2009 International Conference on Advanced Information Networking and Applications

Trust Requirements in Identity Federation Topologies

Uwe Kylau, Ivonne Thomas, Michael Menzel, Christoph Meinel
Hasso Plattner Institute
Prof.-Dr.-Helmert-Str. 2-3, 14482 Potsdam, Germany
{firstname}.{lastname}@hpi.uni-potsdam.de

Abstract

Federated Identity Management describes a model to enable users to use their digital identities in collaborating companies regardless of organizational borders. The essential pre-requisite to build up a federation and to share the user authentication across different security domains is the establishment of trust between the collaborating partners. Usually, this is done by setting up complex contracts, that describe common policies, obligations and procedures to be followed by each federation member. The result is a Circle of Trust*, in which each member is willing to trust on assertions made by someone else. However, federations are no isolated structures and members of one federation might be a member of another federation - a constellation which is possible with current specifications such as WS-Federation. However, whether and how the trust relationships of the federations can be used to allow access even across several federations is a question which has not been answered yet.*

In this paper, we investigate on the trust requirements for identity federation topologies. Starting of from the classical structure of a Circle of Trust*, we go beyond this and identify more complex patterns such as overlapping federations. For each pattern, we identify risks for identity and service providers as well as the necessary trust requirements that must be met to allow such constellations.*

1 Introduction

The design of Service-oriented Architectures allows a seamless communication between applications independent from the platform on which they run and even across domain boundaries; therefore, making them perfectly suitable for the integration of services provided by independent business partners. However, to fully exploit such infrastructures for collaboration, each partner in the network needs to be identified and authorized to access another partner's confidential resources. Traditional approaches for identity management like the isolated model (cf. [5]) require users to register with every single service and to re-authenticate each time they use a service in another trust domain. As businesses have become more distributed, authenticating for each service is not the preferred option anymore.

Federated Identity Management as a new identity model provides solutions for these problems by enabling the propagation of identity information to services located in different trust domains. Several frameworks and specifications for Federated Identity Management have been specified (e.g. SAML 2.0 [4], Liberty Identity Web Services Framework (ID-WSF) 2.0 [10], and WS-Federation [6]). The key concept in a federation is the establishment of trust whereby all parties in a federation are willing to rely on asserted claims about a digital identity (e.g. conveyed in a SAML assertion [2]). In order to engage in interactions, the service provider must trust the authentication assertions of the federation partners, while the federation partners must trust the service provider to handle the user's identity information with adequate care. Trust relationships are usually established by a set of contracts defining obligations and rights each party has and policies each member has to follow. The result is a *Circle of Trust* in which each partner trusts on the assertions made by another partner.

Federations are thus a way to make digital identities available in a global context for the purpose of user identification and access control. Due to the huge effort of setting up underlying contracts, federations are mostly meant to have long-term trust relationships and are therefore relatively static. Adding additional partners requires all federation members to agree on trusting the new member. Another aspect when dealing with federations is that business relationships are much more manifold as can be represented by a single Circle of Trust. A single enterprise has trust relationships with different groups of partners - each requiring different business agreements and therefore requiring separate contracts. Hence, enterprises are usually having contracts with more than one federation leading to overlapping Circles of Trust. This way, whole *trust topologies* exist, which mirror the underlying business relationships. The question arising is whether we can leverage these trust topologies to establish trust for short-term relationships, in which the effort of setting up a new federation would not

outbalance the benefit. In order to facilitate this, identity information has to be shared across federation borders. This results in new risks for all involved parties. In order to minimize these risks, requirements need to be specified for establishing the trust relationships and need to be addressed in the federation contracts.

Current specifications provide the basic mechanisms to establish trust between partners and to set up a federation. However, they do not detail the requirements of the trust relationship. In particular, trust requirements for scenarios involving two or more federations are not set yet. In order to achieve a trustworthy collaboration between business partners, it is important to know: *(a)* which trust requirements need to be met to establish a trust relationship within a federation; and *(b)* which additional trust requirements arise when crossing federation borders.

