Benefits of Federated Identity Management - A Survey from an Integrated Operations Viewpoint

Jostein Jensen

Norwegian University of Science and Technology, Department of Computer and Information Science, Norway
jostein.jensen@idi.ntnu.no

Abstract. Federated Identity Management is considered a promising approach to facilitate secure resource sharing between collaborating partners. A structured survey has been carried out in order to document the benefits of adopting such systems from a user and business perspective, and also to get an indication on how Integrated Operations in the oil and gas industry can benefit from identity federations. This has resulted in a set of benefit categories grouping existing claims from researchers. The literature indicates that adoption of Federated Identity Management in Integrated Operation seems like a good idea, however, there are several challenges that need to be solved.

1 Introduction

Federated Identity Management (FIdM) is a promising approach to facilitate secure resource sharing between collaborating partners in heterogeneous (IT) environments. Such resource sharing is the essence of the ideas of Integrated Operations in the oil and gas industry, as outlined in the next section (section 2). Federation technologies *"provide open, standardised and secure methods for a service provider to identify users who are authenticated by an identity provider"* [30]. Further, identity federations facilitate delegation of identity tasks across security domains [21].

There are different perspectives on Identity Management (IdM) [3], where the first is the traditional way of doing IdM, and the next two are alternatives for Federated Identity Management:

- **Isolated IdM** is the way IdM is commonly done today. Each company establishes, uses and maintains a local user repository where credentials are stored and used for authentication purposes to access company internal resources.
- **Centralised IdM** is one architectural model to realise Federated Identity Management. User data is registered in a central repository. User authentication is performed by this central entity, which issues identity assertion upon a successful authentication process. These assertion, or security tokens, can then be used to access distributed services across company borders.

A M. Tjoa et al. (Eds.): ARES 2011, LNCS 6908, pp. 1–12, 2011.
© IFIP International Federation for Information Processing 2011

– **Distributed IdM** is the opposite of the previous alternative. Each collaborating company or service provider keeps a local user repository. Authentication is performed locally, but the issued security token can be used to prove identity, and as such get access to, distributed services across company borders.

This illustrates the point that FIdM is about inter-organisation and interdependent management of identity information rather than identity solutions for internal use, and that it has emerged with the recognition that individuals frequently move between corporate boundaries [9]. The federation model enables users of one domain to securely access resources of another domain seamlessly, and without the need for redundant user login processes [5]. According to Balasubramaniam et al. [6] an Identity Management solution consists of the following functionality attributes: 1) Identity provisioning, 2) Authentication and authorisation, 3) Storage, management, 4) query/retrieve and indexing of identity information, 5) Certification of identity and credentials, 6) Single-sign-on/single-sign-off, 6) Audit capabilities.

Smith [30] has observed that the predictions of rapid acceleration in the industrial uptake of FIdM technology have not been fulfilled. This is despite the fact that the technological building blocks have been developed for years, and that the technology is relatively mature and well understood. This paper presents partial results of a research project to understand why FIdM processes and tools have not been widely adopted in industry, and what should be done to increase the adoption rate, and/or if there is an actual industrial need for it at all. A company's management need to be convinced of the benefits, challenges and cost of adopting a technology before they make the investment. So as a starting point, we wanted to identify what benefits of deploying FIdM have been reported in scientific literature. The following research questions were stated in this respect, and will be answered in this paper:

RQ1: What are the reported benefits of adopting Federated Identity Management from a user perspective?
RQ2: What are the reported benefits of adopting Federated Identity Management from a business perspective?
RQ3: How can an Integrated Operations scenario benefit from using Federated Identity Management?

The last question is related to the case for the ongoing research project, which is an Integrated Operation (IO) scenario in the Norwegian oil & gas sector. This scenario is presented in the following section. Section 3 presents how the research leading to the the presented results was carried out, while section 4 presents a list of benefit categories obtained by analysing the literature, as well as a discussion on how an IO scenario can benefit from FIdM. Section 5 discuss our results before the paper is concluded and directions for further work are given in section 6.

