Fraunhofer Institut Sichere Informations-Technologie

Supports for Identity Management in Ambient Environments – The HYDRA Approach

I-Centric
26th Oct – 31st Oct, 2008, Sliema, Malta

Hasan Akram
(MSc.-Inform.)
Researcher
Fraunhofer Institute for Secure Information Technology

Mario Hoffmann
(Dipl.-Inform.)
Head of Department "Secure mobile Systems"
Fraunhofer Institute for Secure Information Technology

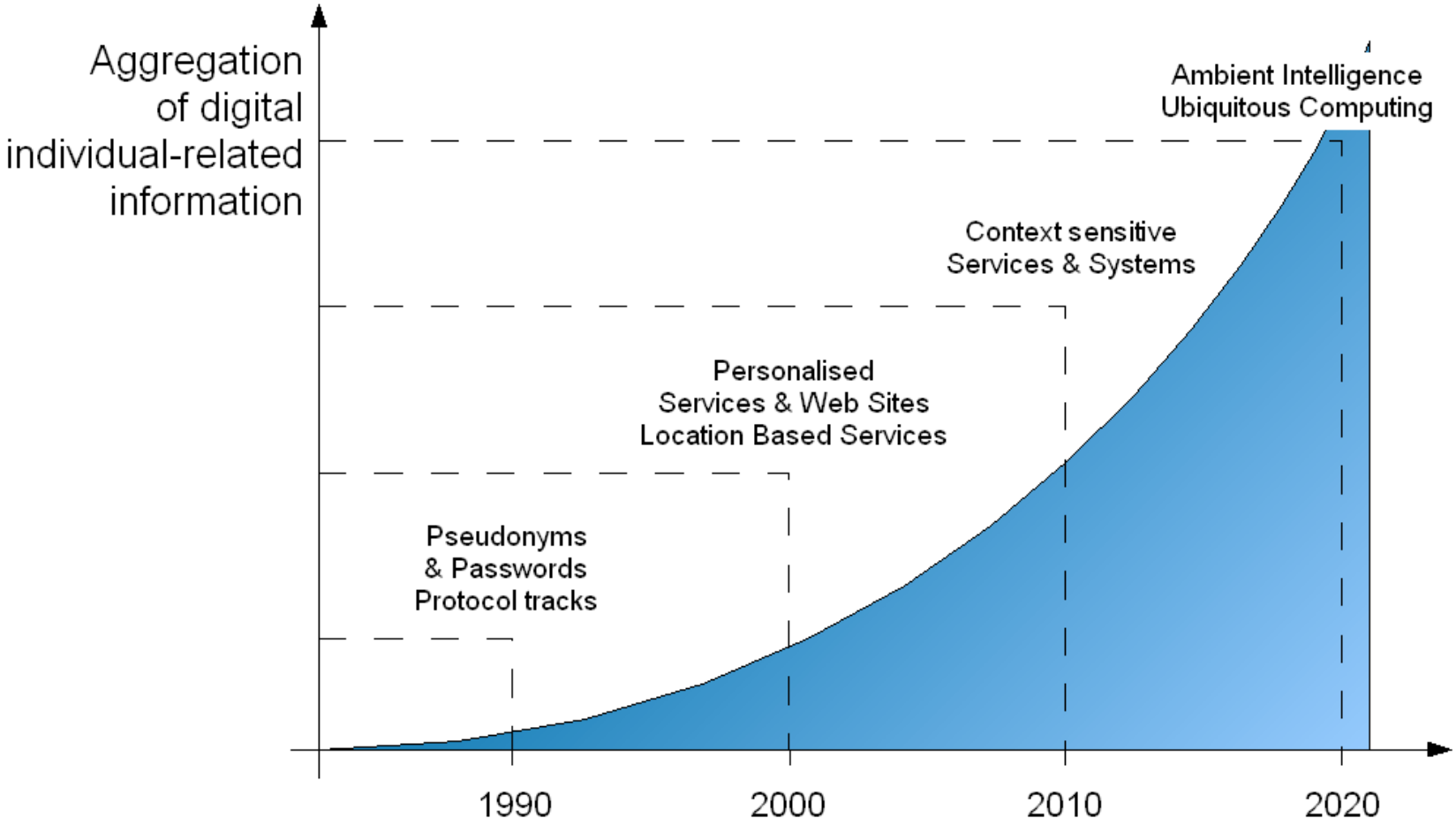
Loss of control

Surveillance

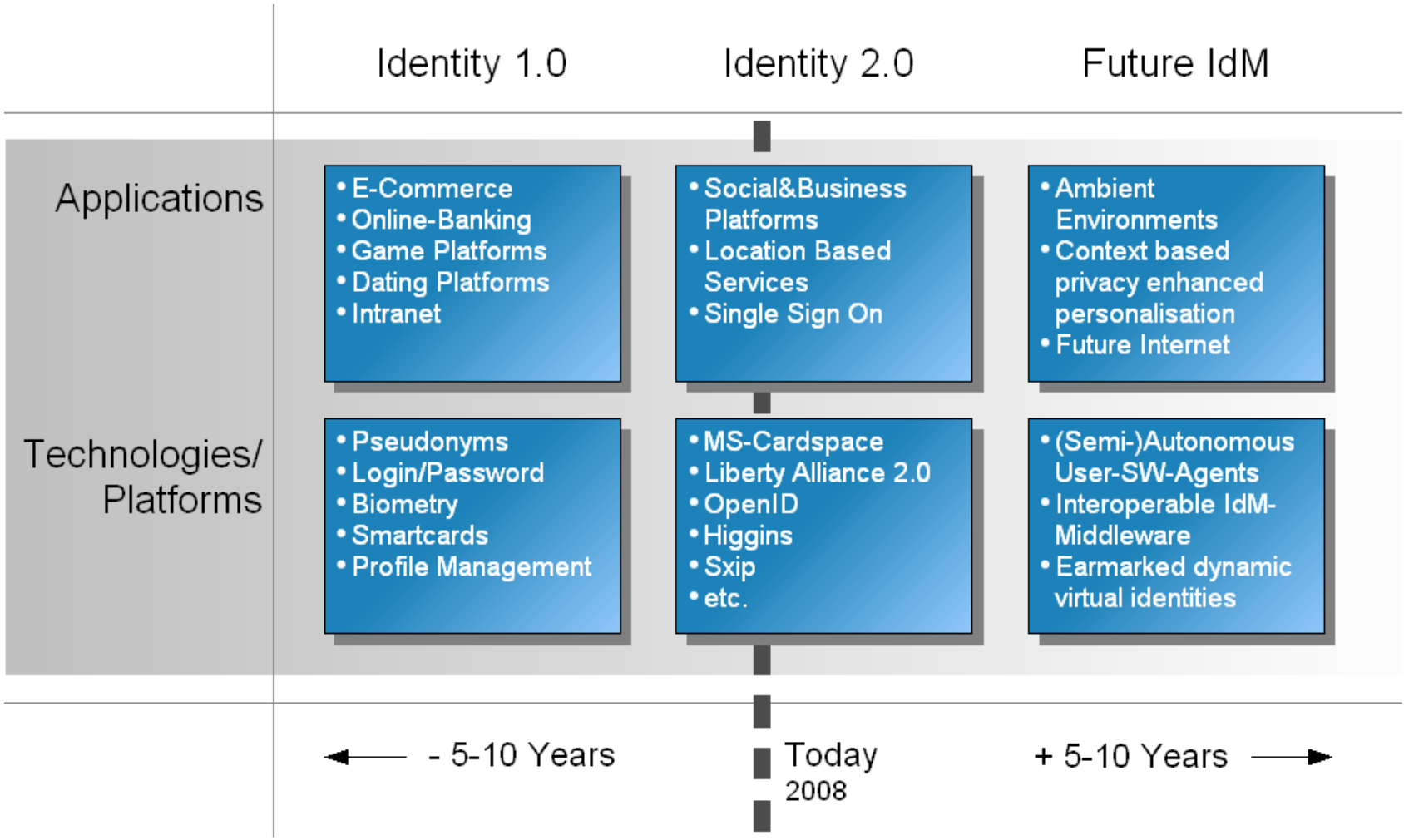
Profiling

(SWAMI-Safeguards in a World of Ambient Intelligence, EU-Project, FP6)

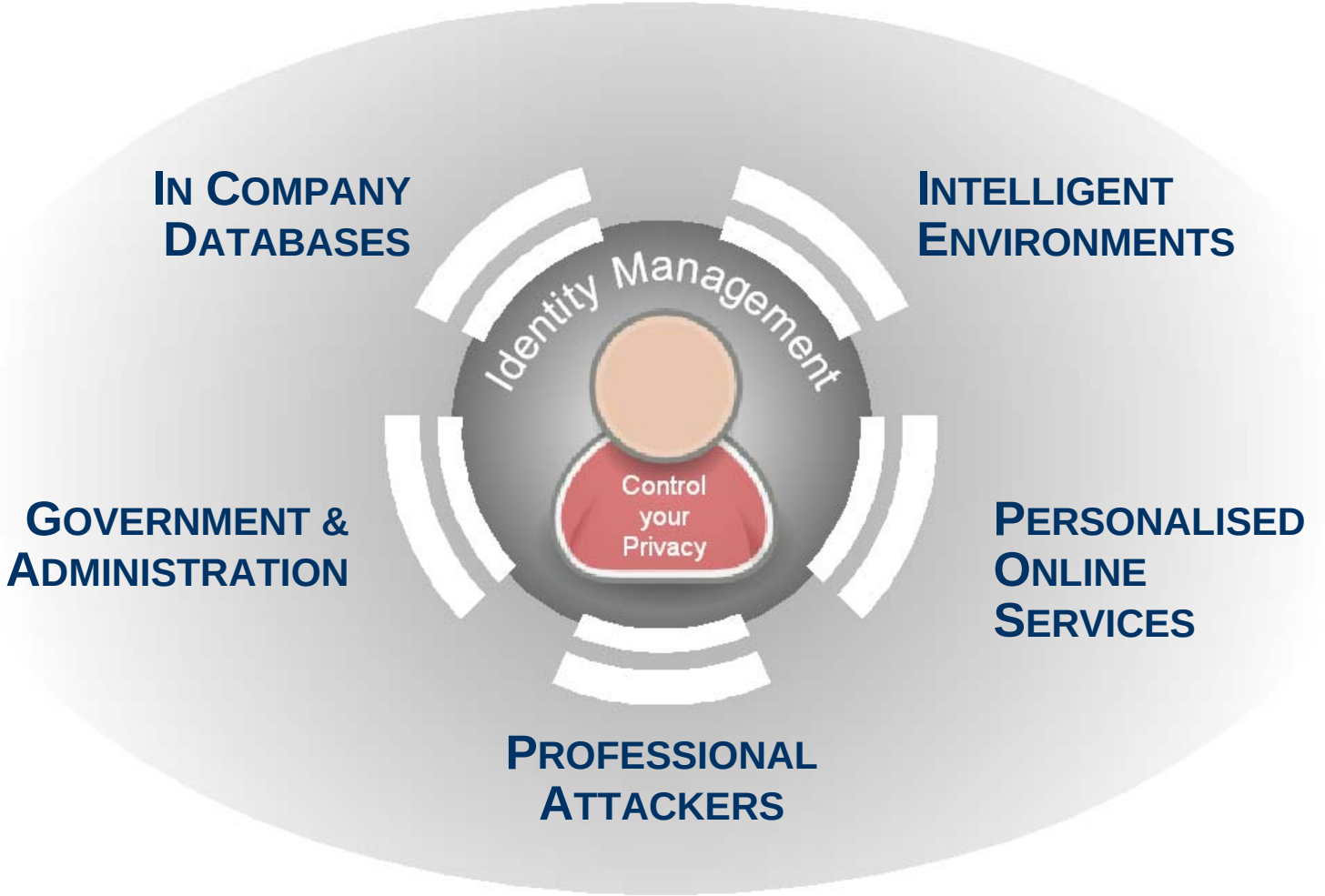
Rapidly Increasing Amount of Personalisable Information



