Identity Metasystem in Location Based Persistent Authentication

Hasan Ibne Akram[1] and Christian Damsgaard Jensen[2] and Mario Hoffmann[1]

[1] Fraunhofer Institute for Secure Information Technology
Munich, Germany
{*hasan.akram,mario.hoffmann*}*@sit.fraunhofer.de*
[2] Technical University of Denmark
Kgs. Lyngby, Denmark
christian.jensen@imm.dtu.dk

Abstract. Persistent authentication in smart environments (PAISE) is a new effective approach that has changed the device-centric paradigm in traditional token based authentication systems to a much more user-centric one. Instead of carrying a security token, such as an RFID tag, all the time the location of a previously authenticated user is simply persistently tracked by sensors in the smart environment, such as cameras. For closed scenarios, recent publications have already shown various advantages, such as consistent user experience across contexts and a decreased probability of impersonation. In order to address even more complex and privacy-enhanced scenarios, we propose to enhance PAISE with Identity Management (IdM). Taking advantage of IdM, users can easily choose among different virtual identities and, at the same time, we can now support open and cross-context application scenarios. This paper addresses the balance between the security requirements of service providers in smart environments and the privacy concerns of users. Therefore, this paper discusses first security and privacy implications in PAISE and evaluates then the adaptability and interoperability of existing identity management systems for persistent authentication in changing and open scenarios. As our main result and in order to ensure interoperability an Identity Metasystem on top of the PAISE architecture will be described in detail.

1 Introduction

Authentication in context aware smart environments is typically device-centric and based on for example RFID tokens, Smartcards or - more advanced - cell or smart phones. Users have to carry these authentication tokens all the time and present them to technical or human safeguards. This makes it relatively easy, however, to impersonate authenticated users by cloning, borrowing or stealing their authentication token. Therefore recent publications [1] proposed a new user-centric paradigm based on user tracking called PAISE - Persistent Authentication in Smart Environments. That means that once you have been authenticated at a particular security gate you will be continuously tracked in a smart

environment, e.g. by sensors or cameras, until you leave the area covered. In this paper we will deal with the implications of this physical single-sign-on experience balancing security requirements and privacy concerns and propose appropriate enhancements to the existing PAISE architecture.

1.1 Persistent Authentication

Persistent Authentication [1] has been proposed as a proactive authentication mechanism, which combines existing authentication mechanisms based on passwords, smartcards or biometrics, with person tracking using "Time-of-Flight" (TOF) cameras. Users are authenticated when they enter the smart environment and the TOF cameras are subsequently used to track the user as he moves around in the smart environment, which makes the event of authentication "stick" to the user, thus making it persistent. This means that the persistent authentication mechanism can proactively authenticate the user to a service in the smart environment whenever the user requests access to that service. Ideally, this means that users would only have to authenticate when they arrive at work in the morning and the system will be able to authenticate them to physical access control services, computing services and other services throughout the day. Similar ideas have been explored in other projects, but these have all required users to carry a small authentication token with them at all times and it is effectively this token that is authenticated, so we refer to such mechanisms as device-centric authentication. The problem with device-centric authentication is that users must always remember to carry the token with them and authentication tokens can be borrowed, lost or stolen. We therefore believe that tracking the user, rather than the token, is a more convenient and secure way to authenticate users in emerging smart environments. However, constant tracking of users will be seen as a serious violation of privacy by many people, so it is important to develop a system that limits the problem of privacy violation in location-based persistent authentication.

