CRISP – WP16

Revised architecture document and development status

CRISP Deliverable D16.2

Document identifier:	**CRISP_D16.2.doc**
Date:	**10 May 2013**
Authors	**RI**
	10th May - First draft by Almudena Montiel Gonzalez
	19th September- Revised version by Lukas Hämmerle
	20th September - Revised version Almudena Montiel Gonzalez
	20th September - Section 7 (Roadmap) Revised by Lukas Hämmerle

Abstract: *This document summarizes the current developments for the Umbrella AAI system.*

FIM Architecture Document

CRISP – Cluster of Research Infrastructures for Synergies in Physics

Work Package 16

Table of Contents

1. Introduction

The main goal of the work done in the Phase 2 of the WP16 is to continue developing the federated identity system to broad the community of users.

In the last years, many solutions arose to solve the federation of identities, as this has been pointed out as a common concern for any kind of community, going from research, social networks, and banking applications. These solutions consist in enabling access to services in other institutes, using their credentials from the home institution, this is the so called *Federated Identity* and the way it is designed, set up and administered is *Federated Identity Management* (FIM). Furthermore, many national networks started to collaborate to benefit from each other. Every of them have implemented their particular solution, based mostly in de-facto standards, although there is still a lack of a common ground. The national borders and the different laws existing, indeed constraint international collaborations, as they stand for different administrations.

The concept proposed here is to enable to join different user communities, this is, different federations, crossing national and organizational borders, that we call *bridging*, explained further in this document.

In “D16.1: FIM Architecture Document” the architecture of a FIM system solution is described. This solution has been coined with the name of Umbrella [1], which points the fact that all the credentials of a user are unified under a unique identification. This system was developed, and is currently being implemented in the Photon/Neutron (P/N) community. Umbrella has been therefore postulated as the starting point for bridging federated identity systems, where use cases are heterogeneous and different to the P/N community. Further developments of Umbrella are the greater part of this piece of WP16 in CRISP project, and are focused on the design of a bridging solution covering other kind of federations.The need of Bridging is discussed first in this document (Section 2 The need of Bridging). The tool Authentic2 has been pointed in the Section 3 Background. Then, the proposal to solve bridging in the context of CRISP is described in Section 4 Bridging proposal within CRISP. In Section 5 Bridging prototypes, a description of the prototypes is given. The difference between web-based and non-web based resources is discussed in Section 6 Web-based vs Non-web based, and finally the outlook and future steps are described in Section 7 Roadmap and Future work.

1.1 Status quo

Several user communities have already federated access to their services. These users own accounts extensively in different communities, from commercial solutions to scientific organizations, including social networks. Those federations are islands on their own and do not share anything between each other. A user from one federation can only use services at that federation at a time.

Nevertheless, many of the existing federations have information in common and they often overlap. For example, a student at a University may be doing also some research for an organization and at the same time is subscribed to a social network, thus, he has credentials to three different federations: the university, the organization and the social network. None of these systems can benefit of the information from each other, and the user needs to remind the credentials to each federation. Hence, bridging federations is important.

Next, some relevant scenarios are described together with their FIM and the Authentication Authorization Infrastructure (AAI) solutions and federations.

Umbrella

The basis of the proposed common solution is an EU-wide federated user database. This system has been postulated as an AAI solution for the participating research infrastructures EuroFEL (PSI), ESRF, ESS, FAIR (GSI), ILL, and XFEL, and is explained in depth in the first document "CRISP WP16 FIM Architecture Document".

The Umbrella approach to FIM consists in a single central Identity Provider, which contains minimum information about the users to uniquely identify them, and a local part with further user information located at each service provider. This design provides a unique and persistent user identification, assuring confidentiality and delegating all the authorization tasks to the local Web User Offices (WUOs). The Umbrella uses an account linking to match central identities with the local ones. This central account still needs to be created at the Umbrella system. This procedure is actually similar to that used in many social networks to access to different internet services with an account from a specific social network.

A global system will only be sustainable on a long-term basis if it is a common one accepted by all facilities. At the moment of writing this document, Umbrella is already in a very advanced status and it is being implemented in several facilities. Therefore, it is considered already a good starting point for bridging and the most realistic scenario.

High Energy Physics

The High Energy Physics (HEP) community is very much present in this phase of development, specifically GSI-FAIR organization. This community is specialized in using particle accelerators and detectors. Depending on the experiment, beams of a certain kind of particles are accelerated and reach a high energy, up to when they are made to collide with each other or with stationary targets. In this moment detectors record the results of these collisions. In this extensive community access to computing resources is done through Grid technology [2], following the experience reached at the World Large Hadron Collider Computing Grid (WLCG) project [3]. This infrastructure allows already the users to access resources in a federated manner, through x509 certificates issued by the national accredited Certificate Authorities of the International Grid Trust Federation (IGTF) [4]. This distributed Public Key Infrastructure (PKI) accomplishes a high level of trust and fine-grained authorization.

This community is making an effort to avoid the user to deal with x509 certificates because this process leads to unwanted long administrative tasks. Several solutions already exist for this issue: CILogon and Terena Certificate Service, which generate certificates from web interfaces.

On the other hand, web accounts for accessing browser-based applications also exist in this community. Therefore, support for web based and non-web based, is required. Access to web based resources could benefit from standard solutions based on Shibboleth or SAML2. But for the access to the Grid, Shibboleth is not a solution. In this case, enabling the option of having a service that could generate x509 certificates from web credentials would simplify the user experience and also the administrative steps of delivering such a certificate.

In section 4.1 Umbrella-x509 is described how to bridge Umbrella to the PKI infrastructure.

National Research and Education Network (NREN)

In the past 10 years many NRENs [5] have established identity federations in their countries. These identity federations enable academic users to use their institute credentials to access services at other institutes, inside the same federation. In the context of the P/N community, where Umbrella has started, there are several NRENs such as, Deutsches Forschungsnet in Germany, JANET in the UK, SWITCH in Switzerland or Surf Net in The Netherlands, to which it would be useful for the users to bridge. Joining a single federation usually includes signing a federation agreement and following certain rules and standards.

Social Networks

Social networks are changing the way of using computing resources for the younger generations. These users expect to find no barriers anymore between personal and professional data, and to control what to share, when and with whom. This fact influences the way they use data, also at work.

In addition, social networks are federating identity of many of the commercial applications, commonly used. In general, web applications are increasingly relying on the intuitive and easy way of enabling access to their resources, taking information from the accounts existing in the Social networks, like Google, OpenID, Facebook, etc. This is a one-step process for accessing resources where users do not need to create an additional account, by hand, with another password to be remembered.

This leads to the necessity of an intuitive solution and friendly interface, which facilitates the access to resources.

EduGain

eduGAIN [6] is a SAML2 based interfederation service developed and operated by the European GÉANT project. It aims at interconnecting different identity federations worldwide by providing a common set of technical standards, rules and policies to secure the exchange of identity information in order to perform authentication and authorization. This allows the organizations participating in eduGAIN to support AAI-enabled services, which can be accessed by all eduGAIN-enabled users in the other participating federations. In order to join eduGAIN it is necessary to join a federation that already is part of eduGAIN. The benefit of this is that it is sufficient to join one single identity federation in order to get access to services of other federations, provided they are also part of eduGAIN.

As of August 2013 more than half of all known identity federations already are members of eduGAIN and many of the remaining world-wide federations are in the process of joining eduGAIN. The number of organizations (e.g. universities) that enable interfederation support via eduGAIN for their services is constantly increasing, which opens many new opportunities for research applications. Even though it is a European research project, eduGAIN embraces also non-European federations.

One drawback of eduGAIN currently is that an organization first has to join eduGAIN before a user can access any eduGAIN services outside his local federation. It takes organizations some time to join eduGAIN, therefore many organizations have yet to take this step and therefore not all organizations from the P/N community are yet eduGAIN enabled.