2 The Integrated Operations Scenario

In mid 1990, oil and gas companies operating on the Norwegian Continental Shelf (NCS) started developing and deploying mechanisms for simple remote operation of offshore installations. In 2002, the Norwegian Oil Industry Association (OLF) initiated a project group to look into this development, and consider the potential benefits and consequences of such initiatives. This resulted in a report [19] describing future scenarios and visions for oil and gas operations in the North Sea. Prior to the remote management initiatives, there had been a distinct separation between onshore and offshore installations. Now, OLF saw that there was an increasing amount of data being made available and shared real-time. With new processes and tools these data could be utilised in decision support processes that would change the way work was organised. They envisioned that the workload between offshore and onshore installations would be changed, and virtual teams would emerge. The operations would be more integrated, and thus the term Integrated Operations (IO) emerged.

The concept of Integrated Operations has been refined and widely deployed in the companies operating on the NCS. Land-based operation centers monitor and control large portions of the daily oil and gas production. However, the current focus has been on intra-organisational collaboration, meaning that systems (more or less) only allow interaction between humans and systems within a single company. One of the visions in the OLF report referred to was, on the other hand, also to enable inter-organisational collaboration where partners (see Figure 1 for an overview of IO participants) could share information and knowledge seamlessly across company borders.

In 2008 a new OLF report was released: Reference Architecture of IT systems for OLF's IO G2 [1]. This report sketched the reference architecture for a common service platform supporting inter-organisational collaboration. The enhanced collaborative capacity has been seen as the next generation of IO systems and as such is referred to as IO gen 2. A Service Oriented Architecture (SOA) has been proposed to facilitate this collaboration.

The OLF architecture report [1] lists various governing principles for the future IO architecture, including those shown in Table 1.

3 Method

A structured literature review approach inspired by Kitchenham [17] was used as research method leading to the results presented in this paper. The focus has been on performing the search phase with rigor. The aim of this systematic survey was to identify scientific literature that could provide answers to our research questions listed in the previous section.

3.1 Identification of Research

The starting point for the survey was a research protocol where the research questions and the search strategy were defined. A rigorous and comprehensive search was key to identify relevant scientific literature.

Table 1. Extract of principles governing the IO gen 2 architecture

Principle	Comment
Loose coupling between systems	Systems should be independent of changes in other systems
A service provider and a service consumer must be able to interact with each other	Reachability is an essential prerequisite for service interaction.
Conform to open standards	
Roles and corresponding responsibilities must be defined	Roles and responsibilities must be described to see who needs what in the patterns
Access should be role and asset based	Users need to be allocated a role for an asset (e.g. an oil field) so that it is possible to see what access is allowed against that asset for that person.
Authentication should be at the local company	Authenticated at his or her own company, for use anywhere.
Build on existing infrastructure	
A service should be reusable	Designed to be used by multiple customers, and also to be used in different contexts (within the scope if its intended use)

We used the following online databases for scientific literature to search for studies:

- IEEE Xplore[1]
- ACM Digital Library[2]
- Compendex[3]
- SpringerLink[4]

For each of these databases we used the following search phrase: *"federated identity management"*. The total amount of papers after this search was 684. Papers were then filtered based on title and abstract after the search, and duplicate publications were removed. All papers clearly not relevant for this study were taken out of the reading list. This process led to 113 remaining papers. The last selection of papers were read in the full, and text indicating benefits of using Federated Identity Management was extracted. This resulted in a total of 30 primary studies considered within the frame of this paper.

[1] `http://ieeexplore.ieee.org/Xplore/dynhome.jsp`
[2] `http://portal.acm.org/dl.cfm`
[3] `http://www.engineeringvillage2.org/`
[4] `http://www.springerlink.com`

4 Results

This section presents the results after analysing all citations reported as benefits of using FIdM. The reported benefits were first split in two categories: those reporting benefits from a user perspective, and those reporting benefits from a business perspective. A further analysis led to categories of benefits as summarised in Table 2.

