PROCEEDINGS OF SCIENCE

User Centric Identity for Grids and Clouds

Luděk Matyska*
Masaryk University, Centre CERIT-SC, Botanická 68a, 602 00 Brno, Czech Republic
E-mail: ludek@ics.muni.cz

Michal Procházka
Masaryk University, Centre CERIT-SC, Botanická 68a, 602 00 Brno, Czech Republic
E-mail: michalp@ics.muni.cz

Identity federations are becoming more and more discussed and deployed as new means to proof our identity in the digital world. Both Grids and Clouds are trying to incorporate identity federations to allow for much easier access to the infrastructure, with clouds best suited due to their web based access nature. However, the more widespread use of identity federations also reveals their drawbacks and limitations, both in technology and with the legal implications. These are demonstrated using our long experience with a service included in high number of national federations. A post-federated Aditi system is then presented as a possible solution, putting users in the centre. This overcomes the legal problems and also provides a fine grain control over information directly revealed to a service provider. The Aditi architecture utilizes current SAML based identity federations as much as possible and requires only minor changes to the data flow. Therefore it can be deployed in existing national identity federations without any obstacles and cloud service provides can start to provide their services to huge amount of users who have an account in the national identity federations without initial barriers. At the end of the paper we also briefly touch the complementary problem of the trust between identity and service providers and give a short introduction into proposed automatic system for trust management in the proposed Aditi schema.

The International Symposium on Grids and Clouds (ISGC) 2012,
February 26 - March 2, 2012
Academia Sinica, Taipei, Taiwan

*Speaker.

PoS(ISGC 2012)035

1. Introduction

Distributed infrastructures usually require proper authentication and authorization of the users in order to deliver the right set of services to the correct users. Grids and clouds as primary representatives of such distributed infrastructures are not an exception. Limiting access to the specific set of resources together with accounting creates demand on the scalable, robust and user friendly AAI infrastructure.

The most used AAI infrastructures in grids and clouds such Kerberos or X.509 certificates possesses several problems which make them hard to use by ordinary user, not an IT trained user. Kerberos does not scale well, X.509 certificates besides their indisputable technical qualities are not user friendly.

Promising solution for the AAI infrastructure in the distributed environments represents identity federations, which utilize existing identity management systems at users' home organizations. User uses her home organization credentials to access the remote service without disclosing them to the service. Although the solution by its design solves problems with scalability, user friendliness and yet-another-user-account, it reveals new problems and challenges.

Because clouds are mainly maintained through the web page where the authentication and authorization is essential requirement, identity federations provides solution which significantly lowers the bar needed for introducing the service for set of new users.

In the first half of the paper we will discuss in detail problems of the SAML based identity federations, which are widely spread in the academic environment. The second half of the paper will present system Aditi as an solution for the discussed problems. Aditi does not try to solve only the current identity federation problems but brings also new features.

2. SAML based Identity Federations

An identity federation is an infrastructure connecting identity management systems from different institutions with service providers (SP), which require authenticated user and may require additional information for authorization decision. Basically identity federations enable to share information about the users through a standardized protocol that is accepted by every party in the federation. Identity federation concept recognizes two main entities, identity providers and service providers. An identity provider service is built on top of identity management of the organization which manages its own users, providing an interface to access authentication information and other attributes about the user, like name, affiliation and unique identifier. Service providers in the federation can obtain this information redirecting user authentication request to proper identity provider and collecting attributes in case of successful authentication. These are used to make authorization decisions at the service level. Service provider does not need to deploy and maintain its own users' management system, instead the identity management system at user's home institution is used for authentication, providing also some data used in the authorization.

The concept of identity federation can be described on next simple example. A user visiting a federated service is first checked and if no authentication information is known to the service provider, the user is redirected to his or her identity provider web page. After the user has successfully authenticated with the identity provider, the identity provider creates a response containing

confirmation of successful authentication and additional information about the user in form of attributes. The response is then sent to the service provider, which verifies the validity of the response and extracts information about the user. Finally, the service provider makes an authorization decision and lets the user in or not.

Therefore, the user needs to maintain only one account and one set of credentials for all service providers within the federations. These credentials are only managed on the identity provider side and not available to service providers, which enhances their security. Identity federation concept is implemented by several frameworks. The most used frameworks in academic environment are SAML based [1] and OpenID [3]. We will focus on SAML based because they are well accepted by the academic institutions and currently there are tens SAML based academic identity federations run in production.

3. Drawbacks of SAML based Identity Federations

The current concept of federated identity includes systematic problem due to the need of direct interaction between identity and service providers. This leads to legal implications, as potentially private data are sent from one organization to another. The identity providers are therefore reluctant to send such information to unknown service providers, requiring formal agreements before any authentication is provided.

