Lucidman

Digital Identity Issues

Johann Vincent
Université de Caen Basse-Normandie, UMR 6072 GREYC, F-14032 Caen, France
ENSICAEN, UMR 6072 GREYC, F-14050, Caen, France
CNRS, UMR 6072 GREYC, F-14032, Caen, France
johann.vincent@ensicaen.fr

15 mars 2012

Abstract

The Identity of a person is a complex notion that can be studied from various angles: psychology, philosophy or biology. With the growth of telecommunication technology, a new field of study has emerged and the term digital identity has been chosen to link a real entity to a virtual one. In this paper, the issues raised by this new concept are presented as well as the admitted vocabulary to describe them.

Contents

0.1 Introduction

An electronic transaction is the dematerialised exchange of information between two entities (individuals or organisations) via computer systems. In today's world, these transactions are everywhere. Individuals use their smartphone to know about the weather forecast, they use electronic badges to enter their office, they use e-banking services on their computer, pay their lunch with a credit card or use an healthcare electronic card to get reimbursement for medical consultation... Such exchange implies the transfer of personal and confidential information, hence the necessity for a trust relationship between these two entities. The entities rely on multiple dimensions to build confidence but the main one is the digital identity of the entities. Securement of the system guarantees user identity as well as data integrity and traceability to provide a proof of transaction. However, system securement implies the implementation of technologies and creates barriers (ergonomic, psychological, technical and financial barriers) that users are not necessarily willing to accept. One of the most important barrier is the privacy protection of the user.

In this report, a focus is made on digital identity and the issues associated. The documment is organized as follows, the first section gives the definitions of trust and introduces digital identity as a main tool to build trust relationships. The second section is focused on digital identity and gives its definitions. The third and fourth section present the issues raised by digital identity respectively security and privacy. They expose the vulnerabilities and the properties that have to be respected to prevent an attacker from exploiting them.

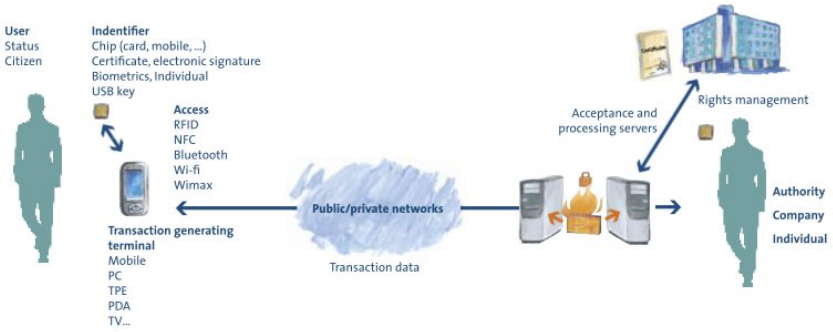

Figure 1: Secure electronic transaction chain perimeter (source E-Secure Transactions Cluster [1])

0.2 Trust

The first issue to be considered when dealing with digital identity is trust. In fact, trust between digital entities is the main reason why digital identity

has been proposed. In the litterature, there have been a number of survey related to trust in various domains. For example, in [2], the authors give an overview of trust with a focus on semantic web issues. There have also been a number of definitions for trust, for Mui et al. [3], trust is "a subjective expectation an agent has about anothers future behavior based on the history of their encounters". This can be viewed as "reputation-based" trust. Grandison and Sloman introduce the concept of "competence" in [4], for them, trust is "the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context". Finally, a third definition is given by Olmedila in [5] where Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X). These definitions have lead to a number of models for trust that are presented in the next subsections. In this first subsection, we present the general models of trust while the reputation-based and policy-based trust are presented next.

