A Taxonomy of Privacy and Security Risks Contributing Factors

Ebenezer Paintsil, Lothar Fritsch

A Taxonomy of Privacy and Security Risks Contributing Factors

Ebenezer Paintsil and Lothar Fritsch
{Paintsil, lothar.fritsch }@nr.no

Department of Applied Research in ICT
Norwegian Computing Center
Oslo, Norway

Abstract. Identity management system(s) (IDMS) do rely on tokens in order to function. Tokens can contribute to privacy or security risk in IDMS. Specifically, the characteristics of tokens contribute greatly to security and privacy risks in IDMS. Our understanding of how the characteristics of token contribute to privacy and security risks will help us manage the privacy and security risks in IDMS. In this article, we introduce a taxonomy of privacy and security risks contributing factors to improve our understanding of how tokens affect privacy and security in IDMS. The taxonomy is based on a survey of IDMS articles. We observed that our taxonomy can form the basis for a risk assessment model.

1 Introduction

A token is a technical artifact providing assurance about an identity. Tokens help authenticate and establish the identity of the end-users. They also help the end-user to remember their identifiers and facilitate information flow in identity management system(s) (IDMS). Figure 1 depicts an example of a simple identity management system. The identity provider (IdP) is an organization that collects the personal information of the end-user and creates a digital identity or identities for it. An IdP issues or helps the end-user to choose an identifier representing the digital identity. The end-user can then use the identifier(s) to identify or authenticate herself to a service provider (SP) in order to access an online service or resource. Each SP may require a different identifier or has a peculiar identification or authentication scheme. The number of identifiers may grow depending on the number of SPs the end-user interacts with and the kind of services or resources the end-user subscribes. The growth may reach a point where the end-user could no long remember all the numerous identifiers and their corresponding SPs. To solve this identifier management challenge, we either employ a software agent to store and select the correct identifier for a SP as in [1] or a hardware device such as a smart card to store and facilitate the selection of the correct identifier for a SP.

In the physical world, identity tokens consist of identifying information or identifiers stored in a physical device such as credit card, passports, a silicon

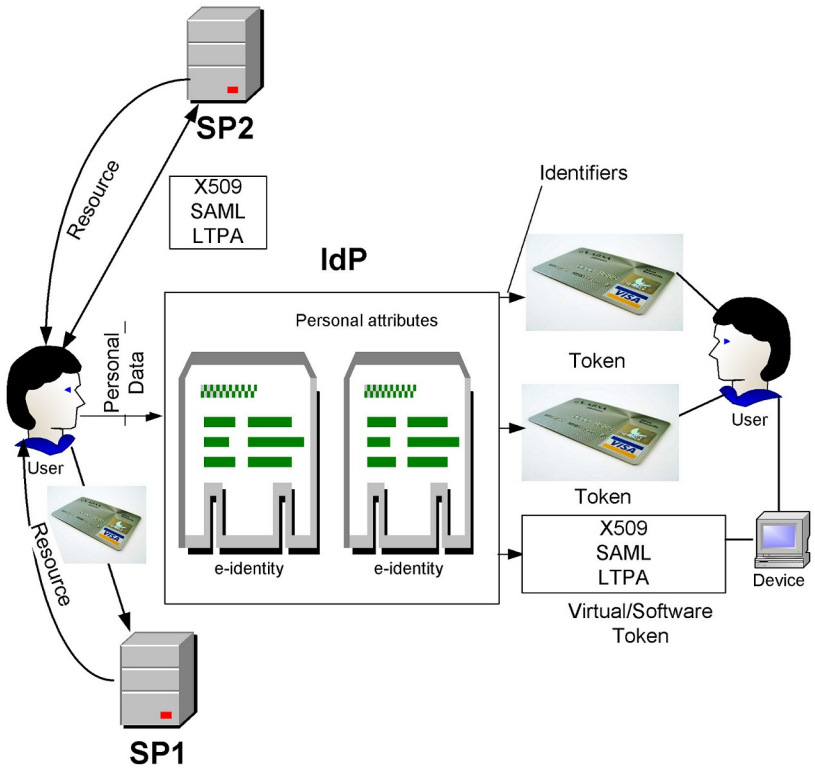

Fig. 1. A Simple Identity Management System, SP1 means service provider 1, SP2 means service provider 2 and IdP means identity provider

