Fraunhofer Institut Sichere Informations-Technologie

Requirements Analysis for Identity Management in Ambient Environment: the HYDRA Approach

Context Awareness and Trust 2008
2nd International Workshop on Combining Context with Trust, Security and Privacy
June 16th, Trondheim, Norway

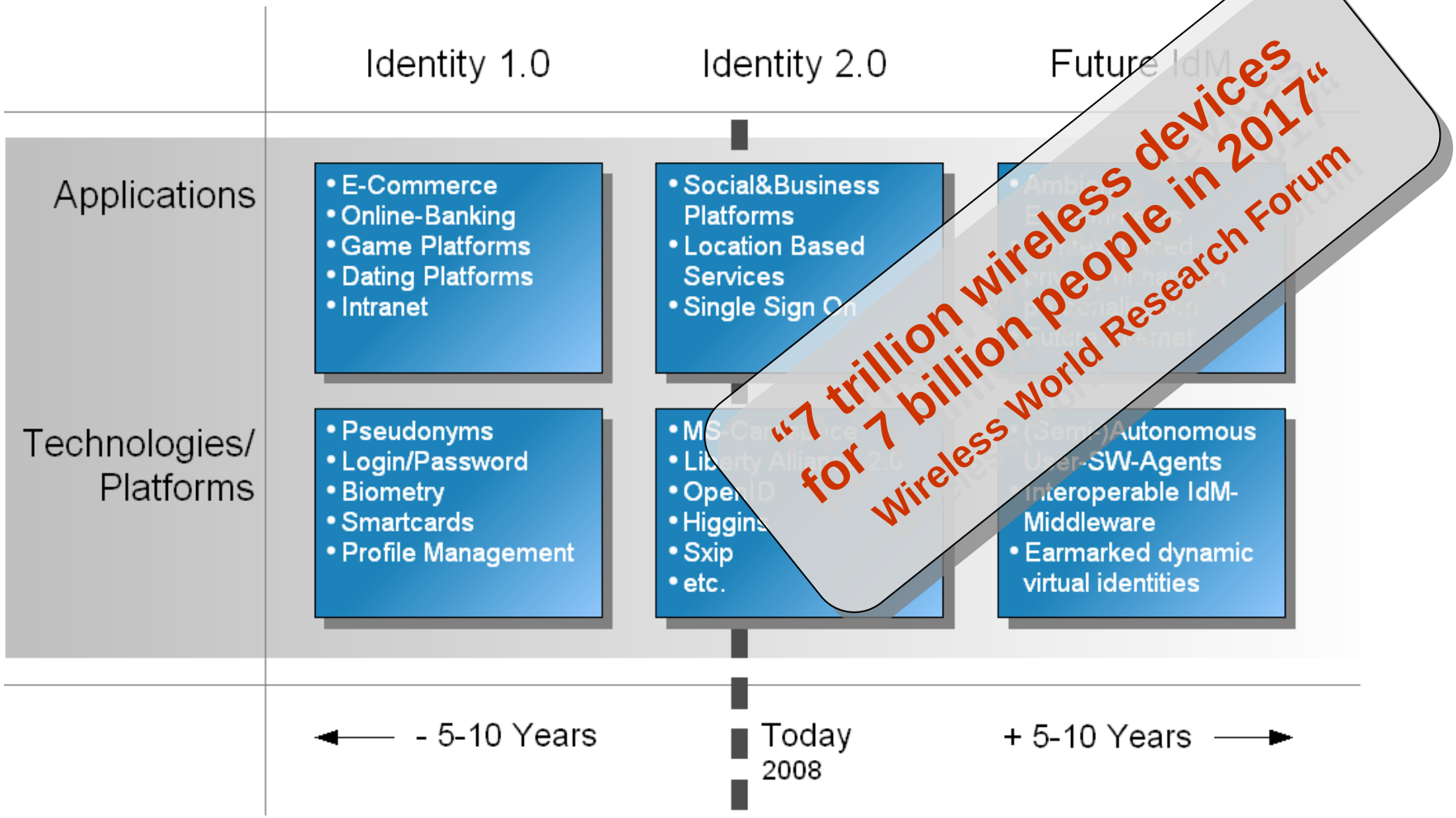
Hasan Akram
Fraunhofer Institute for Secure Information Technology
Darmstadt University of Technology

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

Motivation

- **Identity theft**
  - **loss of $50 billion in US/year**
  - **$5 billion on top to undo the harm**
- **Phishing and Pharming**
  - **Growing at a compound rate of 1000%**
  - **Fastest growing segment of IT industry**
- **Identity Silos**
- **Decoupling identity from rest of the application**