0.2.1 General models of trust

Given the previous definitions, some works have also been done to formalize trust and to express the properties of a trust relationship between two entities. In [6], the author presents four properties: competence (ability to give accurate information), benevolence (willingness to expend the effort), integrity (adherence to honest behavior), and predictability (evidence to support that the desired outcome will occur). Some works omit the predictability, that is the case of [7] for example. Marsh work in [8] is considered as the first to formalize trust and propose a way to compute a trust value between $[-1, 1]$. From this work, Marsh has extracted three kinds of trust:

1. Basic, over all contexts
2. General, between two individuals and all their contexts occurring together
3. Situational, between two individuals in a specific context

This work has also allowed Marsh to identify time as being a relevant information in trust relationships. The efforts on computing a trust metric have been pursued, in particular, some efforts have been done in game theory where Brainov and Sandholm [9] have shown that a maximum utility is reached when the trust level is equivalent. In parallel to those efforts, works have been done in specific contexts to help the establishment of trust relationship between entities. In particular, online where reputation-based trust is the more active and finally in the field of computer security where policy-based trust has been proposed.

0.2.2 Reputation-based trust

Reputation-based trust relies on a personal experience and the experience of others to make a decision about an entity. One solution to obtain trustworthy

information about an entity is to rely on a central trusted database in which reputation is stored. The vast majority of works done in this field avoids this approach and tries to rely on decentralized trust, that is the case in [10] or [11]. This approach allows agents to make trust decision based on their knowledge and the reputation gathered from other agents. An agent that provides trust information about another is called a witness and the trust is viewed as referral trust. Works in referral trust include [12], [13], [14], [15] and [16]. Reputation based trust is especially usefull in peer-to-peer networks and grid [17]. Trust metrics have been proposed to address the issue of the transitivity of trust and they essentially rely on reputation, for example [18] and [19].

0.2.3 Policy-based trust

Policy-based trust relies on policies to express when, for what and how to determine trust in an entity and adopt a "hard security" approach. The application of a given policy is conditioned by the knowledge that the entity designed by it is who or what he is supposed to be. To learn that information, systems rely on a set of information about the entity called a credential, or even a signed credential. This credential can in fact be generalized to a digital identity. The nature and exchange mechanisms of digital identities is discussed in the next section. However, this exchange highlights the two issues raised by policy-based trust and digital identities: the privacy of the entities involved and the security of the digital identity. To address that tradeoff, some works have been done, for example in [20, 21]. Another field of interest of policy-based trust is the management of the chaining of identities with works such as PeerTrust [22], PROTUNE [23] or the RT_0 [24] language. Efforts are finally conducted in the field of policy languages and expression. For security, we can cite the OASIS XACML [25], WS-trust [26] and WS-policy [27] approaches. In the semantic web field, works have also been conducted to represent policies, in [28], Tonti et al. make the comparison of three approaches KAoS [29], Rei [30] and Ponder [31].

As stated before, these policies and their application rely on the exchange of credentials or digital identities. In the next section, a description of what digital identity is and how it is managed in a trust establishment is given.

0.3 Digital identity

This section is dedicated to the definition of what is a digital identity, it starts with the definition of real identity concepts, online identity and finally of digital identity.

0.3.1 Real identity

Before defining digital identity, it is important to separate the real world from the virtual one. For Clarke [32], "an identity exists in the real world, not on disk drives. It is a presentation or role of some underlying entity". An entity can be a physical being as well as an object such as a computer. An entity can have many identities depending on its roles. For example, a person can be an employee when he is at work and be a father when he is at home. An entity is sometimes referred as a subject [33] [34]. Each entity has a number of attributes: a mobile phone for example has a limited amount of memory, a touch screen or WiFi connectivity. Some of the attributes are shared by a number of entities, for example there are some individuals that weight the same or have the same height. However, some of the attributes are unique, for example DNA, fingerprints, or a serial number. These unique attributes are called identifiers [35] [36] [37], they allow an observer to identify an entity or a group of entities. The identification notion is important to define identity, for example the ISO working group JTC 1/SC 27 WG5 defines identity as "a set of attributes that allows the identification of its owner". That is why an identity always depends on an observer, for example a badge id is an attribute for anyone in a firm but does not indicate anything to an external person.

0.3.2 Online identity

In information systems, and in particular on social networks, a person is often represented by its avatar or persona. These avatars are used to write on a blog, make some auctions or play games. The social role of these avatars is called online identity. In [33], the authors classify this kind of identity in four classes that matches the well known authentication classes.