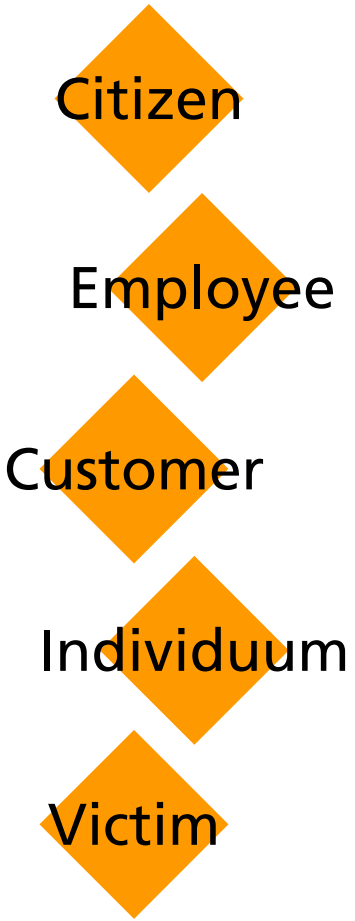
Identity Management Roadmap



User-centricity
A question of the perspective



(Research) Challenges for User-centric Identity Management



- User Empowerment
  - User-controlled Identity Management
  - Informational Self-determination
  - Minimisation of Information Disclosure
  - Transparency
- Support of Anonymity & Pseudonymity
  - Application level
  - Middleware
  - Access and Core Networks
- Privacy-enhanced Personalisation
  - Best Practice
  - Rise Awareness
- New Development Tools for Ambient Environments
  - Efficient and flexible Service Creation
  - Security & Privacy by Design (default configuration)

The Backend for Ambient Intelligent Systems

Networked Embedded System Middleware for Heterogeneous Physical Devices in a Distributed Architecture

The Hydra project is co-funded by the European Commission within the Sixth Framework Programme under contract IST-2005-034891

Partners

1 C International Ltd., UK
2 CNet Sweden AB, SE
3a Fraunhofer Institute for Applied Information Technology, DE
3b **Fraunhofer Institute for Secure Information Technology, DE**
4 In-JeT ApS, DK
5 Priway, DK
6 T-Connect, IT
7 Telefónica I+D, ES
8 University of Aarhus, Dept. of Computer Science, DK
9 Innova S.p.A., IT
10 University of Reading, Informatics Research Centre, UK
11 MESH Technologies, DK
12 Siemens Business Services, DE
13 Technical University of Kosice

The main challenge for implementation of ambient computing in networked embedded systems is to support the self-adaptive interplay of a vast range of existing and new components.

3 major objectives:

- middleware tool that allows developers to develop systems with embedded, autonomic ambient intelligence computing
- middleware tool that hides the complexity of the underlying infrastructure
- make new and existing distributed device networks trustworthy and secure, robust and fault tolerant

