Published as: "Federated Identity Management - We Built It; Why Won't They Come?," in Security & Privacy, IEEE , vol.11, no.2, pp.34-41, March-April 2013, doi: 10.1109/MSP.2012.135, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6336740&isnumber=6493314

Federated Identity Management in Industry – We Built It; Why Won't They Come?

Jostein Jensen[1,2], Martin Gilje Jaatun[2]
[1]Norwegian University of Science and Technology, Department of Computer and Information Science
[2]SINTEF, Department of Software Engineering, Safety and Security
Norway
Jostein.jensen@idi.ntnu.no, martin.g.jaatun@sintef.no

Abstract:

Solutions for Federated Identity Management (FIM) are becoming mature. However, the adoption rate of this technology has not been as expected. Eleven semi-structured interviews with representatives from the Norwegian oil- and gas industry have been analysed to learn more about the perceived benefits and challenges of FIM adoption. Our results show that some of the benefits of FIM adoption are offset by its challenges, which contributes to slowing down the adoption process. Still, we see that the industry is experimenting with the technology in small scale, and our belief is that FIM will be adopted by the industry in some form or another in the future.

Keywords

Federated identity management, case study, security, identity management, single sign on, interviews, industry, FIM, empirical

1 Introduction

Many companies have taken advantage of single-sign-on (SSO) technologies. After a successful login, the authentication service sends the computer a security token, which is subsequently forwarded as proof of authentication every time a protected service is accessed. Examples of services linked to the SSO feature include access to network drives, e-mail services, the corporate intranet, project portals, the company travel agency service, and secured wireless networks. Only a few years ago it would have been unthinkable for all these systems to be linked to a common access control solution.

In the last decade, the SSO model has been extended from intra-organisational use to also allow collaboration on identity management across organizational boundaries, and across security domains - this is known as Federated Identity Management (FIM). The idea is that you authenticate towards your local organization, obtain a security token, and use this token to access resources in other organizations.

Academia has been quite optimistic about FIM technology [1], and Table 1 shows the expected benefits.

Table 1. Benefits of FIM from a user and business perspective

User perspective	Business perspective
Increased privacy protection	Reduced administrative cost
Better security	Improved data quality
Improved usability and efficiency	Increased security
	Simplified/improved user management
	Reduced complexity for service providers
	Secure cross-domain single-sign-on

By looking at these keywords on positive effects of FIM alone, one should think that the industry would run to the store and buy FIM products. However, this is not the case, as it turns out that the FIM adoption rate has been slower than expected [2] [3].

Surveys of academic literature on FIM [1][4] show there are great efforts to move the FIM technology towards academic perfection, but also that there are considerable challenges that are still to be overcome. Industrial experience reports related to FIM adoption, however, are rare. This leaves unanswered questions, such as: What are the industrial expectations regarding FIM? How can the industry benefit from the technology, and which challenges will they face during adoption? Consequently, we decided to carry out semi-structured interviews with all in all eleven persons selected based on the recommendation of our industry contacts, to get an insight into these questions. The interviews were carried out one-on-one, either in person or via telephone, according to a prepared interview guide, but additional follow-up questions were asked to elaborate interesting points. The 11 interviewees represented all the interesting stakeholders in this domain, and since these were in-depth interviews (minimum 45 minutes), this was deemed sufficient to gain a deep insight into the case.

We selected an industry where efficient collaboration is a key to success, namely the Norwegian oil- and gas industry, with its initiatives for Integrated Operations (IO) and digital oil fields. This is a highly technology-driven industry where information and communication technology has an integral role. Our goal is to get a better understanding of the factors having an influence on FIM adoption in complex industrial cases.

Our analysis of the interview data show that there are conflicting interests and views related to adoption of FIM. In some areas our interviewees recognise that FIM adoption will have beneficial effects, but also that these are offset by new challenges, and that FIM is not a silver bullet.

2 Integrated Operations for Oil & Gas production on the Norwegian Continental Shelf

In the past 15 years or so, oil and gas companies operating on the Norwegian Continental Shelf (NCS) have developed and deployed mechanisms for remote operation of offshore installations. In the Integrated Operations (IO) concept, production facilities are heavily equipped with sensors, and land-based control centres monitor and control a large part of the daily production. Today, however, most process control systems used in the IO scenario are designed for intra-organisational use, and many of them are proprietary silo systems. One of the visions of the Norwegian Oil Industry Association (OLF) is to enable inter-organisational collaboration where partners will share information and knowledge seamlessly across company borders.