In this paper, we identify recurring patterns in identity federation topologies and classify them into those based solely on direct trust relationships and those which also include indirect trust relationships. Our main contribution is the analysis of trust requirements inherent to each pattern. Starting from a risks analysis for identity and service provider, we concisely express the trust requirements.

The rest of this paper is organized as follows. In Section 2 and 3, we provide the foundation by defining the concepts of trust and those of identity federation. In Section 4 we introduce our trust patterns and state the trust requirements for each of them. Finally, Section 5 gives an overview about related work in this area and Section 6 concludes this paper.

2 Identity Federation Basics

Managing numerous *digital identities* and associated authentication credentials is cumbersome for most computer users. Nonetheless, service providers often need a portion of our identity to perform a service (*identity–based service*), or to hold us liable in case anything bad happens. As a consequence, a concept for the controlled sharing of identity information was developed, called *Identity Federation*.

The basic building block of *Identity Federation* is the trusted federation relationship established between identity providers and service providers. An *identity provider* (IdP) holds digital identities of registered users for the purpose of provisioning these identities, or portions of them, to a party willing to rely on this information (the *relying party*). A service provider (SP) usually takes the role of the *relying party*. It allows users to authenticate themselves at a federated identity provider and then relies on the assertion issued by the IdP upon successful authentication.

In order to establish the unique user identity at the service provider, several methods can be employed. One way is to purely rely on the identity attributes retrieved from the identity provider and have no local user management (no user account at the SP). If the user previously registered an account at the SP, s/he is offered the option to authenticate at her/his identity provider and link the SP account to the IdP account. A combination of both methods is to initially obtain relevant user data from the identity provider and then automatically create an account for the user.

3 The Concept of Trust

Trust decides about how human beings interact with each other, which and how much information they reveal in a conversation, and how much they are willing to rely on someone else. For this reason, it is the key to cooperative relationships.

A general definition covering the main characteristics of trust has been given by McKnight and Chervany [7] in their survey about the different meanings of trust. According to them, trust is "the extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though negative consequences are possible." Even though this definition is relatively general, it contains three aspects which are fundamental to the definition of trust: 1) the dependence on the trusted party, 2) the reliability of the trusted party and 3) the consequences in case the trusted party does not perform as expected. The implication of this definition is that trust requirements, i.e. the required mechanisms to build up trust, are directly correlated with the risk that the partners in a trust relationship are exposed to in the case of failure. Risk, hereby, is the combination of *(a)* the possibility that an uncertain event occurs and *(b)* the impact of such an event.

Taking the definition, a trust relationship is directional. However, most business relationships do not work without mutual trust. Therefore, a trust relationship is usually used in a two-directional sense, which in fact comprises two single trust relationships. Trust relationships are usually classified into those based on *Direct Trust* and those based on *Transitive or Indirect Trust*. In the *Direct Trust* model, a direct trust relationship exists between two communication partners which has been established by validating the other party's credentials without reliance on any other entity. *Transitive or Indirect Trust* is characterized by the fact that there is no direct trust relationship between an entity A and an entity C. Instead both entities have a direct trust relationship with a third entity B. This relationship is leveraged to assess the trustworthiness of the unknown communication partner.

4 Trust Patterns in Identity Federation Topologies

When looking at the concept of Identity Federation, one can identify certain recurring scenarios how identity providers and service providers affiliate into federations. In

these scenarios, different types and qualities of trust are distributed among the federation participants. We will present those scenarios that are covered by current Identity Federation theory and examine them for their inherent trust requirements. In the following, we refer to them as *patterns*.

For the purpose of simplicity, we assume that an identity provider (IdP) is a single system entity that implements all necessary identity federation services, including registration and issuing credentials. Note that registration and issuing credentials means setting up a local digital identity and local credentials to directly access a provider. Next, we assume that any two providers that are logically described as separate entities are in fact separate in the real world, even though they may be located in the same administrative domain. This means, in a single scenario (or instance thereof) an identity provider cannot be a service provider (SP) and vice versa. Finally, we decided to concentrate on the federation relations between providers and not to consider the user in the analysis, although we know that s/he is part of the trust network. Trust between providers and the user is discussed for example in [5].