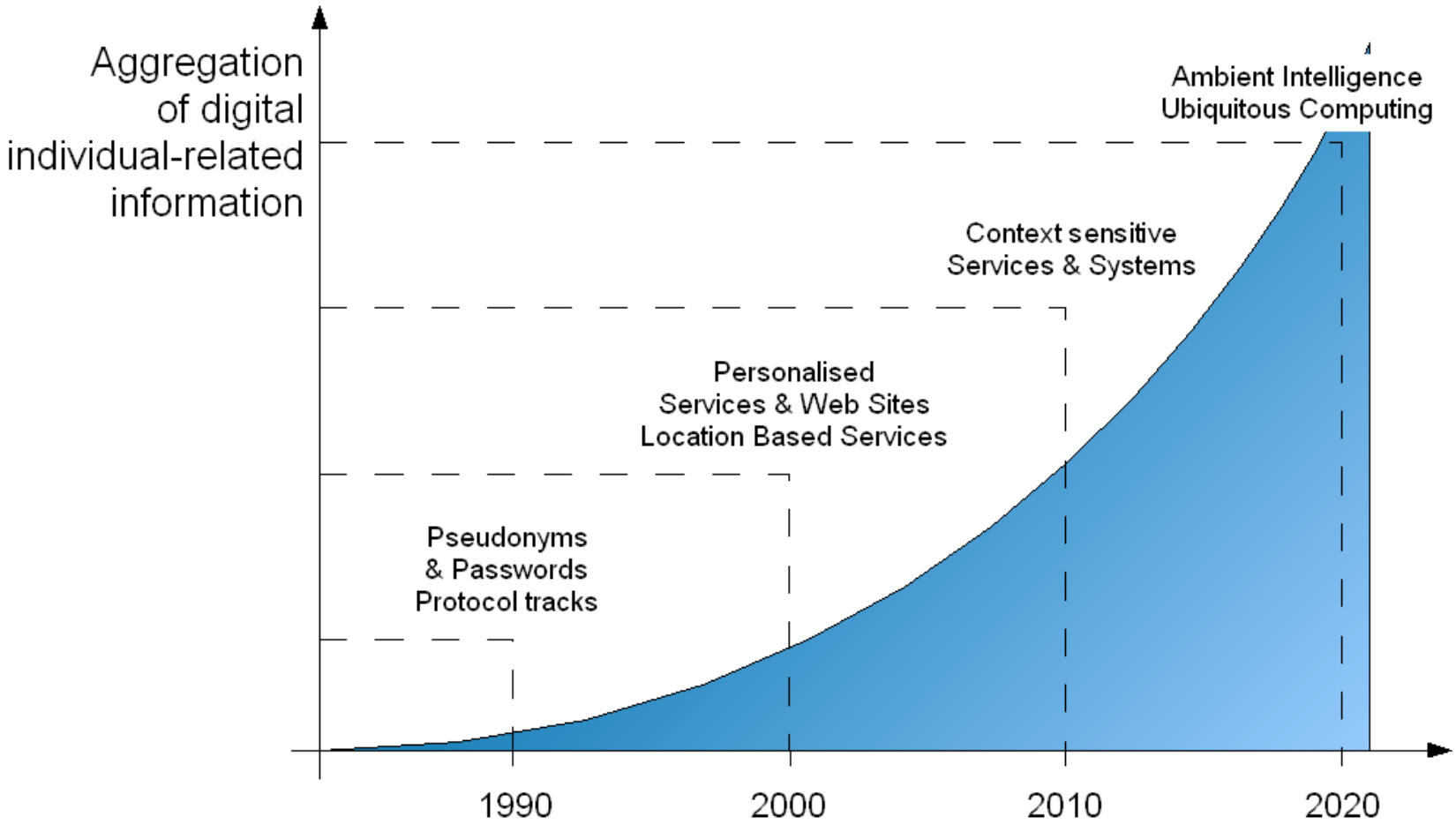
Foreseeing the future – Identity Management Roadmap



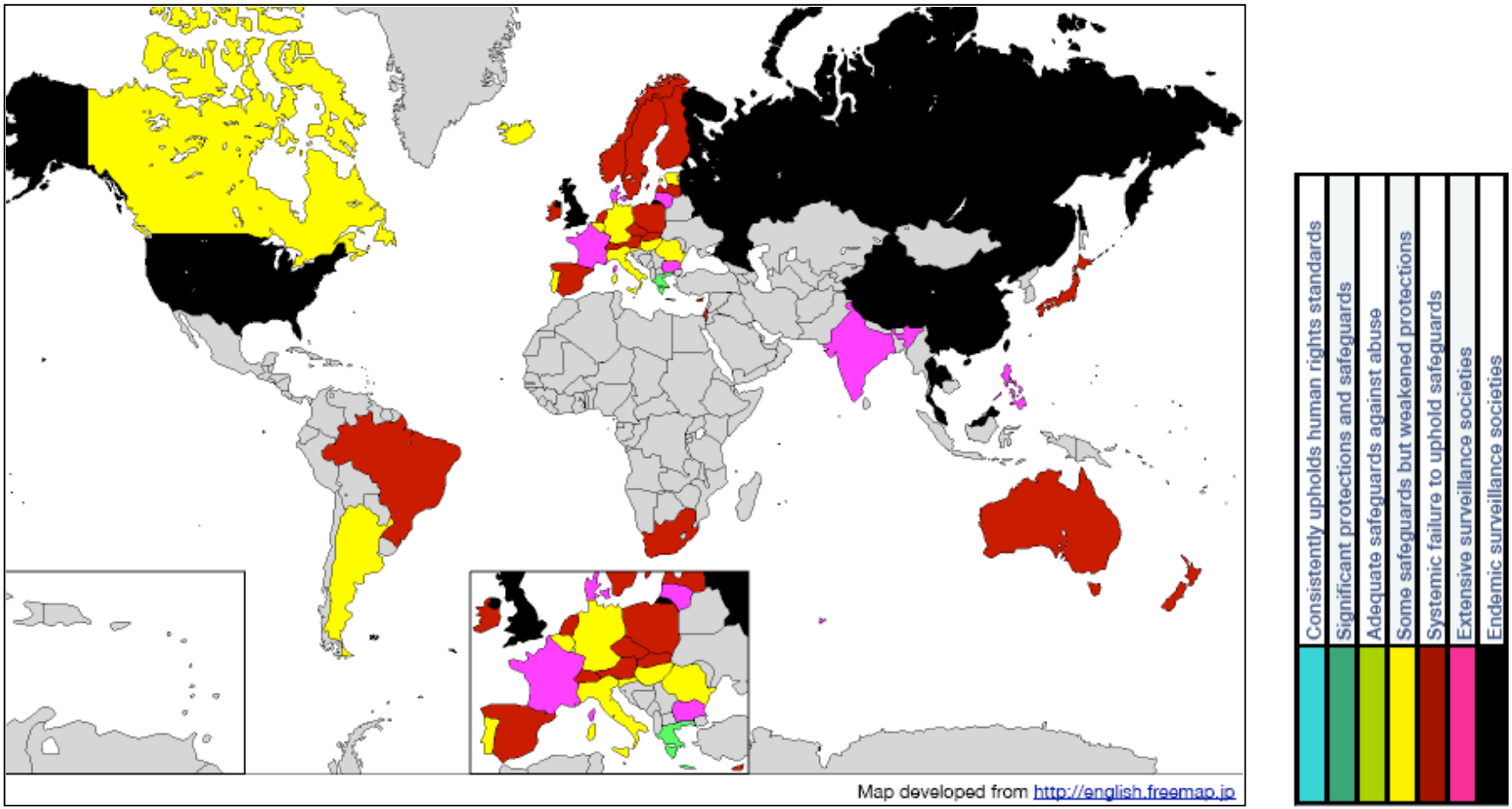
“Requirements Analysis for Identity Management in Ambient Environment: the HYDRA Approach“, - Hasan Akram, Mario Hoffmann