What to bridge

Ideally, the development of a service capable of connecting any kind of federation would be the definite solution, but federations hold different levels of assurance (LoA) and the complexity is too high for such a task. Determining what federations to bridge is therefore the first step. As mentioned before, in the context of P/N community already some NRENs have their own solutions. Those are examples of federations that overlap often in functionality, and users would benefit from the bridging.

A federation worth to bridge is eduGAIN as it already contains many organizations and services from many other federations. This is a very great-extended community and, at the moment of writing this document, is playing a key role in the federation of identities as part of GÉANT network. GÉANT is well placed in the Europe2020 project to make relevant contributions.

In addition, there is an interest from the HEP community to avoid dealing with x509 certificates administration. This community would benefit from the creation of such certificates from web-based credentials.

Furthermore, the majority of the users have accounts in commercial and social networks. Allowing a single interface for single-sign-on would have a positive impact for both, the user and the resources. Therefore, to bridge to Identity Federations as Linked-in, Google, Facebook, OpenID, etc. is also under consideration. However, those federations should also trust and recognize Umbrella as an identity provider in order to get a bi-directional bridge. This case is at the moment out of the scope in this project, because it would require rather lengthy negotiations.

In the Figure 1: Examples of federations where to bridge is shown the idea of having a unique Umbrella identifier that is linked to the other federations where the user has accounts. This way, the user only needs to remember the Umbrella credentials.

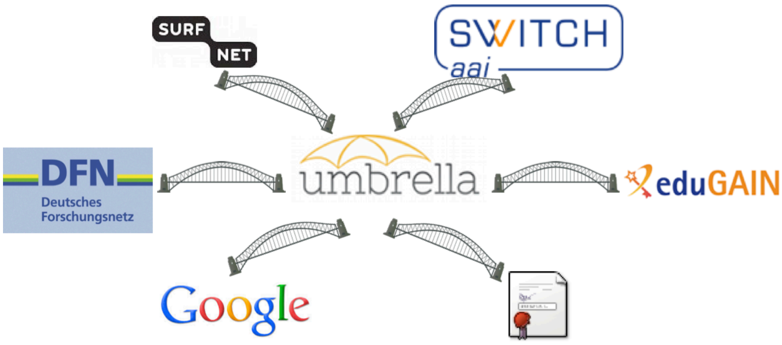


Figure 1: Examples of federations where to bridge

2. The need of Bridging

Setting up inter-federation services would improve user experience towards access to federations: it would enable a user from one federation to access a service in a different federation. The need of inter-federation connection has been already addressed from different kind of communities [7].

There are numerous advantages to bridge:

- Reducing the number of accounts to be remembered by the user.
- Harmonizing security interfaces consolidates a better integration of the resources.
- Having a central system for the users to access to federations eases the burden of administrators, by reducing the helpdesk activities.

- Improving privacy compliance by allowing the user to control what accounts to link.

- Reduce the overlap in between federations.

- Improving body of standards that is facilitating both connectivity and security.

- Participating parts could benefit of the detection of security risks, as those could be rapidly communicated to the rest. For example, an email detected in a black list, could be notified to the rest, saving time and risks.

2.1 Benefits

The scope of the present work focuses on the scientific community. This community has a special interest in a common approach to FIM, as it would benefit to join efforts. In particular, the research community relies on mobility and it is important to ease the users experience whenever resources in different institutions are required.

The interest to go in the same direction has been shown in the Federated Identity Management for Scientific Collaborations (FIM4R) series of workshops [7] [8]. State-of-the-art FIM implementations are discussed in these meetings, which are indeed closely related to CRISP, because it focuses on the scientific community. Umbrella has been present already from the first workshop, strengthening the concept of this alternative.

3. Background

Bridging was a necessity pointed since long, but never widely tackled. There are several solutions existing today in small scale that point to valuable designs.

Authentic2

Authentic2 [9] is an open-source, under GNU AGPL version 3, versatile identity provider. It uses the Lasso implementation of SAML2 protocol. It supports many protocols and standards, including SAML2, CAS, OpenID, LDAP, X509, OATH, and can bridge between them. As this has been pointed as a valuable input tool, a dedicated Annex has been elaborated, comparing this tool against an alternative which consists of a self developed LoginHandler based on Shibboleth.

4. Bridging proposal within CRISP

The consolidation of a wide amount of FIM solutions leads to the idea of bridging them. In order to solve bridging of federations, all the components involved need to be understood: Inside a federation, Identity Providers give information about users to Service Providers via user attributes. Attributes are given certain name and semantics. This semantics and the set of attributes supported is defined in the

Federation, and, therefore, understood by all the members inside. As each federation may use custom sets of attributes inside, new elements need to be in place to translate attributes between federations.

This has been subject of study for some time for eduGAIN. This approach was proposed by TERENA [10]. It requires a strong trust model among the federations, which must agree on the way the Identity providers (IdP) and SPs behave, to become interoperable. This is implemented through a set of policies [11] that every federation must adhere to, a profile [12] to ensure interoperability on a protocol level and a central metadata repository where metadata for Identity and Service providers that have opt-in to eduGAIN are aggregated. The elements in charge of "translation" of attributes among federations are called *mangling*, and consist on XML and regular expression library.

This approach is based on SAML2. Most of the NRENs have implemented their AAI solution in SAML2, which makes them technically interoperable with each other and with eduGAIN. Nevertheless, this approach is rather costly to implement, since several components need to be in place, and most importantly, legal agreements have to be set before hand. It implies a release of information of the users; hence, it has to fit to the data protection laws, which are normally making this process too long.

The **Umbrella** approach overcomes this complexity by enabling a user-initiated process. In this way, it drops legal issues involved with delivery of personal data. This makes the process a bottom-up approach and results in a better user experience, as the bridge is built on demand. It also eases administrative tasks, since the user would manage the bridging process. Only very light new components are added.

This linking of accounts has been coined as *bridging* in this document.

By *bridging*, a user that has got accounts in several federations, could access from a unique Umbrella account to services in the other federations. And vice versa, a user that has got an account in a federation, could access services of the Umbrella federation. Similar to an actual bridge, it would smooth differences among communities and improve mobility.

Federations hold different information for the users. It could even happen that the same piece of information for users has a different naming in different federations, for example the email address could be defined as “mail” or as “email”. Therefore, it is necessary to map such information into Umbrella, similar to the "translation" of attributes mentioned before with the eduGAIN approach. Also, it is needed a mapping between the unique identifier of the user, and the identities in the federations.

4.1 Design

There are two main use cases that are going to be explained further:

- The user wishes to create the bridge. The direction for building the bridge will be from the Umbrella federation to the rest of federations. The concept of Umbrella means to have this unique Umbrella-ID and from this, connect to all the others.

- The user wishes to login by using the bridge. Eventually, both directions will be built. Accessing services of Umbrella by using external credentials has been developed now for a couple of prototypes, and it will be explained in the section 4 Bridging prototypes.

Creating a bridge

To create the actual connection between accounts, a user of one federation must visit the federation interface where he wishes to join. The linking point will show a login for the wished federation and after successful login, the accounts are linked in a linking table, containing a unique identifier of the user from each federation. This process is shown in figure Figure 2: Building bridge.

There are a few new elements included in the Umbrella functionality in order to "translate" the attributes:

- Lookup table: this table contains the map of the Umbrella unique account to all the bridged accounts.

- Attributes mapping table: contains the map between the Umbrella attributes and the attributes in the bridged federation.