Our trust analysis employs a method similar to that described by Povey in [9]. In his work, Povey presents an approach to develop trust policies by starting with a risk management analysis. Risk management explicitly deals with risk as the combination of event uncertainty and event impact. Minimizing one or both of them is the goal of risk management. According to [9] this is generally achieved in a four–step process. First, valuable assets, threats to them and the impact of their compromise need to be identified. Second, threats emerge because of vulnerabilities, which therefore have to be found. Third, the risk of an attack exploiting these vulnerabilities is determined. Finally, a decision must be made whether a risk is accepted or mitigated.

We adapted the risk management procedure to our needs and simplified it to some extent. Initially, we identify assets and potential general threats. Because we almost exclusively deal with sensitive identity information and authentication artifacts, the impact of asset compromise is likely to be severe for all assets. Hence, mitigating risks is absolutely necessary. In a second step we describe threats and vulnerabilities in detail and give a rough estimate of the probability of their exploitation. We have subsumed this examination under the term "risks" and conduct an examination from the viewpoint of every participant or role. This will be helpful for the derivation of trust requirements in the final step, since trust was defined to be directional.

Remarks

- Due to space limitations, we cannot include a detailed discussion about the costs of risk mitigation, satisfaction of trust requirements respectively.
- Some of the presented risks may be attributed to more than one federation role. For instance, the risk of false authentication through an IdP is shared between the user and the SP. The SP has to consider this risk, because in the event of false authentication it is likely that the SP needs to justify its decision to trust the IdP. Being aware of all the risks, including those taken by the user, therefore is essential in order to attain the right set of trust requirements.

4.1 Patterns Based on Direct Trust

We will first introduce the patterns that are based solely on direct trust.

4.1.1 Bilateral Federation

A *Bilateral Federation* (see Fig. 1.a) consists of a single identity provider and service provider. The user has registered a digital identity (account) at both providers and decides to federate (link) them. This enables federated authentication and provisioning of identity information to the SP.

Assets Both identity and service provider are obliged to handle private data according to privacy policies and regulations. This includes the user's usage and transaction history with the SP. Because of federated authentication, the identity provider usually is aware of when and how often a particular user communicates with a service provider. This information must be protected. On the other side, the service provider receives user data supplied by the IdP, which must also remain private and may not be disclosed. Of course, the service provider is also interested that only legitimate (authorized) users gain access to its services.

Service Provider Risks

SP-R.1 The identity provider authenticates an unauthorized user or entity and issues an assertion that specifies an authenticated user as subject. Although hardly considered possible, inadequate user–registration and authentication may give rise to this threat. If the IdP also supplies all claims required for authorization, the result would be unauthorized access to the SP.

SP-R.2 The identity provider authenticates an authorized user or entity and issues an assertion that specifies a different authenticated user as subject. This refers to weaknesses of the authentication and identity mapping procedures employed at the IdP. Similar to *SP-R.1* access could be granted to portions of service provider data the user is not entitled to see or modify.

SP-R.3 The identity provider leaks usage data of a user to unauthorized third parties. Such behavior is definitely

