



**IRUVX-PP**  
**Preparatory phase for the EuroFEL**  
**(ex-IRUVX-FEL) consortium**



**The Umbrella System**

Deliverable N°: 2.5

Deliverable Title: Prototype web-based access point

Work package: WP2

Authors: Björn Abt, Heinz J Weyer

Dissemination level: C

Date April 28, 2011

**Project funded by the European Community**

# Table of Contents

|   |    |
|---|----|
| Introduction .....  | 4  |
| 1 Umbrella prototype status .....   | 5  |
| 1.1 Authentication .....  | 5  |
| 1.1.1 Single Sign-On (Shibboleth SAML2) .....                                   | 5  |
| 1.1.2 LDAP-Directory (OpenDS).....  | 5  |
| 1.1.3 uApprove for Shibboleth .....   | 6  |
| 1.1.4 Basic federation is set-up. ....  | 6  |
| 1.2 Umbrella Application .....  | 6  |
| 1.2.1 Account Creator .....   | 6  |
| 1.2.2 Attribute Updater .....   | 7  |
| 1.2.3 Module Manager .....  | 7  |
| 1.2.4 Facility Manager.....   | 9  |
| 1.3 WUO-Integration .....   | 9  |
| 1.3.1 SAML2-SP .....  | 9  |
| 1.3.2 Sample DUO Integration.....   | 9  |
| 1.3.3 "Single Sign-On" process.....   | 10 |
| 1.3.4 "Match existing user" process.....  | 10 |
| 1.3.5 "Match new user" process .....  | 10 |
| 1.3.6 "Attribute Updater" process with challenge-response handshake.....        | 10 |
| 2 The Umbrella Demo Version.....  | 11 |
| 2.1 Functionalities available.....  | 11 |
| 2.1.1 User registration.....  | 11 |
| 2.1.2 Login .....   | 11 |
| 2.1.3 Account updater .....   | 12 |
| 2.1.4 Module manager .....  | 12 |
| 2.1.5 Facility management.....  | 12 |
| 2.1.6 Social Networking .....   | 13 |
| 2.2 Requirements, installation and setup.....                                   | 14 |
| 2.3 Typical use cases.....  | 15 |
| 2.3.1 Create an Umbrella account .....  | 15 |
| 2.3.2 Login .....   | 15 |
| 2.3.3 Create an account at a service provider without an Umbrella session ..... | 17 |
| 2.3.4 Match Umbrella account with service provider account .....                | 18 |
| 3 Acknowledgements .....  | 20 |
| 4 References.....   | 20 |
| Appendix 1 On the way from the prototype to the production version .....        | 21 |
| A1.1 EAA (Authentication part) .....  | 21 |
| A1.1.1 Single Sign-On (Shibboleth SAML2).....                                   | 21 |
| A1.1.2 LDAP-Directory (OpenDS) clustered over facilities .....                  | 21 |
| A1.1.3 uApprove for Shibboleth.....   | 21 |
| A1.1.4 Extended federation with facilities.....                                 | 21 |
| A1.2 Umbrella Application.....  | 22 |
| A1.2.2 Account Creator .....  | 22 |
| A1.2.2 Attribute Updater.....   | 22 |
| A1.2.3 Facility Manager .....   | 22 |
| A1.2.4 Module Manager.....  | 22 |
| A1.2.5 Coaching Module .....  | 22 |
| A1.2.6 Three different layouts to choose from.....                              | 22 |

|  |    |
|--|----|
| A1.2.7 Affiliation database .....  | 22 |
| A1.3 WUO-Integration.....  | 22 |
| A1.3.1 SAML2-SP at each WUO .....  | 23 |
| A1.3.2 WUO Integration.....  | 23 |
| A1.3.3 Implementation effort at facilities.....                            | 23 |
| A1.3.4 SAML2-SP.....   | 24 |
| A1.3.5 “Single Sign-On” process .....                                      | 24 |
| A1.3.6 “Match existing user” process .....                                 | 24 |
| A1.3.7 “Match new user” process .....                                      | 25 |
| A1.3.8 “Attribute Updater” process with challenge-response handshake ..... | 25 |
| A1.3.9 “Coaching dispatcher” process.....                                  | 26 |
| Appendix 2 Umbrella+ .....   | 26 |
| A2.1 Publication Database.....   | 26 |
| A2.2 Remote Data Access .....  | 26 |
| A2.3 Remote Experiment Access .....  | 26 |
| A2.3.1 Remote Experimenting.....   | 26 |

## Illustration Index

|   |    |
|---|----|
| Illustration 1: Account Creator.....                    | 6  |
| Illustration 2: Challenge Response Mechanism .....      | 7  |
| Illustration 3: Attribute Updater .....                 | 7  |
| Illustration 4: Module Manager .....                    | 8  |
| Illustration 5: Facility Manager .....                  | 9  |
| Illustration 6: User registration .....                 | 11 |
| Illustration 7: Umbrella login .....                    | 11 |
| Illustration 8: Account updater .....                   | 12 |
| Illustration 9: Module manager .....                    | 12 |
| Illustration 10: Facility management .....              | 13 |
| Illustration 11: Social networking application .....    | 14 |
| Illustration 12: Create an Umbrella account .....       | 17 |
| Illustration 13: Click on "login" .....                 | 17 |
| Illustration 14: Umbrella login page .....              | 18 |
| Illustration 15: Logged in at Umbrella .....            | 18 |
| Illustration 16: Login screen at service provider ..... | 19 |
| Illustration 17: Registration form .....                | 19 |
| Illustration 18: Service provider login screen.....     | 20 |
| Illustration 19: Umbrella login .....                   | 20 |
| Illustration 20: Match EAA account.....                 | 21 |
| Illustration 21: Web SSO User Creation Pattern .....    | 26 |

## Introduction

This document describes the prototype version of the European User Umbrella (EUU), which has been developed within Work Package 2 of the EuroFEL / IRUVX project. Its goal is to provide common IT tools for the users of the European neutron and photon research facilities. These will give them new possibilities for easy access to the facilities. The basis of the EUU is the EAA (European Authentication and Authorisation) system, which allows a unique identification of a user with SSO (Single Sign On) capabilities, which then allows the local Web-based User Offices (WUOs) at the participating to assign roles to these users and provide them with access to specific applications. The EAA is designed to provide maximum confidentiality to users and facilities while on the other hand providing the necessary functionalities.