chip and a magnetic stripe [2]. We also have virtual or software identity tokens such as the Microsoft information card (InfoCard or CardSpace) technology. The InfoCard technology consists of identity metadata stored in a visual icon. The identity metadata point to or associate with a digital identity. The digital identity in this case represents the identity of the end-user. We can also find other kinds of tokens such as user name tokens, binary tokens, nonce, XML based tokens and custom tokens[1] such as Keynote [3], [4]. A token can consist of a piece of data, a mechanism, an algorithm, an assertion or a credential.

[1] A user name token consists of a user name and optionally, password information for basic authentication. A nonce is a random generated tokens used to protect against replay attack. Binary tokens are non-XML based security tokens represented by binary octet streams. Examples of binary tokens are X.509 certificates, Kerberos tickets and Lightweight Third Party Authentication (LTPA) tokens. We represent XML based tokens by extensibility markup language. Examples of XML based tokens are, Security Assertion Markup Language (SAML), Services Provisioning Markup Language (SPML) and Extensible rights Markup Language (XrML)

The construction and different uses of tokens contribute to privacy and security risks in IDMS [3]. Camenisch and others have suggested anonymous credential systems as a means of enhancing privacy in IDMS. In such systems, different uses of identity tokens by the same user are unlinkable. However, apart from unlinkability, tokens contribute to security and privacy risks in diverse ways. For example, function creep is as a result of using a token for unintended purpose. Anonymous credential systems also lack practical use and may not be compatible with already deployed IDMS [5], [6]. They may rely on a master secret to protect all the tokens, however accidental disclosure of the master secret could lead to identity theft, linkability and eventual privacy or security risk. Thus, the characteristics of tokens can contribute to privacy and security risks even in anonymous credential systems.

In this article, we introduce a taxonomy of privacy and security risks contributing factors in order to understand the impact of the characteristics of tokens on privacy and security in IDMS. In addition, we introduce the applications of our taxonomy.

We organize this article as follows. In Section 2, we introduce existing works on the effect of tokens on IDMS. Section 3 describes our taxonomy of privacy and security risks contributing factors in detail. We introduce the applications of our taxonomy in section 4. Section 5 states the conclusion and future work.

2 Related Work

There is a large body of literature on identity tokens and how they may contribute to security and privacy risks. However, our work organizes tokens according to their contribution to privacy and security risks.

In [7] D.J. Lutz and R. del Campo used a custom identity token to bridge the gap between privacy and security by providing a high level of privacy without anonymity. They designed a scheme to prevent replay attack and ensure that personal data is not sent to a foreign domain. They did not focus on the effect of the characteristics of tokens on privacy and security risks within a domain.

Furthermore, tokens are used to facilitate single sign-on authentication in federated IDMS [6]. However, this work focuses on a better way of constructing a token but not on the effect of the characteristics of tokens on privacy and security risks.

The identity mix (idemix) scheme proposed in [3], employs anonymous tokens to enhance privacy. The idemix scheme has three main parties. The end-user obtains a pseudonym in a form of an anonymous token from the identity issuer. The verifier verifies the credentials. The end-users can authenticate with a verifier without revealing their pseudonyms. The characteristics of tokens such as token secrecy, can affect this scheme, as one can misuse a pseudonym if the token's secret is inferred or revealed.

Peterson introduces factors for asset value computation and stresses the importance of asset in risk calculation [8]. We can use such factors to quantify the contributions of tokens to privacy and security risks. Peterson derived the asset

value of tokens from their loss, misuse, disclosure, disruption, replacement value, or theft. However, this is just an aspect of the risk contributing factors.

Solove introduces a taxonomy of privacy [9]. He introduces a high-level privacy risk contributing factors. They include data processing, data collection, data transfer and invasion. Nevertheless, the taxonomy is a high-level explanation of privacy principles without paying particular attention to the contributions of tokens to privacy risk.

