Diffusion of Federated Identity Management

Detlef Hühnlein[1], Heiko Roßnagel[2], Jan Zibuschka[2]

[1] secunet Security Networks AG, Sudetenstraße 16, 96247 Michelau,
detlef.huehnlein@secunet.com

[2] Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO), Nobelstr. 12, 70569 Stuttgart
{heiko.rossnagel,jan.zibuschka}@iao.fraunhofer.de

Abstract: In this work, we discuss the diffusion of federated identity management. We base our research on Roger's diffusion of innovation theory, and derive generic factors influencing the diffusion of federated identity management solutions. To validate our model and investigate specific contributions of parameters in specific usage scenarios, we investigate market success of federated identity management systems. We examine several application scenarios in the fields of e-business, Web, and e-government.

1 Introduction

Identity management (IdM) has emerged as a promising technology to distribute identity information across security domains [MR08]. In e-business scenarios, federated identity management is used to connect enterprises along the value chain and enables them to reduce transaction costs significantly. On the web it offers the promise of single sign-on for different domains and service providers, offering a common authentication and authorisation infrastructure that eliminates the necessity of using passwords. This would on one hand provide improved ease of use for the users and at the same time eliminate problems that are caused by password management issues, password reuse [IWS04], and passwords' security flaws [Neu94]. Therefore, it could make a major contribution to improvement of security on the web. In the e-government domain, identity management systems (IMS) could help to introduce the necessary security infrastructure enabling online services that so far could not have been offered by public administration due to security constraints.

Several different solutions for federated identity management (FIM) have emerged over the last couple of years such as Microsofts Passport, Liberty Alliance, Security Assertion Markup Language (SAML), Cardspace and OpenID. The success of these systems in the marketplace has been very diverse. Some systems, such as Passport, have not been successful and have been replaced [CJ07]. Other systems have been highly successful in particular domains, such as SAML in e-business scenarios. In other domains, however, the same systems have not achieved this kind of success.

In this contribution we will examine the market success of FIM systems in different application domains. In particular we want to explore how economic principles affect this success. Since federated identity management is a complex technology that can be applied to several different domains, we distinguish three different usage scenarios and perform

a cross-case study. To do this we apply Roger's diffusion of innovation theory [Rog03], which is a proven economic theory for explaining the market success or failure of innovations, to each scenario and compare and discuss the results.

The rest of the paper is structured as follows. In section 2 we will provide an overview on FIM and diffusion theory in general. We will apply this diffusion theory to FIM and discuss the factors influencing the adoption in section 3. We then validate our arguments from section 3 by taking a close look at three different usage scenario case studies in section 4. Our results are discussed in section 5, concluding our findings.

2 Background and Related Work

2.1 Federated Identity Management

Among the important identity management processes is the authentication, identification and authorization of Users (U) who want to access some resource offered by some Service Provider (SP). For this purpose U is equipped with one or more Credentials, which are presented to the SP. While the SP in a classical IdM scenario must itself understand, verify and accept U's Credentials, those tasks may be delegated to a specialized Identity Provider (IdP) in a federated setup. Hence a FIM system may be viewed as a sequence of entities that transform a Source Credential of U into a Session Credential that is consumable by a SP who makes a decision on whether to grant access to a sensitive service.

Before U is able to use the service offered by the SP, the following steps are typically performed:

1. $UA \rightarrow SP$: The User Agent (UA) contacts the SP and requests some service.
2. $SP \rightarrow UA$: The SP answers the request, possibly including additional information about supported protocols, appropriate IdPs, necessary authentication assurance levels, requested attributes etc.
3. $UA \rightarrow IdP$: The UA connects to the IdP in order to authenticate with the Source Credential and request a Session Credential that can be presented to the SP.
4. IdP: The IdP authenticates U based on the Source Credential, uses an existing session in which authentication has already been performed previously or further delegates the authentication to another IdP.
5. $IdP \rightarrow UA$: If the authentication was successful, the IdP returns a Session Credential to the UA.
6. $UA \rightarrow SP$: The UA sends the Session Credential received from the IdP to the SP.
7. SP: The SP validates the Session Credential and verifies the access rights of the now authenticated U.

