



**Fraunhofer** Institut  
Sichere Informations-  
Technologie

# Identity Metasystem in Location Based Persistent Authentication

---

EuroCAT 2009  
European Workshop on Combining Context with Trust, Security and Privacy  
9 September 2009, Pisa, Italy

## **Hasan Ibne Akram**

M.Sc. Computer Science  
Fraunhofer Institute for Secure Information Technology  
Munich, Germany  
Munich University of Technology  
Munich, Germany

---

# Outline

---

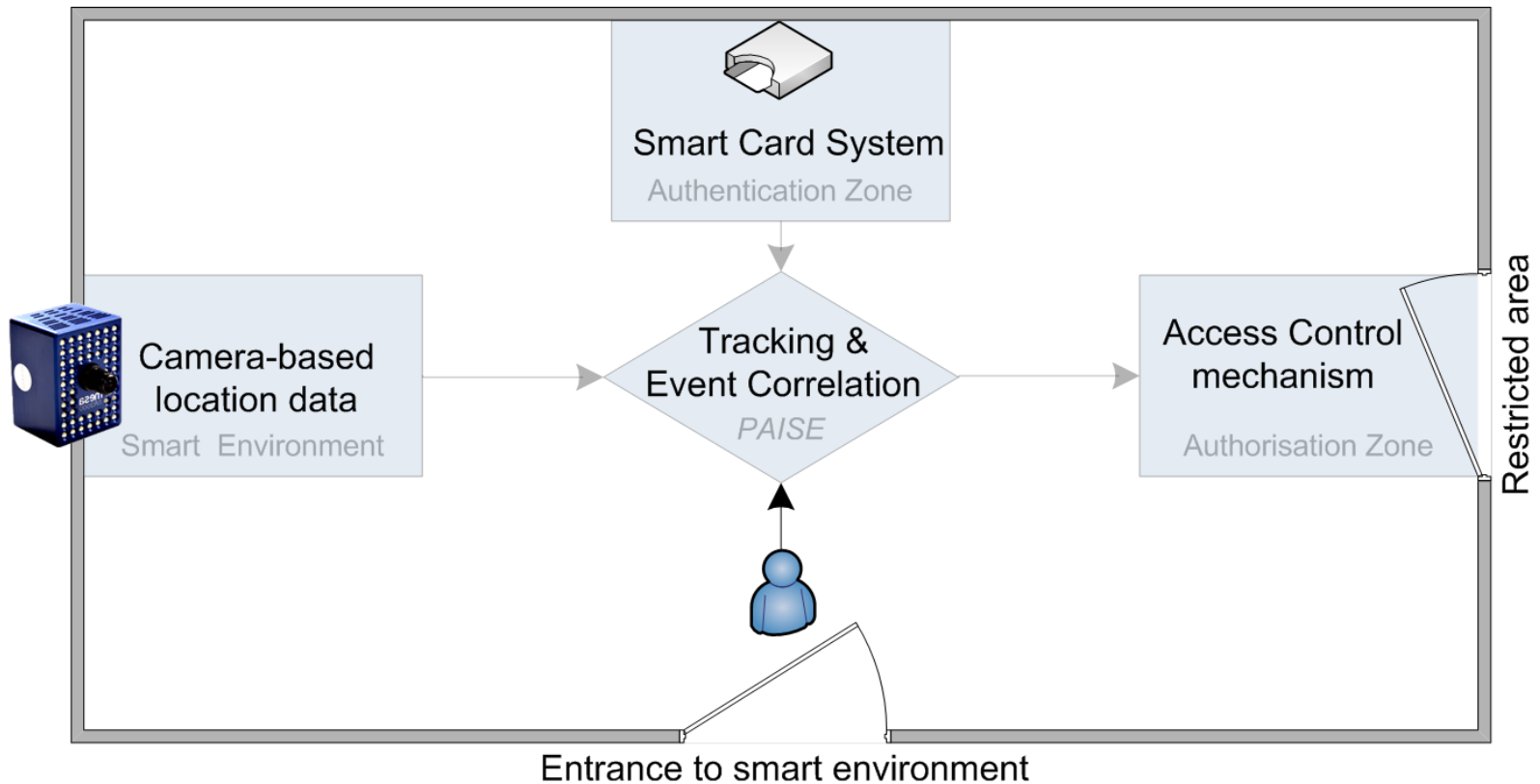
- **Motivation**
- **Introduction to PAISE**
- **Privacy Principles for Smart Environments**
- **Identity Metasystem**
- **Identity Metasystem Technologies**
  - **OpenID**
  - **Windows CardSpace**
  - **Higgins**
- **Proposed Architecture**
- **Evaluation**
- **Conclusion & Future Outlook**