Table 2. Benefit categories from a user and business perspective

User perspective	**Business perspective**
Increased privacy protection	Reduced cost
Better security	Improved data quality
Improved usability	Increased security
	Simplified/Improved user management
	Reduced complexity for service providers
	Facilitate cooperation

4.1 Benefits from a User Perspective

In this section benefits of using FIdM from a user perspective are reflected, and indicates answers to RQ1.

Increased Privacy Protection. Several researchers agree that the use of FIdM can increase the ability to protect personal privacy. Ahn et al. [3] [2] even say that *"The main motivation of FIM* [FIdM] *is to enhance user convenience and privacy "* , which is also supported by Gomi et al. [13]. Both Landau et al. [18] and Bertino et al. [8] claim that FIdM technology can facilitate users to control their personal data, and what is being sent to a service provider. Requirements related to minimal disclosure of information can be fulfilled. Squicciarini et al. [32] say that: *Federated identity management systems [...] enable organizations to provide services to qualified individuals; and empower them with control over the usage and sharing of their identity attributes within the federation.*

Better Security. FIdM may lead to improved security for users. According to Wolf et al. [33] users are released from remembering several credentials due to the single sign-on feature facilitated by FIdM systems. Madsen et al. [20] argue that the reduced number of authentication operations will make it practical for users to choose different and stronger passwords at their Identity Providers. This is also supported by Bhargav-Spantzel et al. [9]. Fewer and stronger authentication events will also help to minimise the risk of ID theft [8].

With the FIdM model, credentials do not need to be sent to/via Service Providers. It is sufficient to send asserted claims [20]. As such the credentials are better protected [18] [26].

Improved Usability. Users can benefit from increased simplicity with FIdM solutions [18] [26]. It is especially the Single-sign-on (SSO) feature that is emphasised in this respect, and Madsen et al. [20] highlight this feature as the archetypical example of a federated application. With SSO users can log in once and access different resources at different service providers [28] [22] [21] [16], without needing to remember multiple ways of authenticating at each site [18] and potentially by only remembering one password [14].

Seamless access to resources, and the elimination of redundant user login processes leads to improved user experience [4]. Satchell et al. [24] add that instead of having several identities at different service providers, FIdM allows all these to be gathered under one umbrella. This does *"not only provide users with vital cohesion but contributes to digital environments that are easily traversable spaces"*. Scudder and Jøsang [26] also state that identity federations release users from the burden of managing an increasing number of online identities.

From this we can deduce that users can experience improved usability since multiple services can be *accessed as a unified whole* [18].

4.2 Benefits from a Business Perspective

This section presents reported benefits of FIdM with respect to a business perspective, and as such indicates answers to RQ2.

Reduced Cost. Several statements from researchers indicate that introduction of FIdM can lead to reduced cost with respect to identity management for an organisation [22] [18] [11]. Madsen et al. [20] claim that the administrative costs of account maintenance for service providers can be reduced, and Ahn et al. [3] say that FIdM allows businesses to share the identity management cost with its partners. Bertino et al. [8] explain the cost saving a bit more: Costs and redundancy is reduced *because organisations do not have to acquire, store and maintain authorisation information about all their partners' users.* Also Kang and Khashnobish say that the redundancy problem in user administration may be solved with FIdM, while Smith [30] claims that multiple corporations in theory can share a single [FIdM] application, and that the consolidation can result in cost savings.

Improved Data Quality. Since identity data is essential to make correct access control decisions it is paramount that they are correct and up to date. FIdM can help improve the overall quality of this data. Bertino et al. [8] argue that identity information can be made available on demand and with low delay in a distributed environment in a FIdM scenario. They also claim that the user data will be more up-to-date and consistent compared to a scenario where user data is stored and maintained several places. Hoellrigl et al. [15] and Han et al. [14] present similar views. Both groups claim that the strength is that the administrative burden of user management is moved from the service provider

to the Identity Provider. As such, redundancy and information inconstancies in identity information can be avoided [15], and the exchange of user's identity information can be optimised.