Privacy Impact Assessment (PIA), a framework for assessing the impact of personal data processing on privacy before an information system is implemented, is introduced in [10]. The PIA is a compliance check of personal data processing to privacy laws, policies, or regulations. It specifies the requirement for privacy risk assessment without any explicit assessment technique or method. Our work differs from PIA in our introduction of an explicit privacy and security risks assessment technique.

The characteristics of tokens affect privacy and security in IDMS. A token characteristic include but not limited to its usages, how it is built, designed or constructed and how it is chosen. Security protocols are often concerned with how to build or construct a security token that can enhance privacy and security in IDMS [3], [7] , [11], [6]. The emphasis may be placed on formal verification of privacy and security risks caused by how tokens are built, designed or constructed. Moreover, tokens contribute in many different ways to security and privacy risks in IDMS. For instance in analogy to [8] tokens can be a good source of security and privacy risk metrics since they can consist of metadata about identity definitions.

3 The Taxonomy

This section introduces our taxonomy of privacy and security risks contributing factors. We based our factors on a literature survey of scientific articles in IDMS such as [8], [12], [3], [13], [14], [15] and many more. Our taxonomy, for the time being, avoids the Pfitzmann-Hansen terminology [16] with its definitions of e.g. linkability and observability, as the terms therein are defined on the background of anonymous communication and information sparsity. We feel that these terms need to be analyzed from our perspective on handling electronic identifiers and their risks. Our future work aims at aligning or re-defining the Pfitzmann-Hansen terminology to be meaningful in our context. Following this, we depict our taxonomy in Table 1. The taxonomy is non-exhaustive list of the characterization of tokens according to the manner in which they contribute to privacy and security risks. We explain the meaning of each contributing factor as listed in Table 1.

Token Mobility: This factor indicates the degree of mobility of a token. The degree of mobility refers to how easy to copy the token or its content, the physical constraints regarding the movement of the token, among others. For example the content of a low cost RFID tag with no additional security could easily be read as compared to the high cost RFID tags that come with additional security.

Risk Contributing Factors	Parameters
Token Mobility	***copyable, remotely usable, concurrently usable, immobile***
Token Value at Risk	***loss, misuse, disclosure, disruption, theft, replacement value***
Token Provisioning	***creation, editing, deletion***
Token Frequency & Duration of Use	***Uses per year, life-time, multiple times, one-time***
Token Use & Purpose	***original, unintended***
Token Assignment & Relationship	***forced, chosen, jointly-established, role, pseudonymity***
Token Obligation & Policy	***absence, present, functionality***
Token Claim Type	***single, multiple***
Token Secrecy	***public, inferable, secret***
Token Security	***origination, identification, validation, authentication, authorization***

Table 1. Taxonomy

The risks created by various forms of mobility directly relate to identity theft, linkability and the risk impacts. We assess the contributions of token mobility to privacy and security risks according to the following:

1. *Copyable*: the token can be copied with limited effort.
2. *Remotely usable*: the token can be used for remote identity management.
3. *Concurrently usable*: the token can be used concurrently in many parallel sessions, transactions, or applications.
4. *Immobile*: the token is not mobile, as it either must be physically present in a form of a user, or even presented to the system that is supposed to accept it.

Token Value at Risk: Finding assets and the value of the asset at risk is an important part of risk assessment (see [17]). Similarly, tokens are assets of IDMS and their value at risk can contribute to privacy and security risks. Thus we can quantify the risk of using tokens by assessing the significance of the token or the value of the token to the operation and security of the IDMS and the privacy of the end-users. In [8], six risk factors for IDMS have been found in analogy to classic risk assessment focusing on asset value at risk. We classify token's value at risk in a similar manner as follows:

1. *Loss*: value at risk when token is lost.
2. *Misuse*: value at risk when token is used in wrongful ways.
3. *Disclosure*: value at risk when token or token-related information gets known to someone else.
4. *Disruption*: value at risk when token doesn't function.
5. *Theft*: value at risk when token gets into someone else's possession without authorization.
6. *Replacement value*: cost (effort, resources, time) to replace a token.