Context Awareness and Trust 2008
2nd International Workshop on Combining Context with Trust, Security and Privacy
June 16th, Trondheim, Norway

Rapidly Increasing Amount of Individual-related Information



The 2007 International Privacy Ranking



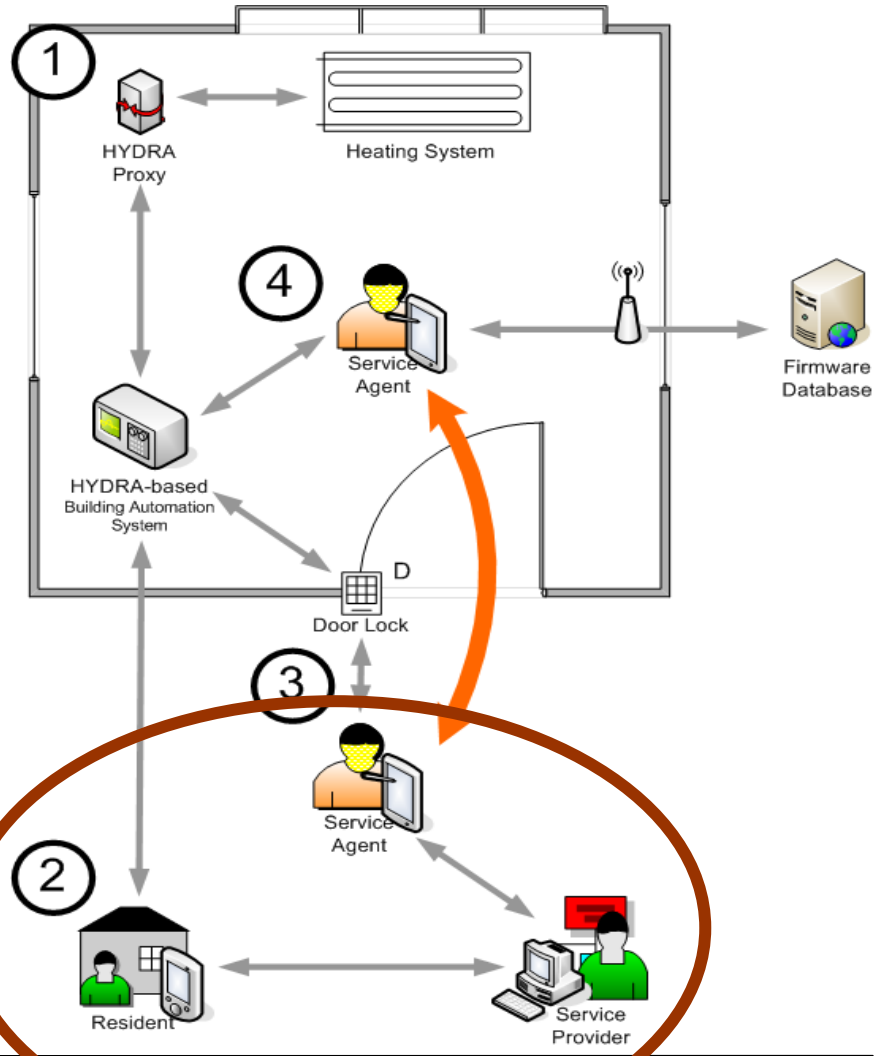
http://www.privacyinternational.org/

Introduction to HYDRA

- EU Project – HYDRA
  - Middleware for Networked Embedded Systems
  - www.hydra.eu.com
  - 07/2006-06/2010
- Projected to 2015
- Focus areas
  - Building Automation
  - Health care
  - Agriculture
- IDON method for futuristic scenario definition

HYDRA Scenario:

1. **Breakdown of the Heating System**
   - Context information to enhance resolution process
2. **Resident receives error**
   - Sends 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



"Requirements Analysis for Identity Management in Ambient Environment: the HYDRA Approach", - Hasan Akram, Mario Hoffmann

Context Awareness and Trust 2008
2nd International Workshop on Combining Context with Trust, Security and Privacy
June 16th, Trondheim, Norway