Increased Security. There are several security aspects that are facilitated by FIdM solutions. Bertino et al. [8] claim that a federation prevents the problem of 'single point of failure'. However, this assumes that a distributed IdM model is followed. Speltens and Patterson [31] call it the 'true holy grail' of Federation, that applications become fully claims aware, and that access control decisions are based on claims. In such a situation the 'minimal disclosure' of information principle can be satisfied in that only required data needed to access a service have to be transmitted to a business partner [8]. Further, a claims based system can facilitate fine-grained authorisation [23]. Also Satchell et al. [24] highlight that FIdM facilitates the assignment of access rights and privileges, and Sharma et al. [27] add that it facilitates possibilities for detailed audit trails. Finally, Balasubramaniam et al. [6] give a general comment that FIdM will lead to minimisation of privacy and security violations.

Simplified/Improved User Management. Federated Identity management can simplify the complex process of managing user accounts [18]. User management tasks can be decentralised among identity and service providers [3] [2] [13], without being worried that the work of managing user identities and attributes is doubled [12]. There is a clear link between this point and *Improved Data Quality* and *Increased Security*. User account provisioning [4] is simplified, and with a holistic view of users' identity data, deprovisioning of user accounts is also better facilitated [33].

Reduced Complexity for Service Providers. By separating identity management tasks from the service providers, they can focus fully on delivering high quality services, while at the same time reducing the complexity [4] [5]. Identity management tasks can be outsourced to a separate IdP.

Facilitate cooperation. In the literature on FIdM there are several researchers arguing that federated solution will facilitate cooperation. Sharma et al. [27] say that FIdM technologies will allow companies to share applications without needing to adopt the same technologies for directory services and authentication. Similarly Brossard et al. [10] state that enterprises can offer services across domain boundaries to users and other services not controlled or defined internally. The technology offers an opportunity to create new business relationships and realise business goals at a lower cost [24]. The typical usecase is cross-domain single-sign-on [5], where a user's identity information can be used across multiple organisations [34] [25]. FIdM help share this information in a protected way based on contractual and operational agreements [8]. Sliman et al. [29] add to the above that final authorisation decisions can be kept at the end application or service, even though user data is stored and authentication is performed in a remote location.

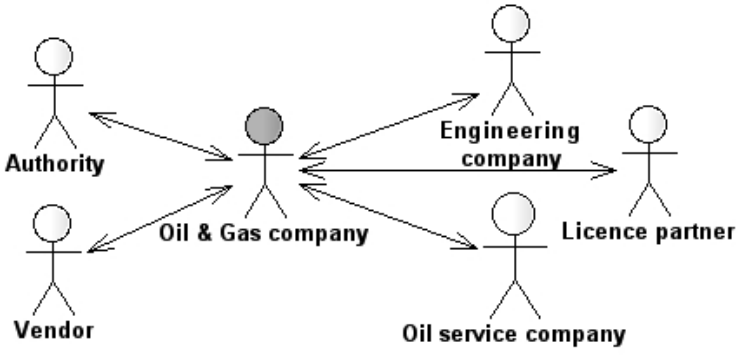

Fig. 1. Collaborating actors. Adapted from [1].

4.3 Benefits from an IO Perspective

As presented in section 2, Integrated Operation is all about inter-organisational resource sharing and collaboration, in a complex environment. In the following we give a brief view on how IO can benefit from adopting a FIdM model (RQ3).

Figure 1 shows part of the complexity associated with implementing IO; there are several actors involved. Examples of collaborative events include, vendors who may need remote access to the equipment they have delivered in order to read status reports and plan maintenance, and authorities who need access to drilling reports to monitor the production [1].