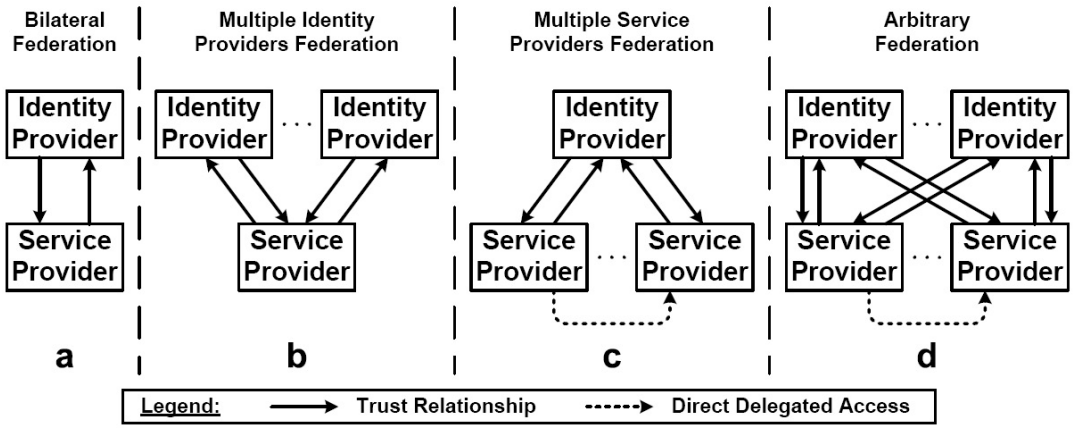

Figure 1. Patterns based on direct trust

not wanted, but conceivable and moderately possible as the identity provider might have incentives to do so (for instance financial benefit).

Identity Provider Risks

IdP-R.1 The service provider leaks private data of a user to unauthorized third parties. Similar to *SP-R.3*, the SP might have incentives to disclose private identity information, making this a moderately possible threat.

Trust Requirements As mentioned earlier, assets of the service provider and identity provider are identity information and internal business data. Both must be protected as much as possible. Thus, the risk of those assets being compromised is too high to just rely on the belief that the other party is trustworthy. As a consequence, the federation relationship is regulated with a federation agreement. This contract defines policies and procedures that divide responsibilities between the federation participants, as well as penalties for not adhering to them.

SP-T.1 The service provider has to trust the identity provider to adhere to the agreed policies and procedures dealing with user–registration, authentication and identity mapping.

SP-T.2 The service provider has to trust the identity provider to adhere to the agreed privacy policies regarding non-disclosure of usage statistics.

IdP-T.1 The identity provider has to trust the service provider to adhere to the agreed privacy policies regarding non-disclosure of user data.

4.1.2 Multiple Identity Providers Federation

This type is a multiplication of the *Bilateral Federation* (see Fig. 1.b). A single service provider is federated to a number of identity providers (greater 1). The identity providers know about each other, but did not necessarily establish federation connections among each other. The user can select where to register a digital identity, but has to tell the service provider upon account federation (linking) which identity provider s/he chose. It is also possible to register digital identities with more than one identity provider, but only one federation connection (between service provider and identity provider) can be active per user at a time.

Assets, threats, risks and trust requirements are the same as in the *Bilateral Federation*, with the addition of one threat. In case the user has registered multiple digital identities and changes her/his IdP frequently, some or all of the IdPs might decide to collude and consolidate usage statistics, which are distributed across the user's providers. This threat is addressed with *SP-R.3* and *SP-T.2*.

4.1.3 Multiple Service Providers Federation

This type is a different multiplication of the *Bilateral Federation* (see Fig. 1.c). A single identity provider is federated to a number of service providers (greater 1). The SPs know about each other and might even allow direct access between each other. The user has registered a digital identity at the IdP and at some of the SPs. Of her/his service provider accounts she decides to federate some to her/his account at the IdP.

Assets are the same as in the *Bilateral Federation* and all threats, risks and trust requirements of that pattern apply, too. However, if complex services are allowed that result in access to services of other providers, an additional threat arises. Complex services that orchestrate other services are one of the major benefits of Service–oriented Architectures. Nonetheless, in the context of users and identity they always entail delegation of access rights. That is, the complex service acts on behalf of the user, for which it needs to be authorized by the user, the identity provider respectively. Of

course, the accessed service provider might have the ability to obtain user consent, but, if no such thing is done, there might be no way for the identity provider to enforce appropriate access control.

Another threat is that service providers could collude and try to accumulate all available user data into a comprehensive user dossier. Normally, each service provider is supplied only with a user–controlled portion of user data. If this set is big enough to be unique, colluding SPs could correlate their respective portions and accumulate data on individuals. *IdP-R.1* and *IdP-T.1* address this issue.