A slow formal process must precede any use of an identity provider for each service provider, creating 1 to 1 relationships between them. Also, each service providers must keep precise information about conditions and constraints, that differ from identity federation to identity federation and sometimes even between individual identity providers in a federation. Also, service provider must actively convince each identity provider that the specified set of attributes is really needed for providing the service.

This approach does not scale, an identity provider has to know about all the service providers and each service provider must negotiate with each federation (in worst case with each identity provider) before users are allowed in. User's consent given during authentication is considered not sufficient legally to free identity providers from legal responsibility of revealing personal information about a user. The negotiation process can take quite a long time, during that period users cannot use the service. If the SP provides services to wide range of users all over the world, full operation of such service cannot be done in a reasonable period. Agreements between identity federation operator or identity providers and service providers have limited life time and from time to time the agreement changes, both in technical or legal requirements. Service providers need to maintain all these agreements and continuously checks if they still comply with them.

Another obstacle is with the single point of failure. An identity provider must be present during the authentication process, when the identity provider is in error, users cannot access any service. Enabled single sign-on on the identity provider side can help to decrease probability of service provider unavailability due to identity provider error. Service providers are in a hard position, because they have to somehow inform the user about an error on the identity provider side and have no way how to quickly fix the problem.

Some service providers may need attributes that are not all kept by a single identity provider. The current SAML based identity federation does not provide means to collect attributes from

several identity providers or to extend the set of attributes with some additional information (e.g., an optional information service provider is asking directly the user for better personalisation of the service).

4. Experiences with Service Provider

Since late nineties we run an extensive digital atlas of histopathological images in high resolution[1] and since 2007 we started to include this service into identity federations worldwide. Currently, the Atlases are available as service for 15 national identity federations in 4 continents. We started to introduce service to identity federations in situation when most of the federations were not yet well prepared to adapt SP from foreign country. As a result, we had to deal with several problems. They can be divided into two main categories. First one represents problems during initial phase of joining the federation. The second one covers obstacles during normal operation of the service.

It is worth mentioning that the Atlases is service provider which requires the lowest set of attributes, particularly only eduPersonTargetedId or eduPersonPrincipalName attribute is needed. An email attribute is optional and is used only to ease user registration process. First category of the problems is the harder one. Service provider operator must check all rules and conditions of each identity federation which usually means read and accept the agreement, identity federation rules and technical requirements. Mostly the agreement must be signed by the liaison person who can delegate administration of the service provider to someone else. The agreement or identity provider national law can require special users' data handling (selective cleaning, anonymization rules, ...). Technical requirements have on the other hand significant impact on the service provider, because some of the requirements can collide among several identity federations, for example digital certificates. Service provider in most cases has to fill sheet which describes the service, however this description is not unified.

Running service as a service provider requires continuous maintenance. Identity federations technical requirements change from time to time, for example it could be due to moving to new profile. The Atlases currently using four different digital certificates because of various demands from the identity federation operators. Also SAML specific session initiators differs between identity federations. Some federations require annual report or change the policy, so the agreement must be signed again.

5. Problems to be addressed

User should have complete control over the information released about her from the identity provider. Ideally not only view them, but organize them, such as add/remove particular attribute from the set of released attributes. Situation when the user will have an account at several identity providers is not so improbable, therefore user should be able to combine attributes from different identity providers.

Trust should be moved where it is really needed. Only service provider has to know the validity of the information provided. The identity provider currently needs to assess the service provider as

[1] `http://atlases.muni.cz/`

some information is directly exchanged between them. If we put another agent—the user—in this flow, identity provider doe snot need any information about services and their providers. In this model, service providers should have a system which helps them to assess the trust of each identity provider, ideally without need of manual checks and negotiations.

The dependency on running identity provider during login process must be removed. Access to the service provider should not be synchronously dependent on the identity provider.

6. Aditi

The current problems and issues could be overcome with *a user centric identity federations*. In this model, users are put in the middle of the information flow between identity and service providers. Users collect information from identity providers and users reveal any necessary information to service providers. However, users are not just a proxy, they can actively participate in the process, selecting which information is revealed or even adding some additional information, too. It is easy to work with several identity providers, are user can approach each one of them in advance, before actually contacting the service provider. Identity providers issue digital tokens (in form of *cards* like in a card deck). These cards contain specific information (particular attribute) about the user. Each card is signed and has a validity timespan, user can not tamper with individual cards but he can build different card decks corresponding thus to different requirements of individual service providers. This design mimics ordinary behaviour of a person in a society, where institutions or companies issue identity cards with the user's information and the user decide which cards (i.e., which attributes) he shows to third parties (and some parties require more than just one card, i.e., birth certificated and driver license).