Today, isolated IdM models are realised by the IO actors. As such, e.g. the Oil and Gas company needs to provision a local user identity to the Vendor representative before he can remotely access equipment in the production environment. This raises several questions, such as: What are the procedures to keep user data up-to-date? What are the procedures when the vendor representative quits his job or changes position? What is the time delay before this is registered at the Oil and Gas company so that they can remove or update access rights?

The whole IO scenario seems as a good match for implementing the ideas of Federated Identity Management, especially considering the reported benefits from a business perspective. Independent of the chosen federation model (see section 1) user data will be registered once. This will *simplify the user management* process, which has the important effect that the *quality and correctness of user data* is always as good as they are collected at the primary source, and synchronisation issues are eliminated. This again is key to maintain a *high security level* in that access is given based on updated data. Instead of spending resources on managing external users, the IO actors can focus on maintaining dynamic access policy sets, and improve the granularity of access constraints based on identity attributes/claims.

With the large number of IO actors it is an unrealistic scenario that all of them will invest in identical infrastructure related to Identity Management. However, selecting a FIdM model using standardised protocols and interfaces will *facilitate cooperation* and make system integration less difficult.

Most communication will go through the Oil and Gas Company, meaning that they will experience most of the overhead related to the current Isolated IdM model. *Cost savings* may thus be considerable for these companies, while the economic incentive to move to a FIdM model might not be as large for the other actors.

In addition to this, FIdM may also facilitate the realisation of the architectural principles for IO as outlined in Table 1 . Systems and services can be loosely coupled, and identity and authentication services will be decoupled from functionality services. FIdM facilitates communication and interaction between service providers and service consumers in that identity data is sent in a standardised way designed for distributed systems. Access may be role based, but can also be made at more granular levels based on claims. Next, the distributed FIdM model is designed for keeping identity data at the local company, and performing local authentication of users.

5 Discussion

A lightweight version of Kitchenham's guide to structured surveys has been used to obtain the results presented in this paper. We have been less strict in the paper selection phase (as there have only been one researcher involved) and data synthesis phase (papers were read, raw data collected and grouped once, without iteration) than what is recommended to pass the strict requirements of the guide. Further, the search phrase we used may prevent us from identifying an exhaustive literature list on the topic; there might e.g. be papers talking about identity federations without mentioning our exact search phrase. Yet, we argue that the process is sufficient to answer the stated research questions, as it allows to get a representative view on existing research on the topic.

Next, it is important to be aware of the fact that the benefit categories listed in this paper are a result of analysing claims from researchers in the field. These claims must to a large extent be considered as expert opinions, which are not necessarily backed up by existing research. E.g. several researchers mention cost savings as a possible benefit of FIdM, however, none of the cited papers report from case studies where real cost savings are presetend.

This being said, FIdM seems like a promising approach to support inter-organisational collaboration, and there seems to be a good match between the reported benefits and the architectural principles for IO in the Oil and Gas sector. However, there are considerable challenges still to be solved, and which might hinder adoption. Trust among the participants in a Federation is one [26]. Baldwin et al. [7] point to the fact that stakeholders might have different assumptions and risk appetite, and as such different requirements with respect to the level of assurance associated with identity claims. These trust challenges are related to people, processes and technology. According to Scudder and Jøsang [26] the degree of needed trust does not foster large-scale federations. Smith [30] raises the issue of liability. What will happen if one of the federation partners fails to follow a proper process for identification of their employees? Another aspect of implementing FIdM is the consequences of single-sign-on functionality

if a digital identity is stolen, or a password compromised [21]. In such cases not only internal resources are compromised, but also potentially those of the federation partners. There are also technological challenges. Wolf et al. [33] point to complexity with respect to standardisation of FIdM protocols and data formats among the collaborators, and that this is essential to reach the goal. These challenges indicate that RQ3 can not be answered by looking at the reported benefits alone. A deeper analysis to answer this question, and a cost benefit analysis, should be done after all challenges are considered, and a risk assessment has been carried out.