1. What you **know**: your friends on a social network...
2. What you **have**: a smartphone, a pc or a tablet...
3. What you **are**: your avatar in a online game...
4. What you **do**: articles written on a blog, wiki, auctions made...

The avatars, as their pysical counterparts, are defined by a number of attributes that are recorded as data in information systems. These data representing the attributes are called digital identities.

0.3.3 Digital identity

In the laws of identity [38], K. Cameron defines digital identity as *a set of claims made by a digital subject about itself or another digital subject.* Those claims extend the concept of attributes of a digital subject as they can also express its relationships with other subjects. They can describe its capacities, can be derived from the attributes and can express contextual information. We

formalize that in saying that a claim is a function of the attributes of a digital subject and write:

$$id = \{c_1, c_2, \ldots, c_n\}$$

Where c_i is a function f_i of the attributes $\{a_1, \ldots, a_m\}$ of the digital entity. For example, if an individual owns the following attributes $\{Name, DateOfBirth\}$ and is willing to express an identity consisting of the following claims $c_1 : Name$ et $c_2 : age > 18$. The digital identity can be written :

$$id = \{f_1(Name), f_2(DateOfBirth)\}$$

$$\text{with } \begin{cases} f_1(Name) = & Name \\ f_2(DateOfBirth) = & Age > 18 \end{cases}$$

As presented before, policy-based trust relies on the exchange of digital identities to establish a trust relationship. In that case, the first purpose of a digital identity is to ensure two security properties: authentication and authorization. But recursively, as sensible data, the security of the digital identity itself has to be assured. Identity management systems (IMS) have been developed to address that issue and make sure that the identity is secured and can be used to build trust. The Future of Identity in the Information Society (FIDIS) project [39] classifies the IMS in three types: for account management, for profile establishment and for user-controlled pseudonym management. In this report, we focus our interest on the first type as it is the one that addresses the trust issue between the digital identity and the entity in charge of verifying it.

The general model for this type of IMS has evolved, over the years, from a centralized model to a more user-centric model. In [40], the authors present four models: the isolated model, centralized model, federated model [41] and finally the user-centric one. The user-centric model simplifies the usage of identity on the user side and provides the user more control over his digital identity. Open Id [42], OAuth [43], Shibboleth [44] or information cards [34] are well known examples of the user-centric model. They introduce a trusted third party called an identity provider (IdP) that is in charge of delivering digital identities to service providers (SP). As explained in [40], that model is network oriented. However, the use of Personal Authentication Device (PAD) can be done to achieve offline use of a digital identity.

0.4 Security

As explained in the first section of this document, policy-based trust is used in computer security to establish trust between entities. We explained as well that digital identity is dependent on an observer and that claims are supposed doubtful until proven otherwise. In fact, digital identity can be attacked just as real identity. In the real world, one can use false id documents, or a desguise that can modify the judgement of an observer. In this section, the security threats that exists for digital identity are presented as well as the security properties that can protect the digital identity from these threats.

0.4.1 Identity theft - Authentication

The first threat that we expose is the identity theft. The attacker uses the digital identity of another honnest identity to impersonate him. That threat is detailled in [45, 46]. An illustration of this threat is the "phishing" attack that consist in impersontating a website and invite users to log in with their digital identity. In a second time, the identity collected will be used to impersonate the users on the legitimate website.

The security property that matches the identity theft threat is the **authentication**. That well known property is defined in many security standards. The authentication consists in the verification of the digital identity of an entity. To do so, four classes of authentication are usually defined: what the entity knows, what she possesses, what she is and what she does. To authenticate the entity presenting a digital identity, a subset of the claims composing the digital identity must belong to one or more of these classes. For example, a password belongs to the knowledge class and a biometric data to the being class. When the claims belong to at least two of the classes, a strong authentication takes place. For example, the NIST level 4 recommendation [47] requires that the entity posseses a cryptographic token to realize strong authentication. The digital identity is a direct answer to that security property. However, it is easy to see that as a sensible data the digital identity needs to be protected.