Token Provisioning: We create a token from personal attributes. The amount of personal information collected during the creation phase could contribute to privacy risk. Data minimality principle prohibits excessive data collection of personal information [18]. In addition, tokens that store excessive personal information may be used for other unintended purposes (function creep) or enable profiling and linkability. There should be a means of updating the token in order to ensure data integrity. Further, there should be a means of deleting or destroying the token when the purpose for its creation is longer in the interest of the end-user or when the end-user decides to do so. This would ensure the privacy of the end-user. Therefore, we distinguish the following phases of the token provisioning life cycle: **creation, editing and deletion**. Each phase can be assumed to have different privacy or security risk impacts.

Token Frequency & Duration of Use: The underlining IDMS information flow protocol could determine if multiple use of the same token is susceptible to privacy and security risks [3]. Different uses of even specifically constructed tokens remain linkable if the underlining IDMS information flow protocol is not designed to prevent such privacy risk. Token's frequency and duration of use are decisive for risks concerning exposure or long-time risk. IDMS that allow a SP and an IdP to share information, a token used often allows for detailed profiling. A token used in association with life-time identification or multiple times causes high risks of secondary use and profiling of the person's life [19]. We classify a token chosen or assigned for life as lifetime token, a token that can be used multiple times but not for life as a multiple times token and a token that can be used once is a one-time token.

Token Use & Purpose: Purpose specification is an important privacy principle. It requires that personal information be collected for a specific purpose and use in an open and transparent manner [20]. Personal information should not be used for purposes other than the original purpose for which it was collected without informed consent. Since tokens may carry personal information or contain identifiers that link to personal information, any form of function creep or misuse could contribute to privacy and security risks. Function creep occurs when a token is used for unintended purpose. For example, in the United States (US), driver licenses have become the de facto general-purpose identity tokens [21], however, in some cases the driver licenses disclose more personal information than actually needed. For example, using a driver license to prove one's age will result in disclosing additional personal information meant for secondary purpose to the SP [22]. Such function creep and lack of selective disclosure pose privacy and security risks. We classify the purpose of a token as original and unintended. In general the intended purpose of a token is identification, authentication or authorization. The abuse of the purpose of a token or how the purpose of a token is achieved may contribute to privacy and security risks.

Token Assignment & Relationship: The need for user-centric IDMS clearly emphasizes the importance of how tokens are assigned or chosen. User-centric IDMS offer the end-users the ability to control their personal information and enforce their consent by determining the choice of their identity tokens [23].

We can determine the amount of personal information to disclose or attach to our identity token with user-centric IDMS (see [24], [25]).

The origin of and control over tokens contribute to privacy or security risk. A token can be chosen by a person, jointly established or forced upon by an authority. They can relate to a role rather than a person, and they could relate to a pseudonym [3]. A role is some sort of authorization, while a pseudonym is a mask with properties and usage patterns that might only occur for a particular purpose.

The token assignment and relationship risk-contributing factor assesses the risk impact if a token is forced on an end-user, chosen by an end-user as in the user-centric IDMS, jointly-established with the end-user or chosen according to the end-user's role. It also assesses the risk impact if a token is chosen under a pseudonym (pseudonymous tokens). Choosing a token under a pseudonym can enhance privacy especially if we cannot profile it various usages [3].

Token Obligation & Policy: We may protect a token with data minimization technique such as idemix [3] or attach a policy expressing the end-user's consent to the token in an IDMS. For policy-based protection, a major factor for the introduction of risks is the question of privacy policy enforcement, the possibilities for auditing and investigation of suspicious system behavior. Recent work suggests combine services' privacy policies [12] with an obligation [26]-a policy expressing the data processing consent that was given by a person. In addition, to ensure audit of processing, an audit trail [13] is suggested. The absence or the presence of privacy policy and a particular functionality (or enforcement mechanism) of the policy based concepts express a potential privacy risk. In the absence of policy or for non-policy based IDMS a particular data minimization technique or functionality can also enhance privacy or contribute to privacy risk (see [3]).