6.1 Design

As an solution we have designed a new system for user centric identity federations, which is called Aditi[2]. As we did not want to create yet another identity federation system, we tried to maximally utilize current SAML based identity federations. Aditi enhances traditional SAML based identity federation with three new components: (i) user's identity provider, (ii) user's service provider, and (iii) card selector. All these components run on the user side and helps user to have full control over the attributes released by her identity provider(s). Existing components, such as identity provider and service provider requires only minor changes and will be backward compatible with clients which are not Aditi aware.

Interaction both with identity and service providers, the user must operate both ends—user's service and identity provider, which consume and issue the attributes, respectively. Institutional identity provider talks only with the user's service provider and only the user's identity provider talks with the service provider, as shown in Fig. 1. There is no need to change the communication interface on service and identity provider side. User also operates user's card selector which manages her own and received attributes, the user can use the attributes to create her own cards, that will represent different user's digital identities. User provides created cards through the user's identity provider to the service provider.

[2]Aditi means "boundless, entire" or "freedom, security" in Sanskrit.

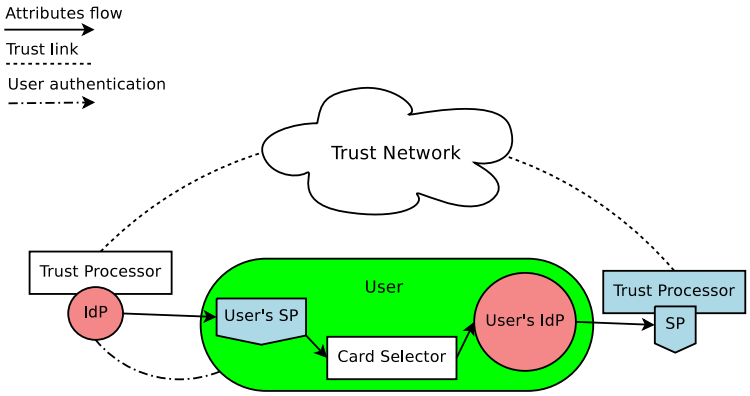

Figure 1: Aditi Model

Compared to systems like CardSpace [5] or Higgins [4] which use cards as well, Aditi use the cards actively. User can add her own attributes (usually used for personalisation) to the card, combine attributes from different identity providers into new cards.

The user does not work as a proxy in communication between identity provider and service provider anymore, it actively enters into the communication and completely breaks the direct communication between them. This approach makes the trust link between the identity provider and service provider only one way. In Aditi the service provider has to trust the identity provider, but not the other way round. The identity providers only communicate with the user. When the user needs attributes from her home organization, she simply authenticates with the identity provider as in a common identity federation, making the identity provider release all attributes to the user's service provider. The user can repeat this step with all the identity providers where she has an account. The user's service provider then provides these attributes to the card selector, where the user can create cards containing any of received attributes together with attributes created by her own.

In our model, a user who is contacting a service provider has to select one of the digital identities (card) containing appropriate attributes. Like in the real world, the service provider needs to know who issued the attributes about the user. Therefore, the service provider must be able to determine the level of trust of the identity provider. Trust management will be discussed in the next section.

6.2 Comparison with existing frameworks

Aditi reduces the communication between the identity provider, user and service provider. Current identity federation frameworks requires user to contact the identity provider before accessing the service provider. In Aditi, the user gets all attributes from the identity provider(s), therefore every consequent communication with the service provider does not involve communication with the identity provider. Temporary identity provider unreachability does not influence service provider operation. From the performance point of view, the identity providers are contacted fewer times since the communication is moved to the client side and performed in advance.

Furthermore, compared to other frameworks like OpenID or Shibboleth, Aditi does not require the HTTP redirection functionality or cookies.

Since Aditi tries to be an enhancement of the existing models, it is obvious that it provides all functionality as the original models do. Aditi aware identity provider can still serve current clients. In addition, we have solved the issue of provisioning of the service provider to the identity federation; service provider can join the federation without any negotiations made with any identity providers or any other party, like the metadata operator. The identity providers and service providers are part of the identity federation without being listed in any central registry, furthermore, the identity providers do not have any connection with service providers. Therefore, the model does not present any obstacles, which can limit the scalability. Our model decreases the communication cost of a service request, since no redirections are involved and all necessary attributes can be supplied by the user in a single message.