# Motivation

- **Authentication in smart environment is traditionally device centric**
  - **If the device is stolen, there is a good chance of your identity being stolen**
  - **User can be impersonated**
- **Traditional Location Tracking System (LTS), e.g., RFID, GPS etc. has been criticized by the privacy proponents**
  - **LTS is inherently lacks privacy principles**

# Introduction to PAISE

- A shift from device tracking paradigm to person tracking paradigm.
- Person tracking using "Time-of-Flight" (TOF) cameras



# Privacy Principles for Smart Environments

---

- **Notice**
- **Choice and Consent**
- **Anonymity and Pseudonymity**
- **Proximity and Locality**

# Federated Identity

---

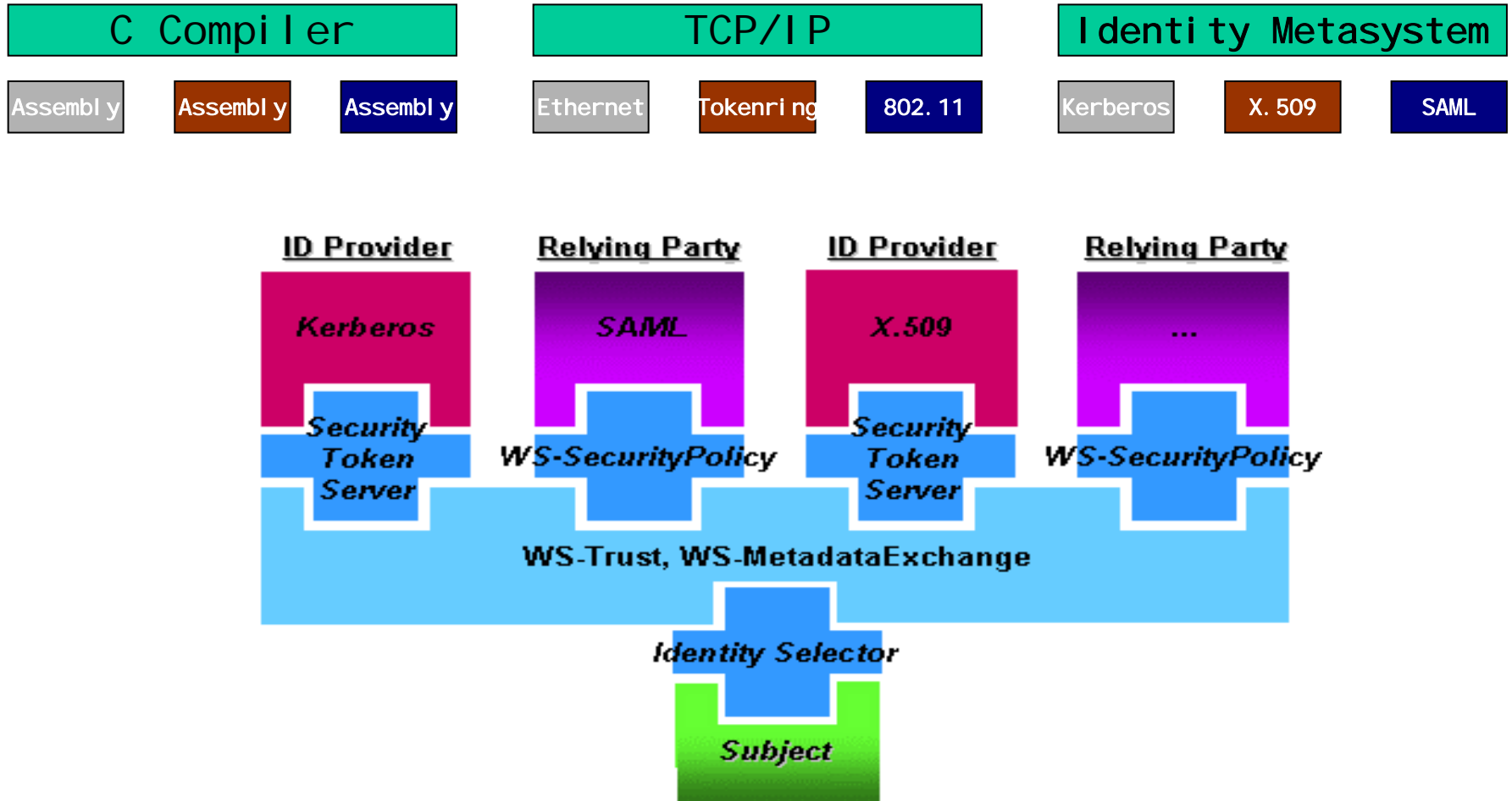
## 3 players of federation

- Identity Provider
- Relying Party
- Subject/User



## Identity Metasystem

# Identity Metasystem



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

# Identity Metasystem Technologies

---

## – OpenID

- Objective: Reduce username and password
- Protocol was developed in 2005
- Main Features of OpenID
  - Light Weight Identity
  - Decentralized
  - Single-Sign-On
- “OpenID is a free and easy way to use a single digital identity across the Internet.” [<http://openid.net/> ]