Identity Provider Risks

IdP-R.2 A service provider uses a legitimately obtained assertion to gain unauthorized access to another service provider, including the sensitive (user) data stored at the provider. The accessed SP does not implement adequate access control mechanisms. Again, this is a rather less likely threat, but has to be considered.

Trust Requirements

IdP-T.2 The identity provider has to trust the service providers to adhere to the agreed policies and procedures regarding access control and delegated access.

4.1.4 Arbitrary Federation (Circle of Trust)

The *Arbitrary Federation* merges all previous patterns (see Fig. 1.d). Multiple service providers are federated with multiple identity providers. All participants know and trust each other, which is why this pattern is also called *Circle of Trust*. Characteristics of user registration are the same as in the *Multiple Identity Providers Federation*. Complex services with delegated access are allowed as in the *Multiple Service Providers Federation*. All assets, threats, risks and trust requirements identified so far apply here.

4.2 Patterns Based on Direct and Indirect Trust

As demonstrated in the last part, most trust requirements are already present in the bilateral federation. Additional requirements emerge by multiplying service providers and/or identity providers. In order to shorten the following analysis of patterns that contain a mixture of direct and indirect trust, we decided to only describe simple and arbitrary patterns.

4.2.1 Two Overlapping Arbitrary Federations

This pattern consists of two federations that share one or more identity providers (see Fig. 2.a for a simple version). Internally, each federation functions like an *Arbitrary Federation*. But, if the user is registered at one of the shared IdPs, it is possible to have direct access between service providers across federation borders. Such interacting service providers do not usually know that they share a set of common identity providers. Nevertheless, a provider might decide to grant access to SPs from outside the own federation, under the condition that federations are alike. That is, providers could be willing to allow external access without re-authenticating the user at their IdP, if the external requester is engaged in a federation with a trusted identity provider and this federation is similar to their own. "Similar" in this case means that policies and procedures are similar. In order for a service provider to be sure to some extent that an external provider adheres to the same rules and really acts on behalf of the user, the identity provider has to act as mediator of this indirect trust relationship.

All aspects of the *Arbitrary Federation* apply. One risk needs to be adapted to cover the new scenario (*IdP-R.2*). The corresponding trust requirement (*IdP-T.2*) is general enough. Finally, we need to address the service providers' viewpoint towards the unauthorized external access threat.

Identity Provider Risks

IdP-R.2a A federated service provider uses a legitimately obtained assertion to gain unauthorized access to another service provider, *which is part of a different federation*. (applies in addition to *IdP-R.2*)

Service Provider Risks

SP-R.4 A service provider from a different federation uses an assertion that was legitimately obtained from a trusted identity provider to gain unauthorized access, even though the IdP vouched that the SP acts on behalf of the user.

Trust Requirements

SP-T.3 The service provider (S) has to trust the identity provider to vouch only for those external service providers that are federated with the identity provider and are trusted to adhere to certain policies and procedures regarding delegated access. Identity provider and service provider (S) agree on these policies and procedures.

4.2.2 Bilateral Federation with External Identity Provider

This pattern deals with the scenario where an identity provider A that belongs to one federation is also federated with an external identity provider B (see Fig. 2.b). This additional federation comprises no service providers. The user has registered a digital identity with the external identity provider B and the service provider. However, the service provider normally accepts no external authentication