8. $SP \rightarrow UA$: The SP serves the requested resource to the UA.

Furthermore, there may be additional steps for identity selection (IS), in which U, UA, and/or the SP interact in order to select an appropriate electronic identity and hence IdP to be contacted in step 3. In addition, there typically is some sort of trust relationship (T) between the SP and the IdP, which allows to verify the integrity and authenticity of the Session Credential.

Federated authentication and SSO systems are around for quite a while [SNS88]. and the most important protocols in this area comprise the Security Assertion Markup Language (SAML) [CKPM05], the WS-* series of standards [NKMHB06] together with the Identity Metasystem Interoperability profile [JM09] and last but not least OpenID [Fou]. Please refer to [LOP04, MR08] for a more complete survey.

2.2 Diffusion Theory

In the information systems literature, a variety of theoretical perspectives have been advanced to provide an understanding of the determinants of usage. An important line of research has examined the adoption and usage of information technology from a diffusion of innovation perspective [Rog03]. This research examines a variety of factors, which have been shown to be determinants of IT adoption and usage, and has been applied to explain the adoption and diffusion of a great variety of innovations ranging from new methods of agriculture to modern communication technology. In his seminal work Rogers defines five attributes of innovations, as perceived by the members of the social system that determine the rate of adoption of an innovation [Rog03]:

Relative advantage is the degree to which an innovation is perceived as better than the idea it supersedes. It is not so important if the innovation has an objective advantage, but rather if the individual perceives the innovation as advantageous. Advantages can be measured in economic terms, but social prestige, convenience, and satisfaction also can play an important role.

Compatibility. is the degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters. An innovation that is consistent with the existing values will diffuse more rapidly than one that is incompatible with the norms and values of the social system.

Complexity is the degree to which an innovation is perceived as difficult to understand and use. Innovations that are easier to understand will be adopted more rapidly than those which require the adopter to develop new skills and understandings.

Triability is the degree to which an innovation may be experimented with on a limited basis. New ideas that can be tried before the potential adopter has to make a significant investment in the innovation are adopted more quickly.

Observability is the degree to which the results of an innovation are visible to others. The easier it is for individual to observe the results of an innovation, the more likely they are to adopt [Rog03].

An interactive innovation is an innovation that is of little use to an adopting individual unless other individuals with whom the adopter wants to communicate also adopt. Thus a critical mass of individuals has to adopt the innovation before it is of use for the average member of the system [MR99]. The individuals who have adopted an innovation form a network and with each new member the overall value of the network increases [MR99]. This fundamental value proposition is being called network effects, network externalities, and demand side economics of scale [SV99]. Until a critical mass occurs in the diffusion process the rate of adoption is relatively slow [MR99]. After the critical mass is achieved the rate of adoption accelerates and leads to a take off in the adoption curve.

The diffusion of security technologies has been discussed by various authors in the context of TOR [ADS03], electronic signatures [Roß06] and smartcards, as well as certificates for web sites [OS06].

Economic aspects of IdM systems have been addressed in the context of possible hindrances for the success of such systems [DD08], and network effects and compatibility have been identified as a decisive factor in the context of certificates and security technologies in general [OS06], however, to our knowledge, no broader discussion of this problem exists, especially covering not only one specific use case (i.e. the Web), but a broader range of identity management deployments.

3 Diffusion of Federated Identity Management

Relative advantage. In the context of identity management, relative advantage is the utility that an IMS can offer to its stakeholders, including both end users, SPs, enterprises, and other players, compared to the previous state of the art (e.g. passwords on the Web). Examples of how a IMS can offer utility include:

- **Reduced sign-on** is one of the main benefits provided by IMS. In the enterprise case, it lowers help desk costs, while on the web, it unburdens users of password management worries.
- **Privacy** is also often mentioned as one of the issues IMS can help address. Integration of anonymization and privacy-enhancing technologies into an IMS [HBC+01] offers value to privacy-sensitive users.
- **Reduction of user interaction** Form-filling reduces the time users have to spend while registering. e-government applications may enable users to carry out admin-

istrative tasks online, rather than at the local authority offices. In the context of Web services, this may also lead to a larger registered user base, as the effort necessary for registration is lowered.