0.4.2 Identity tampering - Integrity/authenticity

To establish trust, an observer needs to make sure that an attacker was not able to tamper with the claims about the entity it wants to identify. It is especially important when dealing with claims that are used for authentication. The **integrity** property can prevent this kind of attack on a digital identity by assuring that a data has not been modified between the time when it is read by the observer and the time it has been released. To do so, many standards have been proposed. For example, the ISO/IEC9797-2 defines three message authentication codes (MAC) based on hash functions. It is also the case of the RFC2104 [48]. The general principle is based on the usage of a secret key shared

between the sender and the receiver. The sender computes a MAC of the message with this key and send it with the message. The receiver also computes the MAC of the message and compares it with the received one. If the two codes are the same, the receiver is assured that the message has not been altered and assured of the authenticity since only that sender knows the key.

As shown above, in addition to the integrity, the methods presented can validate the authenticity of the identity claims. To ensure the authenticity electronic signature can also be used. Based on assymetric cryptography, the sender and the receiver both have a private and a public key which are used respectively to sign messages and verify the signature.

0.4.3 Personal data theft - Confidentiality

Another threat that target digital identity is the data theft. In fact, we have defined a digital identity as a set of claims about an entity, these claims can be sensitive data such as password or biometric data that must remain secret. The **confidentiality** property assures that only the intended entities have access to the content of a message. The usual method to realize that property is to encrypt the messages. The two famillies of cryptographic algorithms (assymetric and symetric) that we presented before can be used. For example, the french ANSSI recommands the use of the symetric algorithm AES to encrypt messages.

0.4.4 Privilege escalation - Authorization

The digital identity as we have defined it also addresses the **authorization** property. In fact, the claims can express the entity capacities so they can refer to specific rights. Most of the case however, the capacity claims are not used and the rights associated to the digital identity are defined in specific separated security policies. It is the case in classic access control solution [49]. The threat associated with the authorization property is called privilege escalation, an attacked tries to obtain more importants rights on a system. It can be achieved by modifying its capacity claims or other claims in order to impersonnate another entity with more rights.

0.4.5 Misuse of identity - Revocation

Just as their real counterparts, the identity claims can change over time. For example, the mailing address may change if the person moves or his access rights can change in case of mutation. When the digital identity is used to access sensitive data it is important to enable the revocation of it. It supposes that a claims has a validity period and that it exists a revocation mecanism to prevent its usage. The revocation property is also important to protect an individual in case of identity theft.

0.5 Privacy

Privacy, as well as identity, is a social and cultural concept that is similar to the concept of individual liberty defined in the universal declaration of human rights. A.F. Westin [50] defines privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". To protect this right in the digital world, legislations aimed at protecting personnal data, it is the case of the European directive 9546CE [51]. That right allows an individual to control, modify and remove any personal data. As we have explained, trust establishment in computer science relies on the exchange of digital identity and therefore of personal data that must be protected from various threats. In this section, the privacy threats are presented as well as the properties that can prevent them. These properties have mainly been proposed by D.J. Solove [52, 53], by A. Pfitzmann and M. Hansen [37] and finally by M. Deng [54].

0.5.1 Linkability - Unlinkability

Unlinkability aims at hiding the link that exists between two or more entities. A. Pfitzmann and M. Hansen [37] give the following definition: "Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attackers perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not". That means that if an individual uses two or more digital identities to access a system, an attacker will not be able to link them. That means as well that if an identity is used on two different systems, an attacker can also not link them to the individual.

0.5.2 Identification - Anonymity and pseudonymity

Paradoxically, there is a threat associated to the fact that a digital identity can provide identification of the individual referred in the claims. In fact, as we have defined that an individual can have several digital identities. If some of the claims that compose it can link the identity to the real individual (his real name, address,...) some of the claims can be anonymous. A. Pfitzmann and M. Hansen [37] give the following definition: "Anonymity of a subject from an attackers perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set". The term sufficiently indicates that there is a threshold from which anonimity is lifted.

For digital identity, the notion of k-anonymity defined by Sweeney [55] and improved by Ciriani et al. [56] can explain that threshold using entropy. The k-anonymity property requires that none of the records of a database characterizes less than k individuals.

