]

Use of Anonymizers / MIXing / TOR?



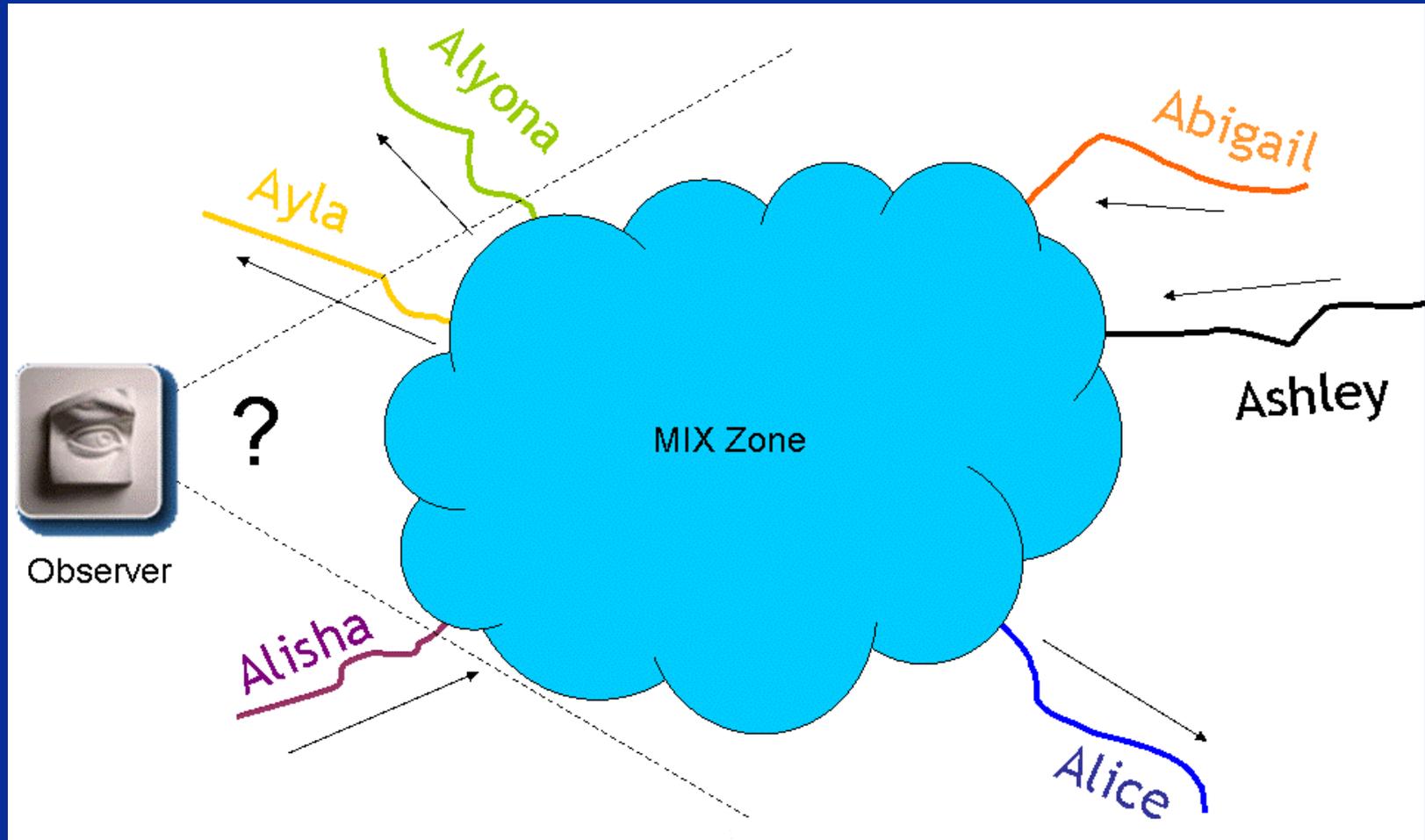
[1]

Cloaking in Time and Space



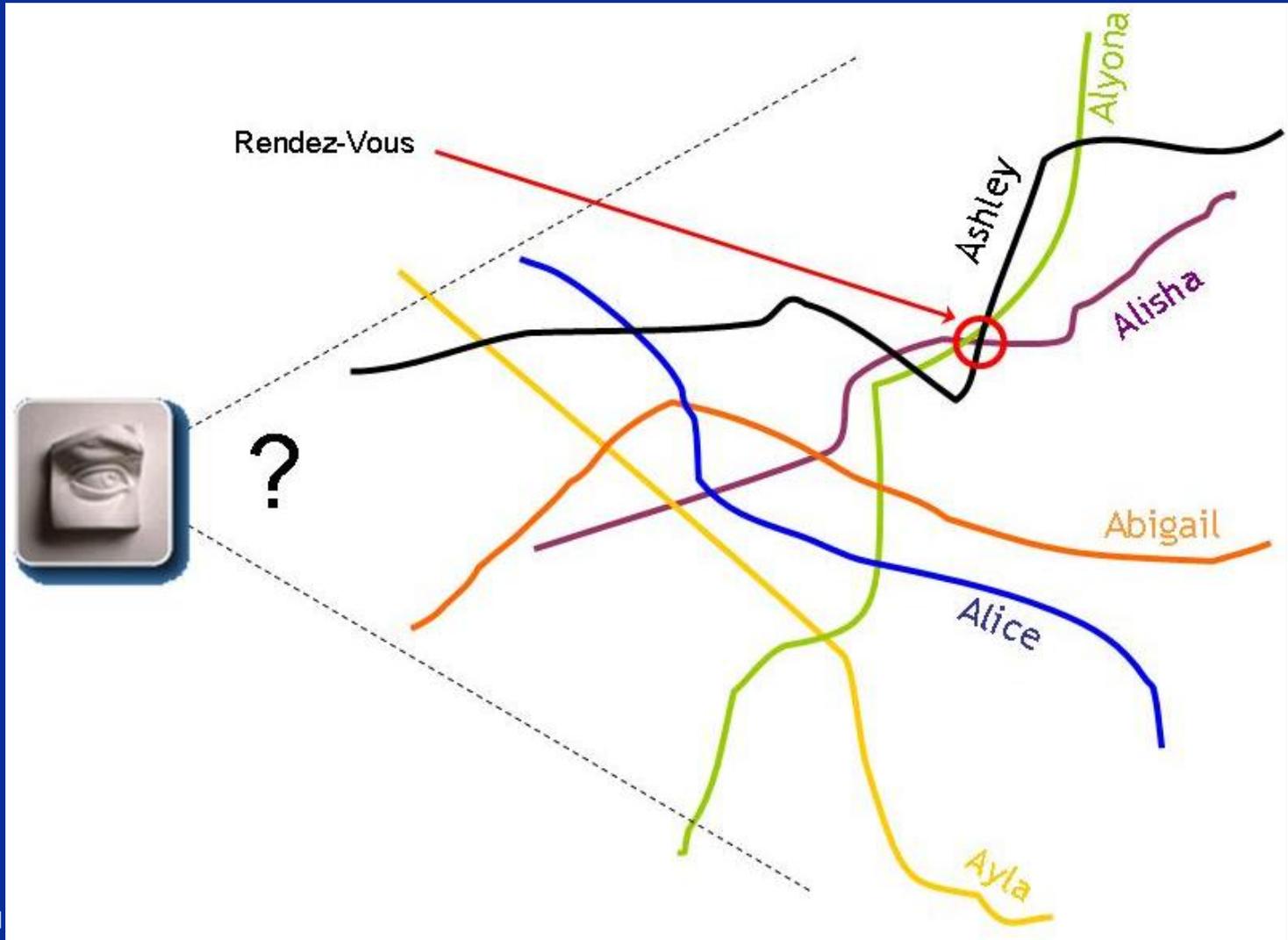
[1]