- **Security:** IMS have the potential to alleviate common security risks of passwords [Neu94]. However, as SSO also adds a single point of failure, IMS also have higher security requirements than analogous decentralized password systems.
- **Identity Intermediation:** The outsourcing of user identity storage and part of the authentication process, offers cost reductions, compliance risk reduction, and increased identity quality to service providers [ZFR+07].

So, all in all, IMS can offer competitive advantage on several levels. However, an IMS may also decrease utility for several reasons.

- **Liability:** Depending on contract, an identity provider may be held liable for the identities it provides. A user employing a signature card rather than a password may find himself bound by contracts and held liable in a way that would not be possible with password-based authentication.
- **Costs** of certification, implementation and other IdM processes may eat up the advantage gained from the other factors.

It should be noted that network effects play a huge role in each scenario because FIM is by nature an interactive innovation. It is quite obvious that a system with a larger user base would be more appealing to service providers, while a system supported by a larger set of services would be of a higher utility to users, offering a meaningful reduction of sign-on processes.

(Social) Compatibility. In the context of IMS, compatibility refers mainly to privacy/trust questions. Trust is a key inhibitor of the broader success of e-business systems, which may be addressed using privacy-enhancing IMS [HBC+01]. However, trust-related previous work shows that technical measures providing trust through security are dominated by user interface issues: a user may distrust even a secure system because it is very complicated to use, it appeals less to him visually, or it produces errors during usage. Those influences have an impact that is at least as strong as technical security across all user groups [LT01]. Also, trust in the SP influences the trust in the system much stronger than the trustworthiness of the system influences trust towards the SP [MCK02]. With regard to compatibility with user expectations, passwords are still dominant. Especially in the web case, passwords will have to be offered simultaniously to reach compatibility with users' authentication expectations. Compatibility could also be an issue for service providers depending on the business model of the IdP.

Complexity. Usability also has a major influence on the perceived complexity of an innovation by users. Many systems require the users to learn a new authentication interaction

paradigm, causing new usability problems [MR08]. If the users have the impression that the system is difficult to use or to obtain, they are unlikely to adopt unless the perceived relative advantage significally outweighs these hindrances. On the other hand, IMS have the potential to offer a significant reduction of complexity to end users, with SSO relieving the users of password management problems, and form filling reducing the time spent while registering.

For SPs the perceived complexity of FIM is not a question of using this technology but rather a question on how easily such systems can be implemented on the server side. This includes potential sunk cost for installing the infrastructure and the operation of several different authentication systems. Even if SPs switch to FIM for user authentication they will still have to support password authentication, because otherwise they would exclude a huge amount of potential customers of using their services.

For enterprises that want to adopt an IMS, a major factor influencing the perceived complexity will be how easily the system can be adapted to and integrated in existing business processes. If major adjustments to existing processes have to be made, the complexity of adopting the innovation increases significally and the costs of adoption will also increase.

Triability is generally not an issue, as many IMS can be experimented with on a limited basis. However, there are also areas where triability is problematic. In the context of enterprise identity management, complete deployments cannot be easily evaluated, and assumptions about the cost savings have to be made. In national e-government IMS, such as eIDs, ex ante costs such as the price of card readers may inhibit users from trying out the system. On the SP side, it may not be trivial to integrate IMS. Even where modular encapsulated interoperable IMS modules for SPs exist, usability issues add another layer of cost and risk to lose users.

Observability. Signalling quality is a problem for FIM [BHTB05]. It's hard to understand and to see the differences in applied security solutions for users. This could lead to a lemons market, which was defined in [Ake70]. In this pioneering article the author argues that information asymmetry and uncertainty about the product quality will lead to a market failure, unless appropriate counteracting mechanisms are undertaken. In a market that contains good and bad (lemons) FIMs, imperfect information about service quality causes the user to average the quality and price of the service used. The information gap enables the opportunistic behaviour of the owner of a lemon to sell it at average price. As a result, the better quality service will not be used since the price it deserves can not be obtained. The consequence of such practice will lead to a continuous fall of both quality and value of services. On the other hand, the advantages of SSO are easily observed by users. The same applies for cost reductions in the helpdesk area reached through enterprise SSO systems. However, the lemon market problem applies, at the very least, to certification authorities acting as a stakeholder in IMS.