A pseudonym is a digital identity that will allow an individual to build reputation on line but that differs from his real identity. A. Pfitzmann and M. Hansen [37] give the following definition: "a pseudonym is an identifier of a subject other than one of the subjects real names".

0.5.3 Non repudiation - Repudiation

Repudiation is explicited by Roe in [57] and defines that some individuals do not wish that an action can be linked to them for privacy reasons.

0.5.4 Detection and observation - Undetectability and Unobservability

A. Pfitzmann and M. Hansen [37] give the following definitions: "undetectability of an item of interest (IOI) from an attackers perspective means that the attacker cannot sufficiently distinguish whether it exists or not. If we consider messages as IOIs, this means that messages are not sufficiently discernible from, e.g., random noise. Unobservability of an item of interest (IOI) means:

- undetectability of the IOI against all subjects uninvolved in it
- anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.

0.5.5 Personal data theft - Confidentiality and Conscience of content

Confidentiality and personal data theft are the same as the property and attack defined in the security section. The conscience of content however, is a property that is introduced by Deng [54] and means that the subject has to be conscious of the personal data he pocesses and he choses to disclose. That property is interesting for digital identity as it is the same as the third Cameron's law [38]: "Justifiable parties". It states that the entities that use digital identity have to do so in a legetimate way and limit the abusive collection of unecessary data. For example, the works on the platform for privacy preferences (P3P) [58] allow a website to declare for what usage it collects a specific data.

0.5.6 Misuse of identity - Policy compliance and consent

The consent and policy compliance is also a property that is introduced by Deng [54] and means that the systems that uses identity have to require the consent of the individual or user. That property is equivalent to the first of Cameron's law : "control and consent" and is also required by many legislations.

0.6 Conclusion

In this report, we have defined trust and showed that in policy-based trust relies on digital identities. We have then defined digital identity as a set of claims made by a digital subject about himself or another subject. We have shown that digital identity implies two major issues that are security and privacy. These two issues have then been defined as well as a number of properties that apply to digital identity.

We have first shown that digital identity is a mean to assure security as it is a direct answer to the authentication and authorization property. However, to trust the digital identity, its security must be assured too, that means relying on another digital identity. Identity management is a recursive model where security validation relies on validations from lower layers. To make these validations, we have briefly presented cryptographic mechanisms that can assure other properties such as integrity.

The privacy issue has also been presented with its properties. Some of these properties may seem to be in contradiction with the security ones. It is sometime considered that the increase in security is done at the expense of privacy. However, that tradeoff is widely questionned nowaday [59] and it seems that in the case of digital identity management the two issues have to be addressed together.

Bibliography

[1] source E-Secure Transactions Cluster. Secure electronic transactions a key issue for tomorrow's society, 2006.

[2] D. Artz and Y. Gil. A survey of trust in computer science and the semantic web. *Web Semantics: Science, Services and Agents on the World Wide Web*, 5(2):58–71, 2007.

[3] L. Mui, M. Mohtashemi, and A. Halberstadt. A computational model of trust and reputation. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pages 2431–2439. IEEE, 2002.

[4] T. Grandison and M. Sloman. A survey of trust in internet applications. *Communications Surveys & Tutorials, IEEE*, 3(4):2–16, 2009.

[5] D. Olmedilla, O. Rana, B. Matthews, and W. Nejdl. Security and trust issues in semantic grids. In *Proceedings of the Dagsthul Seminar, Semantic Grid: The Convergence of Technologies*, volume 5271, page 10. Citeseer, 2005.

[6] D.H. McKnight and N.L. Chervany. The meanings of trust. 1996.

[7] D. Gefen. Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM SIGMIS Database*, 33(3):38–53, 2002.

[8] S.P. Marsh, University of Stirling. Dept. of Computing Science, and Mathematics. *Formalising trust as a computational concept*. Citeseer, 1994.

[9] S. Brainov and T. Sandholm. Contracting with uncertain level of trust. In *Proceedings of the 1st ACM conference on Electronic commerce*, pages 15–21. ACM, 1999.