The structure of the document is as follows: Section 1 describes the current status of the prototype version. Section 2 contains the description of the demo version, which allows a life demonstration of the prototype. Besides providing a hands-on experience of the system in its present form it also allows to get a feeling if the system parameters are set in the right directions for future developments

The document contains two appendices. In Appendix 1 the first experience with the prototype is reflected and those changes and modifications described which should be made before proceeding to a production version. Appendix 2 describes next-step extensions and modifications. They are partly already defined as part of follow-up projects such as CRISP, PaN-Data ODI, NMI3.

# 1 Umbrella prototype status

Confidentiality, both in respect to the users of the facilities as also the facilities themselves is a basic requirement for any system dealing with user-related services at the photon / neutron large facilities. That means that authentication and unique user identification is the basic layer of the Umbrella system. Unique user identification needs a certain central component. In order again to comply with the confidentiality requirement, authentication and other elements of the Umbrella are designed such that the central part is kept minimal, just to provide the necessary functionality. Further information needed for the general operation is kept at the local WUOs.

On top of the authentication layer, further tools are implemented, enabling users to easier access information and services at the facilities. They contain basic services such as Account Creator, Attribute Updater, Facility Manager, Module Manager.

The existing Web-Based User Office (WUO) systems at the local facilities contain the whole cycle of handling an experiment, from proposal submission over experiment handling up to the registration of the final publication. In addition, most WUOs include important off-and on-site user services like facility access control or guest-house registration. All these services should be kept and only missing central services like pan-European user identification should be added (umbrella concept). This requires corresponding modifications for these WUOs to be able to collaborate with and integrate into the umbrella system.

## 1.1 Authentication

The Umbrella authentication system is built upon a user directory where the accounts are stored, and a SAML2 ecosystem, which enables Single Sign-On.

### 1.1.1 Single Sign-On (Shibboleth SAML2)

In recent time, there is a vivid development concerning authentication issues both in the academic and commercial sector. An early decision was not to build the Umbrella system completely from scratch but rather build it on top of an existing authentication system. In this way, the project profits from the existing know-how as well as from novel developments.

After evaluating different authentication systems, e.g. OpenID, Shibboleth, it was concluded that a SAML2 based system fits the needs best regarding user privacy and data security (see also [1]).

SAML2 is an OASIS standard[2] and has wide industry support; members are: AOL, EMC, Hewlett-Packard, IBM, Microsoft, Nokia, Oracle, Red Hat, SAP, Boeing, et. al. It has been widely adapted in Switzerland (SWITCHaai), Germany (DFN-AAI), Denmark (DK-AAI) and other countries with hundreds of thousands of users who work with it on a daily base.

Finally, it has been decided to use Shibboleth2[6] by the Internet2 Middleware Initiative as the implementation of the SAML2 specification.

### 1.1.2 LDAP-Directory (OpenDS)

User account information needs to be persisted and a natural choice for storing account

information is a LDAP-directory. Own attribute types and object types have been implemented to reflect the umbrella needs.

The software used here is OpenDS[5], an open source project from Oracle (formerly SUN).

### 1.1.3 uApprove for Shibboleth

uApprove is a small piece of software which resides close to the SAML2 system. It requires that a user has to agree that his personal account information will be released to the facility of his choice. This has mainly a legal and informative reason, since in this way a user can review the parameters released and also has to agree on it.

uApprove is provided as open source by Switch.

### 1.1.4 Basic federation is set-up.

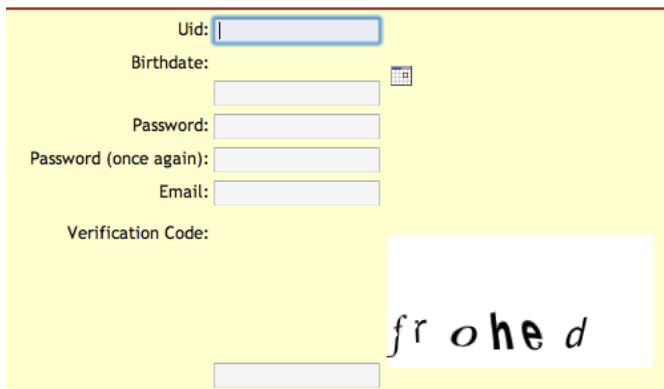
SAML2 is set-up to authenticate users in a federation of service providers and to release a set of metadata with information about a user to the service providers. This is part of the Shibboleth software. A service provider can represent any resource delivering information based on authentication and as foreseen by this project represents a WUO. These entities must be explicitly added to the federation declaration but then form a unity.

## 1.2 Umbrella Application

To enable enhanced functionality to a user base, we must provide them with custom tailored web applications accessible to all members of the federation. This system allows basically manipulation of account information and dissemination of user information to facilities where this user is registered. The Umbrella application is also the starting point of further developments towards Umbrella+.