4 Case Studies

The specific factors influencing diffusion of IMS are dependent on the usage scenario. In the case of Relative Advantage/Usefulness, the main drivers seem to be help desk cost reduction in enterprise settings, SSO in Web scenarios, and security (as enabler for new services) in e-government. Therefore, different systems, which emphasise different characteristics have prevailed in different scenarios. This section investigates e-business, Web and e-government scenarios, and illustrates the effects described in a more general manner in the earlier sections.

4.1 Case 1: E-Business - Circle of Trust

Real world examples can be found in the automotive industry. For example there is a technical recommendation [ODE09] based on SAML v2.0 [CKPM05], which has been developed by an Odette[1] working group consisting of leading automotive enterprises[2] and technical supporters[3] and provides guidance for the implementation of federated SSO scenarios between companies in the automotive sector. In a similar fashion SAML has been proposed for cross-enterprise rights management in the automotive industry [iA09].

In these e-business scenarios federated identity management succeeds along the value-networks forming a circle of trust between the participating enterprises. It is mainly aligned to existing business and trust relationships between enterprises, which act as SP and IdP respectively, and U is typically an employee of either company. In these value-networks dominant stakeholders exist that can act as a champion for the technology influencing other stakeholders to adopt the same technology more rapidly [Rog03].

The dominating driving force for the adoption of federation techniques is the general wish to minimize transaction costs. In particular the SP will spare to issue Credentials to Users at business partners, if there is an IdP, which already did that, supports the same federation protocol as the SP and last but not least may be trusted to perform the authentication on behalf of the SP. Therefore, the perceived relative advantage mainly comprises of cost reduction (due to reduced sign on) and identity intermediation.

4.2 Case 2: Web Identity Management

Passwords have long been the predominant means for user authentication on the web. This is also true for other scenarios, however, in the Web scenario, even adopters of IMS mostly still support passwords. This may be because the lack of coordination in this scenario

[1] See `http://www.odette.org/`.

[2] Including BMW Group, Bosch GmbH, Daimler AG, Hella KGaA, Hueck & Co, Volvo Personbilar Sverige AB and ZF Friedrichshafen AG.

[3] Including Covisint Compuware GmbH, iC Consult GmbH, Microsoft AG, PingIdentity Corporation and Siemens AG.

makes a timed adoption across users unlikely, and gaining a user base is central to the business goals of many Web services. Consequently, the advantage offered by an IMS on the Web would have to outweigh lost users who do not use it. As this is unlikely, passwords will likely not be superseded completely.

Microsoft Passport [Mic] was one of the first deployed systems to translate the idea of SSO to the web. It was based on the architecture of centralized intra-organizational SSO systems geared towards managing user access to individual services within an enterprise. Passport was rolled out as part of the infamous HailStorm initiative, and was soon criticized for privacy and security shortcomings. Those problems were insecurities of the system design [KR00], and the centralized storage of identity information requiring trust in Microsoft. Although Passport had originally been adopted by several big players (such as eBay and monster.com), the infrastructure did not take off, and eventually the early adopter services left. The conventional wisdom from this case study is that insecurity and trust issues can make IMS fail, which was one of the motivators for the privacy-enhancing IdM movement [HBC+01]. However, Passport has recently made quite a comeback under the new name of Windows Live ID [Mic], mainly used for internal SSO across all Live services, and has become one of the top 5 most successful Web IMS (see Figure 1).

As a follow-up to Passport, Microsoft presented the CardSpace IMS [CJ07]. CardSpace is based on the concept of InfoCards, which allow the user to choose the identity to present to a service from a set of partial identities for different use cases. The CardSpace user interface presents a rolodex-like screen for selection of the appropriate InfoCard after the user has (typically) clicked on the log-in icon at a web site. While CardSpace is technologically superior to the original Passport [MR08], CardSpace has not fared any better than Passport during the adoption process, early adopters are already leaving again and the Windows Live ID service in the meantime supports OpenID[4].