# Identity Metasystem Technologies

---

## – Windows CardSpace

- Windows CardSpace is a client software from Microsoft which is a visual metaphor for identity selector for the end-user.
- Windows CardSpace provides controlling power to the end-users on the fact that which information (about the end-users) should reach to the *Relying Party* and which should not.
- It is shipped with Windows Vista (or as an add-on in Windows XP); it is not meant to replace the other standards handling digital identity rather to utilize and extend them.
- CardSpace is token agnostic, i.e. it supports any token type i.e. SAML, OpenID, Kerberos or custom token type.

# Identity Metasystem Technologies

---

## – Higgins

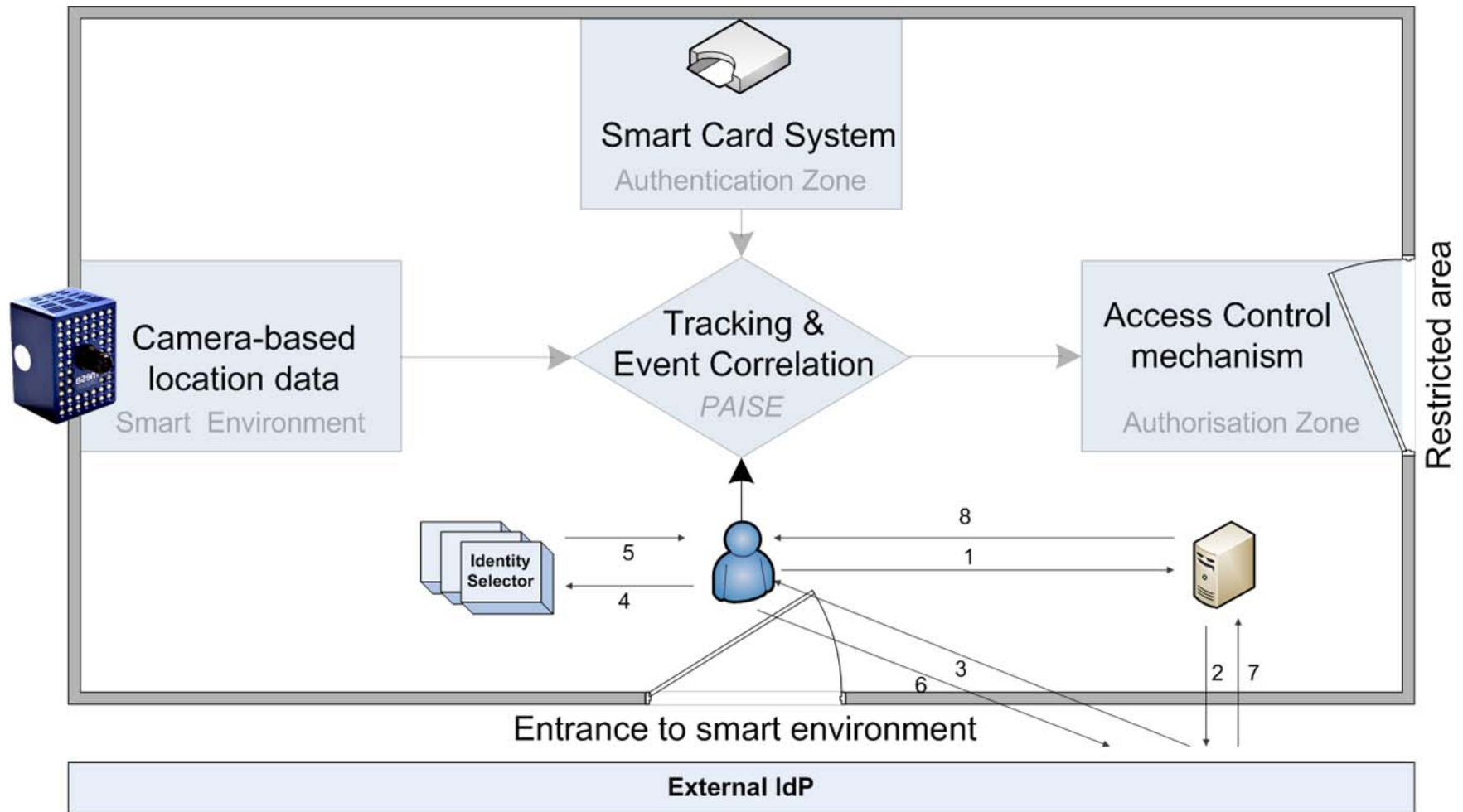
- An open source identity framework being developed at the Eclipse Foundation.
- Higgins is a software infrastructure that supports consistent user experience that works with digital identity protocols, e.g. WS-Trust, OpenID, SAML, XDI, LDAP etc.
- The main objective of the Higgins project is to manage multiple contexts, interoperability, define common interfaces for an identity system.
- Various technologies including LDAP, SAML, WS-\*, OpenID etc. can be plugged into the Higgins framework.