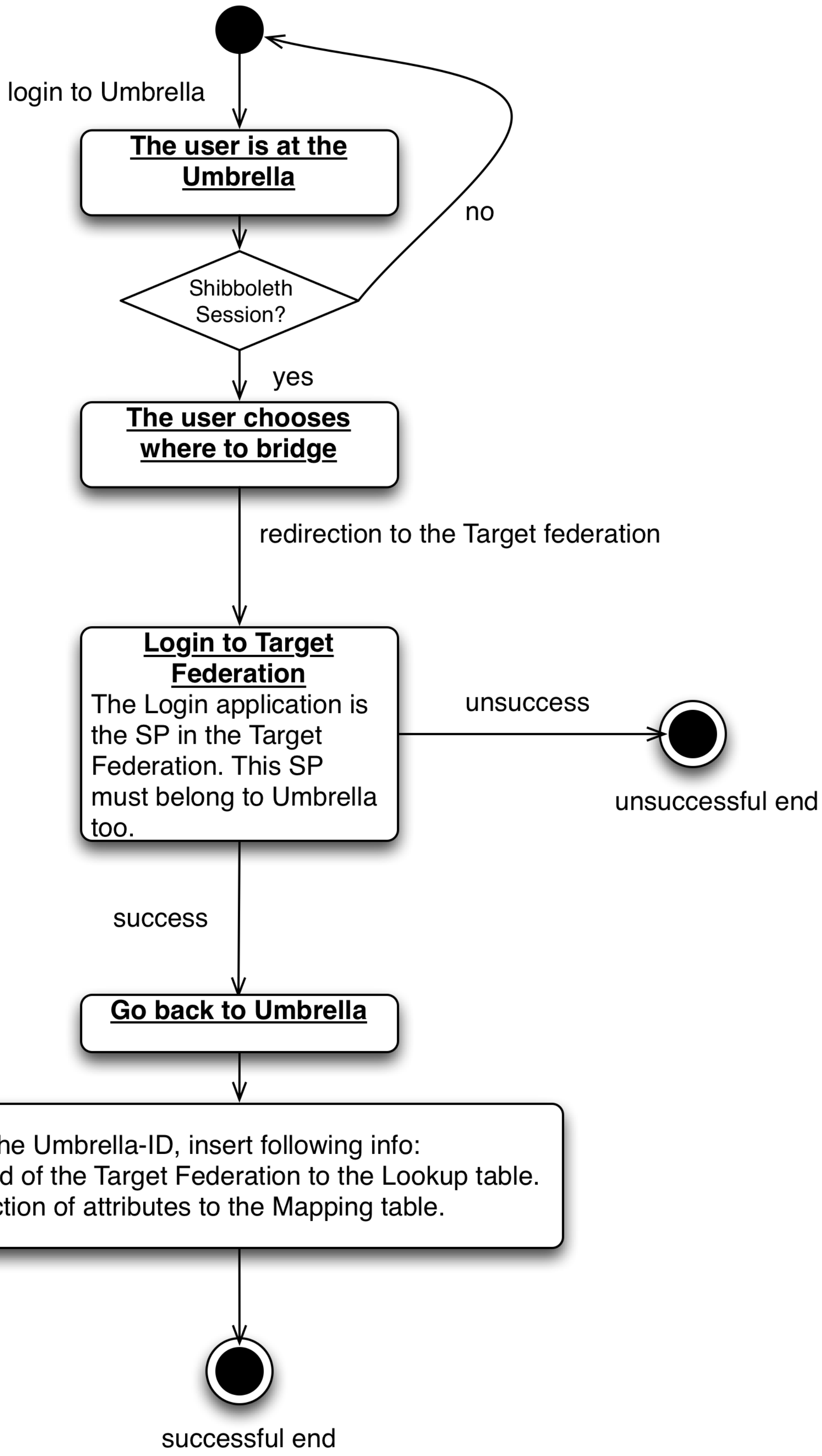
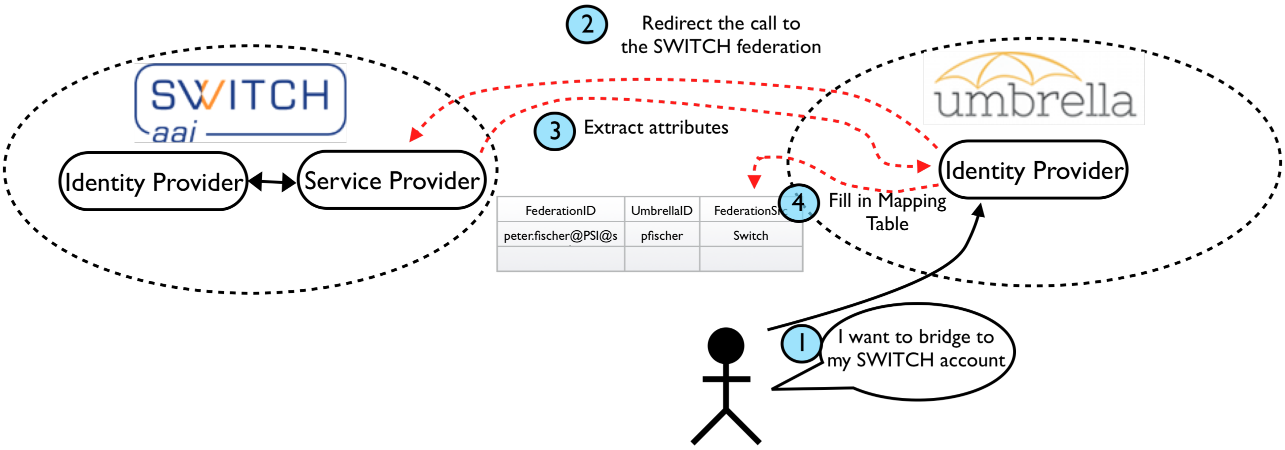

login to Umbrella
The user is at the Umbrella
Shibboleth Session?
no
yes
The user chooses where to bridge
redirection to the Target federation
Login to Target Federation
The Login application is the SP in the Target Federation. This SP must belong to Umbrella too.
unsuccess
unsuccessful end
success
Go back to Umbrella
Take the Umbrella-ID, insert following info:
- userid of the Target Federation to the Lookup table.
- selection of attributes to the Mapping table.
successful end

Figure 2: Building bridge



FederationID	UmbrellaID	FederationS
peter.fischer@PSI@s	pfischer	Switch

Figure 3:Building Bridge

The lookup table in the middle would look like Table 1: Linking of accounts, where three columns are shown:

- FederationID: a cross federation id.
- UmbrellaID: unique identifier of the user in the Umbrella Federation.
- FederationSource: the federation where the identity is coming from.

FederationID	UmbrellaID	FederationSource
peterfischer@ETHZ@SWITCHaai	pfischer	SWITCHaai
peter.fischer@PSI@ SWITCHaai	pfischer	SWITCHaai
p.fischer@DIAMOND@UKAMF	pfischer	UK Acces Management Federation

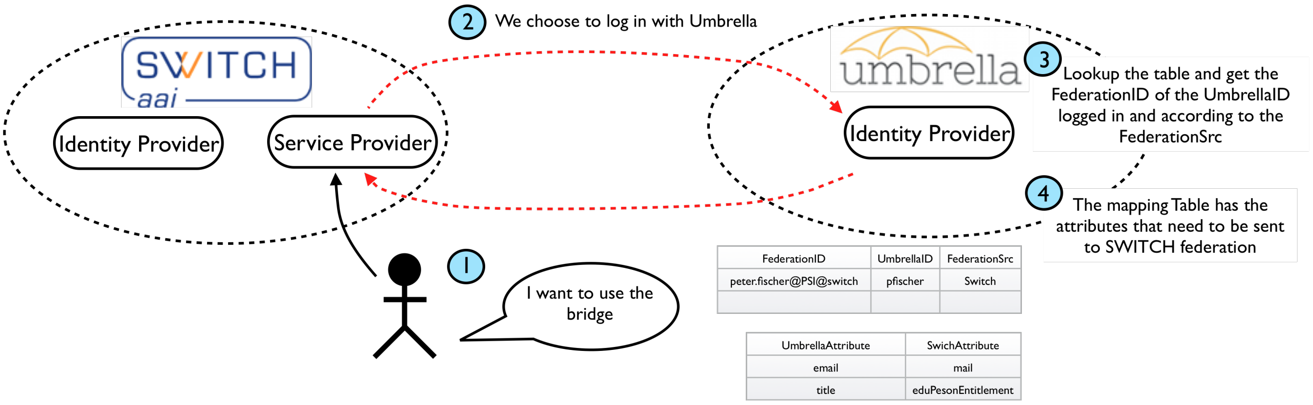
Table 1: Linking of accounts

This lookup table is filled in when the bridge is built, together with the attributes mapping table. These attributes are needed when accessing the bridge further. In order to access a service from the other federation by using the bridge, the set of attributes of the other federation need to be released, those are taken from the table.