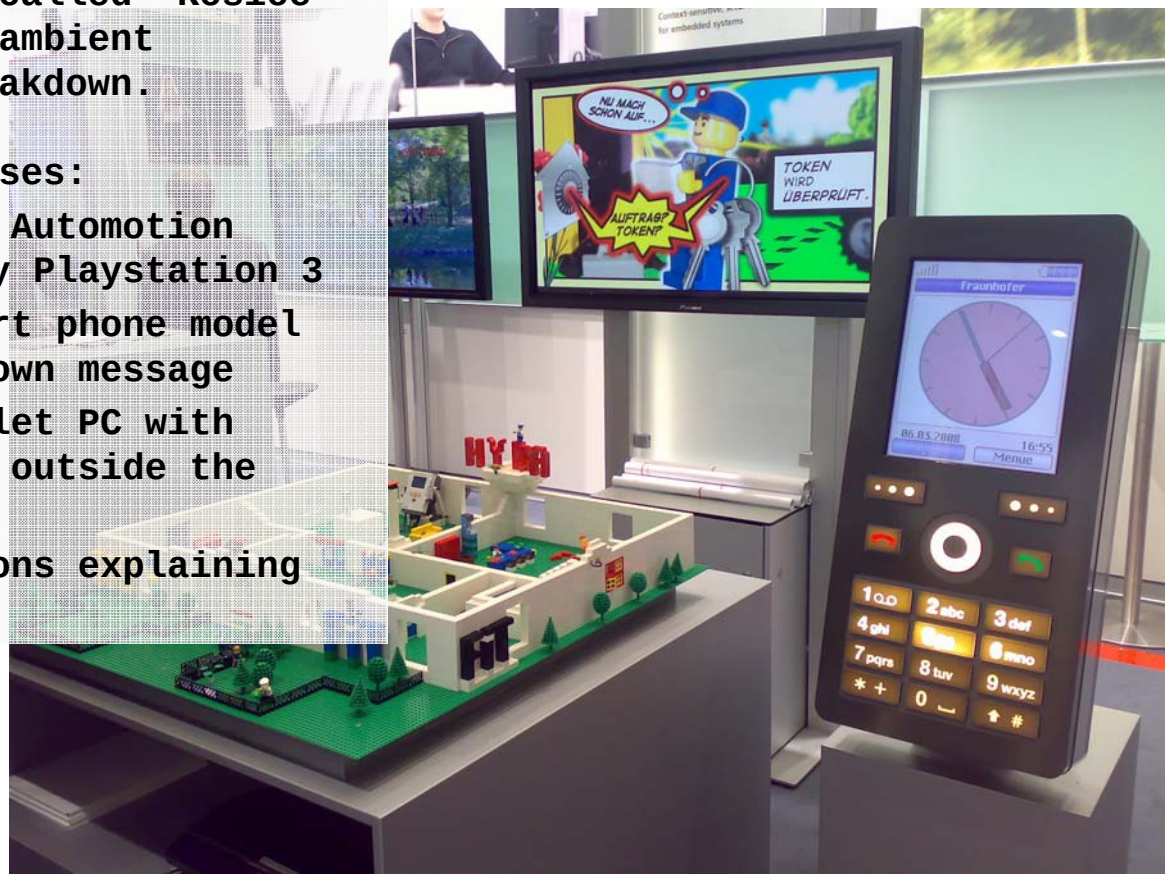
Outlook: Prototype

ICT Summit, 25th-27th Nov 2008, Lyon, France

The photo shows the so-called “Kosice scenario“ realising an ambient intelligent heating breakdown.

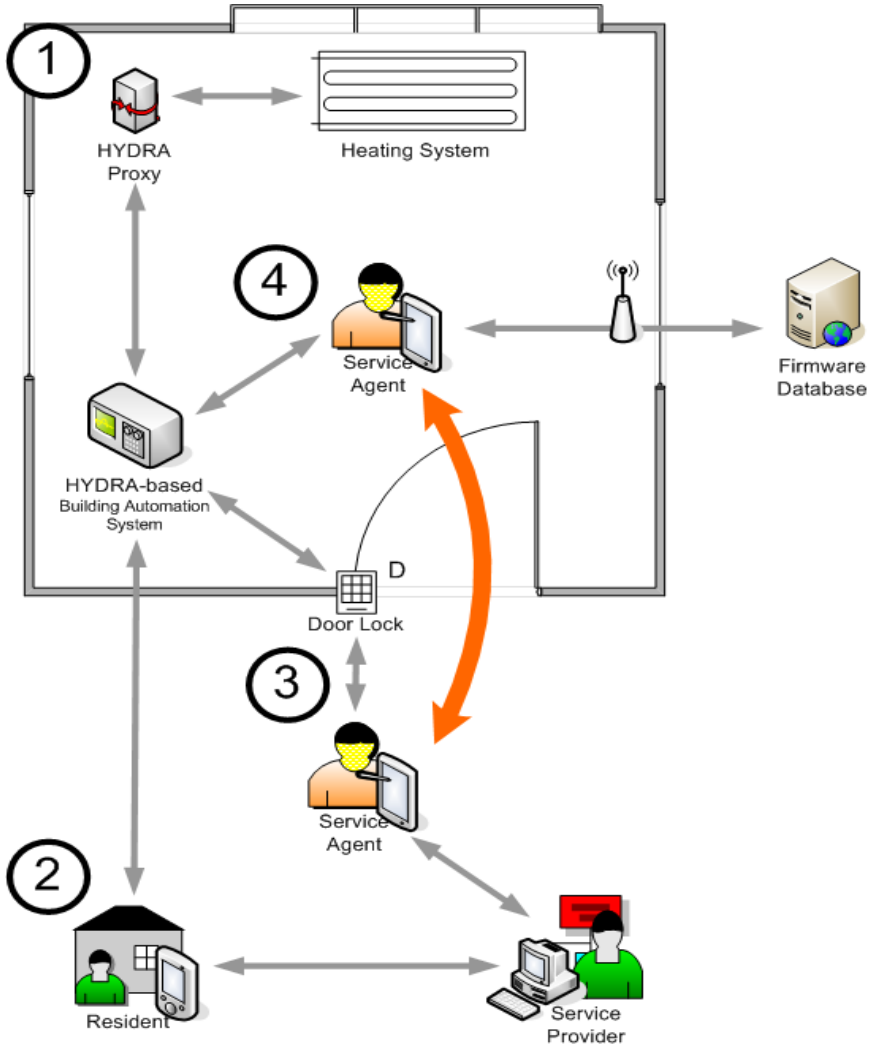
The demonstrator comprises:

- **Hydra-based Building Automotion System (HBAS) on Sony Playstation 3**
- **Larger-than-life smart phone model receiving the breakdown message**
- **The technician‘s Tablet PC with Smartcard unit (left outside the photo)**
- **Animated Flash cartoons explaining the process**