[10] A. Abdul-Rahman and S. Hailes. A distributed trust model. In *Proceedings of the 1997 workshop on New security paradigms*, pages 48–60. ACM, 1998.

[11] B. Yu and M. Singh. A social mechanism of reputation management in electronic communities. *Cooperative Information Agents IV-The Future of Information Agents in Cyberspace*, pages 355–393, 2000.

[12] J. Sabater and C. Sierra. Reputation and social network analysis in multi-agent systems. In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1*, pages 475–482. ACM, 2002.

[13] T. Beth, M. Borcherding, and B. Klein. Valuation of trust in open networks. *Computer SecurityESORICS 94*, pages 1–18, 1994.

[14] S. Xiao and I. Benbasat. The formation of trust and distrust in recommendation agents in repeated interactions: a process-tracing analysis. In *Proceedings of the 5th international conference on Electronic commerce*, pages 287–293. ACM, 2003.

[15] J. O'Donovan and B. Smyth. Trust in recommender systems. In *Proceedings of the 10th international conference on Intelligent user interfaces*, pages 167–174. ACM, 2005.

[16] A. Jøsang, R. Hayward, and S. Pope. Trust network analysis with subjective logic. In *Proceedings of the 29th Australasian Computer Science Conference-Volume 48*, pages 85–94. Australian Computer Society, Inc., 2006.

[17] F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati. Choosing reputable servents in a p2p network. In *Proceedings of the 11th international conference on World Wide Web*, pages 376–386. ACM, 2002.

[18] J. Golbeck and J. Hendler. Accuracy of metrics for inferring trust and reputation in semantic web-based social networks. *Engineering knowledge in the age of the semantic web*, pages 116–131, 2004.

[19] J. Golbeck and J. Hendler. Inferring reputation on the semantic web. In *Proceedings of the 13th International World Wide Web Conference*, volume 316, 2004.

[20] T. Yu, M. Winslett, and K.E. Seamons. Interoperable strategies in automated trust negotiation. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 146–155. ACM, 2001.

[21] T. Yu and M. Winslett. Policy migration for sensitive credentials in trust negotiation. In *Proceedings of the 2003 ACM workshop on Privacy in the electronic society*, pages 9–20. ACM, 2003.

[22] W. Nejdl, D. Olmedilla, and M. Winslett. Peertrust: Automated trust negotiation for peers on the semantic web. *Secure Data Management*, pages 159–182, 2004.

[23] P. Bonatti and D. Olmedilla. Driving and monitoring provisional trust negotiation with metapolicies. In *Policies for Distributed Systems and Networks, 2005. Sixth IEEE International Workshop on*, pages 14–23. IEEE, 2005.

[24] N. Li, W.H. Winsborough, and J.C. Mitchell. Distributed credential chain discovery in trust management. *Journal of Computer Security*, 11(1):35–86, 2003.

[25] T. Moses et al. extensible access control markup language (xacml) version 2.0. *Oasis Standard*, 200502, 2005.

[26] A. Nadalin, M. Goodner, M. Gudgin, A. Barbir, and H. Granqvist. Oasis ws-trust 1.4. *Specification Version*, 1, 2008.

[27] S. Bajaj, D. Box, D. Chappell, F. Curbera, G. Daniels, P. Hallam-Baker, M. Hondo, C. Kaler, D. Langworthy, A. Malhotra, et al. Web services policy framework (ws-policy). *Version*, 1(2), 2006.

[28] G. Tonti, J. Bradshaw, R. Jeffers, R. Montanari, N. Suri, and A. Uszok. Semantic web languages for policy representation and reasoning: A comparison of kaos, rei, and ponder. *The SemanticWeb-ISWC 2003*, pages 419–437, 2003.

[29] A. Uszok, J.M. Bradshaw, J. Lott, M. Breedy, L. Bunch, P. Feltovich, M. Johnson, and H. Jung. New developments in ontology-based policy management: Increasing the practicality and comprehensiveness of kaos. pages 145–152, 2008.

[30] L. Kagal, T. Finin, and A. Joshi. A policy based approach to security for the semantic web. *The SemanticWeb-ISWC 2003*, pages 402–418, 2003.