<u>Log-in through the bridge</u>

A user wishes to use a Resource protected by a SP in an external federation. He is going to use the Umbrella credentials and has created a bridge to his account in the external federation.

The user will access the resource, and it will be asked to login. He gets redirected to the login page of Umbrella. He can create a session with the Umbrella credentials and, because the information is saved in the tables mentioned before, the information returned is the one mapped in those. Therefore the SP understands the information that gets back.


2 We choose to log in with Umbrella
SWITCH aai
Identity Provider
Service Provider
umbrella
3 Lookup the table and get the FederationID of the UmbrellaID logged in and according to the FederationSrc
Identity Provider
4 The mapping Table has the attributes that need to be sent to SWITCH federation
1
I want to use the bridge

FederationID	UmbrellaID	FederationSrc
peter.fischer@PSI@switch	pfischer	Switch

UmbrellaAttribute	SwichAttribute
email	mail
title	eduPesonEntitlement

Figure 4: Connecting through the bridge built

5. Bridging prototypes

Next are presented two prototypes that follow the previous proposal exposed. The complete use cases, requirements, and solution are explained.

5.1 Umbrella-x509

5.1.1 The use case: Grid

As mentioned earlier in this document, the HEP community is successfully running a Federated way of accessing the resources. The grid computing model implements the PKI infrastructure, using x509 certificates. This is one of the target use cases to bridge to Umbrella. In this community, GSI-FAIR [13] organization is a member in the CRISP project; therefore it represents the link to this kind of federation.

4.1.1.1 GSI-FAIR

GSI-FAIR is a new international accelerator facility for the research of antiprotons and ions. It is located nearby GSI-Darmstadt. The GSI facility – once upgraded and together with a new proton linear accelerator – will serve as pre-accelerator and injector for the new complex.

It will gather different experiments and collaborations. There are four main pillars: APPA Physics (Atomic, Plasma Physics and Applications), nuclear matter physics, NUSTAR (Nuclear Structure, Astrophysics and Reactions) physics and physics with High Energy antiprotons. Collaborative work is done among different institutions and Universities.

Different experiments have no conflict of interests, as they try to reach diverse goals. Nevertheless confidentiality of data owned by the user is crucial.

There are two major experiments at GSI-FAIR with very similar computation to HEP experiments: Antiproton Annihilations at Darmstadt (PANDA) [14] and Compressed Baryonic Matter (CBM) [15]. The Grid middleware adopted for those experiments has been AliEn [16]. This is a lightweight Open Source Grid Framework developed by the ALICE (A Large Ion Collider Experiment) Collaboration at CERN that offers to the end user a transparent access to distributed computing and storage resources all over the world. It constitutes the production environment for simulation, reconstruction, and analysis of physics data of the ALICE, and in 2004 was adopted for PANDA, establishing one of the computing solutions. This middleware provides federated access to computational resources as well as a central data catalog. The concept of Virtual Organizations allows to dynamically sharing resources among different physical organizations, joining together people working for the same project.

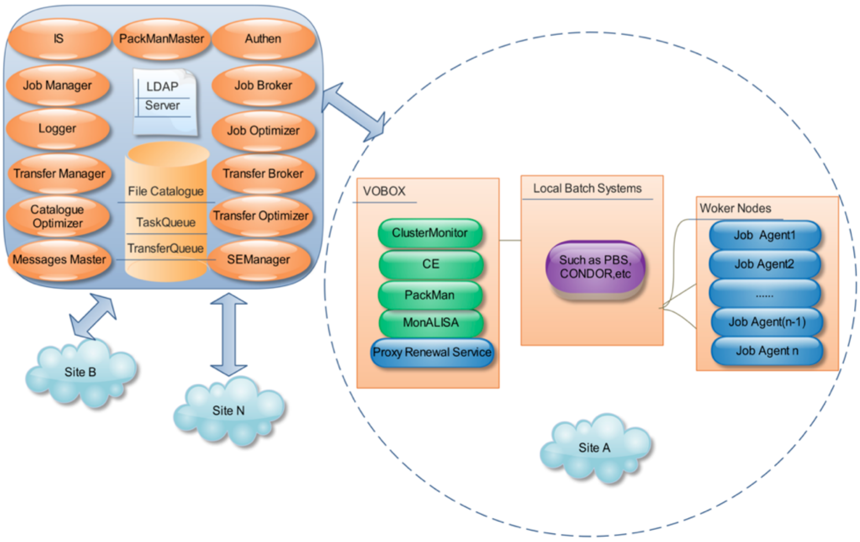


Figure 5: AliEn

The key processes involving authentication and authorization are described in Figure 5: AliEn. Authentication is implemented with x509 PKI. The SOAP messages are transported securely through SSL/TLS encryption. The x509 certificates provide each entity with a unique identifier and a method to assert that identifier to another party through the use of an asymmetric key pair bound to the identifier by the certificate. Proxy certificates are used in order to delegate credentials to remote servers and therefore to allow single-sign-on.

Authorization mechanisms are based on the File Catalog and the quota of each user, relating to job execution and amount of data. This mechanism is implemented inside AliEn and it is a step completely decoupled from Authentication.

Therefore, it is valid to consider that the majority of the users in the FAIR-GSI community hold their own personal x509 certificate.

5.1.2 Design proposal for bridging

The PKI model in the Grid is very scalable and efficient, but some users find it difficult to manage [18], because they have to manually deal with the request, installation, and possible updates of the certificates, and also because of the level of assurance required for a certificate to be trusted. Therefore, some communities have developed some solutions where the administrative tasks are removed by automatically providing certificates through, for example, portals or other tools inside a federation. Hence, a reduction on the administrative costs when having to manage new users.

In particular, Grid does not rely on web technologies. To accomplish the federated access to grids there are two main approaches:

- By leaving the federated identity management to the issuing authority, and generating certificates from accessible interfaces, like web or portals. This approach has been explored already explored from Terena Certificate Service and CILogon.
- Credential Conversion. This approach simply converts one type of credential to another; in this case the technical challenges are on the policy mappings and constraints and levels of assurance. One example in this direction is the EMI Translation Service that is used in the pilot project "CLI" from CERN. Nevertheless, this pilot project has demonstrated that translation of credentials, among other things, implies complex deployment and support.

Therefore, here the first approach is taken. Leaving the federation responsibility to Umbrella enables the possibility to generate certificates for a user from the portal, on demand.

There would be two directions of building the bridge, as seen in the *Figure 6: Bridge AliEn and Umbrella*.

The part of the left in this figure shows that through Umbrella, the user would get an x509 certificate generated from that Federation. Umbrella should be in the Certificate Authorities accepted by the AliEn Grid Federation, in order to be accepted. In this way, the provision of the certificate is immediate and automatic. Still, the authorization is duty of the Virtual Organization, as desired.

The right side of the figure shows the case when having already an x509 certificate. The user would have the possibility of building a bridge to the Umbrella Federation. As a result, the user could eventually have access to those Service Providers (SPs) in the Umbrella Federation, as the mapping would allow the user to release attributes to those SPs.