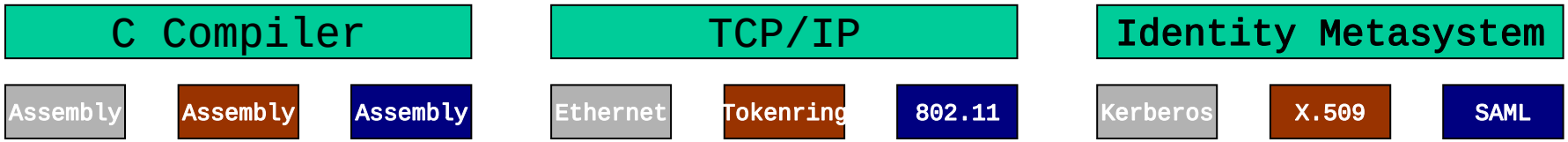
Federated Identity

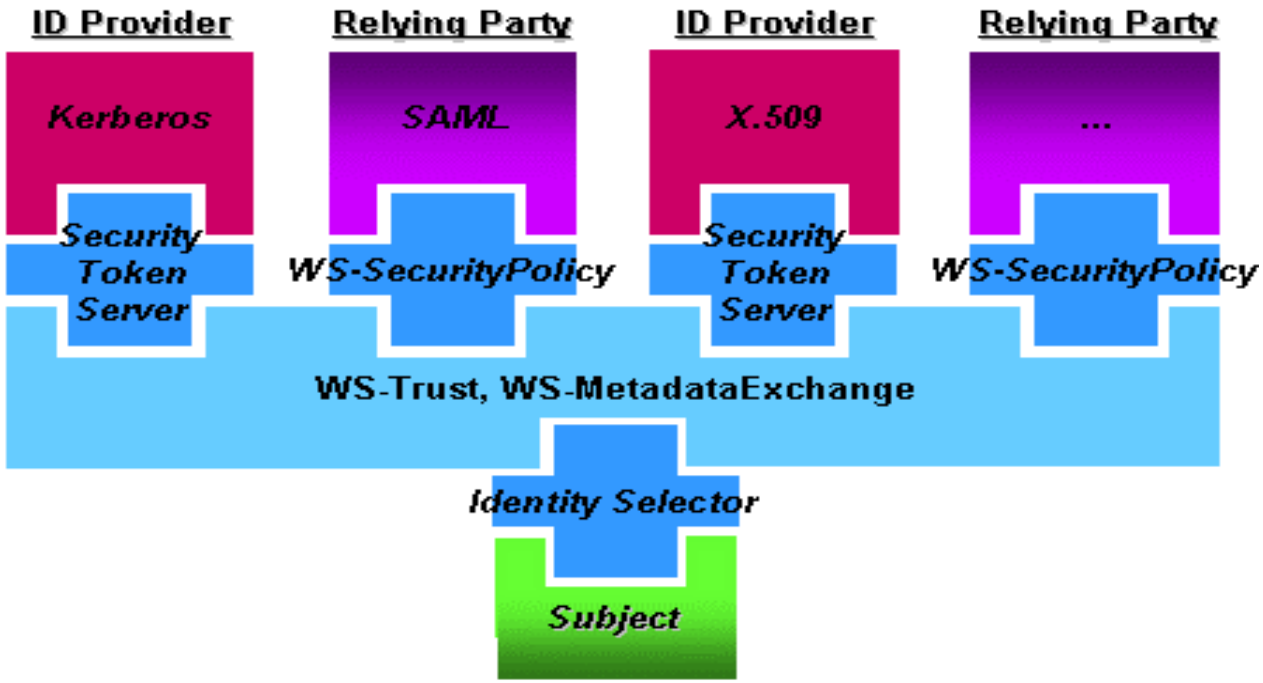
3 players of federation

- Identity Provider
- Relying Party
- Subject/User

Identity Metasystem

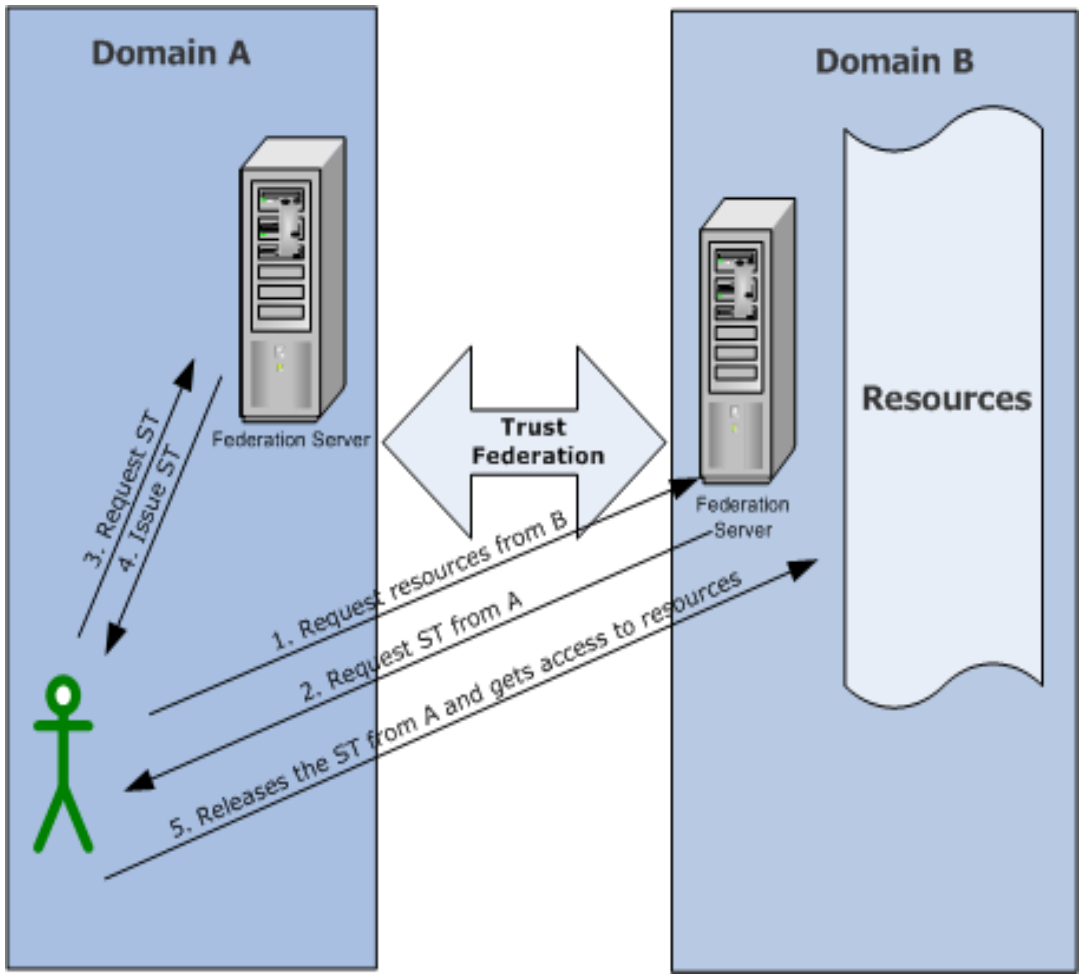