The number of industrial actors on the NCS is high; there are equipment vendors, food suppliers, service companies, engineering companies, oil and gas companies and more. All of these are important for keeping operations running, and they need good IT platforms to collaborate efficiently. At the same time, there is strict competition among them. Compromised information can cause millions of dollars in lost revenue in form of lost contracts, reduced oil and gas production or fluctuations in stock price. In this context **secure** information sharing is essential.

We will refer to the oil & gas company as the *operator,* and to all other actors in the IO domain as *contractors* in the remainder of this paper.

Table 2. Actors in the IO domain – high level

Actor	Description
Operator	Owns a production licence and is responsible for the production on an oil field
Contractor	Includes equipment vendors, engineering companies, service companies and licence partners. These companies support the operators in the daily oil & gas production, and are responsible for delivery of equipment and services that make the production possible.

Three of our eleven interviews were held with representatives from an operator, the remaining eight with representatives from four different contractor companies.

3 Perceived benefits

In his theory on diffusion of innovation, Rogers [5] claims that the consideration of how much a new innovation improves over what already exists is essential for the decision to adopt it. It is therefore interesting to understand how the industry perceives the benefits of adopting FIM in their working environment. The following subsections present our interview candidates' perceived benefits of FIM, and also include related challenges that are unsolved today. This allows us to get an insight into the relative advantage of adopting FIM.

3.1 The effectiveness of user administration and improved data quality

When asked about current challenges regarding identity management, an operator employee replied: *"keeping track of our employees' access rights to various systems. What happens when they change jobs? […] In our company people on average have the same position for about two, two and a half years […]. The average year includes two - three thousand internal job changes."* Further, he explained that the oil industry at large experiences around 40.000 job changes a year, and with an estimated average of two hours administration per change, the industry spends about 80.000 hours a year on administrative overhead related to identity management. The same interviewee said that they have more than 10.000 external users enrolled in their IT-systems, and a contractor mentioned an IT-solution they operate with more then 500 users from one of the operators.

A representative from one of the contractors exemplified the problem of not having updated access lists: An employee had left a contractor in favour of an operator. A part of his job was to serve a number of oil companies, and thus he also had different user accounts on their systems. While his access rights to the contractor's systems were revoked immediately, there were delays in the revocation process towards the operators, which could have given him unauthorised access based on old, but still valid access credentials.

In this situation it is easy to see why more than half of the interviewees mention that they believe that the adoption of FIM will rationalize the user administration process, and improve the quality of recorded identity attributes. One interviewee commented: *"you could rationalize the user account systems at different companies if you have a cooperation among them."*„ and another supplemented: *"It is obvious that there will be less user administration if we could integrate our login systems".* In section 4.1, however, we will see that even if some of the current user administration challenges can be solved with FIM, others will be introduced and that some of the harder access control problems will continue to exist.

3.2 User experience and usability

A contractor often has a business relationship with several operators and other contractors, and the number of systems they need access to can grow large. Many expert systems offshore are currently not integrated with other production or access control systems. A contractor mentioned that there might be situations where a worker onshore is responsible for controlling several offshore facilities and needs to visit 15 to 20 different systems a day. Another interviewee told us that visiting up to five systems with separate logins may be necessary to produce production reports.

Seven of the interviewees mentioned improved usability as a consequence of single-sign-on as a perceived benefit of FIM. Especially the contractors see the advantage of being able to experience fewer login requests in order to do their job.

3.3 Efficient collaboration

Representatives from both operators and contractors talked about improved efficiency of collaboration as a possible benefit of FIM adoption. One of the representatives from the operator drew the parallel between standardization of equipment and standardization of identity and access management within the oil and gas industry: *"The efficiency will increase and thus our cost is reduced, if* [everyone] *meet the same* [access control] *systems when they go from one operator to another*." Another of the operator representatives focused on the number of services they outsource to exemplify possible benefits of FIM. *" In five years* [we may] *end up having a thousand different service providers that we need to exchange identities with."*

The contractors in the study were mostly interested in easy access to data in order to work more efficiently and conveniently. Some of the contractors told us about incidents where they had forgotten their infrequently used password to services delivered by collaborators. A short-term solution was to borrow access credentials from co-workers, since the situation can cause serious delays. Downtime of production facilities can cause millions of dollars an hour in lost revenue, so there is a strong focus on keeping the production up and running. The easy way out is therefore sometimes selected, even if it is in conflict with existing security policies and has implications for the overall security.