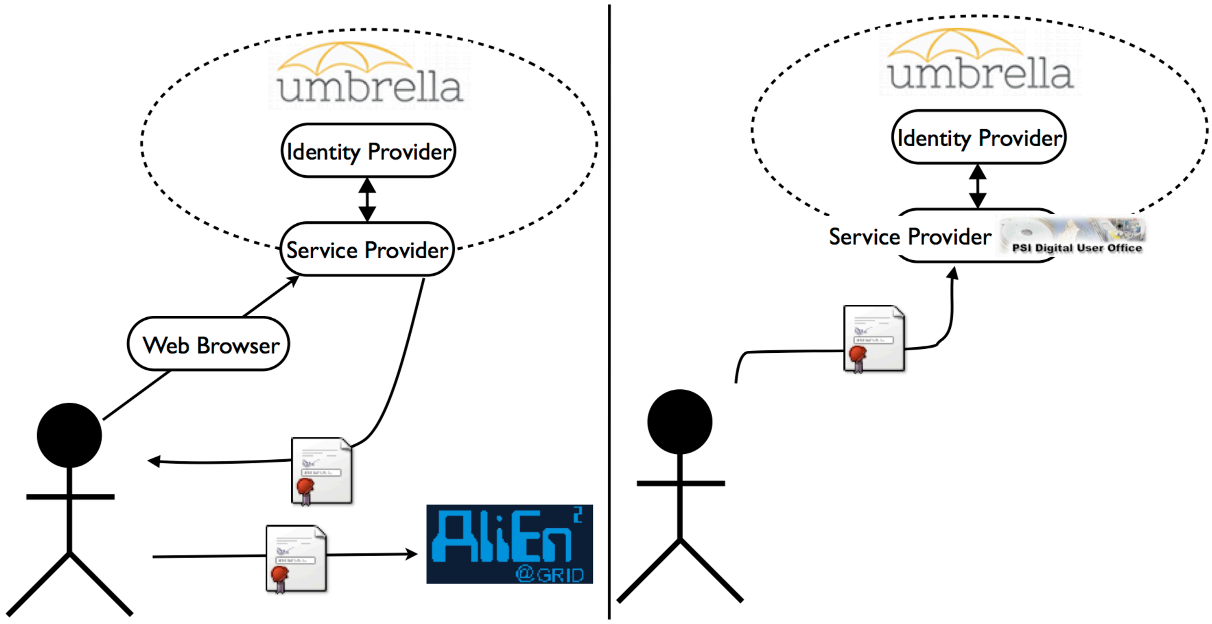


Figure 6: Bridge AliEn and Umbrella

Using x509 to authenticate to Umbrella

Umbrella needs to enable x509 login. Thus, the IdP must accept x509 certificates as a new way of authentication. For this, a x509 login handler [17] from the Shibboleth community is used.

This handler considers the certificates installed in the client browser. It extracts the subject information back to the IdP and sets the authentication context urn:oasis:names:tc:SAML:2.0:ac:classes:X509.

A new login page is also provided, that brings a new possibility for log-in, now with certificates. It is compatible with username password login, presenting in such front page this option too.

These two new components: handler and login page, should then be correctly placed in the handler configuration inside the IdP.

The authentication criteria for the certificates are defined in the web server in the IdP.

There are two phases when logging in: the authentication and, if successful, extraction of attributes. Attributes are extracted from the IdP Data Connector, such as LDAP, JDBC and so on. If the user authenticating is present in the IdP, attributes will be extracted.

A user that builds a bridge to this x509 certificate should authenticate with it. Upon authentication, the subject of such certificate is subtracted and transparently added a new record to the Lookup table that links this subject to the username.

Next, as the user wishes to use any other resource in Umbrella federation, he could choose either the certificate or the username/password of the Umbrella. When using the certificate, then, again transparently to the user, the subject is subtracted and the Umbrella identifier is looked up in the table. Since the bridge is built, then this Umbrella identifier is an existing user in the Umbrella federation.

Using Umbrella authenticate to x509

The project CILogon, already mentioned, aims to ease the administrative tasks of administering x509 certificates. It bridges the world of Institutional SAML Identity Providers and the world of Grid and Research Cyber-Infrastructure. Using CIlogon, a user with campus-provided credentials can download a relatively short-lived proxy certificate for user authentication by logging in to the CILogon service site. This can be used in both browser-based scenarios such as portals and in back-end service scenarios.

This functionality has been tested with a sample federation, and installed into AliEn Grid middleware at PANDA. This solution is promising for the expedition of x509 from the Umbrella federation.

5.2 Umbrella-eduGAIN

Creating a bridge between eduGAIN and Umbrella allows thousands of researchers to access Umbrella services via their institutional login. Using their login name and password they received from their university or research institution, they can access Umbrella services by first choosing their organisation and then authenticating at their organisation's login service. This works provided that the user's organisation is member in an identity federation that participates in eduGAIN. While this is not the case for all organisations participating in federations that are connected to eduGAIN, this is likely to be the case for most universities and research institutions in Europe and the Western world within a few years.

Allowing eduGAIN users to authenticate to Umbrella

The basic idea of this bridging is to extend the Umbrella Identity Provider (IDP) by a SAML Service Provider (SP) that protects the login service of that Identity Provider. The Service Provider then would have to become part of eduGAIN, which implies that it first becomes part of a federation (e.g. SWITCHaai) which is connected to eduGAIN. After a user authenticated at his home institution, the Identity Provider of his institution sends a SAML assertion to the Shibboleth SP protecting the Umbrella IdP login. Because the user managed to successfully authenticate at his home institution, the SP considers the user as authenticated and lets him access the Umbrella IdP login service, which then in turn can consider the user as authenticated based on the presence of any SAML user attributes. The Umbrella IdP login service should store the user's attributes in the LDAP directory that later is used by the

Umbrella IdP to resolve the authenticated user's attributes. In this step the attributes can be filtered, transformed and extended before adding them to the LDAP directory.

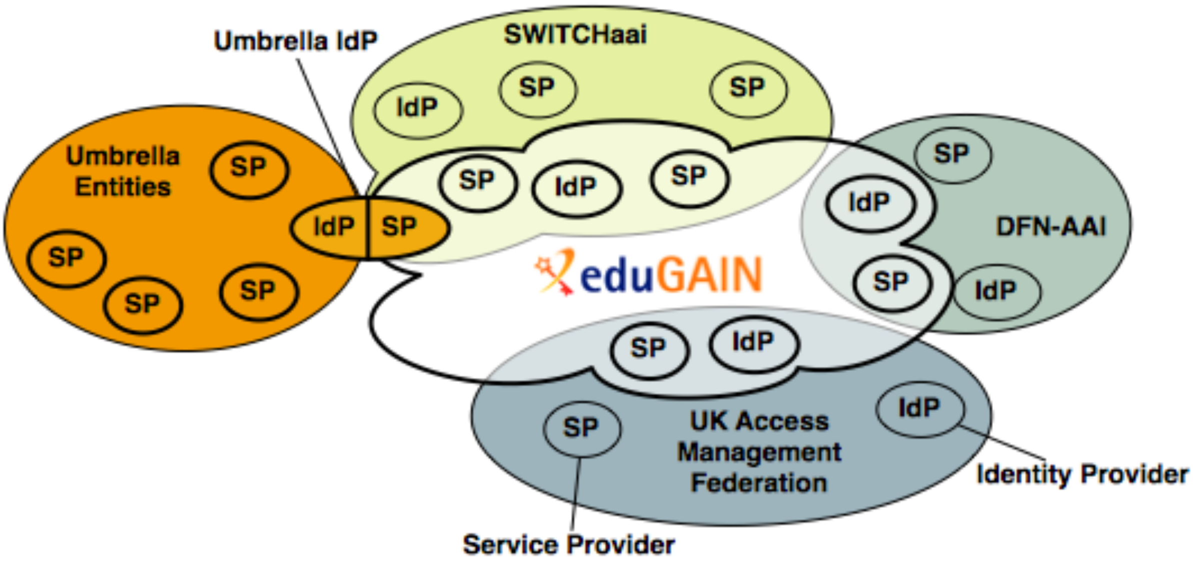


Figure 7: Umbrella and eduGAIN

Allowing Umbrella users to authenticate to eduGAIN services

Provided the Umbrella Identity Provider also supports SAML2 natively, it would be very easy to also expose it to eduGAIN. This then would allow all Umbrella users to access other services operated in eduGAIN.

In order to implement this, the Umbrella Identity Provider would have – as the Service Provider in the other case described above – to become part of a federation that is already connected to eduGAIN. Depending on the federation, there are specific restrictions and limitations when adding an Identity Provider to a federation. Most identity federations operated by NRENS in general accept only Identity Provider s operated by universities, research institutions and schools. Whether the Umbrella Identity Provider can be considered as such depends mostly on the Umbrella Identities. It is however likely, that the Umbrella Identity Provider could join any of the eduGAIN member federations.

