Solutions for federated identity management (FIM) are maturing; however, the adoption rate of this technology hasn’t been as high as expected. Interviews with industry actors reveal that some of FIM’s benefits are offset by its challenges.
to carry out semistructured interviews with people from the industry. We selected an industry whose success depends on efficient collaboration—namely, the Norwegian oil and gas industry. This is a highly technology-driven industry in which information and communication technology has an integral role in its initiatives for integrated operations (IO) and digital oil fields. Our goal was to gain a better understanding of the factors influencing FIM adoption in complex industrial cases.

We carried out 11 interviews one-on-one, either in person or via telephone, according to a prepared interview guide, but asked additional follow-up questions to prompt interviewees to elaborate on interesting points. The 11 interviewees were selected based on our industry contacts’ recommendations, and represented all of the most interesting stakeholders in this domain, including one oil and gas company, two vendors of production equipment and process control systems, one consultancy, and one service company. To gain a deep insight into the case, we conducted in-depth interviews (a minimum of 45 minutes).

Our analysis of the interview data showed that there are conflicting interests and views related to FIM adoption. In some areas, our interviewees recognized that FIM adoption would have beneficial effects, but felt that these would be offset by new challenges.

### Integrated Operations for Oil and Gas Production

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. Production facilities are heavily equipped with sensors, and land-based control centers monitor and control a large part of the daily production. Today, however, most process control systems in this IO scenario are designed for intra-organizational use, and many are proprietary silo systems. One of the Norwegian Oil Industry Association’s (OLF) visions was to enable inter-organizational collaboration in which partners share information and knowledge seamlessly across company borders.

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

In this article, we refer to the oil and gas company as the **operator** and to all other actors in the IO domain as **contractors** (see Table 1).

Three of our 11 interviews were held with representatives from an operator, and the remaining eight with representatives from four different contractor companies.

### Perceived Benefits

In his theory on diffusion of innovation, Everett Rogers claims that the consideration of how much a new innovation improves what already exists is essential in deciding whether to adopt it. Therefore, we aimed to understand how industry actors perceive the benefits of adopting FIM in their working environments.

### The Effectiveness of User Administration and Improved Data Quality

When asked to identify current challenges regarding identity management, an operator 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.” Furthermore, he explained, the oil industry at large experiences approximately 40,000 job changes per year, and with an estimated average of two hours administration per change, the industry spends approximately 80,000 hours per year on administrative overhead related to identity management. The same interviewee said that his company has more than 50,000 external users enrolled in its IT systems. Also, one contractor explained a situation in which his company was responsible for managing external users in their internal systems. In one of its IT solutions, more than 500 external users are registered.

One contractor exemplified the problem of not having updated access lists: an employee had left a

<table>
<thead>
<tr>
<th>Table 1. Actors in the integrated operations domain—high level.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actor</strong></td>
</tr>
<tr>
<td>Operators</td>
</tr>
<tr>
<td>Contractors</td>
</tr>
</tbody>
</table>
contractor in favor of an operator. Part of his job was to serve several oil companies; thus, he had a different user account for each oil company. Although his access rights to the contractor’s systems were revoked immediately, the operators experienced delays in the revocation process, which could have given him unauthorized access based on old but still valid access credentials.

In this situation, it’s easy to see why more than half of our interviewees believed that FIM adoption would rationalize the user administration process and improve the quality of recorded identity attributes. One contractor commented, “You could rationalize the user account systems at different companies if you have a cooperation among them.” Another contractor supplemented, “It is obvious that there will be less user administration if we could integrate our login systems.” However, as we see later, even if some of the current user administration challenges can be solved with FIM, others will be introduced, and some of the more difficult access control problems will continue to exist.

**User Experience and Usability**

Often, contractors have business relationships with several operators and other contractors, and the number of systems to which they need access can grow large. Many offshore expert systems aren’t currently integrated with other production or access control systems. One operator mentioned that there might be situations in which an onshore worker is responsible for controlling several offshore facilities and needs to visit 15 to 20 different systems per day. Another representative from the contractor side told us that visiting up to five systems with separate logins might be necessary to create production reports.

Seven interviewees mentioned improved usability with SSO as a perceived benefit of FIM. Contractors especially saw the advantage of encountering fewer login requests to do their job.