In order to make identity and service providers Aditi aware some changes must be done. Identity provider must sign each attribute separately, so the user is not able to change the values of the attributes released by the identity provider. User can create card decks with attributes from different identity providers, keeping the authenticity of the attributes untouched. Service provider must be able to verify signature and origin of each attribute. Because SAML messages are XML based, therefore additional information in form of attribute digital signature will not influence service providers which are not Aditi aware.

6.3 Legal consequences

As the attributes are revealed to the service provider by the user and the identity provider only confirms it (with its digital signature), the legal liability is no more relevant. The set of attributes within cards can range from small set (just name and eventually e-mail address) to very complex sets (combined information from several identity providers, with age, professional affiliation, position, even health information etc.). During the authentication process, user submits appropriate card (like showing a library card to a librarian) to get an access. It is user who reveals this information, again no third party could be held legally liable for the disclosure. This approach increases the probability that service provider will receive more information about the user, thus can make more precise authorization decision. Also, using a token in a possession of a user makes the authentication (and subsequent authorization) process just a two parties process (user and service)

6.4 Service provider provisioning

The Aditi system reduced substantially the administrative overhead associated with joining the service provider into the federation. The service provider only makes its own trust anchors with the identity providers. Identity providers and even federation operators are not involved in the service provider joining process, it's done solely on the service proved side.

The architecture of the Aditi utilizes current SAML based identity federations as much as possible and requires only minor changes to the data flow. Therefore it can be deployed in existing national identity federations without any obstacles and cloud service provides can start to provide their services to huge amount of users who have an account in the national identity federations without initial barriers.

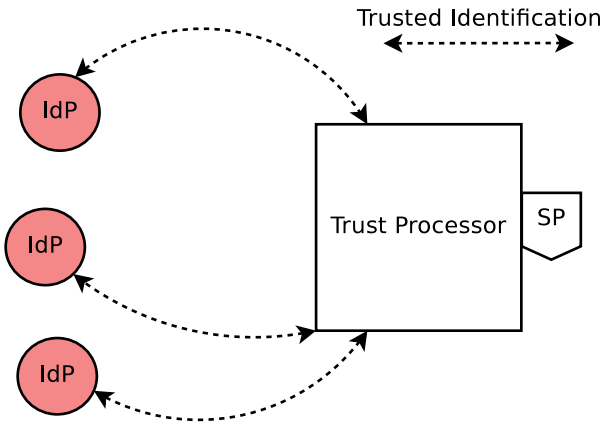

Figure 2: Aditi Trust

6.5 Delegation

The Aditi can also support a delegation, with a card created and signed by the user (including relevant information signed by identity providers) and "given" to a particular service for use when acting on user's behalf. In order to lower risk of misuse the card can have expiry time. If we want to delegate some attributes in secure way to the target service, the public key of the target service can be used to encrypt the attributes.

6.6 Trust Management

As was mentioned, the service providers in Aditi have only unilateral trust relationship with identity providers. Ordinary SAML based identity federation uses special XML document called identity federation metadata, which holds identification of all trusted entities in the federation. The metadata are managed by the identity federation operator. There are usually policies and premises which must each entity fulfill in order to get into the metada. Identity providers searching metadata to check if the service provider is the one who it claims to be. In Aditi only service providers uses information from the metadata document.

Aditi trust management helps the service providers to find out the trustworthiness of identity providers in order to trust the attributes. An identity federations' environment is very dynamic, with service providers and identity providers entering and leaving it from time to time. Therefore, we cannot use any static data set for measuring the trust. We have designed a trust network, which will be used to gather and propagate information about entities to evaluate the identity provider trust level. The trust (depicted in Fig. 2) in Aditi is based on one-way trust like in the real world. The institutions that need to check the identity of a person usually require the client's national ID card, so they trust the issuer of the card without the issuer having to know them. Each service provider could be equipped with a new component called *Trust Processor*, which is connected to the *Aditi Trust Network*.

The *"Aditi Trust Network"*, depicted in Fig. 3, is a decentralized network, which models the relationships between the service providers and identity providers. We intend to employ the peer-to-peer concept to build the trust network. The entities (service providers and identity providers) have to be able to organize themselves into groups within the trust network, with each group defining