[31] N. Damianou, N. Dulay, E. Lupu, and M. Sloman. The ponder policy specification language. *Policies for Distributed Systems and Networks*, pages 18–38, 2001.

[32] R. Clarke. Identification and authentication fundamentals. *Xamax Consultancy Pty Ltd, May*, 2004.

[33] Future of identity in the information society - http://www.fidis.net/.

[34] K. Cameron, R. Posch, and K. Rannenberg. Proposal for a common identity framework: A user-centric identity metasystem. *Identity in the information society: challenges and opportunities. Dordrecht: Springer*, pages 477–500, 2009.

[35] R. Clarke. Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, 7(4):6–37, 1994.

[36] S. Brands. A primer on user identification. In *The 15th Annual Conference on Computers, Freedom and Privacy, Keeping an Eye on the Panopticon: Workshop on Vanishing Anonymity, Seattle*, 2005.

[37] A. Pfitzmann and M. Hansen. Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology, 2005.

[38] K. Cameron. The laws of identity. *Microsoft Corp.*

[39] M. Bauer, M. Meints, and M. Hansen. FIDIS Deliverable D3. 1–Structured Overview on Prototypes and Concepts of Identity Management Systems. *Frankfurt aM*, 2005.

[40] A. Jøsang and S. Pope. User centric identity management. In *AusCERT Asia Pacific Information Technology Security Conference*, 2005.

[41] J. Camenisch and B. Pfitzmann. Federated identity management. *Security, Privacy, and Trust in Modern Data Management*, pages 213–238, 2007.

[42] D. Recordon and D. Reed. Openid 2.0: a platform for user-centric identity management. page 16, 2006.

[43] E. Hammer-Lahav and D. Recordon. The oauth 1.0 protocol. *Internet Engineering Task Force (IETF) RFC5849*, pages 2070–1721, 2010.

[44] T. Scavo and S. Cantor. Shibboleth architecture. *Internet2, Technical Overview June*, 2005.

[45] L.M. LoPucki. Human identification theory and the identity theft problem. *Texas Law Review*, 80:89–134, 2001.

[46] J.W. Moore. Identity Theft Issues for Financial Services Firms. *International Review of Business Research Papers*, 6(1):135–144, 2010.

[47] W.E. Burr, D.F. Dodson, and W.T. Polk. Electronic authentication guideline. *NIST Special Publication*, 800:63, 2004.

[48] H. Krawczyk, M. Bellare, and R. Canetti. RFC 2104: HMAC: Keyed-hashing for message authentication, February 1997.

[49] RS Sandhu and P. Samarati. Access control: principle and practice. *Communications Magazine, IEEE*, 32(9):40–48, 2002.

[50] A.F. Westin. *Privacy and freedom*, volume 97. London, 1967.

[51] Le parlement Europen et le conseil de l'union Europenne. Directive 95/46/ce du parlement europen et du conseil du 14 octobre 1995 relative la protection des personnes physiques l'gard du traitement des donnes caractre personnel et la libre circulation de ces donnes. *Journal officiel des communauts europennes*, 1995.

[52] D.J. Solove. Understanding privacy.

[53] D.J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3):477, 2006.

[54] M. Deng. *Privacy Preserving Content Protection*. PhD thesis, Katholieke Universiteit Leuven, 2010.

[55] L. Sweeney. k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY1. *World*, 10(5):557–570, 2002.

[56] V. Ciriani, S.D.C. di Vimercati, S. Foresti, and P. Samarati. k-Anonymity. *Secure Data Management in Decentralized Systems. Springer-Verlag*, 2007.

[57] M. Roe. Cryptography and evidence. *Doct. Dissert., Univ of Cambridge, UK*, 1997.

[58] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle. The platform for privacy preferences 1.0 (p3p1. 0) specification. *W3C recommendation*, 16, 2002.

[59] R. Wright, L. Camp, I. Goldberg, R. Rivest, and G. Wood. Privacy tradeoffs: myth or reality? In *Financial Cryptography*, pages 147–151. Springer, 2003.