# Identity Metasystem Technologies

## Evaluation w.r.t. the Privacy Principles

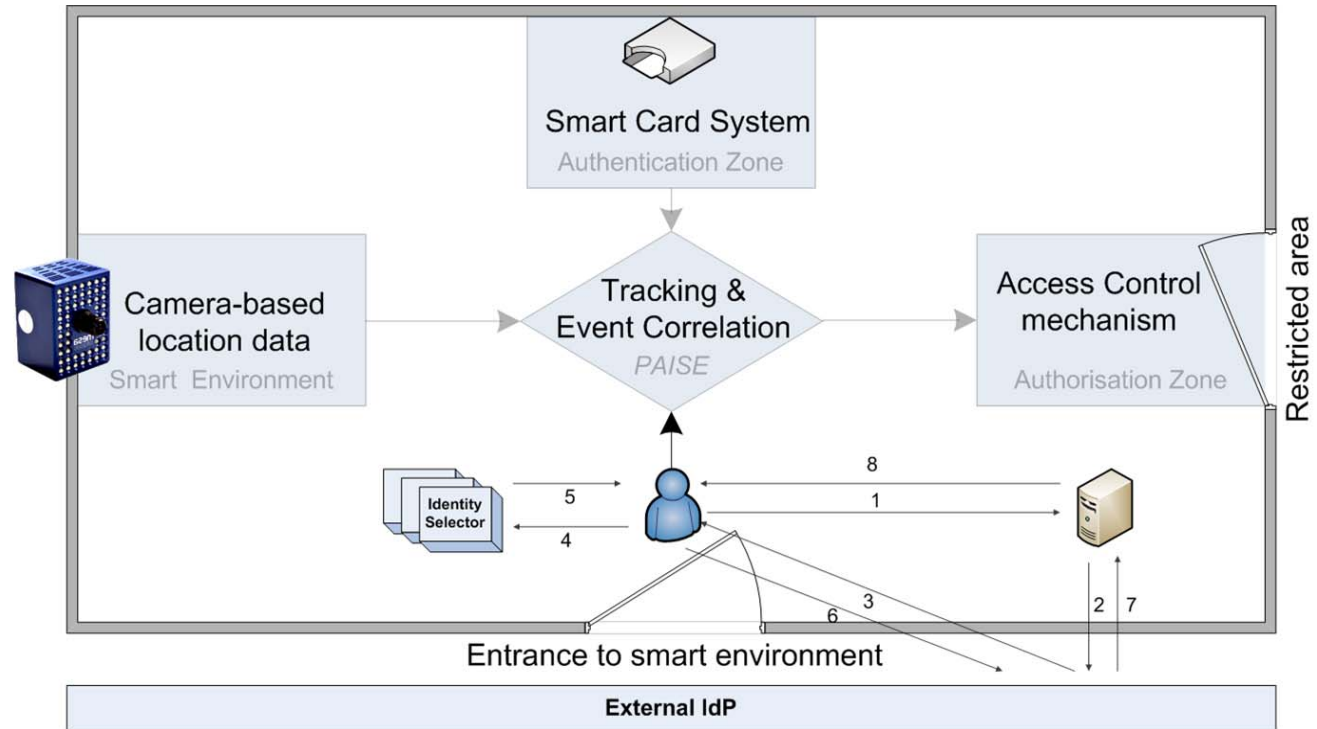
<i>Privacy Principles</i>	<b>OpenID</b>	<b>CardSpace</b>	<b>Higgins</b>
1. Notice	-	+	++
2. Choice and Consent	+	++	++
3. Anonymity and Pseudonymity	+	+	+
4. Proximity and Locality	--	--	--

# Proposed Architecture



# Evaluation

1. Notice
2. Choice and Consent
3. Anonymity and Pseudonymity
4. Proximity and Locality



# Conclusion & Future Outlook

---

- Implementation of the architecture
- Proof of Concept
- Combining the Architecture with ProtectServe of Kantara Initiative Work Group - User Managed Access (UMA)
  - ProtectServe Specification
    - 4 Legged Scenario – User, IdP (the resource provider), RP (the consumer) and a Authorization Manager (AM)
    - Identity Dashboard
    - Web link: <http://kantarainitiative.org/confluence/display/uma/Home>

Thank you for paying attention.

Questions?

Contact:

hasan.akram@sit.fraunhofer.de