6. Web-based vs Non-web based

As demonstrated along this document, a number of solutions are already available for federating access to web-based resources. That is, these solutions allow an organization providing services over the web to consume the identities of its research partners, business partners, customers or other affiliates. However, there is no good solution for to take these FIM solutions beyond the web such as e-mail, instant messaging, file sharing, or remote computing.

It is also of interest of this project to enable SSO federated solutions to access to computing resources and data storage. In this direction, Moonshot [18] is making an effort in implementing a SSO system for providing federated access to non-web-based resources using the eduroam [19] credentials.

Moonshot is an emerging tool that came to the picture of the FIM with the aim to cover the non-web based use cases, that, by the time the project started, there were no so good solutions, like the case of SAML for web based resources.

Moonshot proposes to combine three key security technologies: the Extensible Authentication Protocol (EAP), the Generic Security Services Application Programming Interface (GSS-API) and Security Assertion Markup Language (SAML) to create a solution for federated authentication. EAP is an authentication framework used in the eduroam federation for accessing to wireless network, while GSS-API simplifies integration with application protocols and applications, and SAML provides federation for the web.

The project is now in the phase of running a Pilot where different communities and use-cases will adopt this solution and bring it to a pre-production status.

This tool is particularly interesting; because the provision of the identities is done through SAML, hence open to connect to FIM solutions already existing.

Moonshot is also a good fit for Grid to ease the existing administrative tasks. The approach to be applied here would be the conversion of credentials, this means, authenticate users with Moonshot, and afterwards to convert this credential to a certificate. Here the technical challenges are in the correct conversion, ensuring that the attributes are fetched and converted appropriately.

Some steps have been done in this direction. To demonstrate the concept, there is a sample prototype of the Moonshot solution running on virtual machines at GSI. However, further progress will be left as a Future work because Moonshot is not yet recommended to be deployed or used in any infrastructure by the time of writing this document.

7. Roadmap and Future work.

The work done includes the implementation of a proof of concept bridging solution for X.509 authentication, which would cover a big part of the Grid community. This branch has been kept to a second stage during the development phase of this project, prioritizing the SAML2 federations use case. The SAML2 use case covers a wider set of users, in particular the eduGAIN community that includes users from identity federations all around the world. Therefore, a second proof of concept has been developed to create a bridge to SAML2-base federations. Some code has already been developed to implement such a bridge. It is available at https://github.com/flowedback/FederationBridge.

When developing a bridge for SAML-based federations, we learned about an open-source software called ‘Authentic2’. This software bridges between different protocols and different authenticating methods, which is exactly the case to be solved. As Authentic2 seemed to solve many of requirements and therefore is also an alternative, it has been tested and examined. A table that compares the two approaches, Authentic2 vs using Shibboleth with a custom login handler, can be found in Annex 1.

The brief conclusion is that the community of Authentic2 is rather small and the support as well as documentation seem to be rather limited. Generally, there is the risk that one gets stuck with a software that at some point may not be developed further. For these reasons it is preferred to take this tool only as a reference, but develop a solution based on Shibboleth and a custom Login Handler implementation. This proposal would be the starting point for a design proposal for a bridging solution in coordination with GÉANT3plus project.

Bibliography

[1]. **al., Abt B. et.** Umbrella. [Online] https://umbrellaid.org.
[2]. *The Anatomy of the Grid: Enabling Scalable Virtual Organizations.* **Forster, I. et al.** International Journal of High Energy Physics. 2.
[3]. **Grid, Worldwide LHC Computing.** [Online] http://wlcg.web.cern.ch/.
[4]. International Grid Trust Federation. [Online] http://www.igtf.net/.
[5]. **Wikipedia.** NREN. [Online] http://en.wikipedia.org/wiki/National_research_and_education_network.
[6]. **edugain.** Edugain. *Edugain.* [Online] http://edugain.org.
[7]. **al., Dan Broeder et.** *Federated Identity Management for Scientific Collaborations.* [Online] https://cdsweb.cern.ch/record/1442597.
[8]. **PSI.** FIM4R at PSI. [Online] http://indico.psi.ch/conferenceDisplay.py?confId=2230.
[9]. Authentic2. [Online] http://pythonhosted.org/authentic2/.
[10]. TERENA. [Online] http://terena.org.
[11]. edugain Policy Framework. [Online] http://www.geant.net/service/edugain/resources/Documents/Introduction%20to%20the%20eduGAIN%20policy%20framework.pdf.
[12]. SAML interoperable. [Online] http://saml2int.org.
[13]. GSI-FAIR. [Online] http://fair-center.org.
[14]. PANDA. [Online] http://www-panda.gsi.de.
[15]. CBM. [Online] http://www.fair-center.eu/for-users/experiments/cbm.html.
[16]. **al., Pablo Saiz et.** AliEn2. [Online] http://alien2.cern.ch.
[17]. Shibboleth x509 Login Handler. [Online] https://wiki.shibboleth.net/confluence/display/SHIB2/X.509+Login+Handler.
[18]. Moonshot. [Online] https://project-moonshot.org.
[19]. eduroam. [Online] http://www.eduroam.edu.au.
[20]. **IDaaS.** [Online] https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf.
[21]. Security Assertion Markup Language. [Online] http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf.
[22]. AAI needs for Distributed Computing Infrastructures (DCIs) EU EMI Project. [Online] https://twiki.cern.ch/twiki/pub/EMI/EmiJra1T4Security/AAI_DCI_v0.2.pdf.

Appendix 1

This appendix tries to analyze the tool Authentic2 as possible solution to implement the bridging within Umbrella. The analysis explores the functionality of this tool and compares it against an alternative which consists of a self developed LoginHandler based on Shibboleth.

The main motivation is to consider that pieces of work can be reused, therefore saved from Umbrella project workload.

The organization of this document is first to give a description on how to configure and use the Authentic2 for our use case. This is use is to bridge federations. A central part would save the minimal information to be able to authenticate users into the system. Users would be able to link to other SAML2 federations, SSL systems, etc. The way is thought of being Umbrella the central part, where users are uniquely identified, and enable the possibility of linking such account with all other accounts that users might have in other federations in a persistent way.

In order to write a precise analysis, Authentic2 has been deployed on a server. The test-bed is composed by two different virtual machines, connected in the same private network for the sake of simplicity. The virtualization layer runs on kvm using qemu images. The first machine is called localidp.gsi.de and it runs Debian Wheezy with 3GB of RAM and 3.2 GHz. This machine deploys the elements of the IdP, this is: the Shibboleth IdP software, an LDAP directory with the Umbrella users, and the Tapestry web interface developed at PSI. The second machine is authentic2.gsi.de and it runs Debian Jessy with 512MB of RAM and 1.6 GHz. This one hosts the Authentic2 tool, which consist of Django Framework and is deployed into a Gunicorn server. Additionaly the django_auth_ldap is deployed in order to implement the authentication against the existing LDAP directory.

Additionally, Authentic2 Service Provider has been configured in 2 external federations: Umbrella test (Umbrella.psi.ch) and SWITCH.

The scenario is that Authentic2 will be the IdP with the LDAP backend running on localidp.gsi.de

Authentic2:

Authentic2 is an open-source software, developed under the GNU AGPL version 3. It is essentially a versatile identity provider that uses the Lasso implementation of the SAML2 protocol. Besides SAML2 it supports many protocols and standards, including SAML2, CAS, OpenID, LDAP, X509, OATH, and it can bridge between them.

The whole documentation on how to install and configure the tool is under http://pythonhosted.org/authentic2/index.html .

This tool uses the Django Framework and can be configured to run on different type of servers. The one that comes configured by default with Debian package is gunicorn. Authentic2 has a SQLite database as back-end for the application, and also for storing persistent data related to linking of accounts of users, as well as mapping of attributes among federations.