6 Conclusion and Further Work

In this paper we report benefits of adopting Federated Identity Management systems from a user and business perspective, and a high-level view on perspectives of adopting FIdM in an Integrated Operations environment. Our conclusion is that there is a good match between the benefits of adopting FIdM and the architectural principles suggested for IO. However, we have also mentioned considerable challenges of adopting FIdM, and more research is needed to facilitate adoption in an industrial setting.

As part of a larger ongoing work on FIdM to facilitate IO, similar work as presented in this paper will be carried out with respect to documentation of reported challenges in the near future. The combined results will be used as input to a large case study including the stakeholders on different levels (management, IT operations, system users), from the various actors shown in Figure 1. This case study will result in empirical evidence as to what the enablers for FIdM adoption are, and whether it is realistic in an IO setting or not.

Acknowledgment. This work is supported by grant 183235/S10 from the Norwegian Research Council, and the GoICT project.

References

1. Reference architecture of it systems for olfs io g2. Tech. Rep. OLF report, OLF (2008)
2. Ahn, G.J., Lam, J.: Managing privacy preferences for federated identity management (2005)
3. Ahn, G.J., Shin, D., Hong, S.P.: Information assurance in federated identity management: Experimentations and issues. In: Zhou, X., Su, S., Papazoglou, M.P., Orlowska, M.E., Jeffery, K. (eds.) WISE 2004. LNCS, vol. 3306, pp. 78–89. Springer, Heidelberg (2004)
4. Almenarez, F., Arias, P., Marin, A., Diaz, D.: Towards dynamic trust establishment for identity federation (2009)
5. Arias Cabarcos, P., Almenarez Mendoza, F., Marin-Lopez, A., Diaz-Sanchez, D.: Enabling saml for dynamic identity federation management. In: Wozniak, J., Konorski, J., Katulski, R., Pach, A. (eds.) Wireless and Mobile Networking. IFIP Advances in Information and Communication Technology, vol. 308, pp. 173–184. Springer, Boston (2009)

6. Balasubramaniam, S., Lewis, G.A., Morris, E., Simanta, S., Smith, D.B.: Identity management and its impact on federation in a system-of-systems context. In: 2009 3rd Annual IEEE Systems Conference, pp. 179–182 (2009)
7. Baldwin, A., Mont, M.C., Beres, Y., Shiu, S.: Assurance for federated identity management. J. Comput. Secur. 18(4), 541–572 (2010)
8. Bertino, E., Martino, L., Paci, F., Squicciarini, A., Martino, L.D., Squicciarini, A.C.: Standards for web services security. In: Security for Web Services and Service-Oriented Architectures, pp. 45–77. Springer, Heidelberg (2010)
9. Bhargav-Spantzel, A., Squicciarini, A.C., Bertino, E.: Establishing and protecting digital identity in federation systems (2005)
10. Brossard, D., Dimitrakos, T., Gaeta, A.: Aspects of general security & trust. In: Dimitrakos, T., Martrat, J., Wesner, S. (eds.) Service Oriented Infrastructures and Cloud Service Platforms for the Enterprise, pp. 75–102. Springer, Heidelberg (2010)
11. Chadwick, D.: Federated identity management. In: Aldini, A., Barthe, G., Gorrieri, R. (eds.) Foundations of Security Analysis and Design V. LNCS, vol. 5705, pp. 96–120. Springer, Heidelberg (2009)
12. Elberawi, A.S., Abdel-Hamid, A., El-Sonni, M.T.: Privacy-preserving identity federation middleware for web services (pifm-ws). In: 2010 International Conference on Computer Engineering and Systems (ICCES), pp. 213–220 (2010)
13. Gomi, H., Hatakeyama, M., Hosono, S., Fujita, S.: A delegation framework for federated identity management (2005)
14. Han, J., Mu, Y., Susilo, W., Yan, J.: A generic construction of dynamic single sign-on with strong security. In: Jajodia, S., Zhou, J. (eds.) Security and Privacy in Communication Networks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, vol. 50, pp. 181–198. Springer, Heidelberg (2010)
15. Hoellrigl, T., Dinger, J., Hartenstein, H.: A consistency model for identity information in distributed systems. In: 2010 IEEE 34th Annual Computer Software and Applications Conference (COMPSAC), pp. 252–261 (2010)
16. Kang, M., Khashnobish, A.: A peer-to-peer federated authentication system. In: Sixth International Conference on Information Technology: New Generations, ITNG 2009, pp. 382–387 (2009)
17. Kitchenham, B.: Procedures for performing systematic reviews. Tech. Rep. TR/SE-0401, Keele University (2004)
18. Landau, S., Le Van Gong, H., Wilton, R.: Achieving privacy in a federated identity management system. In: Dingledine, R., Golle, P. (eds.) FC 2009. LNCS, vol. 5628, pp. 51–70. Springer, Heidelberg (2009)
19. Lilleng, T., et al.: Edrift på norsk sokkel - det tredje effektiviseringsspranget. Tech. Rep. OLF report, OLF (2003)
20. Madsen, P., Koga, Y., Takahashi, K.: Federated identity management for protecting users from id theft (2005)
21. Maler, E., Reed, D.: The venn of identity: Options and issues in federated identity management. IEEE Security & Privacy 6(2), 16–23 (2008)
22. Ranga, G., Flowerday, S.: Identity and access management for the distribution of social grants in south africa (2007)
23. Rieger, S.: User-centric identity management in heterogeneous federations. In: Fourth International Conference on Internet and Web Applications and Services, ICIW 2009, pp. 527–532 (2009)
24. Satchell, C., Shanks, G., Howard, S., Murphy, J.: Beyond security: implications for the future of federated digital identity management systems (2006)