1.2 Identity Management

Identity Management (IdM) refers to the maintenance of the complete lifecycle of digital virtual identities. Virtual identities are characterized by a collection of personalized information containing for example names, address(es), eMail and telephone, account data, bank or credit card information, as well as preferences, profiles, histories of service usages and contexts. We can say that virtual identities reflect at least parts of one's real identity and basically consist of an open and dynamic set of attributes for a specific period of time. In smart environments IdM gains even more attention and importance. Smart environments are enabled by IT systems working in the background gathering and reasoning on context information including analyzing and predicting user behavior. On the one hand these systems will provide useful and convenient personalized services in the future - persistent authentication based on TOF cameras is such a service; on the other hand the information collected might - in principle - violate

the users' privacy if you do not establish reasonable mechanisms to tackle these concerns by managing personalized information in a secure way. Identity Management Systems enable both users as well as service providers to manage virtual identities in a secure and effective way. Users are able to maintain for example a set of virtual identities depending on account and authorization information for specific services and contexts. Service providers are at the same time able to distinguish different users acting in different contexts attaching different authorization and access rights in order to assure accountability and the establishment of appropriate security policies. Therefore, we introduce in this paper IdM concepts, including an Identity Metasystem, to PAISE in order to address raising privacy concerns in smart environments equipped with TOF cameras and to balance these concerns with security requirements from service providers. Users who work in such environments IdM helps to choose the right virtual identity with the minimum set of necessary attributes. Service providers who run smart environments relying on persistent authentication IdM helps to attach the right privileges and access rights to users. The proposed Identity Metasystem will finally ensure that different IdM Systems will be able to interoperate across different contexts and scenarios.

1.3 Paper Structure

The paper is organized in the following way: Section 2 presents a short overview of the PAISE model and identifies the privacy concerns that must be addressed if persistent authentication is to be widely deployed. Section 3 introduces the interoperability concept of Identity Metasystems followed by Section 4 where according to the privacy concerns the state of the art in identity management technologies will be analyzed. Section 5 proposes an architecture that integrates Identity Metasystems with the existing persistent authentication architecture and Section 6 presents an evaluation and discussion of the proposed architecture. Finally, we present our conclusions in Section 7.

2 Location Tracking

2.1 The PAISE Model

The PAISE model defines four major components in a persistent authentication system: an authentication system, which is able to authenticate principals; a smart environment, which delivers the sensor data needed for tracking; an access control mechanism, which acts on the result of persistent authentication and the core component of PAISE, which combines the information from the authentication system and the smart environment, tracks authenticated principals in the smart environment and forward the necessary data to the access control mechanism. These components are shown in Figure 1.

In addition to these four components, PAISE also defines authentication zones and authorization zones in the smart environment. An authentication zone

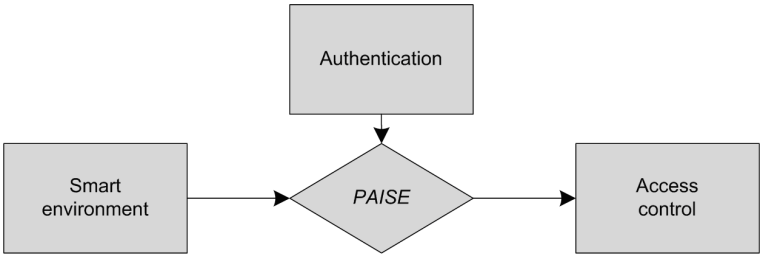

Fig. 1. PAISE Authentication Model.

defines the area in front of the authentication mechanism which is large enough to hold a single principal.

The smart environment delivers a constant stream of sensor data to the core component, but tracking is only initiated when a principal has entered the authentication zone and successfully authenticated himself. The authentication zone must be small enough to ensure that the authentication event can be reliably linked to the principal. A typical authentication zone, in a smart environment, would be an area of 0.5m x 0.5m in front of a swipe-card terminal. An authorization zone defines the area in which the access control policy of a location based service must be enforced. When new principals enter an authorization zone the persistent authentication is forwarded to the access control mechanism of the location based service provider, which is then able to determine whether access should be granted. In the case of access through a door, in a smart environment, the authorization zone must be small enough to ensure that most principals are able to reach and open the door while it is unlocked, but also large enough to ensure that nobody outside the authorization zone is able to pass through the door while it is open. This allows the system to enforce the constraint that the door can only be unlocked if there are no unauthenticated or unauthorized principals inside the authorization zone, thus preventing tailgating.