OpenID [Fou] was originally developed for use in the LiveJournal online community as a lightweight, decentralized way to authenticate commenters [MR08]. It is a web-centric FIM protocol that uses user-supplied web addresses for identifying IdPs, and supports self-hosted IdPs. The user enters the URL of her IdP, and is then logged into a service via the IdP provided. While there have been several security problems with OpenID [MR08, SKS], OpenID has still seen quite a broad adoption, easily outperforming the original Windows Live ID and going head-to-head with Google ID, the SSO system used for Google services such as GMail (see Figure 1), which in the meantime also supports OpenID[5]. What set OpenID and Passport apart may well have been the ability to freely choose (or self-host) the IdP instead of being bound to Microsoft, a compatibility factor.

However, online community sites like Facebook and Twitter have recently implemented their own SSO solutions, specific to their platforms, and transmitting the user's social graph along with classical identity information. As Figure 1 shows, those systems have gained an even stronger traction than OpenID. As of such, the misfortune of Passport should probably be attributed to distrust in Microsoft, rather than generic compatibility/privacy issues.

[4] See `http://dev.live.com/blogs/devlive/archive/2008/10/27/421.aspx`.
[5] See `http://code.google.com/intl/de-DE/apis/accounts/docs/OpenID.html`.

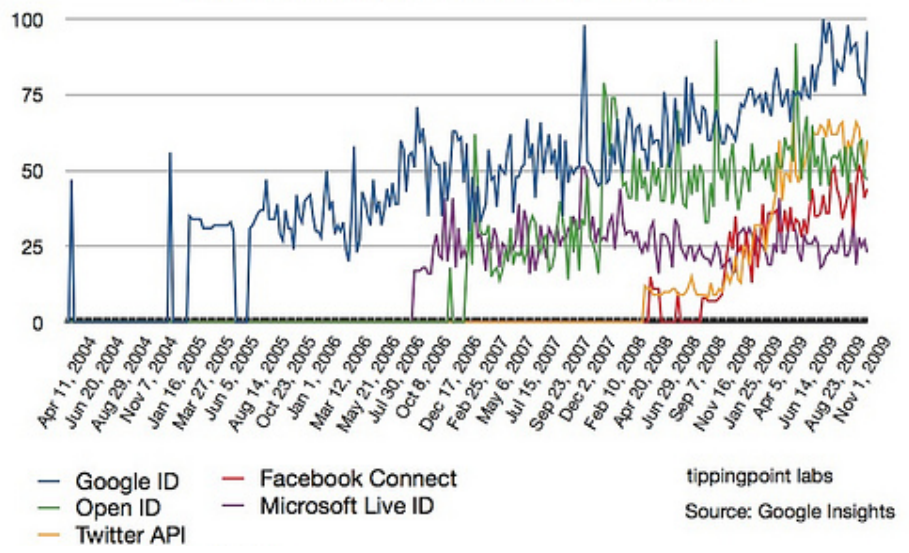

Figure 1: Diffusion of leading Web-scale IMS

The Web is an open scenario, with relatively little coordination and trust between entities (compared to the e-business and e-government scenarios). In this application field, lightweight IMS integrating directly with web user interface paradigms have dominated more elaborate systems offering more advanced security guarantees for several generations. Recent developments seem to demonstrate that systems making available the user's social graph to third parties have a considerably higher adoption rate. This supports the theory that in the Web case, compatibility issues are dominated by complexity issues (on the user side) along with the competitive advantage of user information that can be used e.g. for personalization. Additionally, the case of CardSpace may be taken to illustrate that making an IMS more secure cannot replace trust in the operator of the system, even if the system is privacy-friendly (fully client-side anonymous credentials) and open (e.g. with regards to third party certificates). Rather, those technological complexities seem to put extra burden on those systems.