### 1.2.1 Account Creator

An account creator was established as an entry point for new users. It allows to create an account at the Umbrella system. The system verifies that username and email are unique and asks for a generated “captcha”[7] verification code to prevent automated account creation (Illustration 1)



The screenshot shows a web form for creating an account. The form is set against a light yellow background. It contains the following fields and elements:

- Uid:** A text input field with a blue border.
- Birthdate:** A text input field with a small calendar icon to its right.
- Password:** A text input field.
- Password (once again):** A text input field.
- Email:** A text input field.
- Verification Code:** A label above a white rectangular area containing a captcha image with the text "fr o he d". Below the captcha is an empty text input field.

### 1.2.2 Attribute Updater

An attribute updater allows a user to enter his personal contact information and to update this information at all facilities he is registered at in a single step (Illustration 3). Since we do not save any user to facility relation, we have to utilise a specific challenge-response mechanism to find out at which facilities a user is registered at and then to release the information only to the facilities which satisfy the cryptographic needs (Illustration 2). We allow the selection of an affiliation with hooks to a dummy affiliation database.

Illustration 2: Attribute Updater

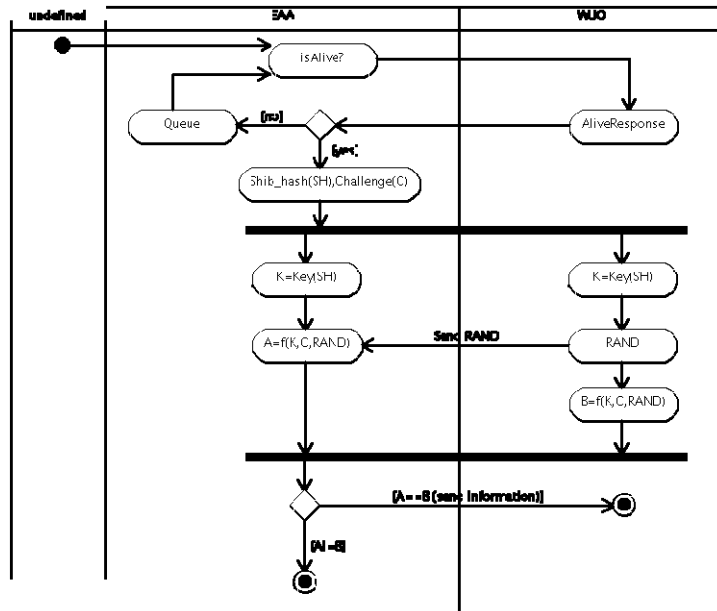


Illustration 3: Challenge Response Mechanism

### 1.2.3 Module Manager

Proposals are the key elements for handling user experiments. As first step for a new experiment, a user team submits such a proposal via the local WJO to the respective facility and a proposal review committee selects the best proposals for access to a facility beamline. These proposals have to be written according to a well-defined format and it takes some time for a team to prepare a reasonable document. As such a proposal displays the scientific plans of an experiment team, contents have to be handled with high confidentiality. In order to obey this confidentiality character and at the same time reduce the administrative burden for the users, another hybrid solution is offered by the Umbrella systems. Proposals are subdivided into a *facility-specific* and a *general, scientific* part. Often experiments are carried out in an iterative style and this general part may change only a little between a previous and the next experiment. The scientific part is split up in *modules*, e.g. background, goal, method, etc. which can be edited with a nifty online editor. The whole scientific part can be downloaded and used for submission at a facility or for personal storage and can again be uploaded at the module manager.

A first version of the general part has been generated and one element of the implementation phase is to harmonise this part between the participating facilities. This will further reduce the administrative load on the proposers and in addition ease the job of the proposal referees when they cross review and rank the different proposals submitted.

TITLE: Study of the transient crystalline phases during the early hydration period of Portland cement.

Sections

BACKGROUND

EXPECTED\_RESULTS

GOAL

JUSTIFICATION

METHOD

REFERENCE

Review

Section: EXPECTED\_RESULTS

Text:

The first goal of the experiment will be the test function and precision of the new combined setup. In addition, we expect also to obtain first experimental results. From the experiments we expect to follow quick reactions and the formation of transient phases without altering the sample [2,3]. In mixtures, actually, it is sometimes difficult to distinguish AFm phases with X-ray diffraction during the hydration process, both because they are often poorly crystalline and because the reaction that leads to the formation of ettringite when sulphate is added is too quick to be followed using a conventional diffractometer. Moreover, in laboratory is common to quench the samples with different techniques, like freezing or treating the material with organic solvents. Up to now, there is no reliable information available if and how these quenching procedures could modify the crystalline structures of the system involved.

Document

Document

Upload Proposal

Choose File

no file selected

Illustration 4: Module Manager



## 1.2.4 Facility Manager

A facility manager is needed as administrator tool for registering facilities and their interfaces to the Umbrella system. It is possible to register the attribute updater endpoint and to enable or disable the dissemination to the specific facility.



The screenshot shows a web interface for managing facilities. On the left, there is a sidebar with a 'Facility' filter and a list of facilities: 'PSI DUO', 'MAX 4 Lund', 'MAX 5 Lund', 'MAX 7 Lund', and 'MAX 8 Lund'. The main area displays a 'Review' for the selected facility, 'PSI DUO'. The review includes the following details:

- Enabled: true
- Name: PSI DUO
- Attribute Update URL: <http://www.google.ch/>
- Contact Person: Bjoern Abt
- Contact Person Email: [bjoern.abt@object.ch](mailto:bjoern.abt@object.ch)
- Last Ping Date: Tue Apr 05 11:01:32 CEST 2011

At the bottom of the review, there are two icons: one for editing (a pencil) and one for deleting (a trash can).