2.2 Privacy Concerns in Location Tracking Systems in Smart Environments

Privacy issue is by no means a new concern in Ubiquitous Computing or smart environments. The foreseer of ubiquitous computing Mark Weiser had already pointed out the issue of privacy in 1991 [2]. Langheinrich showed how potentially privacy can be endangered in such environments without even the consent of the user [3]. Similarly, location based tracking systems (LTS) has been shown to be inherently privacy dissenting. Therefore, the privacy issue in smart environments using LTS must be taken into consideration and requirements for privacy compliance has to be defined. Previous studies show that privacy risk is apparent on LTSs (e.g. RFID, GPS etc.) since LTSs collect information silently, without the consent or even awareness of the user [4–6]. Information can be collected

about an individual and can be aggregated to figure out near-perfect knowledge of the individual's whereabouts and activities. If we refer back to the definition of privacy from Louis Brandeis, 1890 (Harvard Law Review): "The right to be let alone.", LTSs violate privacy of an individual. Although PAISE is inherently designed to be relatively more privacy compliant than other camera based tracking as it uses a non recognizable image (blob) of the object, still it suffers from some traditional privacy issues that any location based tracking system has. If we get back to the definition of Brandeis and try to apply it in PAISE we see that PAISE is even less compliant to privacy because: in traditional device based tracking system, the user is able to switch off the device when he wants to and thus becomes invisible to the system. On the other hand, it is not possible to switch off tracking in PAISE that easily, so the user's right to be left alone is not easily accomplished.

2.3 Privacy Principles in Smart Environments

Requirements and principles of Identity Management have been analyzed and derived in pervasive computing ever since the very beginning of pervasive computing. Obviously, these related works have some commonalities and disparities among themselves. Our objective in this section is to narrow down the privacy principles of Smart Environments suitable to LTS in such environments. Langheinrich [3] identified six principles and guidelines for privacy aware ubiquitous system. It is important to mention that these principles and guidelines do not ensure total privacy. The goals of these privacy guidelines are to get as close as possible to Brandeis' definition of privacy. We have picked four of the privacy principles as they are mostly relevant for persistent authentication using LTS. These four principles are outlined below:

- **Notice:** "Transparency" or "Openness" is the most fundamental principle of any data collection system. When the location data about the user is collected in PAISE but not saved, the user should be notified about that.
- **Choice and Consent:** A mere notice to the user about its location data being tracked is not enough anymore as EU Directive [3] refined and extended the well-known fair information practices. There has to be explicit consent of the user about the location tracking.
- **Anonymity and Pseudonymity:** Since in a LTS it is very difficult to have an explicit consent of the user at any given time, a certain degree of anonymity and Pseudonymity is also necessary.
- **Proximity and Locality:** This principle tells us that information should be locally preserved. In terms of LTS we can clarify the principle in a way that if information is not disseminated out of a certain locality or area, the likability of tracking will be harder and thus it will be more privacy compliant.

[3] European Commission. Directive 95/46/ec of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, November 1995.

3 Identity Metasystem

Identity Metasystem is a notion of abstracting the identity layer from the rest of the system with the intention of gaining interoperability, privacy and usability [7–10]. Identity Metasystem can well be explained using the following analogies: before 1950 programmers had to write assembly codes to fulfill their programming needs. Code pieces written in assembly language required extreme intellectual efforts and more problematically it lacked totally the feature of being portable from machine to machine. Invention of compilers in 1950s and early 1960s brought along an abstraction layer where a generic form of code piece could reside and could be translated back to machine specific assembly code according to need; thus bringing portability to code pieces breaking the machine specific silos. Similarly in the 1970s and early 1980s, before the general adoption of IP, distributed applications were bound to possess network specific knowledge e.g. Ethernet, Token Ring or Frame Relay. But IP was again being an abstraction layer acted as encapsulation of such network specific technologies. Following these two analogies we can think of an Identity Metasystem that acts as such mediator of existing Identity Management systems allowing interoperability and portability of identity [3].