Installation

It is simple for Debian systems to add the specific repositories and install authentic2 package. This procedure deploys and configures authentic2 in the system. The main locations are:

/usr/lib/authentic2/manage.py - which is the main files that runs the application

/etc/authentic2/authentic2.conf – configuration file.

/usr/share/pyshared/authentic2 – python files of the application. Includes the settings.py file and urls.py file, that can be tuned for configuration.

Configuration

In the context of the Umbrella bridging, the goal is to make Authentic2 a SAML service provider proxy. Further information on this topic can be found here: http://pythonhosted.org/authentic2/config_saml2_idp.html

The basic steps:

- Configure Authentication with the existing LDAP. More info: http://pythonhosted.org/authentic2/auth_ldap.html. Specifically in the testbed, these lines have been added to the settings.py file:

```
##for the LDAP

AUTHENTICATION_BACKENDS += ( 'django_auth_ldap.backend.LDAPBackend', )

import ldap

from django_auth_ldap.config import LDAPSearch

# Here put the LDAP URL of your server

AUTH_LDAP_SERVER_URI = 'ldap://localidp.gsi.de:389'

# Let the bind DN and bind password blank for anonymous binding
```

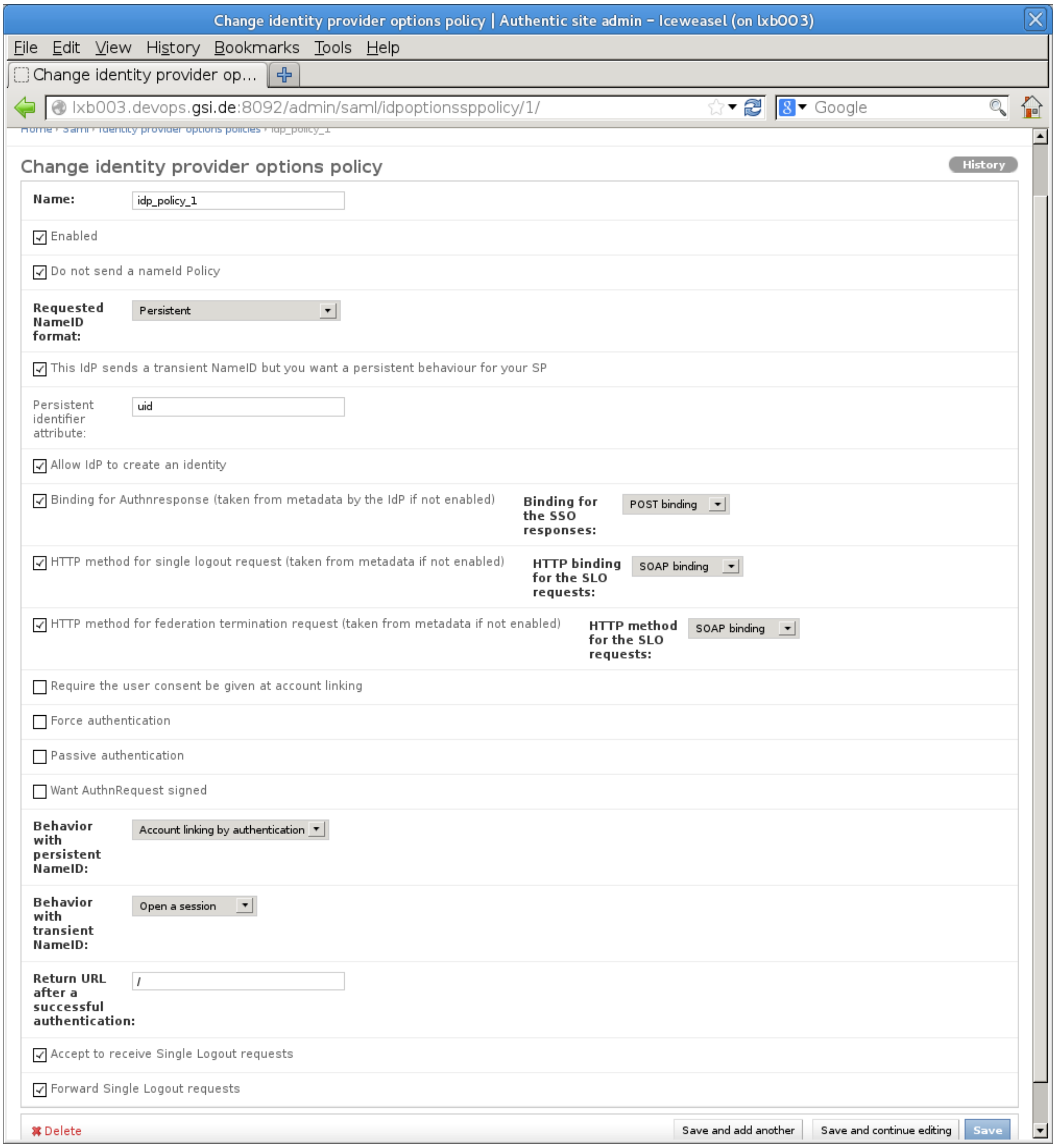
```
AUTH_LDAP_BIND_DN = "XXXX"

AUTH_LDAP_BIND_PASSWORD = "XXX"

# Lookup user under the branch o=base and by mathcing their uid against the

 received login name

AUTH_LDAP_USER_SEARCH = LDAPSearch("ou=people,dc=eurofel,dc=eu",

   ldap.SCOPE_SUBTREE, "(uid=%(user)s)")
```

- Declare Authentic 2 as a SAML2 service provider on tge Shibboleth IdP using the SAML2 service provider metadata of Authentic 2. The metadata is on: http://authentic2.gsi.de/authsaml2/metadata.

- Add and configure a SAML2 identity provider entry in Authentic 2 using the metadata of the identity provider. The metadata of the IdP is under: http://localidp.gsi.de/idp/profile/Metadata/SAML

  http://umbrella.psi.ch/idp/profile/Metadata/SAML

- Define the policies for the IdP, taking into account that for the Shibboleth implementation the “Requested NameID” has to have *Transient.* But also for linking of accounts this information needs to be kept in a persistent way in the system. Therefore, it is important to select the option: “This IdP sends a transient NameID but you want a persistent behaviour ...” Settings of the policy are found in Illustration 1.
  There is the main field that describes which behaviour it is going to follow with a persistent NameID. This option applies when an assertion with a persistent nameID is received and the nameID is not recognized as an existing federation. Two values are possible: “Create new account” and “Account linking by authentication”. The value “Create new account” makes Authentic 2 create a user account associated to the nameID received. The value “Account linking by authentication” makes Authentic 2 ask the user to authenticate with an existing account to associate the nameID to this account. In the case of Umbrella it would be interesting to use the second case, where the user has already an account in Umbrella federation.



Change identity provider options policy | Authentic site admin - Iceweasel (on lxb003)

lxb003.devops.gsi.de:8092/admin/saml/idpoptionssppolicy/1/

Home › Saml › Identity provider options policies › idp_policy_1

Change identity provider options policy

Name: idp_policy_1

☑ Enabled

☑ Do not send a nameId Policy

Requested NameID format: Persistent

☑ This IdP sends a transient NameID but you want a persistent behaviour for your SP

Persistent identifier attribute: uid

☑ Allow IdP to create an identity

☑ Binding for Authnresponse (taken from metadata by the IdP if not enabled) — Binding for the SSO responses: POST binding

☑ HTTP method for single logout request (taken from metadata if not enabled) — HTTP binding for the SLO requests: SOAP binding

☑ HTTP method for federation termination request (taken from metadata if not enabled) — HTTP method for the SLO requests: SOAP binding