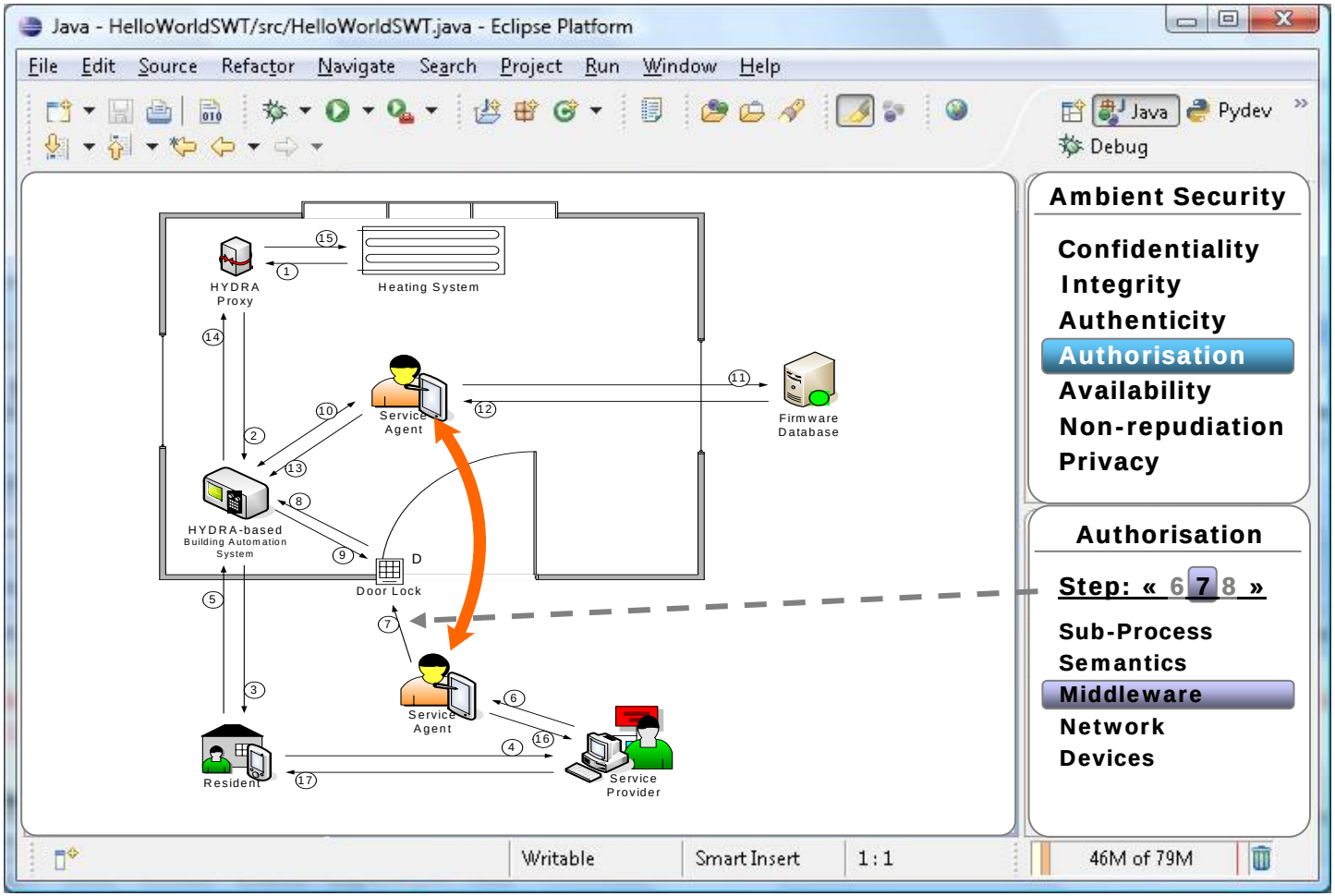


HYDRA Scenario:

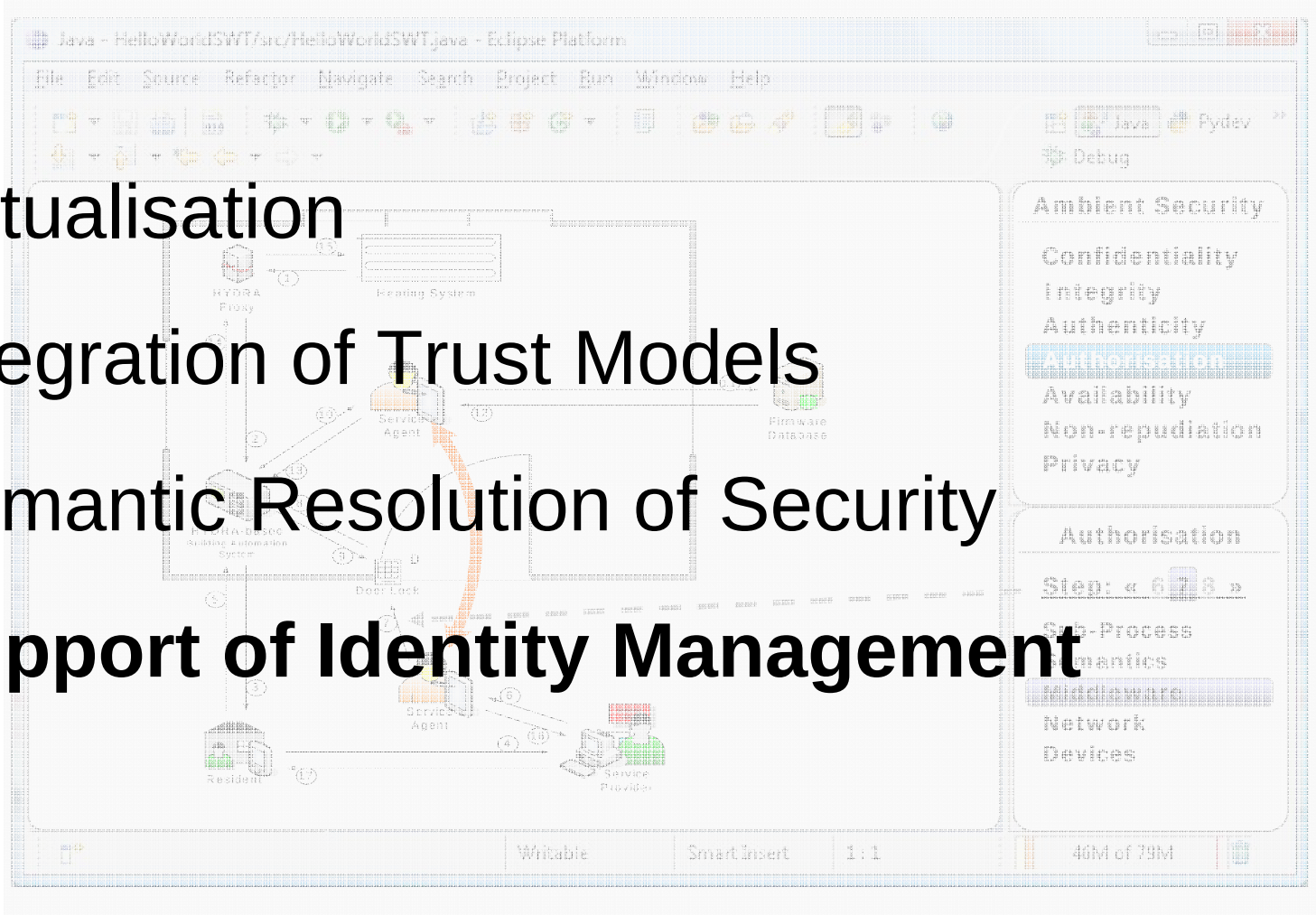
1. Breakdown of the Heating System
   - Context information to enhance resolution process
2. Resident receives error
   - Send request with context specific token
3. Approach of the service agent
   - Token is co-signed by service provider
4. Firmware update
   - Restricted access to internet based on context