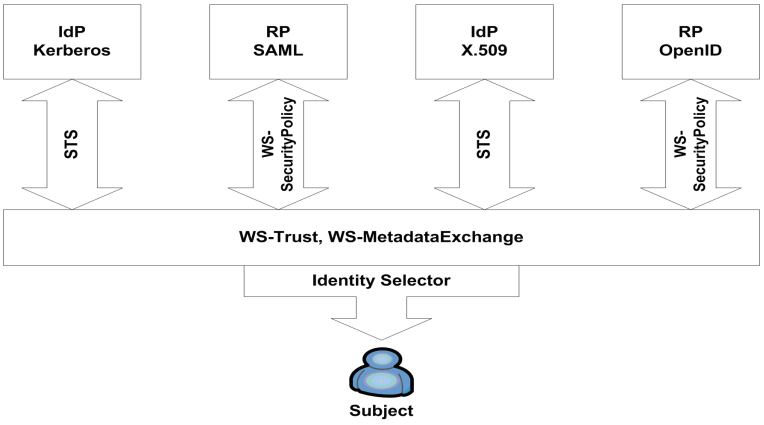

Fig. 2. Identity Metasystem Architecture.

Identity Metasystem is a complex system that integrates the existing IdM systems to provide seamless interoperability and portability. Figure 2 illustrates how IdPs with specific Security Token Services (e.g. Kerberos, X.509 etc.) is federating identity to RPs who accept other types of Security Tokens (e.g. SAML, OpenID). WS-SecurityPolicy is shown to be the policy negotiation mechanism, and WS-trust [11] and WS-MetadataExchange [12] as the abstraction layer.

Having introduced the basic concept of Identity Metasystem in this section, we now address an obvious question that would strike the reader's mind: what is the implication of Identity Metasystem in LTS? In Section 2.3 we examined the principles of privacy in LTS in smart environments. Our objective in this

section is to elaborate on how close to those principles we can bring PAISE by hybridization with Identity Metasystem. First of all, an Identity Metasystem helps users to stay in control of their identity interactions by allowing them to select context relevant digital persona they would like to reveal in a particular instance. These digital personas contain minimum personal information required for a transaction. In case of PAISE the system will only know whether the user is authorized to access a certain resources or not. Secondly, it empowers users to make informed and reasonable decision about disclosing their identity in such environments [13, 14]. Thus, Identity Metasystem can potentially improve privacy in LTS. However, as we have mentioned in Section 2.3, absolute privacy protection is not achievable by the privacy principles from Langheinrich, in a similar way Identity Metasystem will also not provide total privacy protection, rather more privacy awareness.

4 Identity Management Technologies

We have illustrated a conceptual view on Identity Metasystem and its implication in LTS. Before we move into our architectural description of Identity Metasystem in PAISE, in this section we provide an overview of the predominant IdM technologies and compare their compliance with the privacy principles (cf. Section 2.3).

4.1 OpenID

OpenID 1.0 was originally developed in 2005 by Brad Fitzpatrick, Chief Architect of Six Apart, Ltd. OpenID, a protocol for light weighted identity, is adopted by a wide range of websites, especially which have heavy user-generated contents. OpenID Authentication 2.0 [15–17] is a fully backward-compatible open community-driven platform that permits and motivates federated identity. OpenID Authentication 2.0 specification which is a data transfer protocol to support both push and pull use cases. Besides, the community is coming up with extensions to support the exchange of rich profile data and user-to-user messaging. There are three key features of OpenID: Single Sing On, decentralized and light weight identity. According to an article published in German online computer magazine "Heise Online [4]" on 18th January 2008 there were already 370 million OpenIDs existing globally. However, the real number of active OpenID users is still unknown, because big companies like Yahoo and Aol offered an OpenID to all their users, which explains the high number of existing OpenIDs. By Design, the OpenID protocol suffers from serious privacy issues. OpenID allows URL to Identify a subject or a user and the URL that is used to identify the Subject is recyclable. Since OpenID permits URL based identification, it brings the issue of privacy. The privacy of the user using an URL as his

[4] http://www.heise.de/security/Yahoo-will-das-Passwort-Chaos-beenden–/news/meldung/102001, last viewed on Monday, December 01, 2008

OpenID will be compromised somehow the possession of that URL lost. This is how the principles of users' choice, consent, proximity and locality is violated in case of URL recycling.