Identity Metasystem



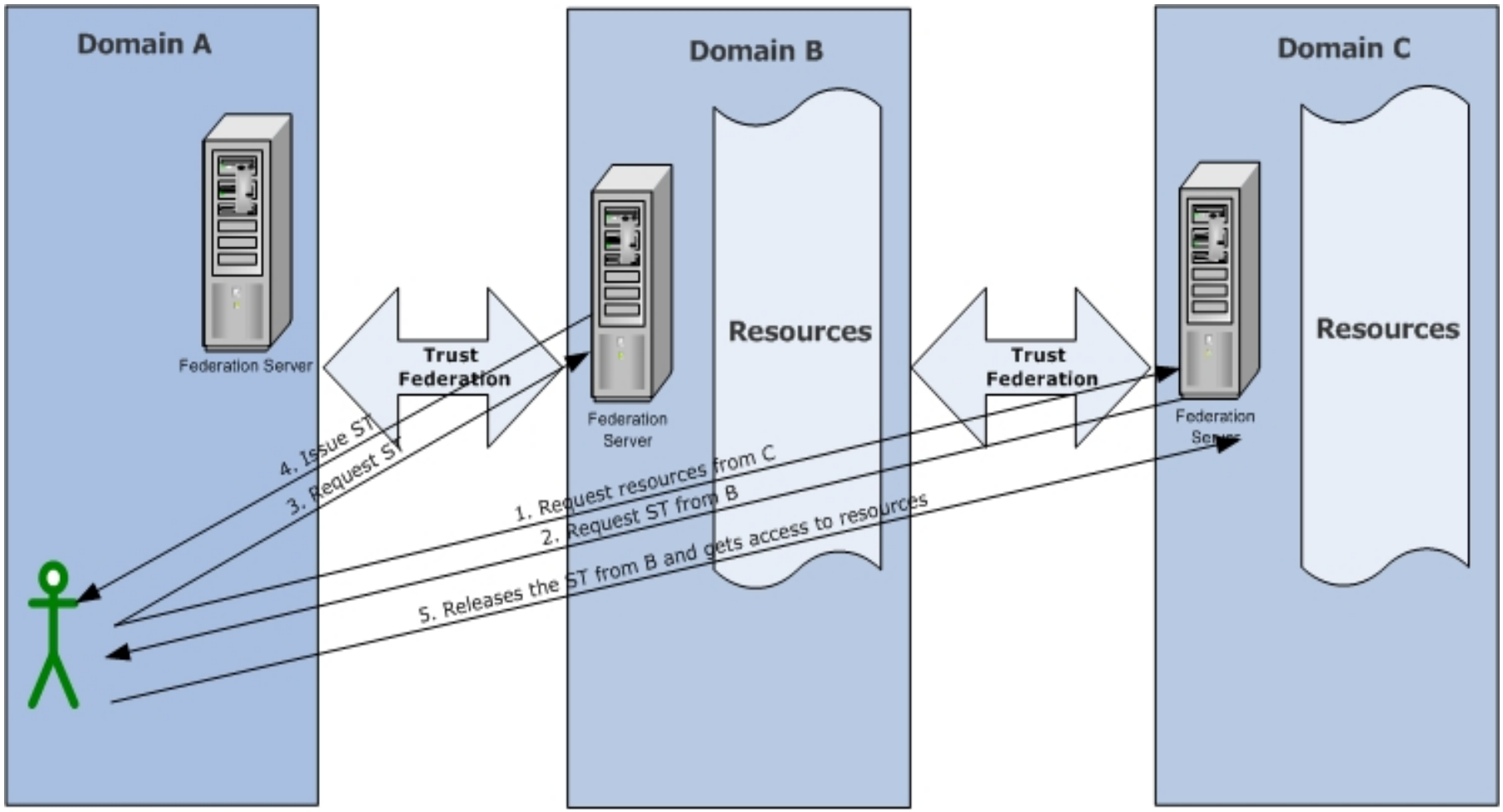


http://www.identityblog.com/stories/2005/07/05/IdentityMetasystem.htm

Federated Identity

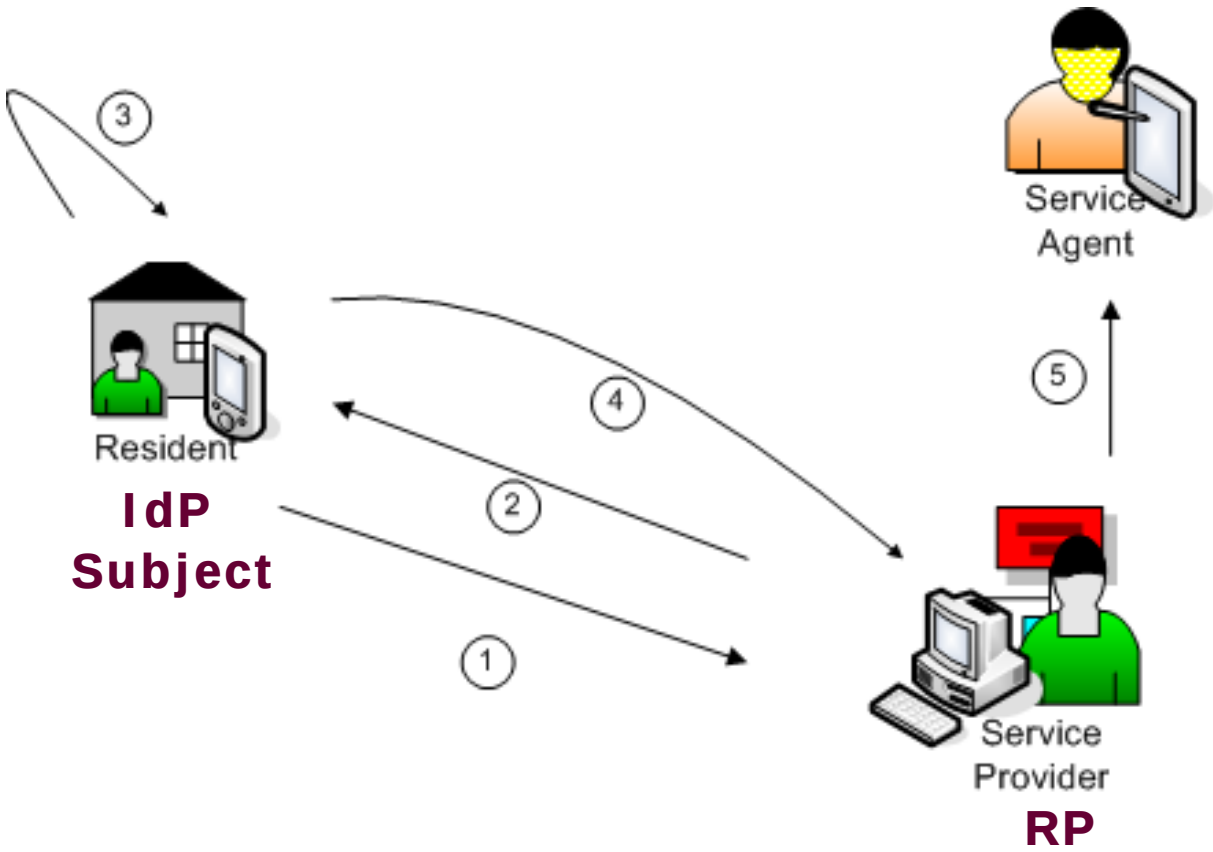


Federated Identity



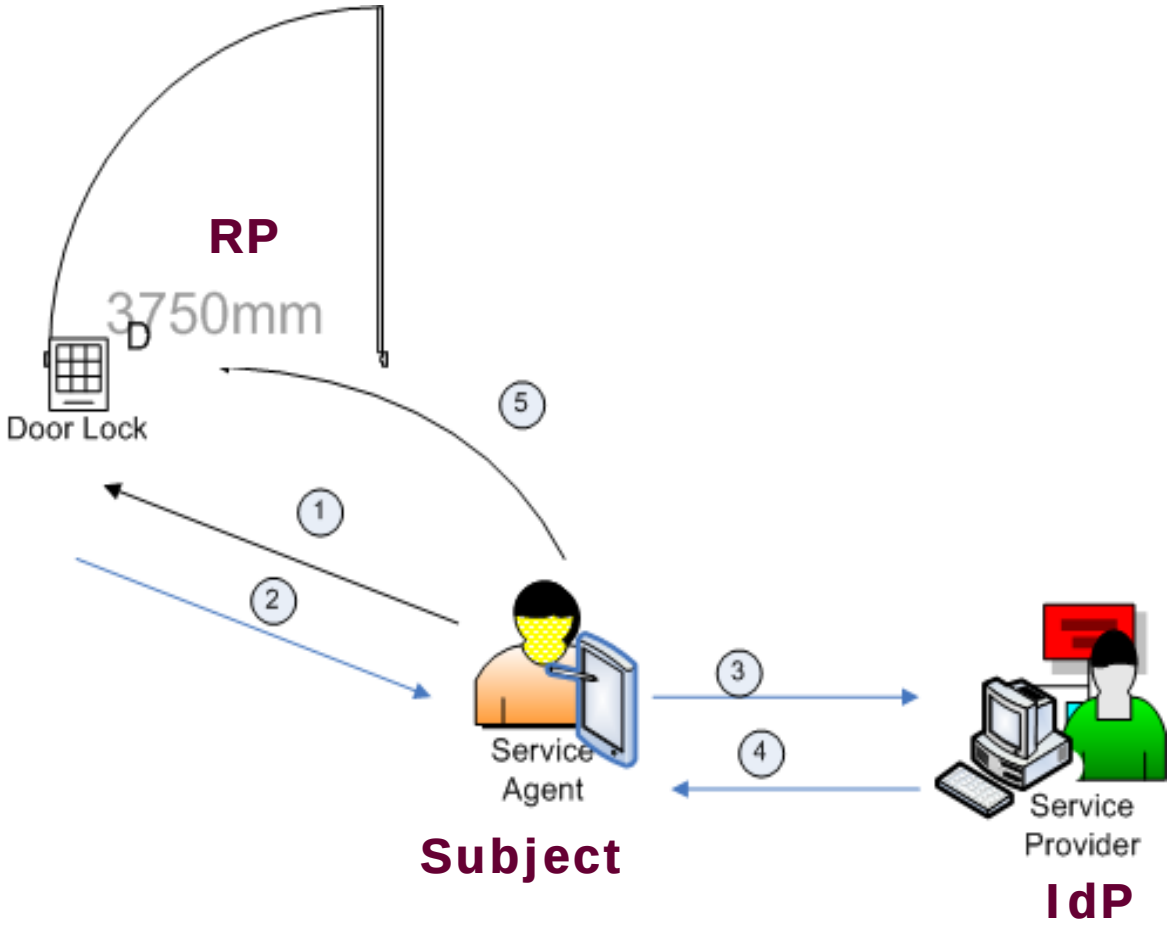