Hydra's Security by Design Approach



Hydra's Security by Design Approach



Virtualisation

Integration of Trust Models

Semantic Resolution of Security

Support of Identity Management

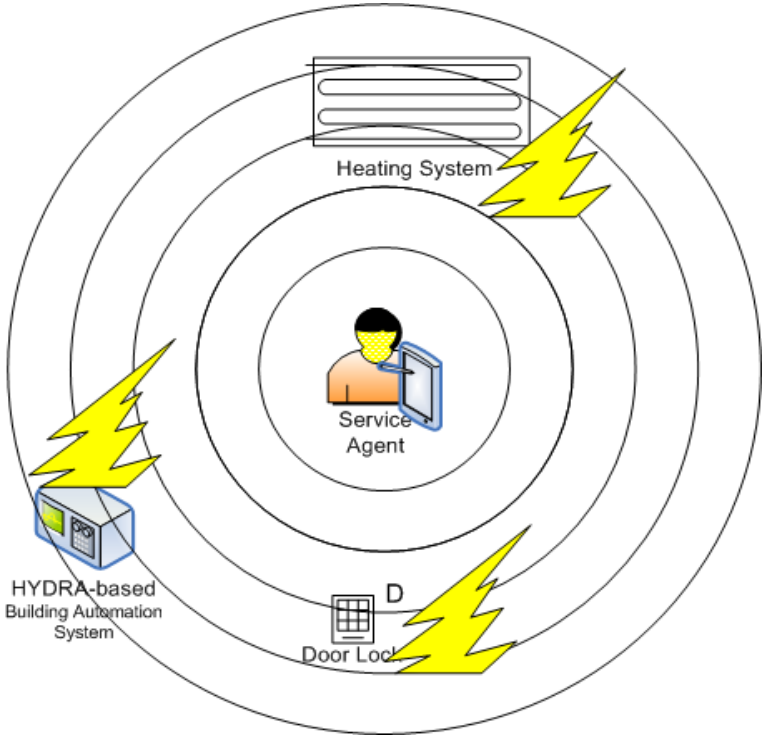
HYDRA's Ten Laws of Identity

1. User Empowerment: Awareness and Control
2. Minimal Information Disclosure for a Constrained Use
3. Non-repudiation
4. Support for directional identity topologies
5. Universal Identity Bus
6. Provision of defining strength of identity
7. Decoupling identity management layer from application layer
8. Usability issue concerning identity selection and disclosure
9. Consistent experience across contexts
10. Scalability