MIX zoning of users



[1]

Dummy Users as Camouflage



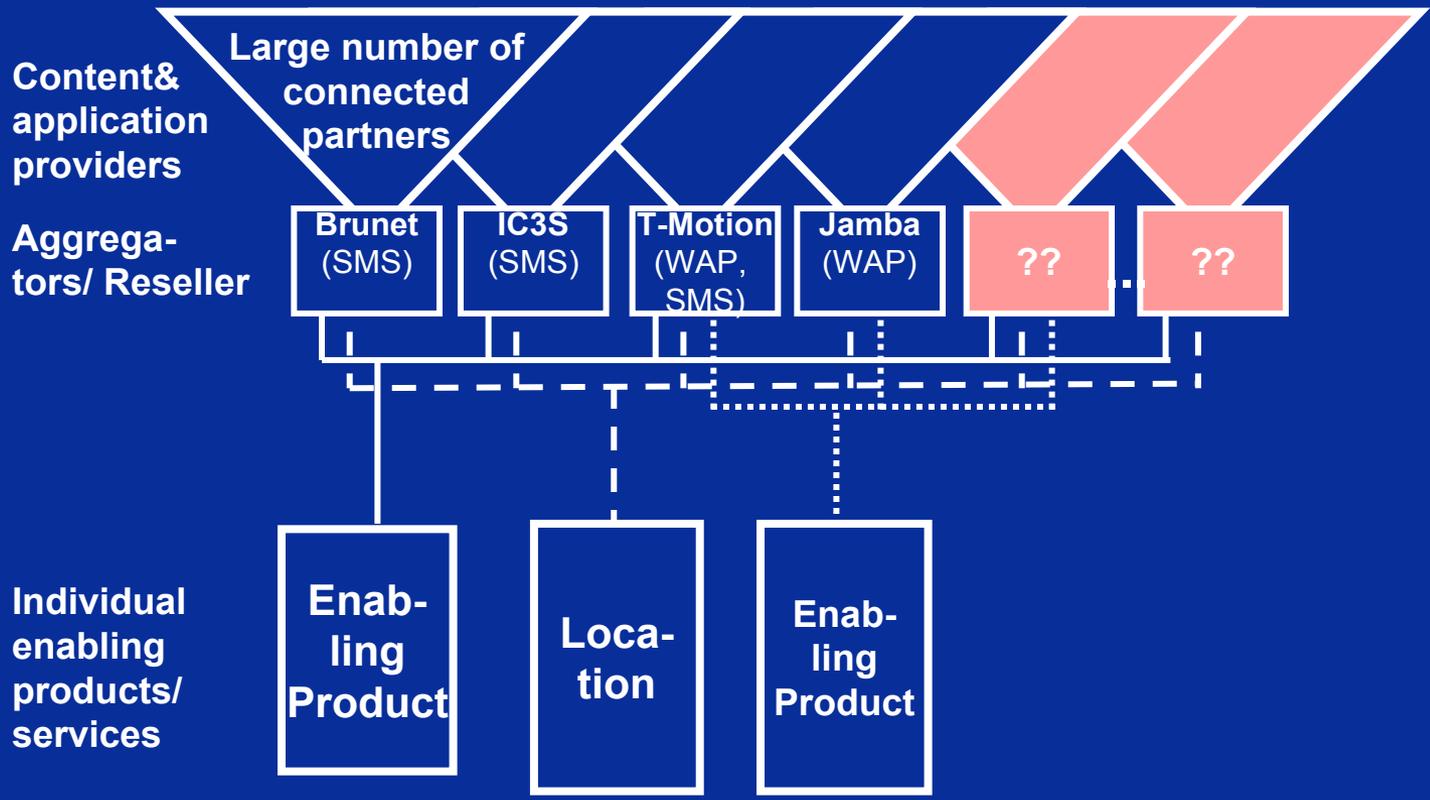
[1]

Two particular solutions

- ▶ **PRIME LBS prototype for T-Mobile** ^[2]
 - Using a 3rd-party service to separate location data from identity data
 - Creation of 3rd-party LBS supplier IDs
 - Management of user location policies at the location source

- ▶ **”Oblivious maps” – anonymous access to mapping** ^[3]
 - Based on ”oblivious transfer” algorithm
 - Basically bundels many user’s access to a mapping service into a batch
 - Cryptographic properties ensure that the mapping server can’t profile users

PRIME: Real-World Reseller business



PRIME: Requirements

- ▶ Enable established business models on a secure, privacy-friendly architecture
- ▶ Ensure efficiency & economy of the solution
- ▶ Enable users to manage policies & their 'online' identities for each service provider and for each usage cycle
- ▶ No processing of localizations violates a user's consent
- ▶ Hide service usage patterns from observers & infrastructure providers
- ▶ Confidentiality of communication content against observers & infrastructure