*Illustration 5: Facility Manager*

## 1.3 WUO-Integration

To be able to participate at the umbrella system the WUOs have to be adjusted to support the functionalities required by such a system. An important component is the SAML2 service provider software as it is needed to communicate with the authentication system to ensure identities and to obtain released information about a user. Another component is the integration of WUO and Umbrella processes though our credo is to reuse existing processes at facilities as much as possible.

### 1.3.1 SAML2-SP

A SAML2 service provider is a piece of software installed at a web server which is able to authenticate users against a central place and to retrieve information about an incoming user.

### 1.3.2 Sample DUO Integration

There is a working prototype of the DUO software (PSI WUO) which has been extended to support the authentication and umbrella processes.

### **1.3.3 “Single Sign-On” process**

To enable the “Single Sign-On” process the WUO has to be extended to check for incoming umbrella sessions and then to retrieve the corresponding user from the local user database and register a WUO session with him.

### **1.3.4 “Match existing user” process**

A participating user might already be registered at a WUO and his user account can have several proposal and publications linked to it and the user don't want to loose this information. For this to happen if a user enters the WUO with an umbrella session but no matching local user, the WUO login screen is displayed and after successful login, the umbrella identification is saved with the local user account for subsequent single sign-on.

### **1.3.5 “Match new user” process**

If an umbrella user has no existing account at a WUO he can create an account at the WUO. For this the already existing “create user” procedure at the WUO is used to gather information and save it together with the umbrella identification.

### **1.3.6 “Attribute Updater” process with challenge-response handshake**

A user might change his personal information. If – as it is often the case – a user is registered at several facilities, it would be very convenient, if it would be sufficient to change this information just once and then disseminate the information to all facilities. On the one hand there could be a security issue if facilities receive user updates from users which are not registered with these facilities. On the other hand, it is not an option to store user-to-facility relations.

The solution is therefore to use a challenge-response mechanism to find out if a user is registered at a facility. Since a user leaves traces at the facilities he has visited, these can be queried and a facility can only feedback the right answer, in case a user has already visited that specific facility. The WUO then receives an update of user data which then should be incorporated into the local user database.

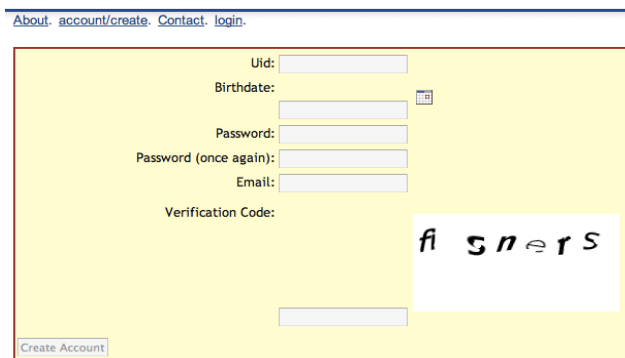
## 2 The Umbrella Demo Version

There is a fully functional demo version hosted at PSI. It runs on a VMware infrastructure and the virtual machine can easily be transferred to another place. This demo version can be used as playground for testing the functionalities of the prototype phase. In addition, it can be used as a starting ground for further distributed developments and as a possibility to test implementations of single WUOs.

### 2.1 Functionalities available

#### 2.1.1 User registration

The user registration application enables users to create an account at the Umbrella. This is the starting point to use the Umbrella system.

A screenshot of a web browser showing a user registration form. The browser's address bar displays "About account/create Contact login". The form itself is on a yellow background and contains several input fields: "Uid:", "Birthdate:" (with a calendar icon), "Password:", "Password (once again):", "Email:", and "Verification Code:". To the right of the "Verification Code:" field is a CAPTCHA image showing the text "fi 5 n e r S". At the bottom left of the form is a button labeled "Create Account".

*Illustration 6: User registration*

#### 2.1.2 Login

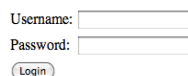
A login window is used to authenticate users to the umbrella system. After this procedure the user is logged-in to all Umbrella applications.



#### Example Login Page

This login page is an example and should be customized. Refer to the [documentation](#).

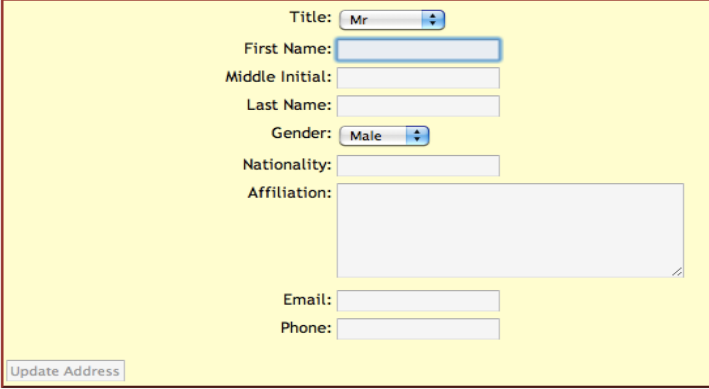
**Shibboleth Identity Provider Login to Service Provider <https://eurofel01.psi.ch/>**

A simple login form with two input fields. The first is labeled "Username:" and the second is labeled "Password:". Below the password field is a small button labeled "Login".