- User Empowerment: Awareness and Control

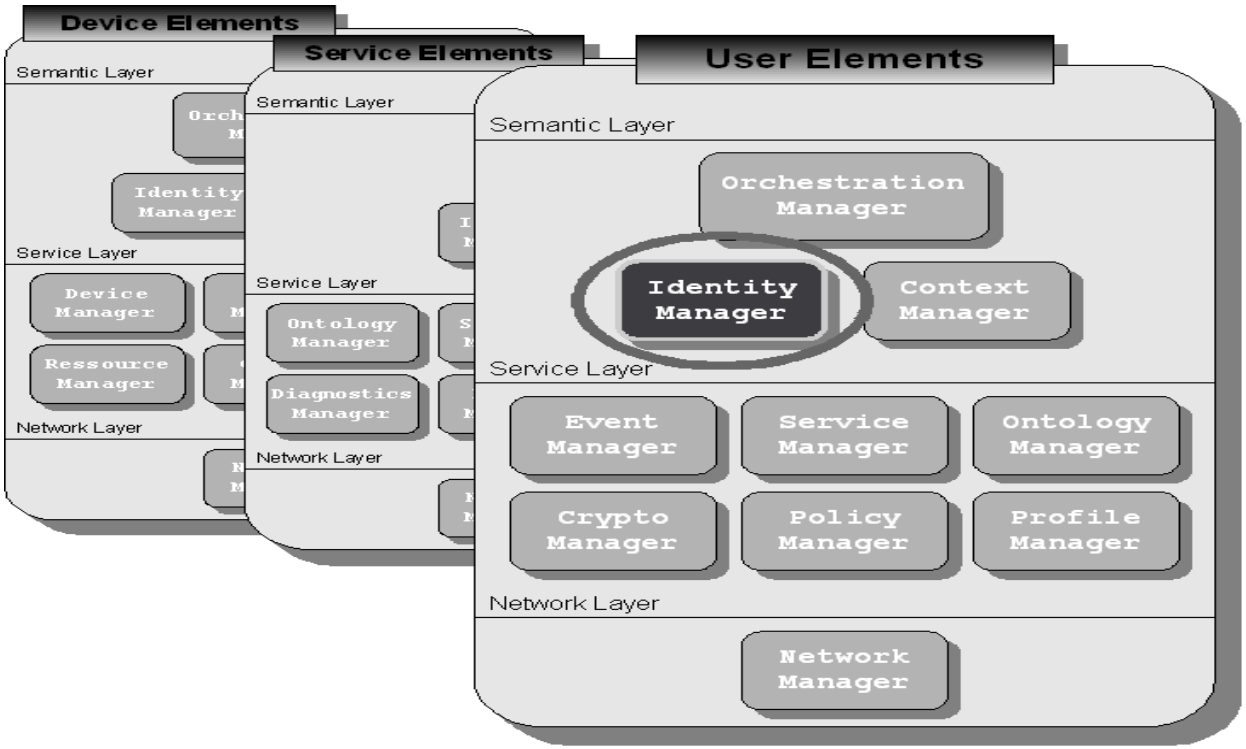
HYDRA Identity Law 4

- Support for directional identity topologies

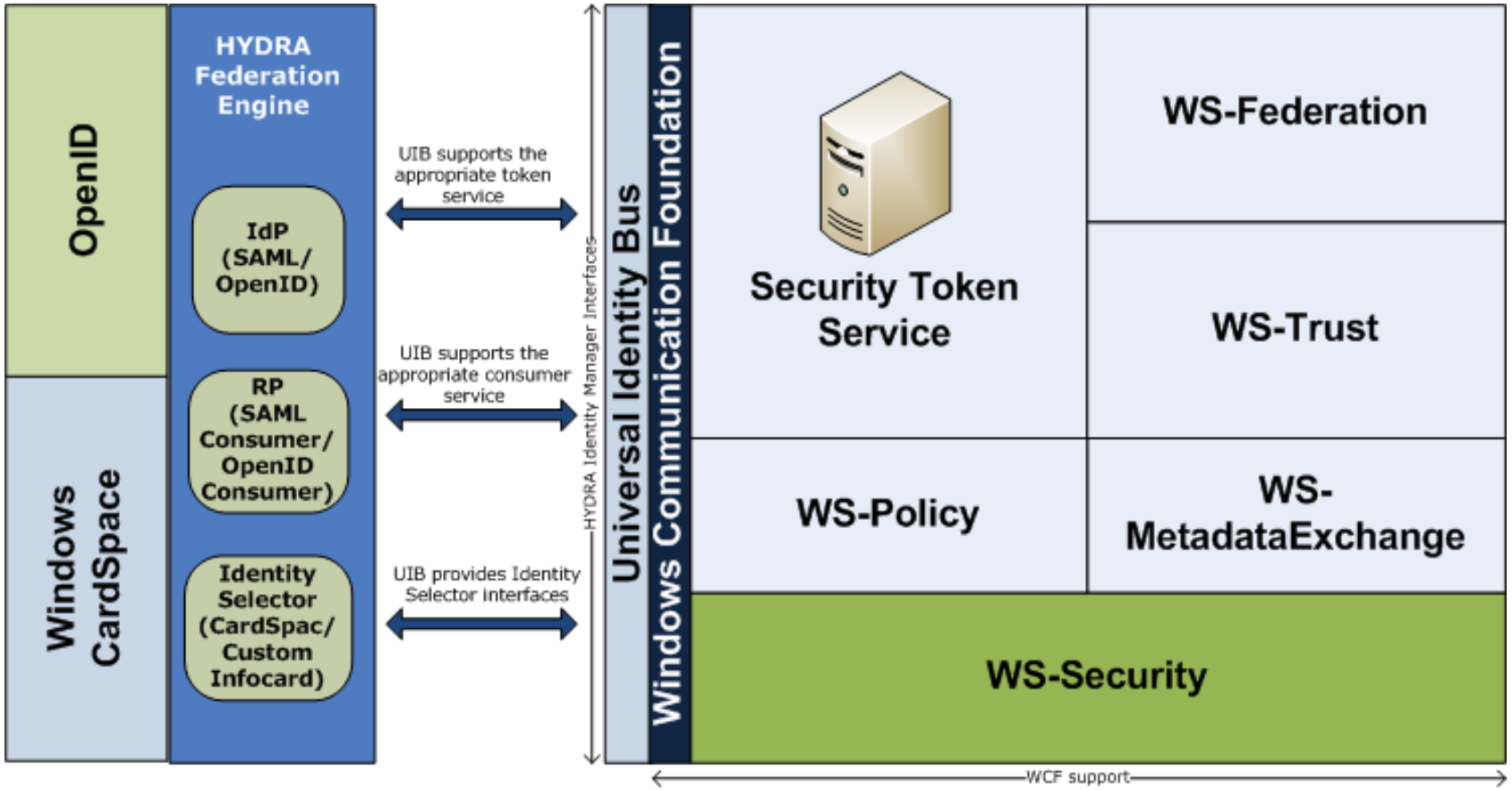


HYDRA Identity Law 7

- Decoupling identity management layer from application layer



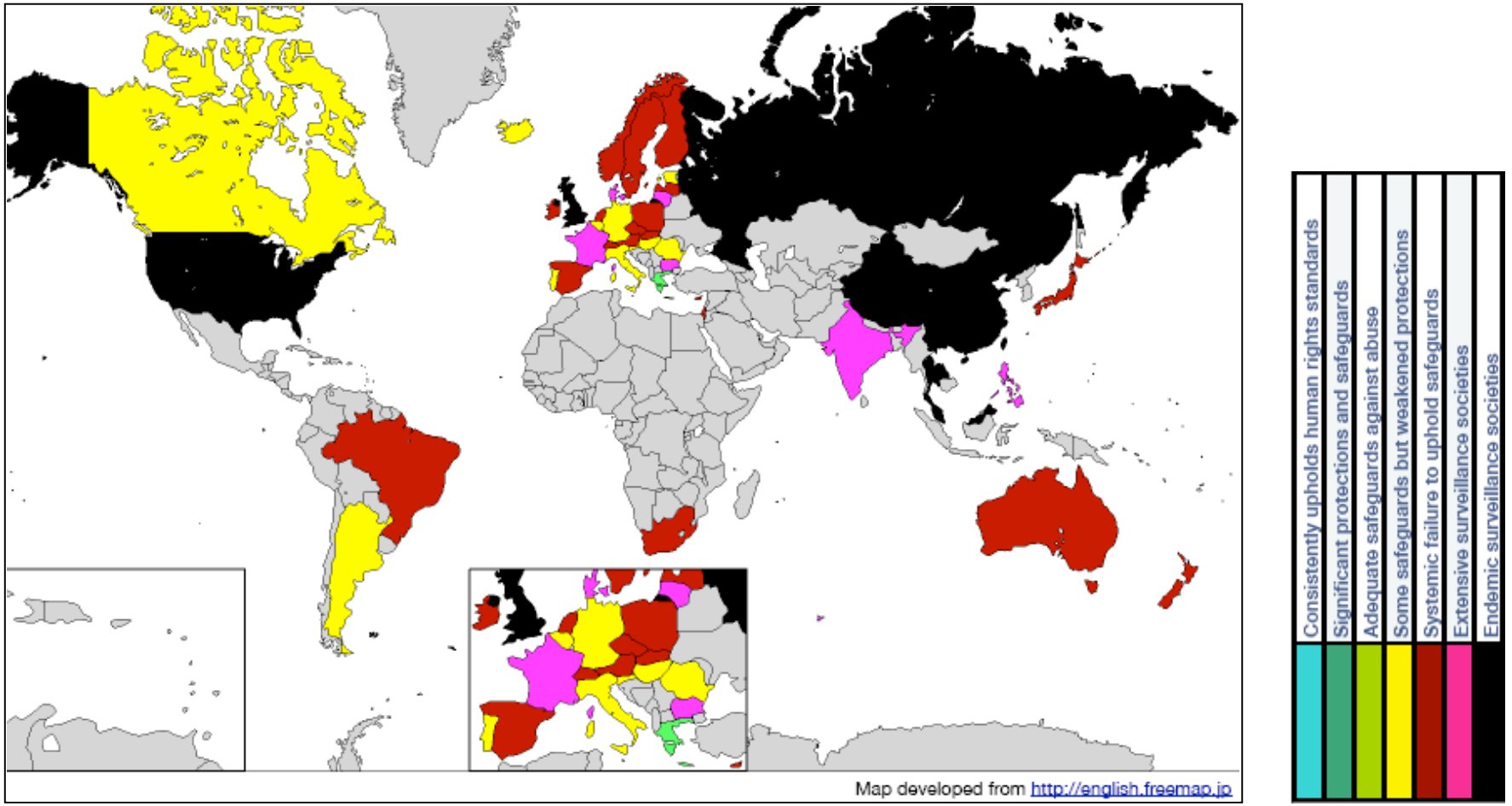
Architecture/Implementation



State of the Art Evaluation

Hydra Identity Laws	SAML	OpenID	CardSpace	Shiboleth	Higgins	Liberty	HIM
1. User Empowerment	-	-	++	-	-	-	++
2. Minimal Disclosure	+	+	+	++	+	+	++
3. Non-repudiation	-	-	o	-	+	o	+
4. Directional Identity	o	++	++	-	++	+	++
5. Universal Identity Bus	-	-	+	-	++	++	+
6. Strength of Identity	-	-	-	-	-	-	+
7. Decoupling Layers	-	o	++	o	++	o	++
8. Usability	-	o	++	o	++	o	++
9. Context Consistency	+	++	++	-	++	++	++
10. Scalability	++	++	++	+	++	++	+

Socio-Political Frameworks & Legal Aspects



http://www.privacyinternational.org/

Summary

- Different perspectives allow different interpretations of the term “user-centric”
  - The perspective of the user is decisive!
- Privacy enhancing technologies (e.g. on middleware layer) have to enable developers to design privacy preserving applications
- Socio-political environments and legal constraints have to be taken into account
- Privacy and data protection needs support from politics and society

Contact

Mario Hoffmann (Dipl.-Inform.)
Head of Department “Secure mobile Systems“

Address Fraunhofer Institute for
Secure Information Technology
Rheinstrasse 75
64295 Darmstadt
Germany

Tel +49-(0)6151/869-60034
Fax +49-(0)6151/869-224
e-Mail mario.hoffmann@sit.fraunhofer.de