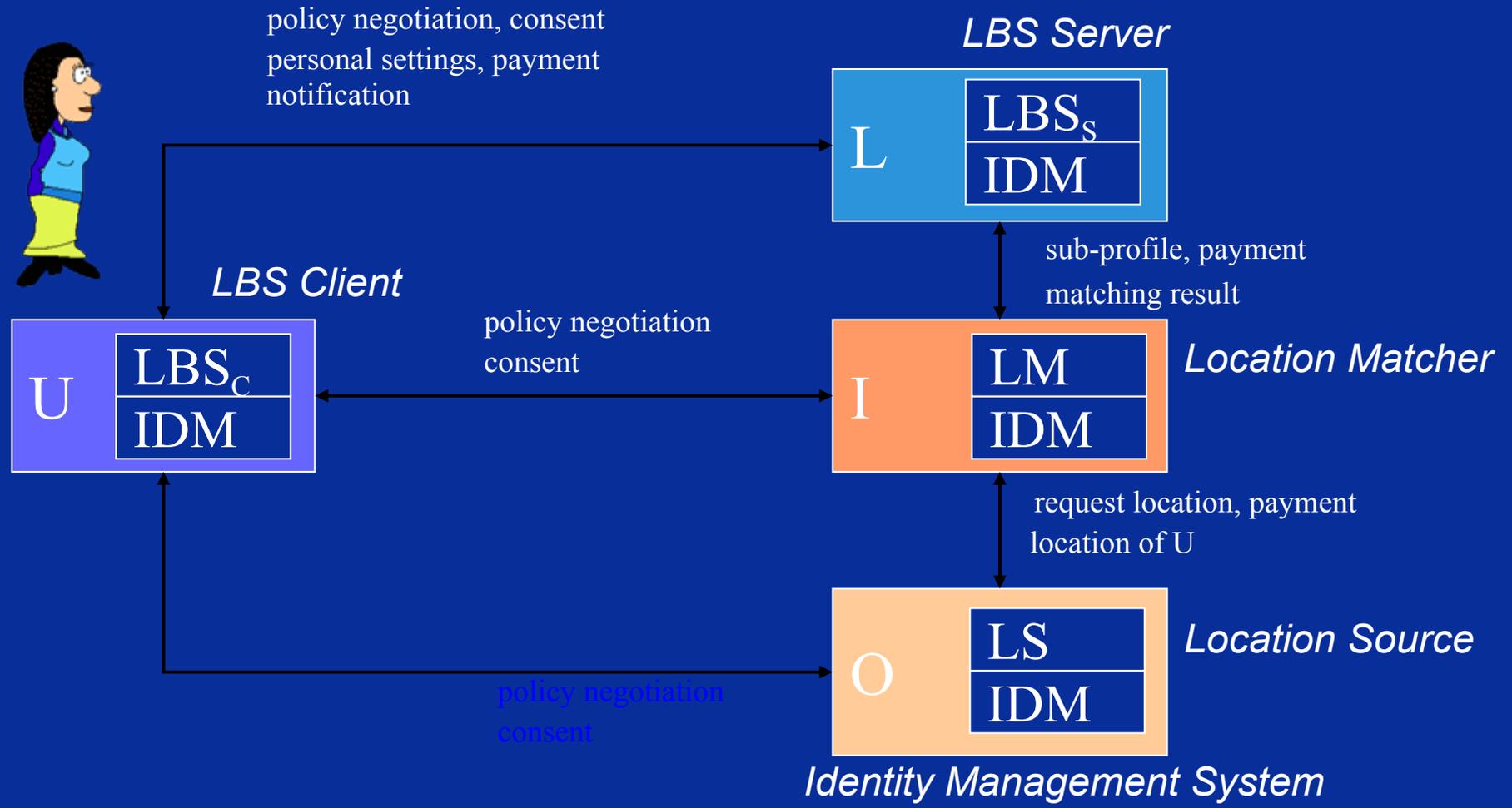
Business Models & Economic Rationale

Policy Management & Consent Requirements

Privacy Solutions

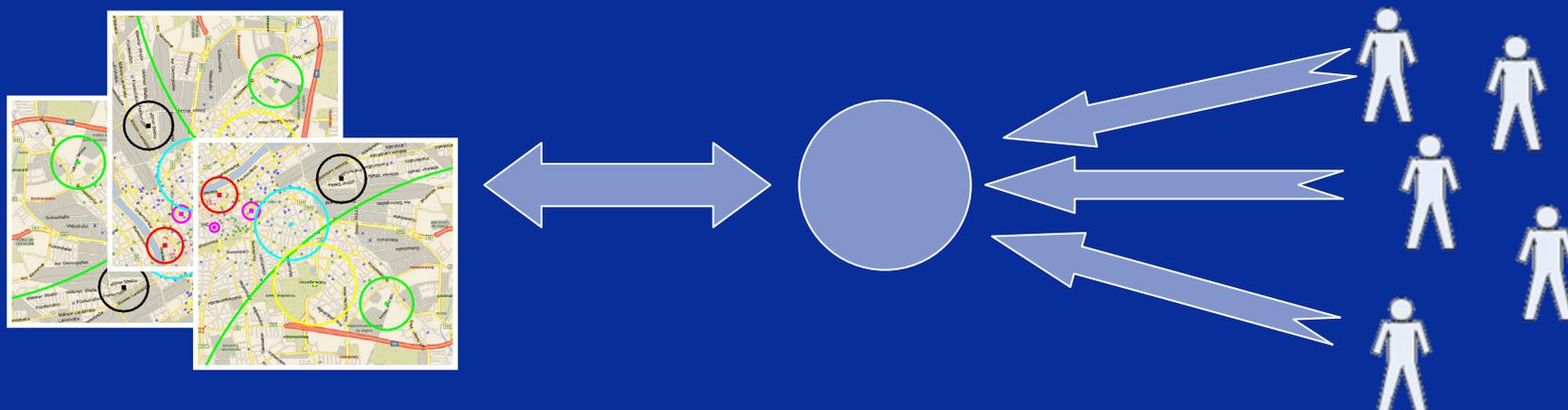


PRIME: LBS privacy architecture



Oblivious Maps

- ▶ Based on "tiling" of the map structure
- ▶ Bundling of requests to tiles through cryptographic methods
- ▶ Mapping server always sends a batch of tiles to a number of users through an "Oblivious transfer" protocol that hides tile receivers



Contents

- ▶ **Location Privacy**
 - Concepts
 - Technology
- ▶ **Privacy by Design**
 - Planning vs. Patching
 - Design Process
- ▶ **Business Incentives for Privacy**
 - Customer damage is business damage
 - Businesses want privacy, too!