3.4 Reduced cost

Efficient user administration and efficient collaboration are factors directly linked to a desire to reduce cost. Both the operator side and the contractor side can gain from rationalized user administration. The operator has an expectation that FIM can reduce cost due to more efficient work processes. In section 4.4, however, we will see that while the interviewees see cost reduction in some areas as a benefit of FIM adoption, cost will increase in others.

3.5 Audit

Some of today's systems operate with service accounts, which are shared by several engineers. While this simplifies everyday work tasks, it makes detection and audits of potential misuse difficult. A benefit mentioned by one of the interviewees is that FIM is perceived to facilitate audit in the systems since every user has a personal user account, and that it will be beneficial to be able to trace who does what.

3.6 Better protection

A representative from one of the contractors gave a good illustration of the current identity situation. During the interview he accessed his software-based password manager: "I have 184 user accounts to systems at different clients". This was the number of accounts he had to manage in order to do his job. A number of the other interviewees told us about the same situation; the number of usernames/passwords that need to be remembered is so large that they are written down in books. Previous studies [6] indicate that this often leads people to use the same password for several services, although generally only for services with the same perceived security level.

With adoption of FIM the interviewees expect fewer user accounts and passwords to relate to, which led one of them to express that "*the perceived security will increase. Fewer passwords will be written down on paper.*"

The interviewees believe that the quality of user attributes, which is used to make authorisation decisions, will increase and that the access revocation process will be more efficient. This is highly relevant to ensure good protection of company resources.

Adoption of FIM will not solve all security challenges related to identity management. Section 4.7 illustrates that there is a conflict in our interview candidates' views on whether or not FIM will lead to better protection of company resources.

4 Perceived challenges

Rogers' diffusion of innovation theory also operates with the factors compatibility and complexity to describe whether innovations will be adopted or not. Will the new technology be compatible with existing technology and support existing business processes? How difficult or complicated will it be to use the new technology? By looking into which challenges the different actors in the industry can foresee with implementation of FIM we can also gain an understanding of what can possibly hinder or delay adoption.

4.1 Identity and access management

A major challenge related to identity management in general is to keep user databases and users' access rights up to date. One of the foreseen benefits of FIM is that it will be easier to keep the identity data up-to-date. However, more than

half of the interviewees still think there will be challenges, despite identity federations. *"I'm not so sure if we will experience less administration with such a system. I guess we […] will get fewer users to administer, but I'm not sure about this simplification."* He continues to argue that there will still need to be processes to trust each specific user before they can be authorised to access systems, and that it will be necessary to implement processes to verify the quality of federation partners' identity management processes.

The interviewees emphasized the need to fully control the authorization part of the access control. The authentication service can be outsourced to a trusted third party or users can be authenticated within their home organization, but there is still a need to have strict control on which, or what type of users have access to the organisation's resources. However, here there is a risk of confusing identity management with authorisation, since this authorisation process is already being performed today, only with the added chore of local identity management in each case.

4.2 Trust in collaborators

Smith [3] argues that trust is the fundamental concept underlying federations. At the same time he points to the fact that there are challenges related to establishment of trust. Trust issues are highly relevant for the inter-organisational collaboration, which is taking place in the IO domain. One of the representatives we talked with said: *"We […] collaborate with a license partner in one oil field. […] At the same time we are strong competitors, so it is essential that only information concerning the collaboration is available to them."* Whether you trust other companies or not is very context-dependent, and the level of trust is difficult to define. One interviewee pointed to one of the reasons: *"I think people are slightly more sceptical of the neighbouring business considering the big money that swirl around in the oil and gas industry.*"

"The contractors will never be able to handle the processes behind federation." This statement by one of the representatives from the operator is illustrative to the question of whether the collaborators find each other trustworthy enough to perform all identity management within each company. At the same time he said that it would be easier to trust some of their large contractors with which they have well-established cooperative frameworks. A body similar to the credit rating bureaus could be established within the oil and gas industry. This would be useful to do a professional audit of key characteristics of collaborators' identity management practices, and which could affect the trust relationships, he said.