Use Case Analysis – Federation in HYDRA scenario

1. Requests resources
2. Requests STS
3. Issues STS
4. Releases STS
5. Resource provided



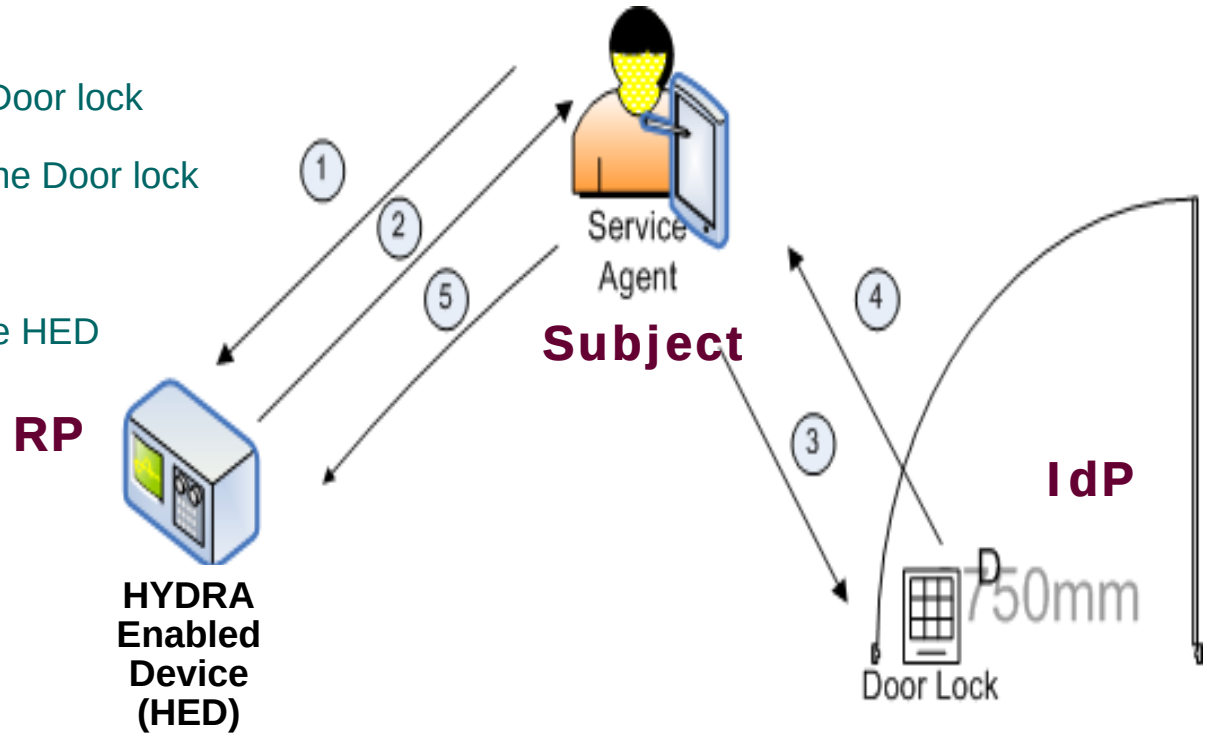
Use Case Analysis – Federation in HYDRA scenario