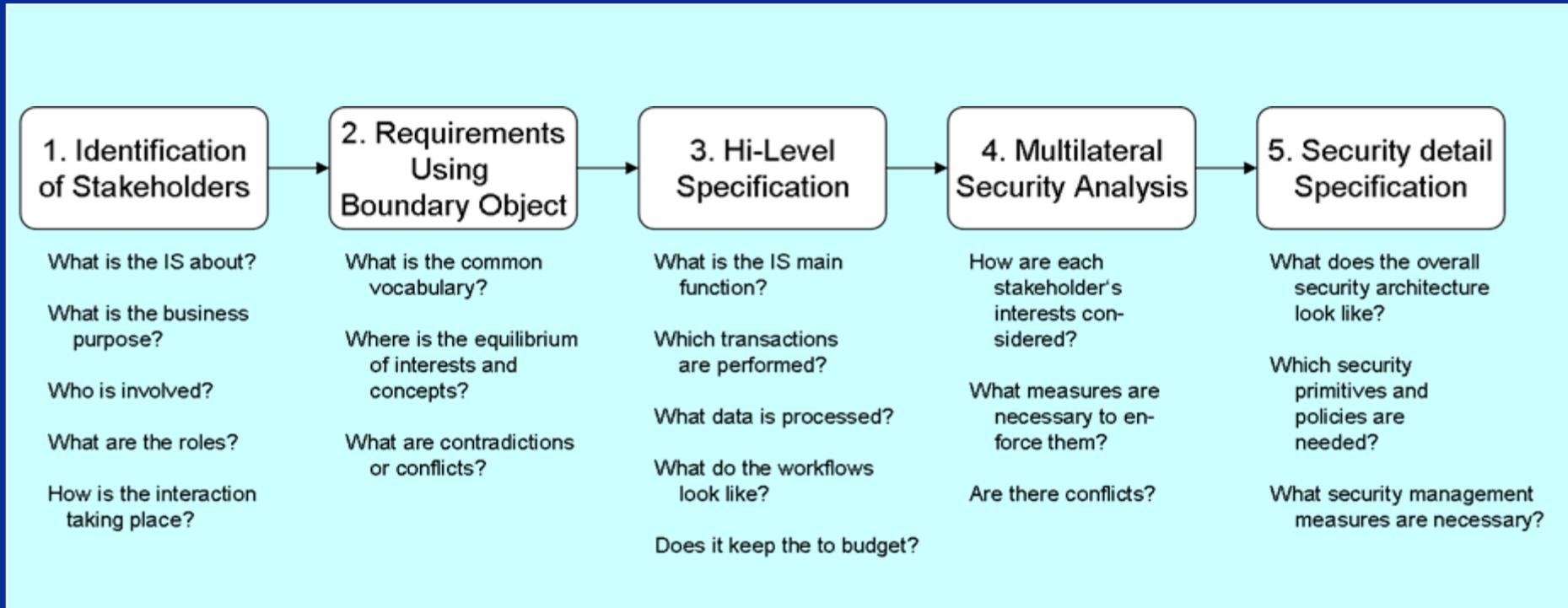
Cost of software maintenance:

- cheapest early in development
- Privacy & Identity Management are expensive to change!



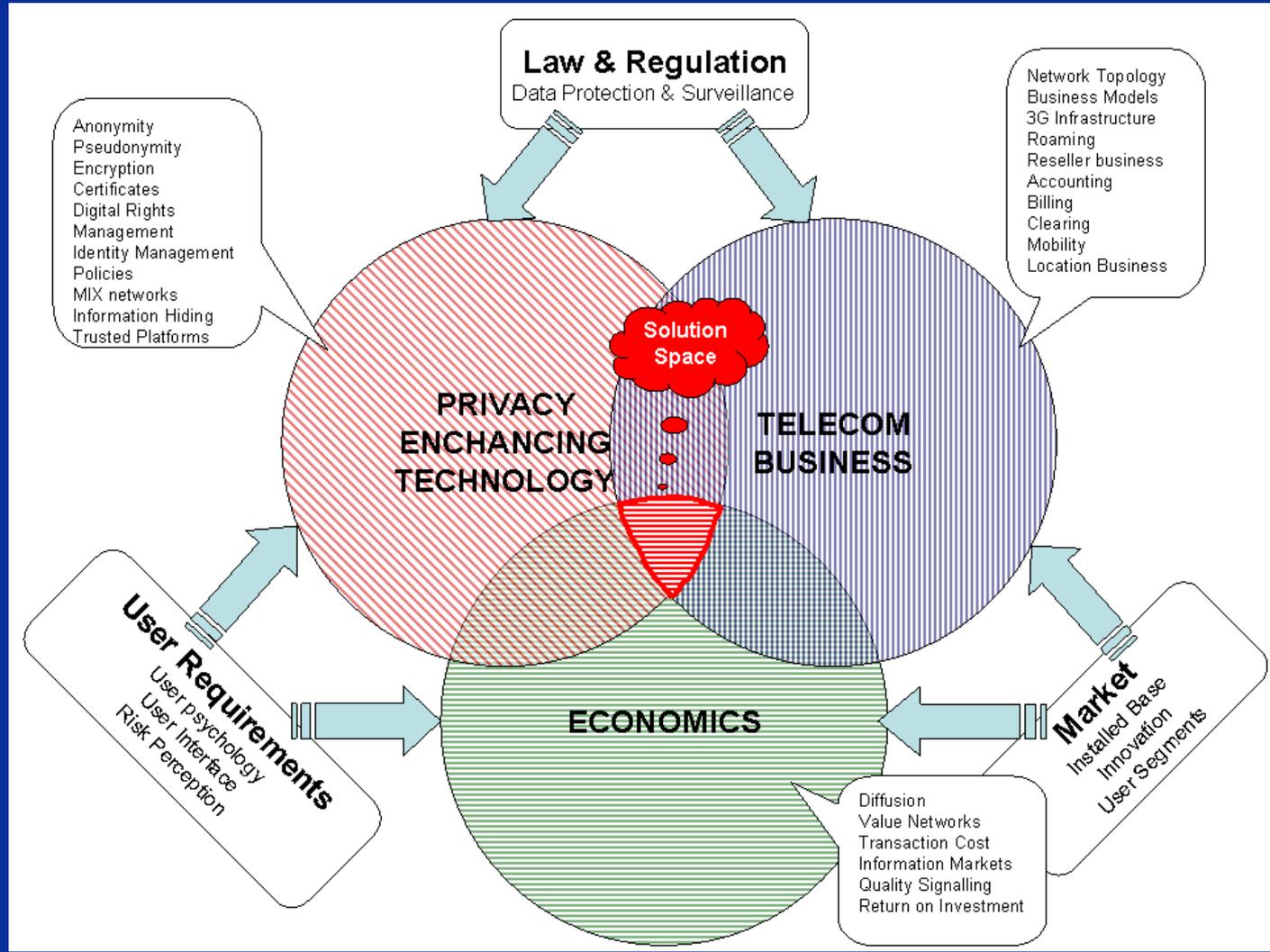
Privacy by Design provides cheaper results

Privacy by Design



[4]

Find a stakeholder consensus!