4.3 Case 3: E-Government

There are several services in e-government scenarios that, if they are performed online by citizens, could lead to a major cost reduction within the public administration. So far many of these services can not be offered to a broad audience, because the technology to address the necessary security requirements has not been adopted by the general population. In the past electronic signatures have been proposed as a suitable solution to address the

demanding security requirements of e-government processes. However, they have not been successful on the market. An analysis of the reasons for their lack of market success can be found in [Roß06]. As is evident by the various real world projects listed in the following, FIM could provide a major contribution to close this gap:

Secure idenTity acrOss boRders linKed (STORK) is a project, which aims at establishing a European eID Interoperability Platform, which allows cross-border recognition of national eID tokens. For this purpose there will be Pan-European Proxy Services (PEPS) in the different EU member states, which are connected through a SAML-based interface as specified in [AMHAJ+09].

SuisseID uses hardware tokens and X.509-based certificates for authentication as core of a more comprehensive "Claim Assertion Infrastructure" based on SAML [CKPM05] and WS-Trust [NGG+07].

An eID-Server is necessary for accessing the identity attributes stored on the forthcoming German eID-card and provides a SAML-based interface [BSI10].

Secure Access to Federated e-Justice/e-Government (S.A.F.E.) aims at providing a scalable Federated Identity Management architecture for the German e-justice sector, which complements the existing OSCI-based infrastructures with components based on international standards.

The success of FIM systems in e-government scenarios will highly depend on the services that can be offered based on this technology and the perceived relative advantage these services can provide to the citizens. In use cases where security requirements and the perceived value are high, FIM solutions that are issued by the government could be very successful, as from a users perspective the relative advantage of FIM in e-government mainly comprises of form-filling and security. In comparison to solutions that are prevailant in the web scenario, infrastructures that are supported by the government do not face the problem of signaling their quality, as citizens tend to put more trust into those solutions.

There is hope that once adopted in an e-government scenario the same technology will spread to other use cases and in particular to the web use case. From a technological perspective this assumption is very sound, since secure solutions can also be applied to scenarios that do not require such an amount of security. However, from an economic perspective the success of these systems in other domains such as the web scenario is rather unlikely, because they have to compete with incumbent technologies, that already offer similar services. The main relative advantage of e-government solutions compared with other FIM systems will then be the higher degree of security. However, it is rather unlikely that this will be a driving factor for user adoption.

5 Conclusion

Federated identity management systems are a promising technology to achieve cross domain user authentication. Several different systems have emerged and have achieved a

mixed success in the marketplace. We examined the market uptake of FIM, by applying the diffusion of innovations theory to explain the success (and lack thereof) of various FIM-Systems in different usage scenarios. Our results show that in enterprise scenarios the diffusion of FIM follows established trust and business relationships along the value-network. In the web scenario we conclude that reducing complexity is by far more important than achieving a high degree of compatibility. The most promising e-government scenarios are those that provide a high value to users while at the same time demand high security standards.

References

[ADS03] Alessandro Acquisti, Roger Dingledine, and Paul Syverson. On the Economics of Anonymity. In *Financial Cryptography*, pages 84–102. 2003.

[Ake70] George A. Akerlof. The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84(3):488–500, August 1970.

[AMHAJ+09] J. Alcalde-Moraño, J. L. Hernández-Ardieta, A. Johnston, D. Martinez, and B. Zwattendorfer. Interface Specification. STORK Deliverable D5.8.1b, 08.09.2009, September 2009.

[BHTB05] James Backhouse, Carol Hsu, Jimmy C. Tseng, and John Baptista. A question of trust. *Commun. ACM*, 48(9):87–91, 2005.

[BSI10] BSI. eID-Server. Technical Directive (BSI-TR-031030), Version 1.1, 08.02.2010, 2010.

[CJ07] Kim Cameron and Michael B. Jones. Design Rationale behind the Identity Metasystem Architecture. In *ISSE/SECURE 2007 Securing Electronic Business Processes*, pages 117–129. 2007.

[CKPM05] Scott Cantor, John Kemp, Rob Philpott, and Eve Maler. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15.03.2005, 2005.

[DD08] Rachna Dhamija and Lisa Dusseault. The Seven Flaws of Identity Management: Usability and Security Challenges. *IEEE Security & Privacy Magazine*, 6(2):24–29, 2008.