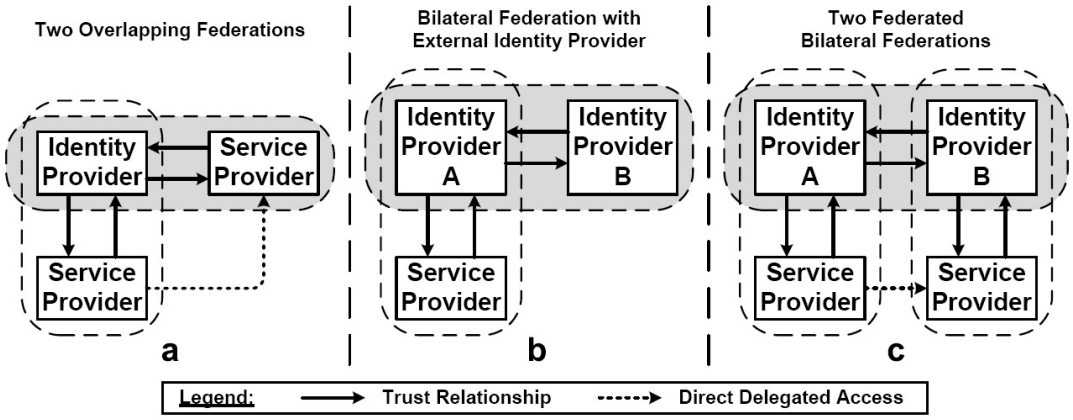

Figure 2. Patterns based on direct and indirect trust

assertions and the identity provider B does not disclose user data to unfederated parties. In order to achieve federated authentication and account linking, identity provider A has to mediate between the two parties, which probably do not even know each other.

Basically, assets, threats, risks and trust requirements are the same as in a *Multiple Identity Providers Federation*. Some of the risks and trust requirements have to be extended to apply here. Most important for this pattern are the threats arising with delegated authentication, assertion consumption and user data disclosure. Again, an indirect trust relationship has to be established, which is not trivial when dealing with identity information.

Service Provider Risks

SP-R.1a Identity provider A *or an authorized federated identity provider* authenticates an unauthorized user or entity and issues an assertion that specifies an authenticated user as subject.

SP-R.2a Identity provider A *or an authorized federated identity provider* authenticates an authorized user or entity and issues an assertion that specifies a different authenticated user as subject.

SP-R.5 Identity provider A authorizes a federated identity provider for delegated authentication, even though this identity provider does not meet expectations of the service provider. Assumed that there are guidelines for the authorization process, this threat should have a low probability.

Identity Provider A Risks

IdP-R.3 Identity provider B authenticates an unauthorized user or entity and issues an assertion that specifies an authenticated user as subject. Probability is similar to *SP-R.1*.

IdP-R.4 Identity provider B authenticates an authorized user or entity and issues an assertion that specifies a different authenticated user as subject. Probability is similar to *SP-R.2*.

Identity Provider B Risks

IdP-R.1a Identity provider A *or an authorized federated service provider* leaks private data of a user to unauthorized third parties. (in addition to *IdP-R.1*)

IdP-R.5 Identity provider A authorizes a federated service provider to receive assertions and private user data, even though this service provider does not meet expectations of identity provider B.

Trust Requirements Risks *SP-R.1a* and *SP-R.2a* are partly addressed with *SP-T.1* (referring to IdP A). The part not addressed and all other risks have been treated with one or more trust requirements (indicated at the end of each item).

SP-T.4 The service provider has to trust identity provider A to authorize only those federated identity providers for delegated authentication that adhere to certain agreed policies and procedures (dealing with user–registration, authentication and ID mapping). (refers to *SP-R.1a*, *SP-R.2a* and *SP-R.5*)

IdP-T.3 Identity provider A has to trust identity provider B to adhere to the agreed policies and procedures dealing with user–registration, authentication and identity mapping. (refers to *IdP-R.3* and *IdP-R.4*)

IdP-T.1a Identity provider B has to trust identity provider A to adhere to the agreed privacy policies regarding non-disclosure of user data. (refers to *IdP-R.1a*; applies in addition to *IdP-T.1*)