Token Claim Type: We can enforce the security of identifiers stored in a token or protect the misuse of identifiers by attaching a secret or a claim to the tokens. The type of claims are generally classify as *"something we know"* (a secret e.g. password), *"something we are"* (something we cannot share with others, e.g. finger print, iris etc) and *"something we have"* (e.g. possessing a smart card, key card or a token etc) [21]. Each claim type is a factor. Token claim type considers the impact of the number of factors used to secure a token in IDMS. Some tokens may require no additional secret in order to protect it content. We refer to such tokens as single claim tokens since the possession of the token itself is a factor. A token that requires a factor such as a personal identification number (PIN) in order to access its content is referred to as a two-factor or multiple claim token. We refer to a token requiring multiple factors such as PIN and finger print as multiple claim tokens or a three-factor token.

For example, an X509 token may require the possession of a physical smart card and a PIN [1]. The smart card is inserted into a card reader and a PIN is used to access the certificate's private key. The possession of the card is a factor representing what the end-user has or possesses and the PIN is a second

factor representing what the end-user knows. This is an example of a two-factor authentication token.

The number of authentication factors or factors may determine the complexity and security of the token. For example, current master cards may require no additional secret PIN when used for online transactions. We regard such token as a single factor authentication token. A single factor authentication token would be less secure and easy to use than a three-factor authentication token such as an X509 token that requires a PIN and a biometric factor. We therefore classify tokens into single claim and multiple claim tokens.

Token Secrecy: Tokens have claim type as discussed above. The secrecy or the constraints of authentication factors such as physical presence can contribute to security or privacy risk in IDMS. If a token's additional authentication factor is public then the claim type of such a token is always single. The secrecy of the additional authentication factor and the constraint attach to the additional authentication factor may determine the claim type.

Furthermore, secrecy is essential for maintaining unique mapping between identifiers and persons [8]. We can facilitate identification by how much secrecy a token possesses. A token with additional authentication factor such as "mothers' maiden name" used in the past for telephone authentication with credit cards [27] is easy to guess or infer. We classify such tokens secrecy as inferable. We consider the secrecy of a token as public if the additional authentication factors or claims are known by a number of people, group and organization or exist in many databases, at the disposal of an unknown number of persons and organizations.

We classify the secrecy of a token as *"secret"* or an additional authentication factor of a token as *"secret"* if it is private or not shared with others because it is link to a valuable resource such as our bank account (see [3]). A possible example of private "secret" is a private cryptographic key and a PIN.

Token Security: The security of token can contribute to the security of the IDMS. If a token used in an IDMS is a credential then the system should have a mechanism for checking the authority who issued the token. If the token is a mere assertion then the IDMS should provide a different mechanism to ensure the authenticity of the assertion. In order to ensure token security, there should be a means of ensuring the validity, identity and legitimacy of the token. Similar to [21] we describe token security as follows:

1. *origination*: the token is issued by the indicated legitimate authority
2. *Identification*: token identifies the subject-the entity possessing the token.
3. *Validation*: token has not expired, its lifespan is within the validity period or has passed the validity test.
4. *Authentication*: token belongs to the entity presenting it to the IDMS.
5. *Authorization*: token grants relevant permissions to the entity possessing it.

The IDMS should provide functionality for checking the above security properties of the token.

4 Applications of Taxonomy

We can fairly estimate the privacy and security risks of an IDMS based on the characteristics of token as explained in our taxonomy. This section explains the possible application of our taxonomy for privacy and security risks assessment. We state the possibilities of conducting privacy and security risks assessment based on the characteristics of tokens used in the IDMS. We follow the following steps:

Known Security Risks in IDMS: We examine the IDMS in order to determine all the possible system tokens. We assess how the characteristics of the system tokens may affect the achievement of the information security objectives of the IDMS. Thus, which of the characteristics of tokens listed in table 1 contribute to the breach of information security such as unavailability, loss of confidentiality, repudiation and lack of integrity [28] and in what way do they contribute to security risk. For example we may assess the impact of multi-factor authentication scheme on the security of the IDMS. We may assess if the IDMS employs a two-factor authentication tokens or a three-factor authentication tokens. A two-factor authentication token is simpler but may provide less secure authentication [21].