1. Requests for access
2. Requests for STS from SP
3. Requests for STS by SA to SP
4. Issues of STS for Door Lock
5. Access given to the SA



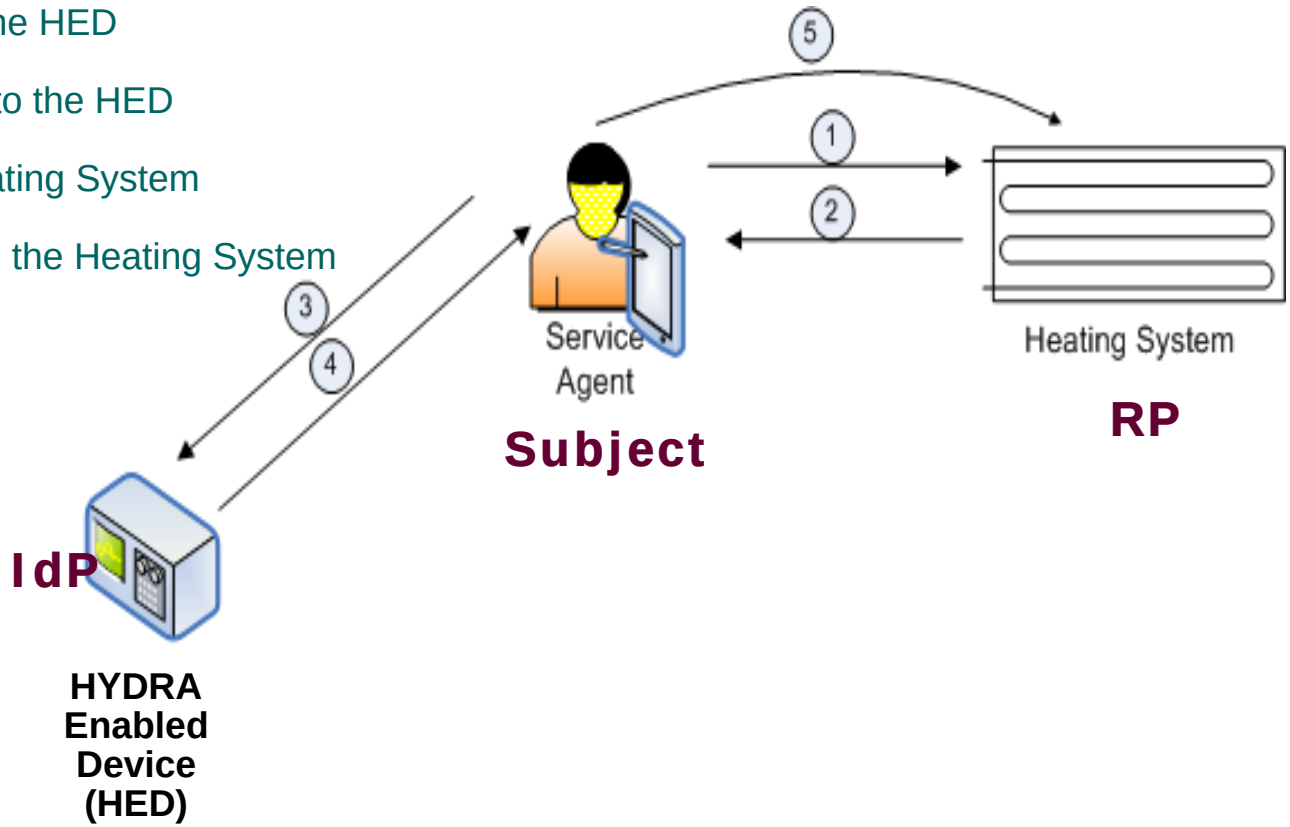
Use Case Analysis – Federation in HYDRA scenario

1. Requests for access to HED
2. Requests for STS from the Door lock
3. Requests for STS by SA to the Door lock
4. Issues of STS for the HED
5. Access given to the SA to the HED



Use Case Analysis – Federation in HYDRA scenario

1. Requests for access to the Heating System
2. Requests for STS from the HED
3. Requests for STS by SA to the HED
4. Issues of STS for the Geating System
5. Access given to the SA to the Heating System