	SP-R								IdP-R								SP-T					IdP-T					
Pattern	1	1a	2	2a	3	4	4a	5	1	1a	2	2a	2b	3	4	5	1	2	3	3a	4	1	1a	2	3	4	5
Bilateral	X	-	X	-	X				X	-							X	X				X	-				
Multiple IdPs	X	-	X	-	X				X	-							X	X				X	-				
Multiple Sps	X	-	X	-	X				X	-	X	-	-				X	X				X	-	X			
Arbitrary	X	-	X	-	X				X	-	X	-	-				X	X				X	-	X			
2 Overlapping	X	-	X	-	X	X	-		X	-	X	X	-				X	X	X	-		X	-	X			
Bilateral + IdP	-	X	-	X	X			X	X	X				X	X	X	X	X			X	X	X		X	X	
2 Bilateral / 2 Arbitrary	-	X	-	X	X	X	X	X	X	X	X	-	X	X	X	X	X	X	-	X	X	X	X	X	X	X	X

Figure 3. Trust patterns and their risks and trust requirements

IdP-T.4 Identity provider B has to trust identity provider A to authorize only those federated service providers for delegated assertion and user data consumption that adhere to certain agreed policies and procedures (dealing with non–disclosure of user data). (refers to *IdP-R.1a* and *IdP-R.5*)

4.2.3 Two Federated Bilateral Federations

In this pattern two independently operating bilateral federations are connected through the additional federation of their identity providers (see Fig. 2.c). The pattern is a logical combination of the previous two. Hence, one question is how the federation structure can enable direct access between service providers from separate federations. Again, the likeness principle can be applied. If the accessed service provider is sure to some extent that the external federation between identity provider A and its service provider is founded on the same policies as the local federation, it will allow delegated access without re-authentication.

Assets, threats, risks and trust requirements are the same as in the previous pattern. Additionally, the threat of unauthorized delegated access is addressed with the following risks and trust requirements, which were taken from the *Two Overlapping Arbitrary Federations* pattern and were adapted for the current pattern (*IdP-T.2* again applies unchanged).

Identity Provider B Risks

IdP-R.2b A service provider *federated with identity provider A* uses a legitimately obtained assertion to gain unauthorized access to a service provider, *which is part of the local federation*. (applies in addition to *IdP-R.2*)

Service Provider Risks

SP-R.4a A service provider (S) from a different federation uses an assertion to gain unauthorized access. The assertion was legitimately obtained from identity provider A. IdP A vouched that the service provider (S) acts on behalf of the user and IdP B trusted this voucher. (in addition to *SP-R.4*)

Trust Requirements

SP-T.3a The service provider has to trust its identity provider B to authorize only those federated identity providers for authorizing delegated access that adhere to certain agreed policies and procedures.

IdP-T.5 The identity provider B has to trust the the identity provider A to authorize only those federated service providers for delegated access that adhere to certain agreed policies and procedures.

4.2.4 Two Federated Arbitrary Federations

This is a logical extension of the previous pattern and therefore requires no further explanation. Assets, threats, risks and trust requirements do not change.

4.3 Summary

Figure 3 gives an overview of the cumulative risks and trust requirements of each presented pattern. What we can clearly observe is that the number of risks and requirements increases with the complexity of the pattern.

Of course, it is an arbitrary decision to stop with two connected federations. Theoretically, there could be a long chain of them with the ends of the chain engaging in an interaction. However, the probability that all intermediate IdPs show expected behavior decreases exponentially when the chain gets longer. In turn, the probability of negative consequences increases, and with it the risk. Hence, it becomes more and more complex to manage trust and ensure liability in case of a trust breach. Thus, it is to be expected that chains will not exceed a small number of participants.

5 Related Work

Research work considering explicitly the case of multiple federations has been conducted by Latifa Boursas [1].

She presents an approach to set up a Circle of Trust among overlapping federations. The idea is to include the identity providers which are in both federations dynamically into a virtual Circle of Trust. This constellation is described in our classification by the *Two Overlapping Arbitrary Federations* pattern.

Delessy et al. [3] present three architectural patterns for identity management which focus on constellations within one federation. They describe the following patterns: a Circle of Trust, which they define as a set of service providers federating their user's identity information, an Identity Provider Pattern, in which the users' identity data is administrated centralized and an Identity Federation Pattern, which describes the federation of identity data to service providers the user has no account with. In Delessy et al.'s considerations the focus lays clearly on the architectural and behavioral aspects, while our focus is on the trust requirements which must be met to establish a relationship between two entities. Furthermore, opposed to our work, there are no patterns for multiple federations.