During the conversation about trust issues, some of the interviewees mentioned the option to have a trusted third party to host the authentication service. One of the contractors said: *"I have some trouble imagining that access to external resources can be given if* [the identity management process] *is to be handled within each company. I feel that it has to be organised by a common entity."*

4.3 Standardisation, interoperability and technology management

The complexity of IT systems in the IO domain is high, and span regular office tools to small tailored expert systems on the software side. At the network layer they operate both with traditional IP-networks and specialized process control systems. One of the interviewed security professionals stated: *"It would be a dream come true if everyone could connect to a common platform - an information bus - where all information could be shared securely [...] but it is hard to believe that it will be possible.*" Further, he explained that identity federations might be possible in the future for some of their large partners and for some of their large systems. It can, however, be more difficult for smaller systems originating from small companies, who might not have the competency or economic baseline to integrate their systems with other federated systems according to standardization and interoperability needs.

Representatives from the operator told us they have tried open source federation technologies in a few cases. However, they experienced some technological challenges, especially related to the technology management. *"It is much easier to rely on technology from Microsoft, for instance, rather than a product from a party that is not as big commercially*". With this he implied that the large software companies would have to come up with solutions that fulfil the industry's needs before they will consider the technology in a larger scale. A second interviewee stated: *"The challenge with federated identities, as I understand it, is that there is no dominating standard. [...] You need a bouquet of different technologies."*

A software developer with primary focus on data integration complained: *"We are in the year 2012, but we are still struggling with some basic needs. [...] Even video conferencing can be complicated.*" His argument was that despite the rapid development of technology that can have high benefit internally in a company, such as video conferencing, there are still considerable challenges as soon as you get outside company borders where you meet equipment from different vendors, different security policies, firewall setting and so on. He continued to argue that even if software and hardware interfaces were compatible, there are still challenges with the interpretation of data originating from different systems, especially regarding semantics. These considerations are very valid when looking at integration of identity management systems. Both software and hardware interfaces must be standardized. Protocol options must be defined so that all the equipment is interoperable and the semantic meaning of identity attributes must be defined and agreed upon. Several of the interviewees mention that the industry must agree on common guidelines for FIM at a detailed level for it to be successful.

4.4 Investment cost

During the interviews we asked the candidates if they saw any potential showstoppers for adoption of a common FIM platform in the Norwegian IO context. *"Who's gonna pay for the fun?"* was the immediate response of a consultant in our study. He then elaborated: *"It is obvious that all the participants in such collaboration will have to make major changes to get this up and running.*

That is a cost I'm not sure they are willing to take." Representatives from three of the four contractors in our study confirmed this view. "*We have to consider that we are delivering services* [to oil companies] *globally. It will be costly for us to implement a system for collaboration only with our Norwegian partners*", one of the interviewees said. The two other representatives were concerned about the funding for implementation of federation technology. "*We don't develop anything that is not paid for by someone."* Even though the representatives from the operator did not mention funding as a factor, they all recognized that the investment cost of a FIM solution will be considerable.

4.5 Privacy

Privacy aspects related to FIM is currently a hot research topic. However, only one of the interviewees mentioned privacy as a concern. "*It would be fantastic to just have one digital identity to relate to, which you could use for everything. The drawback, however, is that you can trace what people are doing. [...] It might not be that important in this context, but often it is ok to know that you act anonymously so that you don't have to account for everything you do.*" This can be seen as an indication that privacy concerns are real, but not considered of primary concern in a professional context.

4.6 Organisational maturity

"What holds [FIM] *back is the same challenge we experienced when we first introduced the Integrated Operations concept. People are satisfied with the way they work today, and do not want change."* Another interviewee was asked whether there had been discussions concerning integration of user databases: "*That question has never been raised. Most oil companies have clear rules preventing it*". At the same time a third interviewee from one of the contractors commented that there is a constant change in attitude when it comes to taking advantage of new communication technology to facilitate sharing of data. "*Ten years ago, when some of our customers started* [with IO], *it was nearly impossible to get inside their premises with a computer. Now we get access to networks, get IP addresses, and so on.*"

4.7 Security challenges

"Our biggest fear is that someone unauthorized can get access to, and control a production process."