We also assess how the security of the token contributes to security risk of the IDMS. In other words, we examine if the IDMS has a method for checking the security of the tokens. That is, we assess if the IDMS has a mechanism to check the legitimacy of the token, validity of the token, identity of the holder of the token, authenticity of the token and level of authorization the token has.

Finally we assign or compute the risk impact of token security, token secrecy etc of the IDMS.

Known Privacy Risks in IDMS: Similar to security risk assessment, we examine the IDMS in order to understand the information flow of the system. We examine how the IDMS tokens are designed and used. We assess if the information flow in the IDMS can contribute to the misuse of personal data, accidental disclosure of personal data etc. We determine if these privacy risks are caused by the construction of the IDMS tokens using the risk contributing factors listed in table 1. We then determine the impact and the possibility of the known risk occurring. For example, how will the token mobility contribute to accidental disclosure of personal data and what will be the impact of accidental disclosure on the IDMS?

Stakeholders Risk in IDMS: Usually tokens are created to reflect the needs of the system stakeholders. However, lack of extensive taxonomy of token characteristics to guide this process may contribute to future privacy and security risks of the IDMS. This taxonomy will aid the stakeholders of the IDMS to ask the necessary questions before designing or consenting to use any identity token. Furthermore, the stakeholders can now, before they take an IDMS that was designed for a different purpose into a new application context, thoroughly analyze its properties and the possible risks and consequences. For example, the stakeholders can now assess how an IDMS with high token mobility contribute to

function creep. How does function creep affect their interest such as the reputation? Furthermore, how does multiple claim authentication token inconvenience the end-user and how does it protect against identity theft in IDMS? We can also examine how token assignment contributes to privacy and security risks from the stakeholders' point of views. For example, user-centric IDMS may allow the end-users to exercise selective disclosure by choosing tokens on their own. This enhances the privacy of the end-user but the other stakeholders may be deprived of information for auditing and accounting [24], [1].

5 Conclusion

Identity tokens are constructed without extensive assessment of their affect on privacy and security risks in identity management system (IDMS). The understanding of the contribution of tokens to privacy and security risks can aid in managing privacy and security risks in IDMS. This article defines a token and how tokens affect privacy and security in IDMS. We introduced a taxonomy of risk contributing factors for IDMS based on the characteristics of tokens and the application of the taxonomy for privacy and security risks assessment. We explained how the taxonomy contributes to privacy, security, and the stakeholders' risk in IDMS. Finally, we showed that tokens are rich sources of privacy and security risks metric for IDMS and can serve as a basis for privacy and security risks assessment model.

We intend to investigate the development of a privacy and security risks assessment model based on our taxonomy in our future work.

6 Acknowledgment

The work reported in this paper is part of the PETweb II project sponsored by The Research Council of Norway under grant 193030/S10.

References

[1] CORPORATION, M.: The identity metasystem: Towards a privacy-compliant solution to the challenges of digital identity. White paper, MICROSOFT CORPORATION (2006)
[2] Clarke, R.: A sufficiently rich model of (id)entity, authentication and authorisation. http://www.rogerclarke.com/ID/IdModel-1002.html (2010)
[3] Camenisch, J., Herreweghen, E.V.: Design and implementation of the idemix anonymous credential system (2002)
[4] IBM, C.: Overview of token types. Framework document, IBM (2010) http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/cwbs_tokentype.html.
[5] Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: EUROCRYPT '01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, London, UK, Springer-Verlag (2001) 93–118