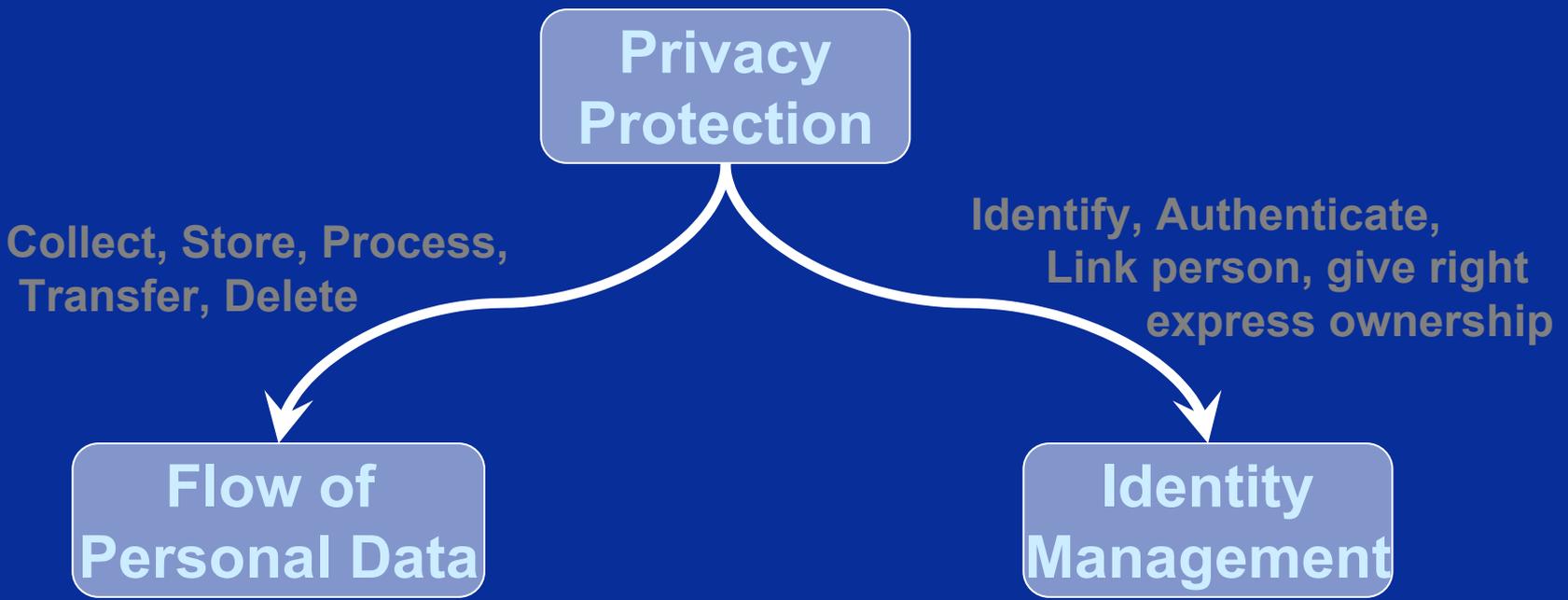


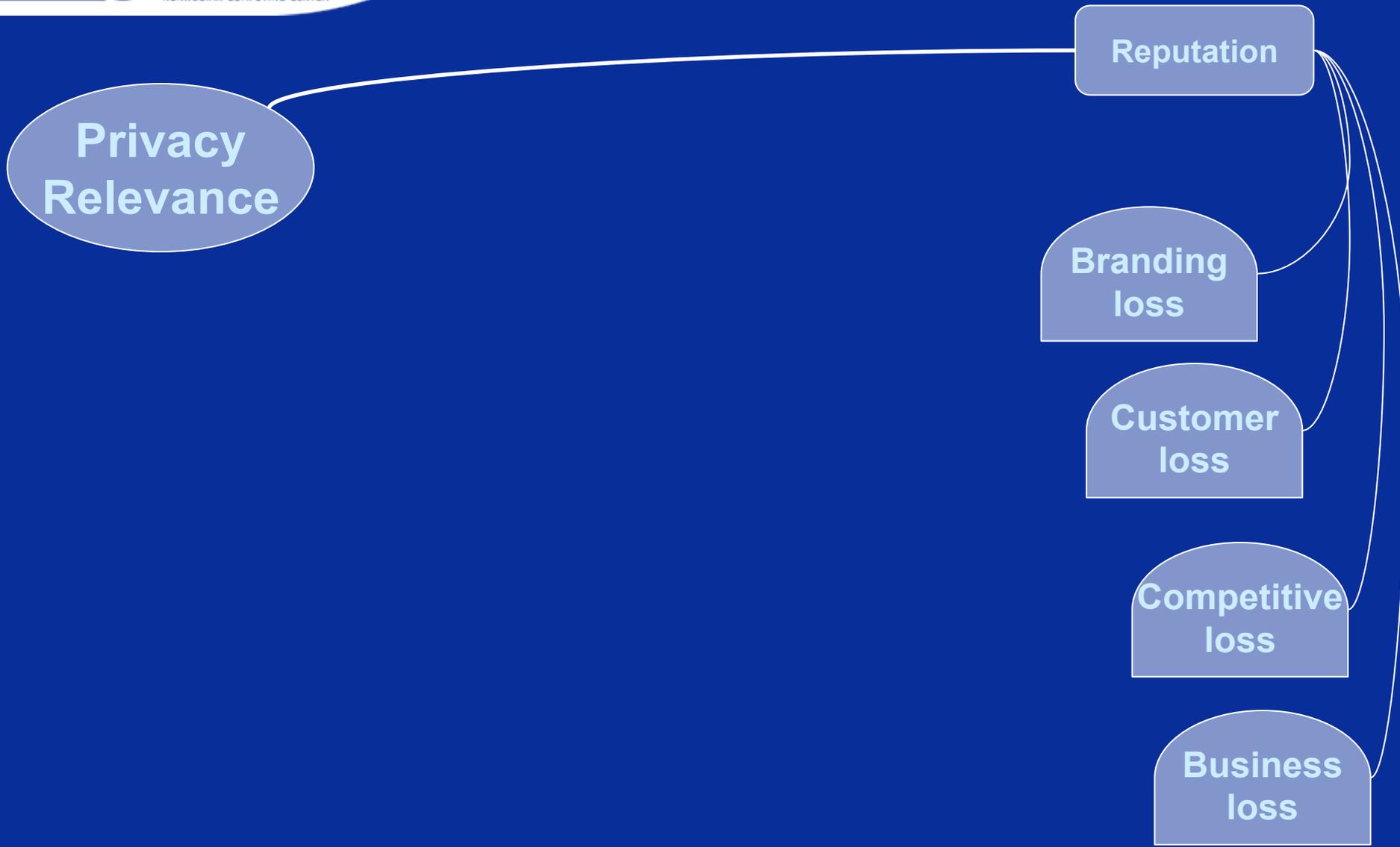
[4]