4.2 Windows CardSpace

Windows CardSpace 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 (RP) and which should not. Windows CardSpace is a production of Microsoft 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 [18]. Windows CardSpace is token agnostic. Microsoft codename "Geneva" is coming up with the next version of Windows CardSpace. "Geneva" is a claim based access platform, which includes three components: "Geneva" Server, Windows CardSpace "Geneva" and "Geneva" Framework [19]. Windows CardSpace has major privacy flaws: firstly it relies on the users' judgments on the trustworthiness of RPs. A CardSpace user is given the freedom to choose one of the options of high-assurance certificate belonging to the RP, ordinary certificate belonging to the RP or RP with no certificates [20]. In terms of the first privacy principle (choice and consent) this certainly gives a lot of power to the user. At the same time the option of allowing RP with no certificates weakens the compliance with the fourth principle (proximity and locality) as information may leak out to an unwanted domain. The second vulnerability is that Windows CardSpace rely on a single layer of authentication. The user has to be authenticated to the IdP using traditional authentication mechanism. If a working session is somehow hijacked or password is cracked, the security of the whole system is compromised. This has been practically showed by two IT-Security students at Horst Grtz Institute for IT Security (HGI), Bochum, Germany where they manipulated the DNS server to implement dynamic pharming attack [5].

4.3 Higgins Trust Framework

Higgins is a software infrastructure that provides a consistent user experience across multiple digital identity protocols, e.g. WS-Trust, OpenID, SAML, XDI, LDAP etc. The main objectives of the Higgins project are the management of multiple contexts, interoperability, and the definition of common interfaces for an identity system. Various technologies including LDAP, SAML, WS-*, OpenID etc. can be plugged into the Higgins framework. The first version, Higgins 1.0 was released in February 2008. The next version, Higgins 1.1 was supposed to be released by June 2009. There are also ideas and concepts in discussion beyond Higgins 1.1 [21].

[5] On the Insecurity of Microsoft's Identity Metasystem CardSpace, Press release, Bochum, Germany, May 27, 2008, http://demo.nds.rub.de/cardspace/PR-HGI-TR-2008-003-EN.pdf

Since Higgins supports various IdM protocols and technologies it inherently takes over the flaws and vulnerabilities of those technologies and protocols. It also does not fourth principle (proximity and locality). However, the combined approach to provide an umbrella framework for IdM allows Higgins users to choose the best combination of technologies suited to their requirements. Moreover, Higgins architecture is most compliant to other three privacy principles (Section 2.3) among the state of the art technologies that have been considered in this evaluation. Therefore, in our architecture we have taken some of the Higgins architectural approach and integrated to our need. In the next section the evaluation result is summarized.

4.4 Evaluation of the State of the Art

Figure 3 shows the summary of our evaluation result. We came up with a scale of poor (-) to very good (++) to show the suitability of the three IdM technologies for getting close to the privacy principles stated in Section 2.3. As we can see, Higgins provides more supports to implement the privacy principles than OpenID and Windows CardSpace. In the following section we will present a generic architecture for Identity Metasystem in PAISE that will be implemented using the Higgins framework in future.

Privacy Principles	OpenID	CardSpace	Higgins
1. Notice	-	+	++
2. Choice and Consent	+	++	++
3. Anonymity and Pseudonimity	+	+	+
4. Proximity and Locality	--	--	--

Fig. 3. A ranking based on our evaluation.

5 Proposed Architecture

Our proposed architecture is based on Identity Federation between three entities: the user, the IdP and the RP. The user requests for access to a certain resource from a RP in the smart environment and gains the access upon required credential is federated by an IdP. Note that same entities can play the role of IdP or RP depending on the context. By means of Identity Federation the proposed architecture will bring more privacy features on top of the PAISE authentication mechanism.