**Efficient Collaboration**

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

The contractors in our study were mostly interested in easy access to data to work more efficiently. Some told us about incidents in which they had forgotten their infrequently used passwords to collaborators’ services. A short-term solution was to borrow access credentials from coworkers, because delays can cause serious problems. Downtime of production facilities can cause millions of dollars per hour in lost revenue, so there’s a strong focus on keeping the production up and running. Therefore, the easy way out is sometimes selected, even if it conflicts with existing security policies and has implications for the overall security.

**Reduced Cost**

Efficient user administration and collaboration are directly linked to a desire to reduce cost. Both operators and contractors can gain from rationalized user administration. Operators expect that FIM will reduce costs with its more efficient work processes. However, while a cost decreases in some areas, it will increase in others.

**Audit**

Some of today’s systems operate with service accounts that several engineers share. Although this simplifies everyday work tasks, it makes detecting and auditing potential misuse difficult. One contractor interviewee mentioned that FIM should facilitate system audits because each user would have a personal account, which helps track who does what.

**Better Protection**

During one interview, a contractor 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 to do his job. Several other interviewees related similar situations; the number of usernames and passwords they needed to remember was so large that they’d often write them down in books. Previous studies indicate that this often leads to people using the same password for several services, generally with the same perceived security level.6

With FIM adoption, the interviewees expected fewer user accounts and passwords, which led one operator to express that “the perceived security will increase. Fewer passwords will be written down on paper.”

The interviewees believed that the quality of user attributes to make authorization decisions would increase and that the access revocation process would be more efficient. This is highly relevant to ensure good protection of company resources.

However, FIM adoption won’t solve all security challenges related to identity management.

**Perceived Challenges**

Two of the attributes Rogers’s diffusion of innovation theory considers to determine whether innovations
Identity and Access Management
A major challenge related to identity management in general is keeping user databases and access rights up to date. One of the foreseen benefits of FIM is that it will make keeping identity data up to date easier. However, more than half the interviewees anticipated challenges, despite identity federations. One of the operator representatives claimed, “I’m not so sure if we will experience less administration with such a system. I guess we … will get fewer users to adminster, but I’m not sure about this simplification.” He continued to argue that processes to establish trust for each individual user will still be necessary before he or she can be authorized to access systems, and processes must be implemented to verify the quality of federation partners’ identity management processes.

The interviewees emphasized the need to fully control the authorization mechanisms that restrict access to resources. The authentication service can be outsourced to a trusted third party, or users can be authenticated within their home organization, but organizations still need strict control on which users or types of users have access to their resources. However, there’s a risk of confusing identity management with authorization, because this authorization process is already being performed today—with the added chore of local identity management in each case.

Trust in Collaborators
Don Smith argues that trust is the fundamental concept underlying federations. At the same time, he notes that there are challenges related to establishing trust. Trust issues are highly relevant for inter-organizational collaboration, which takes place in the IO domain. One operator 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.” Trust in other companies depends on context, and trust levels are difficult to define. One contractor indicated one of the reasons: “I think people are slightly more skeptical of the neighboring business concerning the big money that swirls around in the oil and gas industry.”

“The contractors will never be able to handle the processes behind federation.” This statement from one of the operators highlights 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 it would be easier to trust some of their large contractors with which they have well-established cooperative frameworks. A body similar to a credit rating bureau could be established in the oil and gas industry. It could perform professional audits of key characteristics of collaborators’ identity management practices, which could affect the trust relationships, he said.

During the conversation about trust issues, some interviewees mentioned the option of having a trusted third party host the authentication service. One contractor 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 organized by a common entity.”

Standardization, Interoperability, and Technology Management
The complexity of IT systems in the IO domain is high, spanning regular office tools to small, tailored expert systems on the software side. At the network layer, they operate with both traditional IP networks and specialized process control systems. A security professional from an operator 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.” Furthermore, he explained that identity federations might be possible in the future for some of their large partners and their large systems. However, this is more difficult for small companies’ systems, which might not have the competency or economic baseline to integrate with other federated systems according to standardization and interoperability needs.