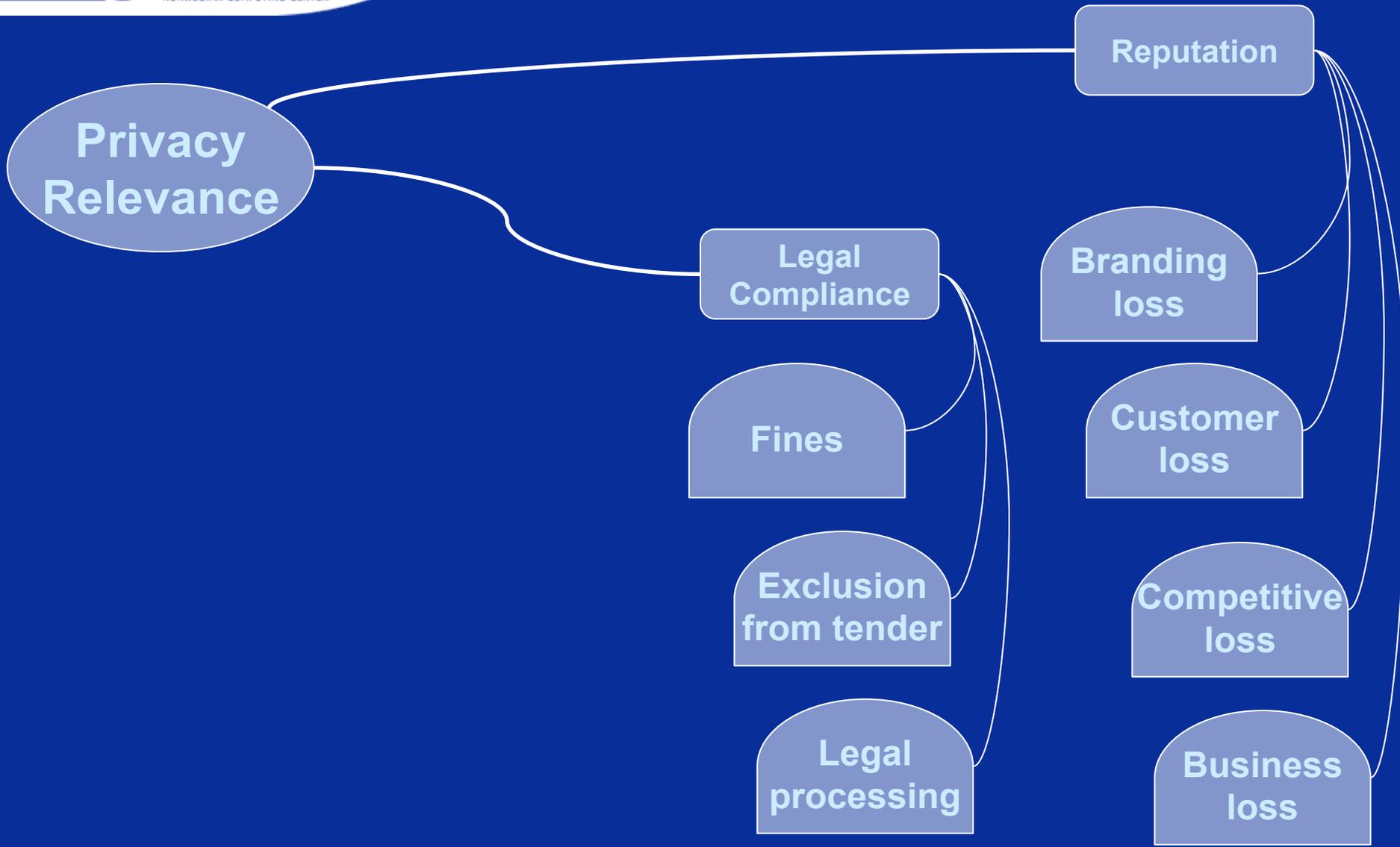
Contents

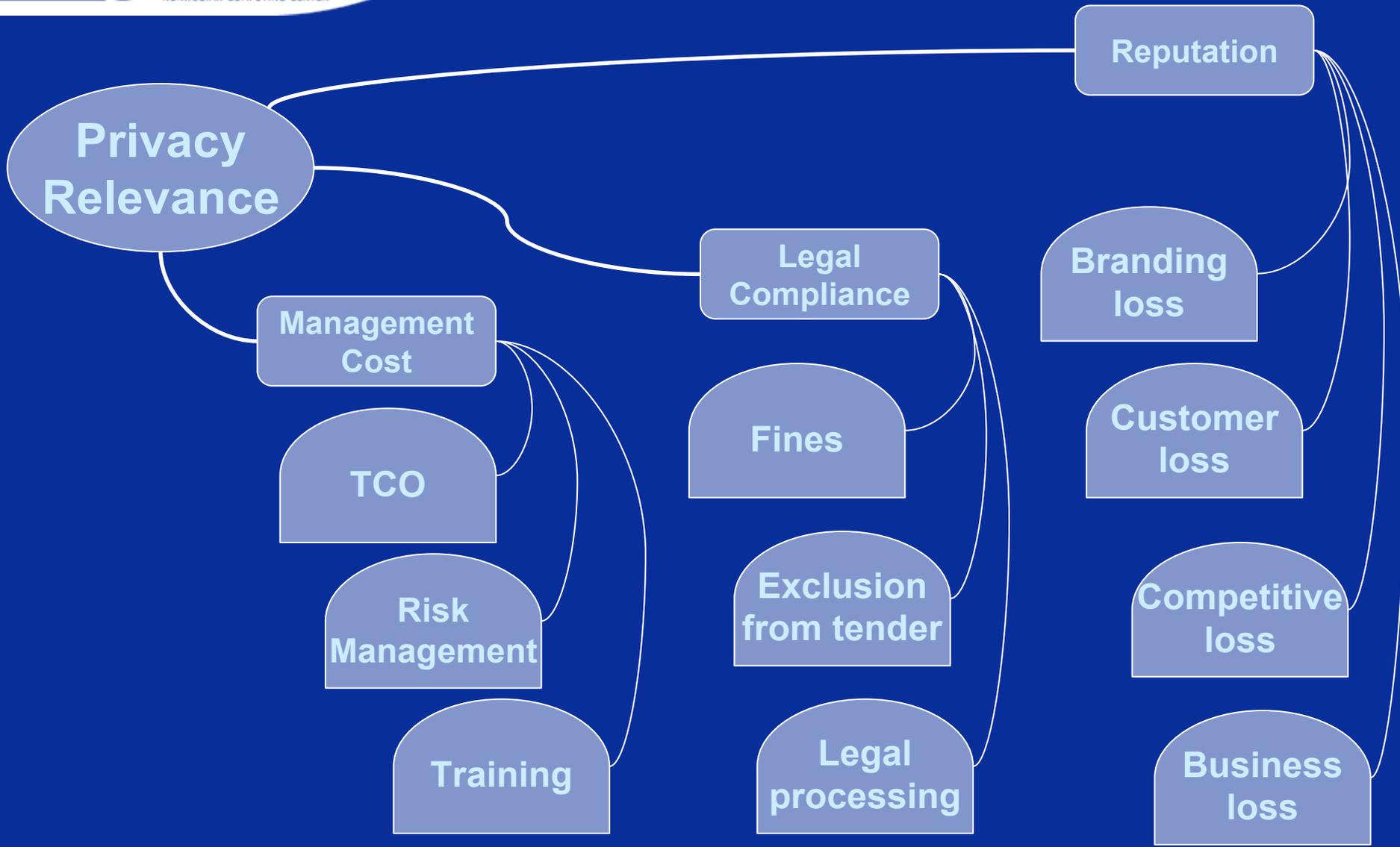
- ▶ **Location Privacy**
 - Concepts
 - Technology
- ▶ **Privacy by Design**
 - Planning vs. Patching
 - Design Process