The communication protocol shown in Figure 4 works the following way:

1. The user requests for accessing certain resources.
2. The user is redirected to an IdP by the RP.

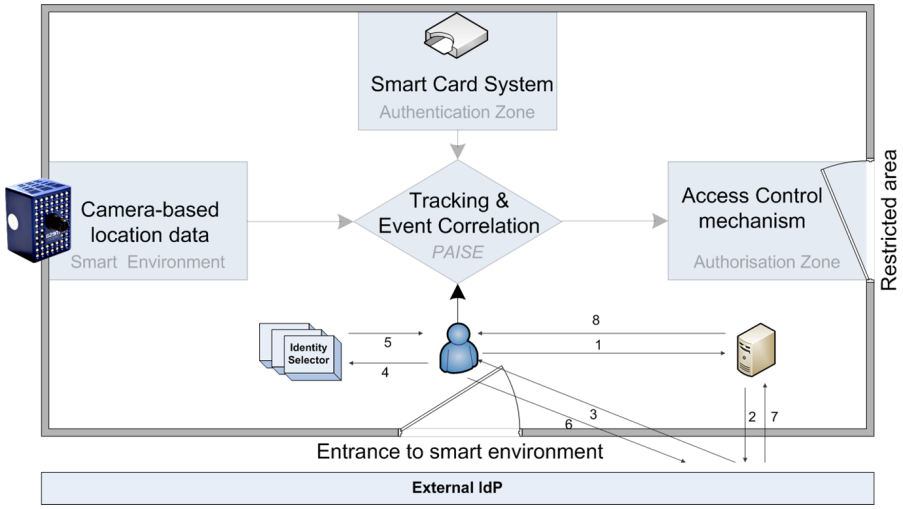

Fig. 4. Communication view point on the PAISE architecture.

3. The IdP requests the user for his credential.
4. The user looks at his InformationCard repository.
5. User selects an InformationCard.
6. The user reveals his credential to the IdP.
7. The IdP releases a token to the RP.
8. The RP grants access to the requested resources. The RP can then use this token to authenticate the user or for some other purposes.

This architecture allows decoupling of user identity from IdP and RP, i.e., users can use different identities and possibly different IdPs towards different RPs in the environment. This is how it captures the essence of being ambient in smart environment and switch identity to plug into different contexts. It leverages location tracking feature of PASIE and identity federation features of Identity Metasystem to enable multi-party federation in an ambient manner.

6 Discussion

In this section we briefly discuss how the proposed architecture accomplishes the privacy principles described in Section 2.3.

– **Notice:** First of all, the user is able to choose an InformationCard as a visual metaphor of his digital identity, which allows him a human readable mechanism to understand exactly what information about him is fed to the system, i.e., the data collection system is more "open" and "transparent" to the user. This exactly reflects the first privacy principle "notice" mentioned in Section 2.3.

- **Choice and Consent:** Secondly, when the user is sending a request for a resource, he is redirected to his IdP and the IdP requests for his credential. In this case the user can choose a suitable digital persona for the given context. This brings the privacy principle "choice and consent" to be applicable in PAISE.
- **Anonymity and Pseudonymity:** Moreover, when the user is federated by an external identity provider to access resources to a smart environment, the system only knows if the user has the right credential to access a certain resources. Obviously, there has to be a predefined trust mechanism between the external IdP and domain of the smart environment the user is accessing. This allows the user a certain degree of anonymity within the area where he is tracked by the PAISE system, i.e., he is not identified as an individual entity rather as an entity belonging to a group.
- **Proximity and Locality:** Finally, his tracking data does not go beyond the locality of his foreign domain, i.e., his IdP who has his actual identification does not gain access to his movement data. Thus it allows the fourth privacy principle "'proximity and locality" to be applicable up to a certain degree.

7 Conclusion & Outlook

To summarize the implication of the "Identity Metasystem" as an add-on to the PAISE model it is important to highlight some benefits of Federated Identity and InformationCard. First of all federated identity makes data collection fragmented, thus leads to less unlinkability without losing the possibility of traceability. Accountability vs. anonymity has been a classic debate between proponents of privacy and security. Federated Identity somehow meets the balance between these two. Another significant addition is an InformationCard. InformationCard provides a clear and usable representation of digital identity. It allows context aware identity selection, empowerment of the user and usability. Although the user is not able to switch off his tracking, by means of identity selector he can choose InformationCard selecting different identities and contexts. This is how PAISE is one step closer to the old definition of privacy given by Brandeis, i.e., the right to be leave one identity mask and select a new one has been accomplished.