More than half of the interviewees were concerned that FIM will increase the attack surface of their systems. "*The drawback is that someone could authenticate as another user. She would then automatically get access [...] to all the companies where this user has access rights.*" Identity theft is obviously a serious concern, but the interviewees are not only worried about hackers with sinister intentions: "*The risk of unintended errors increases. Someone can cause situations by mistake since they don't understand the consequences beyond their own company."* Some are also concerned that there will be fewer explicit barriers between systems of different criticality. They feel that they lose control when the systems are being accessed transparently.

5 Are identity federations attractive for the industry?

Technologies for Federated Identity Management are becoming mature. Despite examples of successful implementations of FIM, however, there is an agreement among researchers that the adoption rate has not been as high as expected [2] [3] [6]. Hinton and Vandenwauver [6] conclude that *"federation technology is not driving its own adoption"*.

We have already mentioned Rogers' theory on diffusion of innovation, which states that there are five variables that determine the rate of adoption of innovations: the perceived attributes of innovations, the type of innovation decision, the communication channels, the nature of the social system and the extent of change agent's promotion efforts. In our study we provide insight into the first of these variables, which is further divided into five attributes:

- Relative advantage
- Compatibility
- Complexity
- Trialability
- Observability

We found that the last two attributes, Trialability and Observability, did not figure prominently in the minds of the interviewees. Some of the actors have performed limited testing of open-source FIM solutions (section 4.3.), but these efforts sound more like playing around with the technology than bona-fide trials. Furthermore, FIM mainly affects processes and software components that are not observable by the general audience.

In the following discussions we will use our interviewees' perception of FIM and relate them to these attributes, contrasted with Landau and Moore's work [2] on factors affecting FIM adoption.

5.1 Relative advantage

Rogers claims that the perceived relative advantage of adopting new innovations is one of the strongest predictors of its adoption rate. Both academia and the industry representatives in our study come up with several areas where FIM will lead to improvements of current practices, as shown in chapter 1 and 3. Still, we see that FIM adoption is slow. Landau and Moore have looked specifically at adoption of FIM, and the factors influencing the adoption of this technology. They state the following questions:

1. Who gets to collect transactional data?
2. Who sets the rules of authentication?
3. What happens when things go wrong?
4. Who gains and who loses from interoperability?

The first question is interesting for identity and service provisioning on the open Internet. The major identity providers on the Internet today, such as Facebook and Google, are driven by business models based on selling targeted

advertisements. The more they know about their users, the better match for their ads. In return, at least Facebook provides a rich user profile to the service providers that use them as identity provider. This is a gain for both parties and promotes adoption of FIM. However, the situation in an industrial context is different. Business models are built on selling services or products, and the identity and authentication processes are merely a "necessary evil" to facilitate secure information sharing.

Still, being able to monitor and discover misuse of system resources is an important security requirement for most companies. With FIM the industrial service providers will be able to log system use for specific users, while the users' home organisations (acting as identity providers) will be able to follow up on their employees' interactions with their customers. The ability to do audits was one of the perceived benefits our interviewees recognised, and although section 4.5 suggests that some users may be concerned about privacy aspects of FIM, we believe that audit will trump privacy on enterprise systems.

The fourth question is essential for the industrial domain. All parties must benefit from a federation of identity management systems for the adoption to be successful [2], but the effect size for each actor's perceived benefits will vary. The majority of services and systems are delivered by the operator. This company is also the one with most external users enrolled in their user databases, while the contractors offer a very limited set of services, and with a limited number of external users that need access. Where the operator may have an economic incentive to introduce FIM to reduce the cost of user administration, there is limited effect of this for the contractors. The operator also expects a cost reduction due to a more efficient supply industry. This is in conflict with the view of the contractors where they state that adoption of FIM will be costly due to major investments in new processes and technology, and that someone has to pay them to adapt to the new access control solutions. Their implicit statement is that this someone is the oil company. That being said, our impression of the oil and gas industry is that if the operator should decide that FIM is a good idea, it would be rapidly implemented – the contractors would have to comply, or the operator would take its business elsewhere. We do not believe contractors, their size and multi-national characteristics notwithstanding, would drop their Norwegian business due to new requirements from the operator. The risk of losing market share in this competitive environment is too high.