- ▶ **Business Incentives for Privacy**
 - Customer damage is business damage
 - Businesses want privacy, too!

Privacy Protection in IT

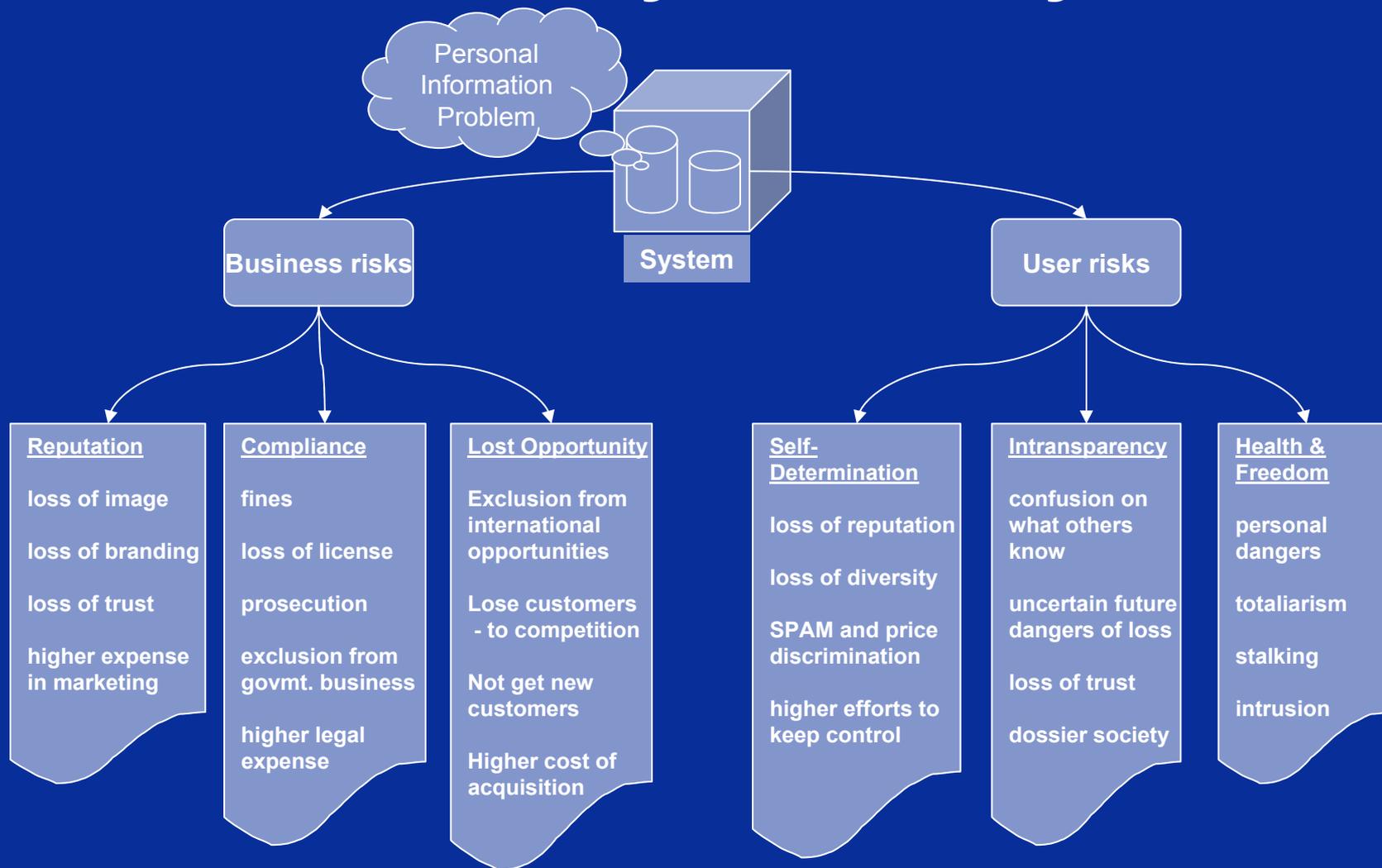








Duality of Privacy Risks



Businesses need privacy, too.