*Illustration 7: Umbrella login*

### 2.1.3 Account updater

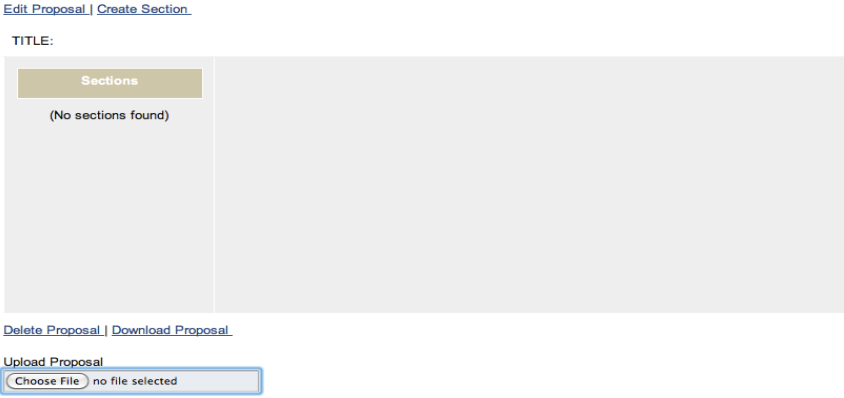
The account updater application is used to, by user request, update address information at all service providers, where the user is registered at.

A screenshot of a web form titled 'Account Updater'. The form is set against a light yellow background and contains several input fields. At the top, there is a 'Title' dropdown menu with 'Mr.' selected. Below it are text boxes for 'First Name', 'Middle Initial', and 'Last Name'. The 'Gender' field is a dropdown menu with 'Male' selected. The 'Nationality' field is a text box. The 'Affiliation' field is a large, empty text area. At the bottom, there are text boxes for 'Email' and 'Phone'. A small 'Update Address' button is located at the bottom left of the form.

*Illustration 8: Account updater*

### 2.1.4 Module manager

To be able to edit scientific modules of a proposal, a module manager is provided.

A screenshot of the 'Module Manager' interface. At the top, there are two links: 'Edit Proposal' and 'Create Section'. Below these is a 'TITLE:' label. The main area is divided into two columns. The left column has a header 'Sections' and a message '(No sections found)'. The right column is empty. At the bottom, there are two links: 'Delete Proposal' and 'Download Proposal'. Below these is a section titled 'Upload Proposal' with a 'Choose File' button and the text 'no file selected'.

*Illustration 9: Module manager*

### 2.1.5 Facility management

A facility management software provides administrators the functionality to add new facilities to the Umbrella, which then can be configured to follow the challenge-response push-mechanisms of the Umbrella system.

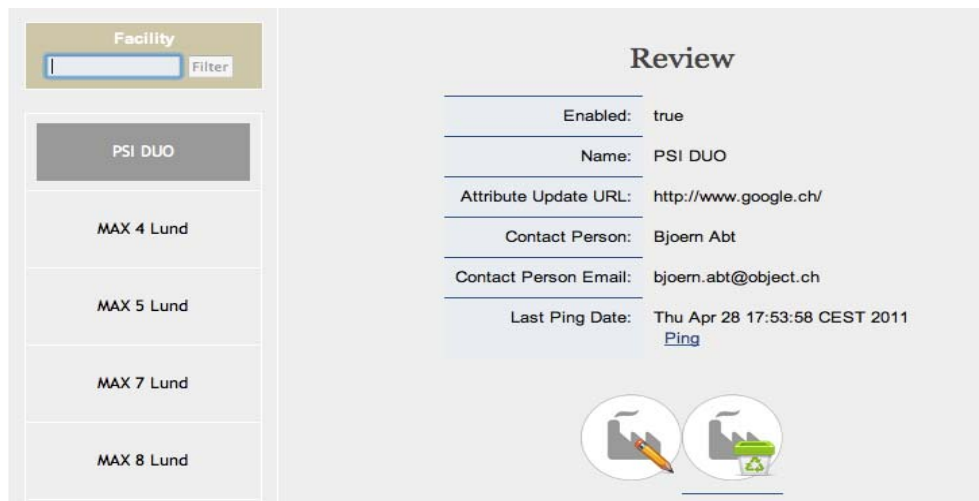


Illustration 10: Facility management

## 2.1.6 Social Networking

A social networking application was added to the Umbrella demo system to get an impression on what the implementation effort was in implementing a 3<sup>rd</sup> party system into the Umbrella and to have a better showcase for demonstrating the Umbrella to the users.

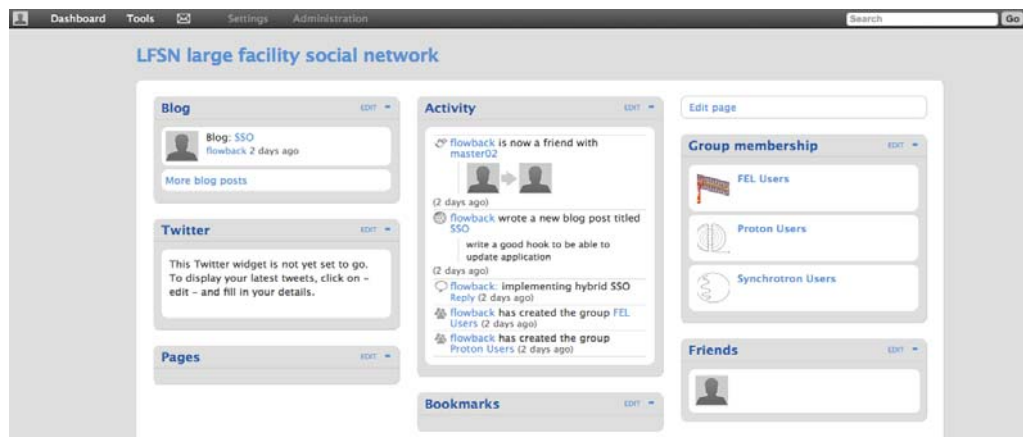


Illustration 11: Social networking application

## 2.2 Requirements, installation and setup

To use the Umbrella demo version the user just needs a computer with a browser and an internet connection. There is no installation of any additional software necessary. The user has to create an account in order to use the full Umbrella functionalities.