References

1. Hansen, M., Kirshmeyer, M., Jensen, C.: Persistent authentication in smart environments. In Proceedings of the 2nd International Workshop on Combining Context with Trust, Security, and Privacy (CAT08) (June, 2008) 31–44
2. Weiser, M.: The computer for the 21st century. SIGMOBILE Mob. Comput. Commun. Rev. **3**(3) (1999) 3–11
3. Langheinrich, M.: Privacy by design - principles of privacy-aware ubiquitous systems. In: UbiComp '01: Proceedings of the 3rd international conference on Ubiquitous Computing, London, UK, Springer-Verlag (2001) 273–291

4. Lockton, V., Rosenberg, R.S.: Rfid: The next serious threat to privacy. Ethics and Inf. Technol. **7**(4) (2005) 221–231
5. Michael, M.G., Fusco, S.J., Michael, K.: A research note on ethics in the emerging age of überveillance. Comput. Commun. **31**(6) (2008) 1192–1199
6. Perusco, L., Michael, K.: Control, trust, privacy, and security: evaluating location-based services. Technology and Society Magazine, IEEE **26**(1) (Spring 2007) 4–16
7. Cameron, K.: The laws of identity. Microsoft Corporation, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (2005)
8. Akram, H., Hoffmann, M.: Supports for identity management in ambient environments - the hydra approach. Systems and Networks Communications, 2008. ICSNC '08. 3rd International Conference on (Oct. 2008) 371–377
9. McLaughlin, L.: What microsoft's identity metasystem means to developers. Software, IEEE **23**(1) (Jan.-Feb. 2006) 108–111
10. Cameron, K., Jones, M.B.: Design rationale behind the identity metasystem architecture (2006)
11. Lawrenc, K., et. al.: Ws-trust 1.3. OASIS Standard, http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html (19 March 2007)
12. Ballinger, K., et. al: Web services metadata exchange, version 1.1. http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-mex/metadataexchange.pdf (August 2006)
13. Akram, H.I., Hoffmann, M.: User-centric identity management in ambient environments. International Journal on Advances in Intelligent Systems **vol 2, no 1** (year 2009) 254 – 267
14. Akram, H., Hoffmann, M.: Laws of identity in ambient environments: The hydra approach. In: UBICOMM '08: Proceedings of the 2008 The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Washington, DC, USA, IEEE Computer Society (2008) 367–373
15. Miller, J.: Yadis 1.0. http://yadis.org/papers/yadisv1.0.pdf (March 2006)
16. Recordon, D., Reed, D.: Openid 2.0: a platform for user-centric identity management. In: DIM '06: Proceedings of the second ACM workshop on Digital identity management, New York, NY, USA, ACM (2006) 11–16
17. Recordon, D., Fitzpatrick, B.: Openid authentication 1.1. http://openid.net/specs/ (2006)
18. Mercuri, M.: Beginning Windows CardSpace: From Novice to Professional. Apress, Berkely, CA, USA (2007)
19. Brown K, Mani, S.: Microsoft code name "geneva" framework whitepaper for developers. Microsoft Corporation, http://download.microsoft.com/download/7/d/0/7d0b5166-6a8a-418a-addd-95ee9b046994/GenevaFrameworkWhitepaperForDevelopers.pdf (2008)
20. Alrodhan, W.A., Mitchell, C.J.: Addressing privacy issues in cardspace. In: IAS '07: Proceedings of the Third International Symposium on Information Assurance and Security, Washington, DC, USA, IEEE Computer Society (2007) 285–291
21. Ruddy, M., Trevithick, P., Nadalin, T., Olds, D.: Higgins trust framework. Digital ID World (2006)