- ▶ Or... bad things might happen anytime soon...

The Boycott Photo



←----- 3G data connection -----→

Web community

Boycott
**FLATFISK
ASA!**

Boycott all
farmed
salmon!

Get 2 for the
price of 1 at
FJORDFISK!



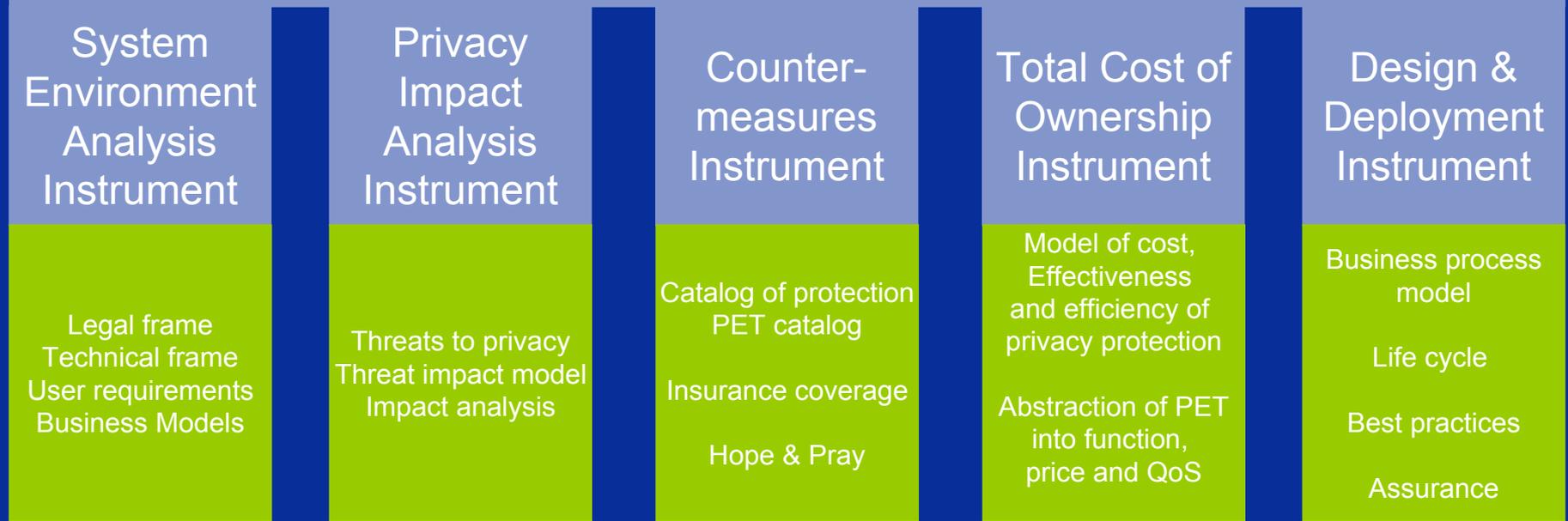
Supermarket cart

RFID future uses – the two-edged sword ^[5]

Imagine a world where...

- ▶ A vendor's trash (packages, products) will be tracked around the globe, even 20 years after production, until it turns up on a polluted site in Africa – and on some NGO's agenda;
- ▶ The city trash removal facilities read RFIDs on package waste to bill the producers for the trash processed;
- ▶ Corporate tax & toll is adjusted based on scanners at borders, ware houses and waste dumps.
- ▶ Does the "kill" function kill TID tag serial numbers?

Privacy by Design Instruments



Further reading

- [1] Fritsch, Lothar. (2008) Profiling and Location-Based Services, in: M. Hildebrandt und S. Gutwirth (Eds.): Profiling the European Citizen - Cross-Disciplinary Perspectives, April 2008, Dordrecht, Springer Netherlands, pp. 147-160.
- [2] Zibuschka, Jan; Fritsch, Lothar; Radmacher, Mike; Scherner, Tobias und Rannenber, Kai (2007) Privacy-Friendly LBS: A Prototype-supported Case Study, 13th Americas Conference on Information Systems (AMCIS), Keystone, Colorado, USA,.
- [3] Kohlweiss, Markulf; Gedrojc, Bartek; Fritsch, Lothar und Preneel, Bart. (2007) Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker, in: N. Borisov und P. Golle (Eds.): Privacy Enhancing Technologies, 7th International Symposium, PET 2007 (LNCS 4776), Berlin, Springer, pp. 77-94.
- [4] Fritsch, Lothar (2007) Privacy-Respecting Location-Based Service Infrastructures: A Socio-Technical Approach to Requirements Engineering, Journal of Theoretical and Applied E-Commerce research (2:3), pp. 1-17.
- [5] Fritsch, Lothar. (2009) Business risks from naive use of RFID in tracking, tracing and logistics, in: VDE Verlag GmbH (Eds.): RFID SysTech 2009 - ITG Fachbericht 216, 16.Jun. 2009, Berlin, pp. ch. 7.
- [6] Fritsch, Lothar und Abie, Habtamu. (2008) A Road Map to the Management of Privacy Risks in Information Systems, in: Gesellschaft f. Informatik (GI) (Eds.): Konferenzband Sicherheit 2008, Lecture Notes in Informatics LNI 128, 2-Apr-2008, Bonn, Gesellschaft für Informatik, pp. 1-15
- [7] Jan Camenisch, Lothar Fritsch, Markulf Kohlweiss, Mike Radmacher, and Dieter Sommer: LBS Application Prototype, "Requirements and Concepts", PRIME internal presentation, 2005

Contact

NR Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Lothar Fritsch

forsker · research scientist
DART · department of applied
research in information technology

dir. phone: (+47) 22 85 26 03
mob. phone: (+47) 968 85 758
Lothar.Fritsch@nr.no

Norsk Regnesentral · Norwegian Computing Center
Gaustadalléen 23, P.O. Box 114, Blindern
NO-0314 Oslo, Norway
www.nr.no · nr@nr.no

phone:
(+47) 22 85 25 00
fax:
(+47) 22 69 76 60