## 2.3 Typical use cases

### 2.3.1 Create an Umbrella account

1. Open <https://eurofel01.psi.ch/euu>
2. Click on “account/create”
3. Fill in your data in the form
4. Click on “Create Account” button

[About.](#) [account/create.](#) [Contact.](#) [login.](#)

Uid:


Birthdate:  

Password:

Password (once again):

Email:

Verification Code:



*Illustration 12: Create an Umbrella account*

### 2.3.2 Login

1. Open <https://eurofel01.psi.ch/euu>
2. Click on “login”

[About.](#) [account/create.](#) [Contact.](#) [login.](#)

Welcome to the European Authentication and Authorization (EAA)!

*Illustration 13: Click on "login"*

3. You will be forwarded to the Umbrella login page
4. Enter your valid credentials



## Example Login Page

This login page is an example and should be customized. Refer to the [documentation](#).

**Shibboleth Identity Provider Login to Service Provider <https://eurofel01.psi.ch/>**

Username:

Password:

*Illustration 14: Umbrella login page*

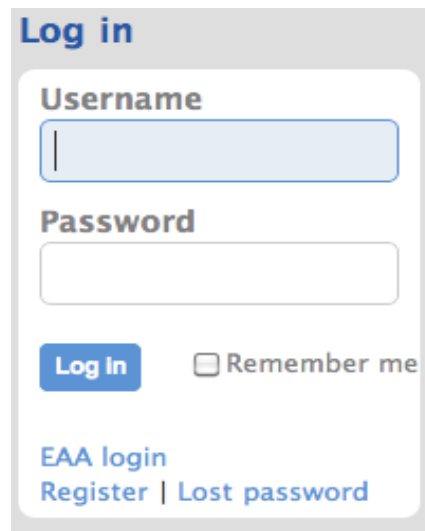
5. You will now be logged in at the umbrella and will have extra options available

5

[About.](#) [account/update.](#) [proposal/overview.](#) [facility/view.](#) [Contact.](#)

### 2.3.3 Create an account at a service provider without an Umbrella session

1. Close all of your browser to be sure that no Umbrella session is active
2. Visit the service provider at: <https://eurofel01.psi.ch/elgg>
3. Click on “register”

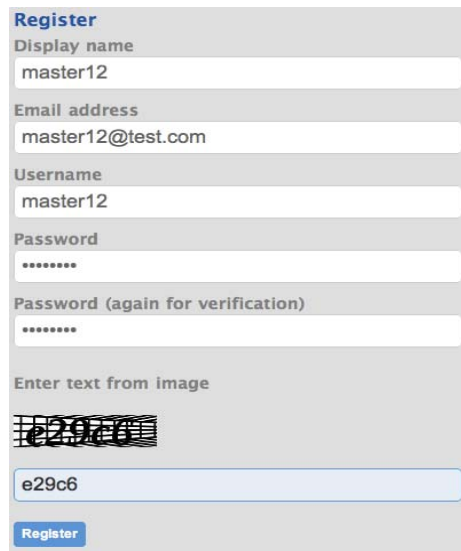


The image shows a login interface with a light gray background. At the top, the text "Log in" is displayed in blue. Below this, there is a white rounded rectangle containing the login fields. The "Username" label is in bold black text above a light blue input field with a vertical cursor. The "Password" label is in bold black text above a white input field. Below the password field, there is a blue "Log In" button and a "Remember me" checkbox with the text "Remember me" in gray. At the bottom of the white box, there are three links: "EAA login" in blue, "Register" in blue, and "Lost password" in blue, separated by vertical bars.

*Illustration 16: Login screen at service provider*

4. Enter your credentials in the following form and click on “Register”



A screenshot of a web registration form titled "Register". The form contains several input fields: "Display name" with the value "master12", "Email address" with "master12@test.com", "Username" with "master12", "Password" with masked characters "\*\*\*\*\*", and "Password (again for verification)" also with "\*\*\*\*\*". Below these is a CAPTCHA section labeled "Enter text from image" showing a distorted image of the text "e29c6". A text box below the image contains the typed text "e29c6". At the bottom is a blue "Register" button.

**Register**

Display name  
master12

Email address  
master12@test.com

Username  
master12

Password  
\*\*\*\*\*

Password (again for verification)  
\*\*\*\*\*

Enter text from image  
e29c6

e29c6

Register

*Illustration 17: Registration form*

5. Send an email to [bjoern.abt@psi.ch](mailto:bjoern.abt@psi.ch) saying that you registered and wait until your account has been validated
6. Login at the login screen using your credentials

#### **2.3.4 Match Umbrella account with service provider account**

1. Be sure to have an Umbrella account and a service provider account
2. Visit the service provider at: <https://eurofel01.psi.ch/elgg>
3. Click on "EAA login"

*Illustration 18: Service provider login screen*

4. You will be forwarded to the Umbrella login
5. Enter your umbrella credentials and click on login



### Example Login Page

This login page is an example and should be customized. Refer to the [documentation](#).

**Shibboleth Identity Provider Login to Service Provider <https://eurofel01.psi.ch/>**

Username:

Password:

*Illustration 19: Umbrella login*

6. Notice the “Match EAA account” button – now you need to enter your service provider credentials to match the two accounts and then click on the button to match. This step enables the single sign-on.