[Fou] OpenID Foundation. OpenID Authentication 2.0. Final, December 5, 2007. `http://openid.net/specs/openid-authentication-2_0.html`.

[HBC+01] Marit Hansen, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, and Michael Waidner. Privacy-enhancing identity management. *Information Security Technical Report*, 9(1):35–44, 2001.

[iA09] ProSTEP iViP Assocation. Enterprise Rights Management. PSI-Recommendation 7, Version v0.9, Annex B, Cross-Enterprise-ID, 2009.

[IWS04] Blake Ives, Kenneth R. Walsh, and Helmut Schneider. The domino effect of password reuse. *Commun. ACM*, 47(4):75–78, 2004.

[JM09] Michael B. Jones and Michael McIntosh. Identity Metasystem Interoperability Version 1.0. OASIS Standard, July 2009.

[KR00] David P. Kormann and Aviel D. Rubin. Risks of the Passport single signon protocol. *Computer Networks*, 33(1-6):51–58, June 2000.

[LOP04] Javier Lopez, Rolf Oppliger, and Günther Pernul. Authentication and authorization infrastructures (AAIs): a comparative survey. *Computers & Security*, 23(7):578–590, October 2004.

[LT01] M.K.O. Lee and E. Turban. A trust model for consumer Internet shopping. *International Journal of Electronic Commerce*, 6(1):75–91, 2001.

[MCK02] D. Harrison McKnight, Vivek Choudhury, and Charles Kacmar. Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *INFORMATION SYSTEMS RESEARCH*, 13(3):334–359, September 2002.

[Mic] Microsoft. Windows Live ID/Passport Network. https://accountservices.passport.net/ppnetworkhome.srf?vv=700&lc=1031.

[MR99] Alwin Mahler and Everett M. Rogers. The diffusion of interactive communication innovations and the critical mass - The adoption of telecommunication services by German banks. *Telecommunications Policy*, (23):719–740, 1999.

[MR08] Eve Maler and Drummond Reed. The Venn of Identity: Options and Issues in Federated Identity Management. *IEEE Security & Privacy Magazine*, 6(2):16–23, 2008.

[Neu94] Peter G. Neumann. Risks of passwords. *Commun. ACM*, 37(4):126, 1994.

[NGG+07] Anthony Nadalin, Marc Goodner, Martin Gudgin, Abbie Barbir, and Hans Granqvist. WS-Trust 1.3. OASIS Standard, 19.03.2007, 2007.

[NKMHB06] Anthony Nadalin, Chris Kaler, Ronald Monzillo, and Phillip Hallam-Baker. Web Services Security: SOAP Message Security 1.1. OASIS Standard, 01.02.2006, 2006.

[ODE09] ODETTE. SESAM specification for building up federated Single-Sign-On (SSO) scenarios between companies in the automotive sector. ODETTE Recommendation, Draft of 15.07.2009, July 2009.

[OS06] A. Ozment and S. E Schechter. Bootstrapping the adoption of Internet security protocols. In *Fifth Workshop on the Economics of Information Security*, Cambridge, UK, 2006.

[Rog03] Everett M. Rogers. *Diffusion of Innovations*. Free Press, New York, 5 edition, 2003.

[Roß06] Heiko Roßnagel. On Diffusion and Confusion - Why Electronic Signatures Have Failed. In *Trust and Privacy in Digital Business*, pages 71–80. Springer, 2006.

[SKS] Pavol Sovis, Florian Kohlar, and Jörg Schwenk. Security Analysis of OpenID. in the present proceedings.

[SNS88] J.G. Steiner, B.C. Neuman, and J.I. Schiller. Kerberos: An Authentication Service for Open Network Systems. Usenix Conference Proceedings, 1988.

[SV99] Carl Shapiro and Hal R. Varian. *Information Rules - A Strategic Guide to the Network Economy*. Harvard Business School Press, Boston, 1999.

[ZFR+07] Jan Zibuschka, Lothar Fritsch, Mike Radmacher, Tobias Scherner, and Kai Rannenberg. Enabling Privacy of Real-Life LBS. In *New Approaches for Security, Privacy and Trust in Complex Environments*, pages 325–336. 2007.