Some operators told us that they tried open source federation technologies in a few cases but experienced some technological challenges, especially related to technology management. One said, “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 fulfill
the industry’s needs before they would consider the technology at a larger scale. A second operator 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 from a contractor with a 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 rapid technology development that can benefit a company internally, such as video conferencing, considerable challenges exist outside company borders, where you find different equipment, security policies, firewall settings, 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 valid when looking at integrating identity management systems. Both software and hardware interfaces must be standardized. The oil and gas industry must define protocol options so that all the equipment is interoperable and define and agree on the semantic meaning of identity attributes. Several interviewees mentioned that the industry must agree on common, detailed guidelines for FIM for it to be successful.

Investment Cost
We asked the interviewees 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 one consultant’s immediate response. “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.” Three of the four contractors in our study concurred. “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 said. The two others 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 operator interviewees didn’t mention funding as a factor, they all recognized that the investment cost of a FIM solution would be considerable.

Security Challenges
FIM privacy aspects are currently a hot research topic. However, only one of the contractor 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. However, the drawback is that you can trace what people are doing. ... It might not be that important in this context, but often it is okay 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 a primary concern in a professional context.

Organizational 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,” said one operator. We asked another 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 contractor commented that attitudes change when it comes to taking advantage of new communication technology to facilitate data sharing: “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.”

Are Identity Federations Attractive for the Industry?
FIM technologies are maturing. However, despite examples of successful FIM implementations, researchers agree that the adoption rate hasn’t been as high as expected.2,3,7 Heather Hinton and Mark Vandenwauver conclude that “federation technology is not driving its own adoption.”7 Rogers’s theory on diffusion of innovation states that five variables determine the adoption rate 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 a change agent’s promotion efforts.

We provide insight into the first of these variables, which is further divided into five attributes:

• relative advantage,
• compatibility,
• complexity,
• trialability, and
• observability.

We found that the last two attributes, trialability and observability, didn’t figure prominently in the interviewees’ minds. Some actors performed limited testing of open source FIM solutions, but these efforts sounded more like playing around with the technology than bona fide trials. Furthermore, FIM mainly affects processes and software components that aren’t observable by the general audience.

We use our interviewees’ perceptions of FIM and relate them to the first three attributes, contrasted with Susan Landau and Tyler Moore’s work on factors affecting FIM adoption.2

Relative Advantage
Rogers claimed that the perceived relative advantage of adopting new innovations is one of the strongest predictors of its adoption rate. Both academia and industry representatives in our study came up with several areas in which FIM will lead to improvements of current practices. Still, FIM adoption is slow. Landau and Moore looked specifically at FIM and the factors influencing its adoption, asking the following questions:

• Who gets to collect transactional data?
• Who sets the rules of authentication?
• What happens when things go wrong?
• 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 its service providers that use it as an identity provider. This is a gain for both parties and promotes FIM adoption. However, the situation in an industrial context is different. Business models are built on selling services or products, whereas identity and authentication processes are merely a necessary evil to facilitate secure information sharing.

Still, for most companies, the ability to monitor and discover misuse of system resources is an important security requirement. With FIM, industrial service providers can log system use for specific users, while the users’ home organizations (acting as identity providers) can follow up on their employees’ interactions with customers. Although some users might be concerned about privacy aspects of FIM, we believe that the ability to perform audits—one of our interviewees’ perceived benefits—will trump privacy on enterprise systems.

The fourth question is essential for the industrial domain. For FIM adoption to be successful, all parties must benefit from a federation of identity management systems, but each actor’s perceived benefits will vary. The operator delivers the majority of services and systems. This company is also the one with the most external users enrolled in its user databases, whereas contractors offer a very limited set of services with a limited number of external users who need access. Whereas the operator might have an economic incentive to introduce FIM to reduce user administration cost, there is limited effect of this for the contractors because they administer relatively few external users in their systems. The operator also expects a cost reduction due to a more efficient supply industry. This conflicts with the contractors’ view that FIM adoption will be costly due to major investments in new processes and technology, and that someone—presumably the oil and gas company—has to pay them to adapt to the new access control solutions. That said, we believe that if the operator decides that FIM is a good idea, it would be rapidly implemented; contractors would have to comply, or the operator would take its business elsewhere. We don’t believe contractors—their size and multinational 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.