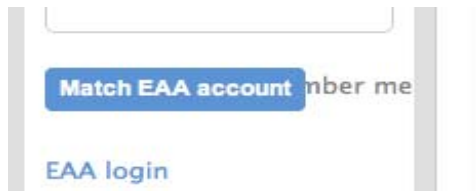
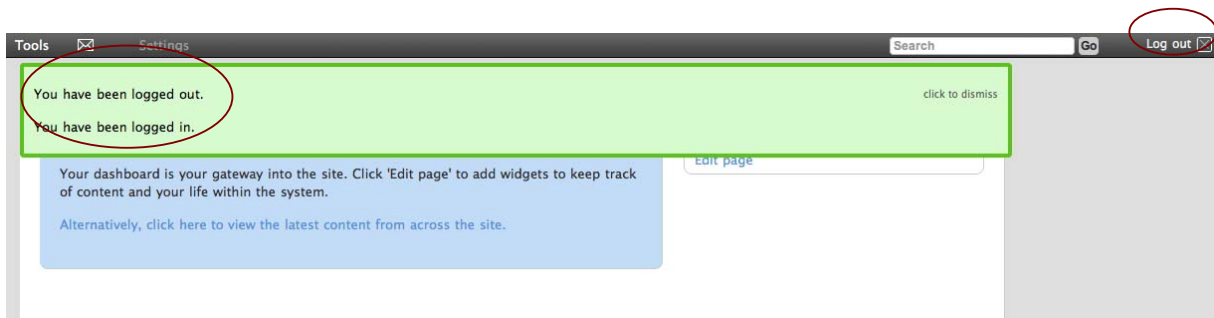


Illustration 20: Match EAA account

7. Now you should be logged in and by clicking on “Log out” you should be logged-out and in automatically because of the single sign-on.



8. Close your browser and repeat from step 1 to 5. Now you should be logged-in without the need to enter your service provider credentials to match.
9. Now close your browser again and repeat steps 1 and 2. At the service provider login enter your service provider credentials.
10. Now you should be logged-in again.
11. Step 8, 9 and 10 show the hybrid aspect of the Umbrella system, allowing users to enter a system directly or over the umbrella

### 3 Acknowledgements

This prototype has been defined and developed in close cooperation with the members of Work package 2 of IRUVX-PP and also with the colleagues from the strongly related work in ESRFUP and ILL22. In numerous discussions and workshops the details of the system have been derived. We like to mention explicitly R. Treusch (DESY), D. Herrendoerfer, O. Schwarzkopf (HZB), D. Ornela, G. Paolucci (Fermi/Elettra), A. Gleeson (STFC), U. Johansson (MaxLab), and R. Dimper, D. Porte (ESRF). Clearly, the work could not have been performed without the continuing home support at PSI by R. Abela, M. van Daalen, S. Egli, S. Janssen and M. Knecht.

### 4 References

- [1] <<http://identitymeme.org/doc/draft-hodges-saml-openid-compare.html>>
- [2] <[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)>
- [3] <<http://www.switch.ch/aai/index.html>>
- [4] <<http://www.edugain.org/>>
- [5] <<http://www.opens.org/>>
- [6] <<http://shibboleth.internet2.edu/>>
- [7] <<http://www.captcha.net/>>
- [8] Functional Description of the EUU / EAA Tools, R. Dimper et al. (2010)
- [9] Umbrella Architecture Document, Dimper et al. (2010), B. Abt, Heinz J Weyer (2010)

## **Appendix 1 On the way from the prototype to the production version**

This part describes the steps necessary to implement the umbrella as a production system and also further developments planned to enhance the functionality of the umbrella system.

### **A1.1 EAA (Authentication part)**

#### **A1.1.1 Single Sign-On (Shibboleth SAML2)**

The single sign-on system should be clustered to support failover and load balancing thus enhancing the uptime of such a system.

#### **A1.1.2 LDAP-Directory (OpenDS) clustered over facilities**

LDAP directories can be easily replicated and allow a setup where each facility has a full-fledged LDAP server with the whole user base on it giving us following advantages:

- Fault tolerance, there are still systems available if one fails
- Load balancing, there is a distribution of the computational load, minimizing the load on a single node
- No facility has an advantage over another, since all facilities have all the information

#### **A1.1.3 uApprove for Shibboleth**

uApprove needs to be extended to disable the storage of the user to service provider relationship, leaving us the possibility to say that a specific user agreed to send his personal information at a specific time to a facility, but not to which facility.

#### **A1.1.4 Extended federation with facilities.**

The federation declaration must be extended with the WUO descriptions of the participating facilities to allow them to play a role in this ecosystem.

There are already existing federations like SWITCHaai[3] or eduGAIN[4] and there are also possibilities to interface those existing federations and allow access for our user base to use other services. The ability to interface with other federations is an important point for the future, since membership of our federation will not become a dead-end street but is open to vibrant federations worldwide.

## **A1.2 Umbrella Application**

Following extensions or enhancements must be fulfilled to enable the umbrella application:

### **A1.2.2 Account Creator**

The account creator must be extended with real-world features like email verification and even more user input validation.

### **A1.2.2 Attribute Updater**

The attribute updater must be extended to reflect all the wanted properties about a user.

### **A1.2.3 Facility Manager**

The facility manager allows manipulation of facility data. A facility contains the attribute update URL and contact information. This might need to be extended for future applications in Umbrella+

### **A1.2.4 Module Manager**

For the module manager application there should be an agreement on what extra features should be enabled in the editor. There is a wide range of possibilities to add, from simple sub- and superscript till online LaTeX equation editors.