Further, the perceived benefit of achieving better protection due to a reduced number of passwords that have to be remembered, more up-to-date identity attributes and a better revocation process is offset by the increased risk of identity theft, passwords gone astray and the larger attack surface. AlFayyadh and colleagues [6] claim that federated identity management will not solve all password overload issues, which is true if users are participants in several different federations, with different identity providers. In our case there are several systems of different criticality. An obvious solution to mitigate the risk of identity theft and increased attack surface would be to bundle systems at the same criticality level, each in separate federations. Consequently, federation

technologies would reduce the number of credentials for each user, but not eliminate the password problem.

The fact that identity management and user administration is a challenge today makes us also question the effect of identity federations' influence on having more-updated identity attributes and better revocation processes if each company will hold the role of identity provider. Legal obligations between the companies might help, but we agree with some of our interviewees who express that a trusted third party should hold the role of identity provider. A third party entity with a business model based on identity provisioning will have as primary interest of keeping user info up-to-date, including revocation of access credentials.

The increased effectiveness of user administration is offset by demands for new processes to audit and rate collaboration partners' identity management processes and a remaining focus on building good access rules. What we end up with is the fact that users, especially contractor employees, will embrace a FIM solution due to usability and efficiency aspects.

5.2 Compatibility

Compatibility is defined by Rogers as: *"the degree to which an innovation is perceived as consistent with the existing values, past experiences, and needs of potential adopters"*.

The second of the four questions by Landau and Moore is relevant to the compatibility attribute: who sets the rules of authentication? Among the companies we have investigated, there are examples of varying rules for authentication. This is illustrated by the authentication mechanisms, where the operator requires two-factor authentication for all system users, while some of the contractors rely merely on usernames/passwords. At the same time, representatives in our study acknowledge the importance of having common rules for authentication in a FIM scenario. "*There will be consequences for all other companies if one company is careless and has weaker security barriers than the rest".* However, there would be organisational resistance among the contractor employees if their organisations had to convert to two-factor authentication based on demands from a collaboration partner. Even today there is evidence of resistance towards this type of authentication: "*People are in general dissatisfied with two-factor authentication. Either you have to wait for an SMS to have a code, or wait for a secure-ID token, or […] it is bothersome to use* [two factors] *in a working situation.*" (Security professional). FIM implementation will require a common password regime, including the number of authentication factors, password strength, frequency of passwords changes, and so on, to achieve a common assurance level.

Many of the current solutions are not standardised or interoperable. To be able to integrate all systems through FIM will require considerable investments in new integration solutions, which also will also increase the complexity of already complex systems.

5.3 Complexity

The complexity attribute is related to the perceived difficulty or simplicity of understanding and using an innovation. When it comes to FIM, this can be viewed from two angles: the user perspective or the organisational perspective. For users we have already mentioned the benefit of single-sign-on and improved usability. Consequently, the complexity for users will decrease. On the other hand, we have also exemplified increased complexity for the involved organisations. Trust issues, interoperability issues and cost issues are some of the challenge areas.

What happens when things go wrong? Landau and Moore's third question leading to a better understanding of FIM adoption can be used to illustrate the increased complexity that raise from identity federations. They explain two fault situations [2]:

- The authentication process can fail so that unauthorised persons can access resources as if they were valid system users,
- The authentication system can become unavailable with the consequence that people will not be able to access IT resources and do their job.

In today's situation in the IO domain, the owner of an information system issues user IDs and provides authentication services. Consequently, the system owner is responsible for setting the level of assurance and the authentication requirements, and they are responsible for keeping the authentication services up and running. In a federated environment, these responsibilities will be transferred to the organisation where a system user belongs. *"Today, we have a responsibility to protect our customers' data, and it is an enormous responsibility for us to ensure that it is not being misused"* (contractor). Are the collaboration partners willing to assume even more risk? Are they willing to accept liability for downtime on production facilities, which is caused by employees not being able to access and monitor, e.g., safety critical processes? Introduction of FIM will add new complexity to liability issues.