[6] WP3: D3.1: Structured overview on prototypes and concepts of identity management systems. Deliverable 1.1, Future of Identity in the Information Society (2005)
[7] D.J. Lutz, R.d.C.: "bridging the gap between privacy and security in multi-domain federations with identity tokens". In: 2006 Third Annual International Conference on Mobile and Ubiquitous Systems. (2006) 1–3
[8] Peterson, G.: Introduction to Identity Management Risk Metrics. IEEE Security & Privacy **4**(4) (2006) 88–91
[9] Solove, D.: A taxonomy of privacy - GWU Law School Public Law Research Paper No.129. University of Pennsylvania Law Review **154**(3) (2006) 477
[10] Office, I.C.: Privacy impact assessment handbook - version 2. Technical report, ICO, London, UK (2009)
[11] Lutz, D.J.: Secure aaa by means of identity tokens in next generation mobile environments. In: ICWMC '07: Proceedings of the Third International Conference on Wireless and Mobile Communications, Washington, DC, USA, IEEE Computer Society (2007) 57
[12] Ardagna, C., Bussard, L., De Capitani di Vimercati, S., Neven, G., Paraboschi, S., Pedrini: PrimeLife Policy Language. In: W3C Workshop on Access Control Application Scenarios, Luxembourg (2009)
[13] Hansen, M.: Concepts of Privacy-Enhancing Identity Management for Privacy-Enhancing Security Technologies. In Cas, J., ed.: PRISE conference proceesings: Towards privacy enhancing security technologies - the next steps, Wien (2009) 91–103
[14] Iwaihara, M., Murakami, K., Ahn, G.J., Yoshikawa, M.: Risk Evaluation for Personal Identity Management Based on Privacy Attribute Ontology. In Li, Q., Spaccapietra, S., Yu, E., Oliv, A., eds.: Conceptual Modelling - ER 2008. Volume 5231 of Lecture Notes in Computer Science (LNCS). Springer, Berlin (2008) 183–198
[15] WP2: D 2.1: Inventory of topics and clusters. Deliverable 2.0, Future of Identity in the Information Society (2005)
[16] Pfitzmann, A., Hansen, M.: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management A Consolidated Proposal for Terminology - v0.29. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (2007)
[17] ISACA: The Risk IT Practitioner Guide. ISACA, 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA (2009) isbn: 978-1-60420-116-1.
[18] Bygrave, L.A.: Data Protection Law Approaching Its Rationale, Logic and Limits. Kluwer Law International (2002)
[19] Fritsch, L.: Profiling and Location-Based Services. In Hildebrandt, M., Gutwirth, S., eds.: Profiling the European Citizen - Cross-Disciplinary Perspectives. Springer Netherlands, Dordrecht (2008) 147–160
[20] Hansen, M., Schwartz, A., Cooper, A.: Privacy and identity management. IEEE Security and Privacy **6**(2) (2008) 38–45
[21] Mac Gregor, W., Dutcher, W., Khan, J.: An Ontology of Identity Credentials - Part 1: Background and Formulation. Technical report, National Institute of Standard and Technology, Gaitersburg, MD, USA (2006)
[22] Camenisch, J., shelat, a., Sommer, D., Fischer-Hübner, S., Hansen, M., Krasemann, H., Lacoste, G., Leenes, R., Tseng, J.: Privacy and identity management for everyone. In: DIM '05: Proceedings of the 2005 workshop on Digital identity management, New York, NY, USA, ACM (2005) 20–27

[23] Bramhall, P., Hansen, M., Rannenberg, K., Roessler, T.: User-centric identity management: New trends in standardization and regulation. IEEE Security and Privacy **5** (2007) 84–87
[24] Bar-or, O., Thomas, B.: Openid explained. http://openidexplained.com/ (2010) [Online; accessed 18-Aug-2010].
[25] Kruk, S.R., Grzonkowski, S., Gzella, A., Woroniecki, T., Choi, H.C.: D-foaf: Distributed identity management with access rights delegation. In Mizoguchi, R., Shi, Z., Giunchiglia, F., eds.: ASWC. Volume 4185 of Lecture Notes in Computer Science., Springer (2006) 140–154
[26] Mont, M.C., Beato, F.: On parametric obligation policies: Enabling privacy-aware information lifecycle management in enterprises. In: POLICY '07: Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks, Washington, DC, USA, IEEE Computer Society (2007) 51–55
[27] Anderson, R.J.: Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc., New York, NY, USA (2001)
[28] Siponen, M.T., Oinas-Kukkonen, H.: A review of information security issues and respective research contributions. SIGMIS Database **38**(1) (2007) 60–80