25. Schell, F., Dinger, J., Hartenstein, H.: Performance evaluation of identity and access management systems in federated environments. In: Mueller, P., Cao, J.N., Wang, C.L. (eds.) Scalable Information Systems. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, vol. 18, pp. 90–107. Springer, Heidelberg (2009)
26. Scudder, J., Jøsang, A.: Personal federation control with the identity dashboard. In: de Leeuw, E., Fischer-Hübner, S., Fritsch, L. (eds.) Policies and Research in Identity Management. IFIP Advances in Information and Communication Technology, vol. 343, pp. 85–99. Springer, Heidelberg (2010)
27. Sharma, A.K., Lamba, C.S.: Survey on federated identity management systems. In: Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D. (eds.) Recent Trends in Networks and Communications. CCIS, vol. 90, pp. 509–517. Springer, Heidelberg (2010)
28. Shim, S.S.Y., Geetanjali, B., Vishnu, P.: Federated identity management. Computer 38(12), 120–122 (2005)
29. Sliman, L., Badr, Y., Biennier, F., Salatge, N., Nakao, Z.: Single sign-on integration in a distributed enterprise service bus. In: International Conference on Network and Service Security, N2S 2009, pp. 1–5 (2009)
30. Smith, D.: The challenge of federated identity management. Network Security (4), 7–9 (2008)
31. Speltens, M., Patterson, P.: Federated id management - tackling risk and credentialing users. In: ISSE/SECURE 2007 Securing Electronic Business Processes, pp. 130–135. Vieweg (2007)
32. Squicciarini, A.C., Czeskis, A., Bhargav-Spantzel, A.: Privacy policies compliance across digital identity management systems (2008)
33. Wolf, M., Thomas, I., Menzel, M., Meinel, C.: A message meta model for federated authentication in service-oriented architectures. In: 2009 IEEE International Conference on Service-Oriented Computing and Applications (SOCA), pp. 1–8 (2009)
34. Zuo, Y., Luo, X., Zeng, F.: Towards a dynamic federation framework based on saml and automated trust negotiation. In: Wang, F.L., Gong, Z., Luo, X., Lei, J. (eds.) Web Information Systems and Mining. LNCS, vol. 6318, pp. 254–262. Springer, Heidelberg (2010)