5.4 What then?

The relative advantage of an innovation is found to be one of the strongest predictors of its adoption rate [5]. Our study shows that there are perceived advantages of adoption of federated identity management for all collaborators in the Norwegian Oil & Gas industry, but that some of these are offset by either compatibility issues or increased complexity. At the same time, there are examples where FIM is being tested, and from our discussion on organisational maturity we see that there is willingness in the industry to proceed.

One important aspect that none of the interviewees picked up on, is that FIM can be seen a move toward role-based or attribute-based access control. Today, Contractor employee John Doe is granted access to a third-party system, and retains this access until it is revoked, no matter what happens with his employment situation. With FIM, the access would be restricted to

john.doe@contractor, meaning that as soon a John's employee relationship with Contractor ceases, so would his access to the third-party system.

FIM is security technology that interferes with, but is not a part of a primary business process. It is a preventive innovation, which according to Rogers *"has a particularly slow rate of adoption because individuals have difficulties in perceiving its relative advantage."* So maybe it is not strange that the adoption process is slow in the industry? Our findings are in line with Smith's [3] claim that adoption of FIM will be an evolution, rather than an overnight revolution.

6 Conclusion

Our interviews paint a picture of a complex industrial IT landscape, currently lacking the maturity level needed to implement a global, ubiquitous FIM solution. There is also scepticism among the interviewees as to whether systems of different criticality should be connected at all, now or in the future. The vision might be too ambitious, and certainly comes in conflict with Ross Anderson's observation that: "*There are always systems that don't fit.*" [7].

We believe, however, that the broader industrial audience will adopt some form of federated identity management sooner or later. The fact that they have started experiments with the technology is a good indication, and the perceived benefits are clear. The challenges are complex, but being aware of them will stimulate discussions among collaborators so that palatable solutions can be found.

7 References

[1] J. Jensen: Benefits of federated identity management - a survey from an integrated operations viewpoint. In: Availability, Reliability and Security for Business, Enterprise and Health Information Systems, Lecture Notes in Computer Science, vol. 6908, pp. 1–12. Springer (2011)

[2] S. Landau and T. Moore: Economic tussles in federated identity management. In: Proceedings of the Tenth Workshop on the Economics of Information Security (WEIS), (Jun 2011)

[3] D. Smith: The challenge of federated identity management. Network Security 2008(4), 7–9 (2008)

[4] J. Jensen: Federated Identity Management Challenges. Presented at the 7th International Conference on Availability, Reliability and Security, IEEE CS, Prague, August 2012

[5] E.M. Rogers: Diffusion of Innovations. 5th ed. Free Press (2003)

[6] B. AlFayyadh, P. Thorsheim, A. Jøsang and H. Klevjer: "Improving Usability of Password Management with Standardized Password Policies", *Seventh Conference on Network and Information Systems Security,* Cabourg, May 2012

[7] H. Hinton and M. Vandenwauver: "Identifying Patterns of Federation Adoption," in *ISSE 2006 — Securing Electronic Business Processes*, ed: Vieweg, 2006, pp. 151-160.

[8] R. Anderson: Can we fix the security economics of federated authentication?, 19th international workshop in Security Protocols, Cambridge, UK, 2011.

Author bios

Jostein Jensen is a PhD Candidate at the Norwegian University of Science and Technology (NTNU) since 2009 and Scientist at SINTEF ICT, where he has been employed since 2007. He received his MSc degree in Communication Technology from NTNU in 2007, and has professional background as signal officer from the Norwegian Armed Forces. His research interests include identity management, risk management and secure software development.

Martin Gilje Jaatun is a Senior Scientist at SINTEF ICT, where he has been employed since 2004. He received his MSc degree in Telematics from the Norwegian Institute of Technology (NTH) in 1992. Previous positions include scientist at the Norwegian Defence Research Establishment (FFI), and Senior Lecturer in information security at the Bodø Graduate School of Business. His research interests include security in cloud computing and security of critical information infrastructures. He is vice chairman of the Cloud Computing Association (cloudcom.org) and a Senior Member of the IEEE.

Contact information

Jostein Jensen
Postboks 4760 Sluppen
7465 Trondheim
Norway
Phone: +4792401809
E-mail: jostein.jensen@sintef.no

Martin Gilje Jaatun
Postboks 4760 Sluppen
7465 Trondheim
Norway
Phone: +4790026921
E-mail: martin.g.jaatun@sintef.no

View publication stats