HYDRA Identity Manager: Requirements

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

HYDRA Identity Law 1

- User Empowerment: Awareness and Control

HYDRA Identity Law 2

- Minimal Information Disclosure for a Constrained Use

Spend it like Beckham
London, Friday 13.06.08
http://www.thisislondon.co.uk

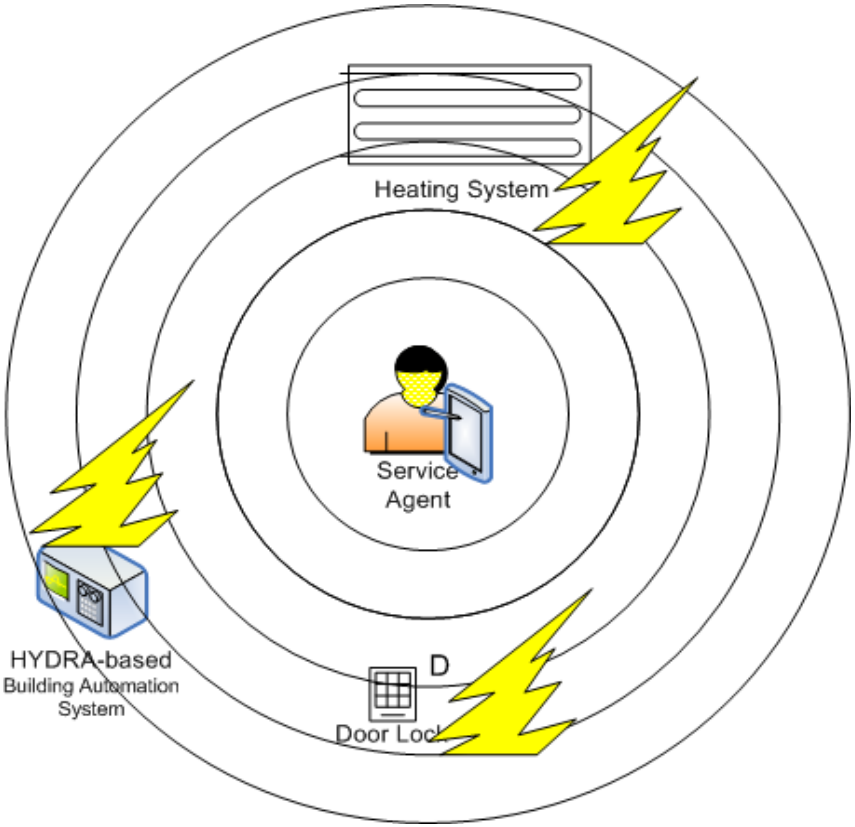
HYDRA Identity Law 3

- Non-repudiation
- Not the legal meaning
- Authenticity, integrity and time stamp

Who? What? When?

HYDRA Identity Law 4

- Support for directional identity topologies



HYDRA Identity Law 5

- **Universal Identity Bus**
  - **“Identity Bus” was coined by Stuart Kwan, Microsoft**
- **UIB in HYDRA**
  - **Interoperability issue**
  - **Developers’ viewpoint**

“Requirements Analysis for Identity Management in Ambient Environment: the HYDRA Approach“, - Hasan Akram, Mario Hoffmann

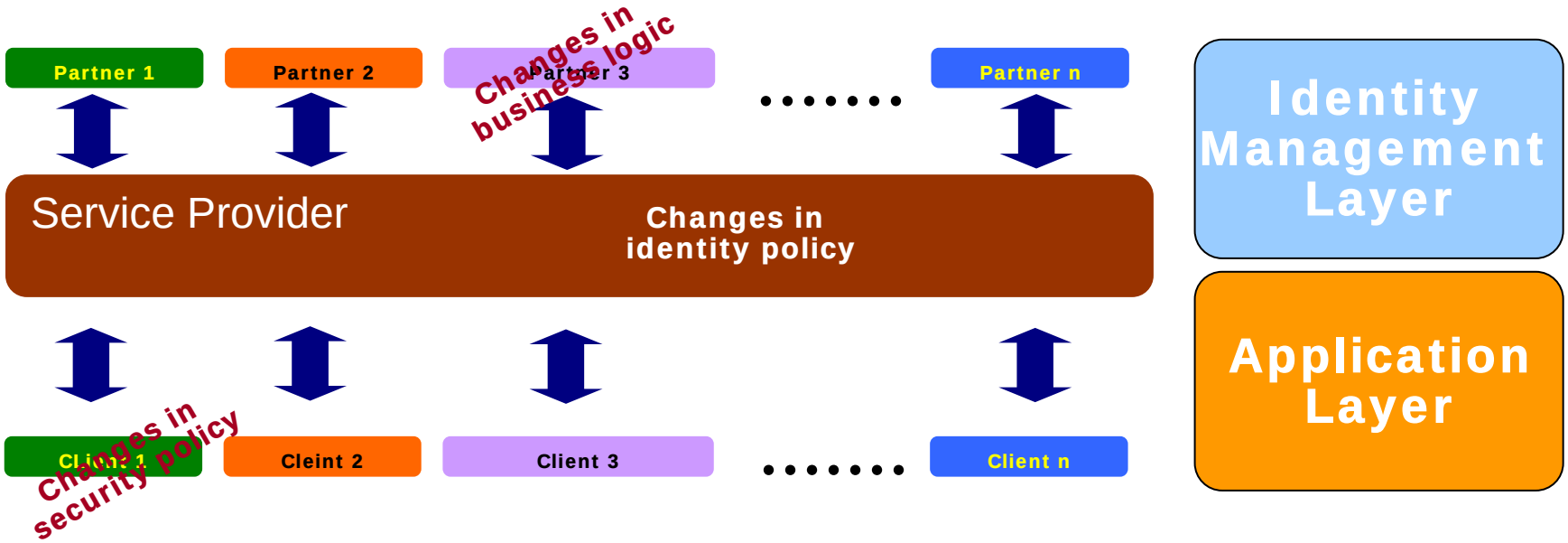
Context Awareness and Trust 2008
2nd International Workshop on Combining Context with Trust, Security and Privacy
June 16th, Trondheim, Norway

HYDRA Identity Law 6

- Provision of defining strength of identity
  - HYDRA devices and users paradigm
  - A device can be related to many users and a user can be related to many devices (n:m relationship)
  - Identity of a device or a user is a set of attributes based on a set of claims
  - In case of device identity
  - Device identity can depend on the identity of the device owner
  - Scale of identity (weak, medium and strong etc.)

HYDRA Identity Law 7

- Decoupling Identity Management layer from application layer



HYDRA Identity Law 8

- Usability issue concerning identity selection and disclosure
  - Without usability feature law 1 is impossible to be realized
  - Developers' tool for usability implementation
- CardSpace, DigitalMe, Sxip….
- How about custom InfoCard?
- Iconic trust (e.g. SSL icon )
- Iconic identity

HYDRA Identity Law 9

- Consistent experience across contexts
  - Profiles
  - Context awareness
  - Multiple persona

HYDRA Identity Law 10

- Scalability
  - Ambient environment
  - Unpredictability of nodes joining in and out

Comparision with Related Works

- M. Langheinrich - „Privacy by Design – Principle of Privacy-Aware Ubiquitous Systems“ (2001)
- Jendricke - „Pervasive privacy with identity management.“ (2002)
- Roy Champbell – „Towards security and privacy for pervasive computing.“(2002)
- Kim Cameron - „Laws of Identity“ (2005)

Future Outlook

- Architecture
- Proof of Concept
- SDK will be made available by the end of this year

"Identity is the Hotel California of technology. You can come in any time you like, but you can never leave." - Kim Cameron

Thank you for paying attention.

Questions?

Contact:

hasan.akram@sit.fraunhofer.de