Furthermore, 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, stolen passwords, and a larger attack surface. Bander AlFayyadh and his colleagues claim that FIM won’t solve all password overload issues,6 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 a separate federation. 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 are challenges today makes us question the effect of identity federations’ influence on having more up-to-date identity attributes and better revocation processes if each company acts as identity provider. Legal obligations between companies might help, but we agree with those interviewees who believed that a trusted third party should act as an identity provider. A third-party entity with a business model based on identity provisioning would focus on keeping user information 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 as well as good access rules. Therefore, users, especially contractor employees, will embrace a FIM solution because of its usability and efficiency.

Compatibility
Rogers defines compatibility 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 Landau and Moore’s four questions is relevant to the compatibility attribute: Who sets authentication rules? Among the companies we investigated, there are varying rules for authentication. Some operators require two-factor authentication for all system users, while some contractors rely merely on usernames and passwords. However, our study participants acknowledged the importance of common authentication rules in FIM. “There will be consequences for all other companies if one company is careless and has weaker security barriers than the rest,” said an operator employee. However, some contractor employees might resist converting to two-factor authentication based on demands from a collaboration partner. Even today, there is evidence of resistance to this type of authentication. Said a security professional from an operator, “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. ... It is bothersome to use [two factors] in a working situation.” FIM implementation will require a common regime, including the number of authentication factors, password strength, frequency of passwords changes, and so on, to achieve a common assurance level.

Many current solutions aren’t standardized or interoperable. Integrating all systems through FIM will require considerable investments in new integration solutions, which will also increase the systems’ complexity.

Complexity
Complexity 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 perspectives: the users’ and the organizations’. Users’ complexity will decrease; we’ve already mentioned the benefit of SSO and improved usability. On the other hand, we also exemplified increased complexity for the involved organizations. Trust, interoperability, and cost issues are some of the challenge areas.

What happens when things go wrong? Landau and Moore’s third question illustrates the increased complexity from identity federations. They explain two fault situations:

- the authentication process fails, allowing unauthorized persons to access resources as if they were valid system users; and
- the authentication system becomes unavailable so users can’t access IT resources and do their job.

In today’s IO domain, the information system’s owner issues user IDs and provides authentication services. Consequently, the system owner is responsible for setting the assurance level and authentication requirements and for keeping the authentication services up and running. In a federated environment, these responsibilities are transferred to the organization in which 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,” said a contractor. Are collaboration partners willing to assume even more risk? Are they willing to accept liability for downtime on production facilities?

Are collaboration partners willing to assume even more risk? Are they willing to accept liability for downtime on production facilities?
What Then?
The relative advantage of an innovation is one of the strongest predictors of its adoption rate. Our study shows that there are perceived advantages of FIM adoption for all collaborators in the Norwegian oil and gas industry, but that some of these are offset by either compatibility issues or increased complexity. At the same time, there are examples in which FIM is being tested in the industry, and from our discussions on organizational maturity, we see that there is a willingness to proceed.

One important aspect that none of the interviewees picked up on is that FIM can be seen as a move toward role-based or attribute-based access control. For instance, today, contractor employee John Doe is granted access to a third-party system and retains this access until it’s revoked, no matter what happens with his employment situation. With FIM, access would be restricted to john.doe@contractor, meaning that as soon as John’s employee relationship with the contractor ceases, so would his access to the third-party system.

FIM security technology interferes with but isn’t a part of a primary business process. It’s 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’s not strange that the adoption process is slow in the industry. Our findings are in line with Smith’s claim that FIM adoption will be an evolution, rather than an overnight revolution.

Our interviews paint a picture of a complex industrial IT landscape, currently lacking the maturity level necessary to implement a global, ubiquitous FIM solution. There was also skepticism among 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 conflicts with Ross Anderson’s observation that “there are always systems that don’t fit.”

However, we believe that the broader industrial audience will adopt some form of federated identity management sooner or later. The fact that they’ve 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.

References

Jostein Jensen is a PhD candidate at the Norwegian University of Science and Technology (NTNU) and a research scientist at SINTEF ICT. His research interests include identity management, risk management, and secure software development. Jensen received an MSc in communication technology from NTNU. Contact him at jostein.jensen@sintef.no.

Martin Gilje Jaatun is a senior scientist at SINTEF ICT. His research interests include security in cloud computing and security of critical information infrastructures. Jaatun received an MSc in telematics from the Norwegian Institute of Technology. He’s vice chairman of the Cloud Computing Association and a senior member of IEEE. Contact him at martin.g.jaatun@sintef.no.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.