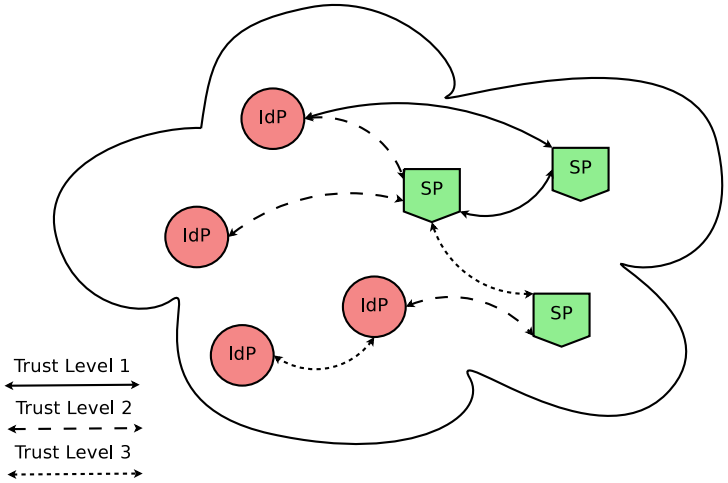

Figure 3: Aditi Trust Network

different levels of trust. The entities within one group trust each other and every entity can be bound to multiple groups. An entity can contact another one and ask it for its identification or information about the entities which are known to it. The obtained information is used for computation of the trust level.

The *"Trust Processor"* is connected to the Aditi trust network. It gathers information from various sources like identity federation metadata, X.509 certificates and certificate authorities and computes the level of trust for each issuer (identity provider). The trust processor provides a set of trust modules for the trust level computation. Some of the modules are exact, like a PKI one, where trust is defined by design. Other modules use methodology from the reputation systems and utilize the trust network through the *Trust Network Node* to get the data. A very promising solution for the reputation modules is provided in [2], where the author proposed using hypergraphs to build a reputation system for peer-to-peer networks. We plan to adopt this approach in our trust network and trust processor.

The trust processor can also be used by the identity provider to obtain the trust level of other identity providers. A hierarchy of the identity providers will certainly decrease a number of the credentials that a user needs to maintain. The approach is again taken over from real life. For example, banks accept the national ID cards as a proof of identity (authentication) and then issue a payment card, which is a different proof of identity. Generally, one identity provider accepts attributes from a different trusted identity provider as a sufficient proof of identity instead of requiring use of the credentials (e.g., username and password).

6.7 Complementary Features

SAML based identity federations are focused on the web environment, Although more and more services becomes available through the web browser, where the SAML based identity federation provides suitable solution, there still remains a big portion of non-web applications which require user's authentication. Aditi can help through its ability to store user's credentials and attributes from identity providers at the card selector, allowing it to make conversion of the credentials

into other type like Kerberos or X.509 certificate.

There is still uncertainty about new regulation approved by the Council of the European Union which requires the user's consent when a web server wants to store cookies in the user's browser. In Aditi, where the user operates the user's service provider and user's identity provider, we do not need to use cookies at all. The user's identity provider can send a complete set of attributes in every request to the service provider.

Scalability, which is a problem of Shibboleth, is solved by the design itself, since there is no central point in the proposed model. Provisioning of the new identity provider or service provider does not require any communication with other entities in the federation. No entity in the federation needs to know the whole state of the federation and the process of transferring attributes from the identity provider to the service provider only involves these entities. The trust network also does not have scalability problems, because it is built on the basis of a decentralized peer-to-peer network.

7. Conclusion

Based on our experiences with running service provider in tens of identity federations, we have designed post-federation concept based on user centric identity federations. The user is the one who controls which information in which form and to whom it will be disclosed. This approach solves problems with legal liability of the identity providers and significantly eases service provider provisioning. We have also presented system Aditi which implements the idea of the user centric identity federation. Aditi also provides system which helps service providers to compute the trustworthiness of each identity provider.

Grids and clouds systems can benefit from Aditi, they will be able to provide the services to huge amount of users by simply selecting trustworthy identity providers. Also access control lists could be much more precise, because users can provide any information which their identity provider holds.

8. Acknowledgment

Financial support of project CERIT-SC No. CZ.1.05/3.2.00/08.0144 is highly appreciated.

References

[1] S. Cantor, J. Kemp, R. Philpott, E. Maler and et al., *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS, 2005.

[2] R. Špánek, "Self-organizing and Self-monitoring Security Model for Dynamic Distributed Environments", PhD thesis, Technical University of Liberec, 2008.

[3] D. Recordon and D. Reed, "OpenID 2.0: a platform for user-centric identity management", DIM '06: Proceedings of the second ACM workshop on Digital identity management, Alexandria, Virginia, USA, 2006.

[4] "Higgins: Open Source Identity Framework", Higgins [website], February, 2010, Available: http://www.eclipse.org/higgins/.

[5] D. Chappell, "Introducing Windows CardSpace", Microsoft MSDN [website], 2006, Available: http://msdn.microsoft.com/en-us/library/aa480189.aspx.