☐ Require the user consent be given at account linking

☐ Force authentication

☐ Passive authentication

☐ Want AuthnRequest signed

Behavior with persistent NameID: Account linking by authentication

Behavior with transient NameID: Open a session

Return URL after a successful authentication: /

☑ Accept to receive Single Logout requests

☑ Forward Single Logout requests

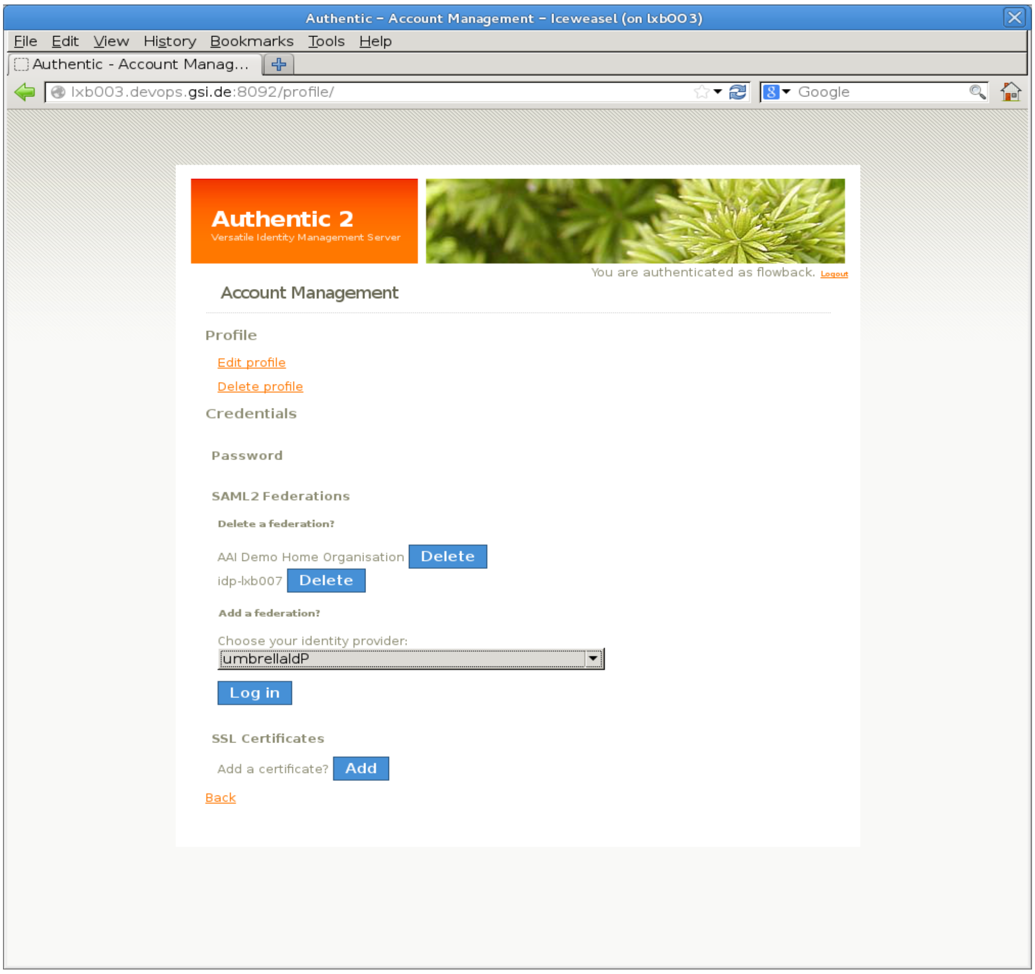
File Edit View History Bookmarks Tools Help
Change identity provider op...
Google
History
Delete
Save and add another
Save and continue editing
Save

Figure 8: Definition of IdP policies

Up to this point, Authentic2 is authenticating users locally against the LDAP directory running on localidp.gsi.de.

Enclosed in Authentic2 is the bulk script that facilitates the bulk load of IdPs and SPs from a metadata file (http://pythonhosted.org/authentic2/sync-metadata_script.html), and after having deal with the *slug* column (the slug column name was being taken from the name of the DisplayName in the metadata, which is not unique. Uniqueness is a requirement of slug column) we have the SAML2 federations from SWITCH. Also, I have enabled my local federation and the umbrella test federation on “umbrella.psi.ch”.

We can see in the next screen a sample of the administrative tasks that a user can accomplish, Illustration 2. The user has a local account in the system for accessing Authentic2, at the moment configured with LDAP back-end. This user is able to link her account to any of the federations registered in Authentic2, or in this case, to an X509 certificate too. This linking will only proceed if after successful authentication against the target federation. This linking information is saved on the authentic2 database in a persistent way, therefore when the user connects to any of those linked accounts will get the local account.


Authentic - Account Management - Iceweasel (on lxb003)
File Edit View History Bookmarks Tools Help
Authentic - Account Manag...
lxb003.devops.gsi.de:8092/profile/
Google
Authentic 2
Versatile Identity Management Server
Logout
Edit profile
Delete profile
Delete
Delete
Log in
Add
Back

You are authenticated as flowback.

Account Management

Profile

Credentials

Password

SAML2 Federations

Delete a federation?

AAI Demo Home Organisation

idp-lxb007

Add a federation?

Choose your identity provider: umbrellaIdP

SSL Certificates

Add a certificate?

Figure 9: User administration panel

Manage attributes:

User attributes can be taken from LDAP directories, the user Django profile or taken from the user Django session if Authentic 2 is also configured as a SAML2 service provider. Indeed, when Authentic 2 acts also as a SAML2 service provider, attributes contained in the SAML2 assertion received from third IdP are put in the user session. Attributes can thus be proxyfied during SSO with Authentic 2 configured as a SAML2 proxy.

By default, the namespace and format of attributes in assertion is SAMLV2.0 X500/LDAP Attribute profile.

The mapping of attributes is the most interesting part. It is useful to use the attributes from the session pushed by third SAML2 identity providers. This is implemented and can be configured in a fine-grained way. http://pythonhosted.org/authentic2/attributes_in_session.html

The mapping is saved in the table saml_libertysessionsp, some fields are:

- id- identifier
- django_session_key- this is the key of the django session that identified the user locally.
- federation_id – identifier of the federation where it has been linked.

Another tables keep the correspondance between attributes. These are: saml_authorizationattributemap and saml_authorizationattributemapping.

Approach for Bridging	**Use Authentic2**	**Use Shibboleth and a Custom Login Handler**
Description	Install and configure standard Authentic2. Some development work required.	Install a standard Shibboleth IdP and SP. Connect them via a custom IdP login handler, which is protected by the SP. Development work required to create custom login handler.
License	GNU AGPL version 3	Shibboleth uses Apache 2 license, any license could be used for the custom login handler.
Protocols supports	Authentic2 supports SAML2, CAS, OpenID, LDAP, X509, OATH	Shibboleth supports SAML1, SAML2. There are login handlers for Jaas (LDAP, MySQL, …), CAS, Kerberos, X.509, HTTP Basic Auth, Facebook, and some more.
Documentation	Limited to the use cases that it solves. Only one website: http://pythonhosted.org/authentic2	Extensive documentation on official Shibboleth wiki and the Shibboleth website. Divided into “General documentation” and “Developers documentation”. In addition many issues and questions were discussed already on the Shibboleth mailing lists in the past 10 years.
User	Unknown, but probably small and	Large community because it is the de-

community	focused on France.	facto standard FIM software for academic organisations world-wide.
Support, Activities and Sustainability	Recent submissions of code. Mailing-list inactive (tried to send several mails even individually to the main developers with no answer). Code seems to be mostly maintained by the French company Entrouvert.	Active mailing-list with many active users answering in less than one day on average. Support can also be received via the local federation (e.g. SWITCHaai). The sustainability of project is ensured by Shibboleth consortium that is funded by many federation and organisations that use Shibboleth.
Framework/ Development	Django. Developed in Python.	Development centre exists. Shibboleth is developed in Java (Identity Provider) and C++ (Service Provider).
Deployment	Possibility of deployment of Django is by WSGI, that can be integrated into Apache, gunicorn or uWSGI servers. This is yet another application to be maintained.	Identity Provider has to be deployed in a servlet container like Jetty, Apache Tomcat, Jboss Tomcat or Glassfish. The deployment of a custom LoginHandler would mean adding the new .jar to an existing standard Shibboleth IdP installation.