Jøsang et al. [5] define trust requirements for several identity management models. Besides the federated identity management model, they also consider other models as the isolated or the centralized identity management model. In their paper, they focus on the trust requirements of the users into the service and identity providers as well as on the trust relationships between identity providers and service providers. Our work explicitly concentrates on the federated identity management model and extends their studies by considering also scenarios with multiple federations.

6 Conclusion

Managing digital identities across trust domains is crucial to improve efficiency of business collaborations. Before sharing user data between trust domains, all involved parties need to be trusted. Setting up a federation for Federated Identity Management is one way of providing the necessary platform for collaboration. However, the variety and complexity of trust relationships in business scenarios is not representable solely by federations. One reason for this are the complex contracts necessary to set up a federation making them unsuitable for short-term business relationships. In such cases, building up a trust relationship across federation borders can be a promising and cost-saving option.

In this paper, we identify possible trust patterns, which are observable in identity federation topologies. Based on a risks analysis, we precisely discuss the trust requirements of each pattern. In particular, our study provides a foundation to assess the effort necessary to meet the trust requirements when setting up a federation. Our results can be used to compare different federation strategies, i.e. establishing federations with all business partners versus leveraging existing, but more complex, trust structures.

A look at current standards shows that all identified patterns can be realized with state-of-the-art technologies. However, trust requirements are rarely described in detail so far. Current specifications assume that a trust relationship exists without stating concrete qualities. We believe that some standardization work might still be necessary to manage digital identities in a truly efficient and for the user convenient manner, while at the same time not jeopardizing a user's privacy. For example, a standardized description is necessary to express trust requirements at system level. This would enhance system control of fine-grained trust requirements in a federation relationship. We plan to address these issues in the future.

References

[1] L. Boursas. Virtualization of the Circle of Trust amongst Identity Federations. *1st International DMTF Academic Alliance Workshop on Systems and Virtualization Management: Standards and New Technologies*, Oct 2007.

[2] S. Cantor, J. Kemp, E. Maler, and R. Philpott. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, 2005. OASIS Standard.

[3] N. Delessy, E. Fernandez, and M. Larrondo-Petrie. A Pattern Language for Identity Management. *2nd IEEE Int. Multiconference on Computing in the Global Information Technology*, Jan 2007.

[4] J. Hughes, P. Madsen, E. Maler, R. Philpott, N. Ragouzis, and T. Scavo. Security Assertion Markup Language (SAML) V2.0 Technical Overview. http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf, 2008. Commitee Draft.

[5] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, and S. Pope. Trust requirements in identity management. In R. Buyya, P. D. Coddington, P. Montague, R. Safavi-Naini, N. P. Sheppard, and A. L. Wendelborn, editors, *ACSW Frontiers*, volume 44 of *CRPIT*, pages 99–108. Australian Computer Society, 2005.

[6] H. Lockhart, S. Andersen, C. Kaler, and Nadalin, A. et al. Web Services Federation Language (WS-Federation), Version 1.1. http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/WS-Federation-V1-1B.pdf, 2006.

[7] D. H. McKnight and N. L. Chervany. The meanings of trust. *Technical Report, University of Minnesota*, 1996.

[8] A. Nadalin, M. Goodner, M. Gudgin, A. Barbir, and H. Granqvist. WS-Trust 1.3. http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/ws-trust.pdf, 2007. OASIS Standard.

[9] D. Povey. Developing Electronic Trust Policies Using a Risk Management Model. In R. Baumgart, editor, *CQRE*, volume 1740 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 1999.

[10] J. Tourzan and Koga, Y. et al. Liberty ID-WSF Web Services Framework Overview, Version: 2.0. http://www.projectliberty.org/liberty/content/download/889/6243/file/liberty-idwsf-overview-v2.0.pdf, 2006. non-normative specification.