### **A1.2.5 Coaching Module**

Because of time limitations for the coaching module only the concept could be developed. The real system will have to be built from scratch.

### **A1.2.6 Three different layouts to choose from**

It turns out that the layout (i.e. visible components) of the EUU is very critical. Therefore, from the beginning a certain flexibility has been foreseen. We can deliver the umbrella application with a facility specific look-and-feel depending on the DNS name used, e.g. eaa.psi.ch, eaa.desy.de. We should also provide about three different layouts for facilities to choose from.

### **A1.2.7 Affiliation database**

An affiliation database must be built up to extend the attribute updater with real values. There has already been conceptual planning activities together with ESRF.

## **A1.3 WUO-Integration**

To unleash the umbrella application, all WUOs must implement some or even all of the necessary functionality. Luckily, in Europe the WUO systems cluster around only three different systems (VUO from Elettra, SMIS from ESRF and DUO from PSI), which keeps the overall integration effort minimal, since new developments can then be reused.

### A1.3.1 SAML2-SP at each WUO

Each WUO must install a SAML2 service provider software on a web server. This is absolutely necessary to implement the single sign-on process. The service provider is completely standardised and there are different implementations.

### A1.3.2 WUO Integration

Following processes must or should be implemented at each WUO participating:

- “Single Sign-On” process
- “Match existing user” process
- “Match new user” process
- “Attribute Updater” process with challenge-response handshake

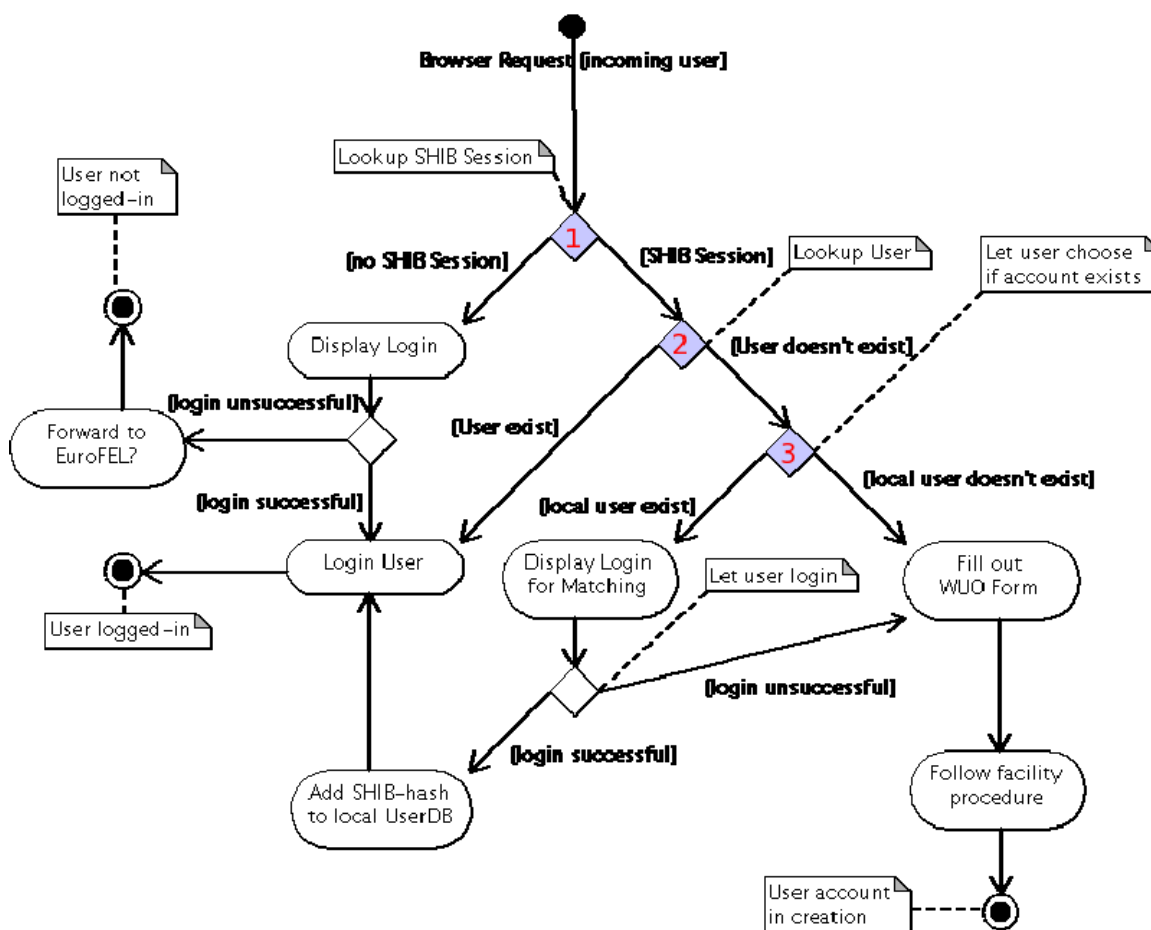


Illustration 21: Web SSO User Creation Pattern

- “Coaching dispatcher” process

### A1.3.3 Implementation effort at facilities

It's always difficult to estimate an amount of work for something unknown but we gathered experiences with the implementation of the DUO web user office software and base our estimations on this work.

Illustration 21 shows the process of “single sign-on”, “match existing user” and “match new user” which are absolutely necessary to be implemented, since they found the corner of the authentication system.

### A1.3.4 SAML2-SP

The WUOs must install a SAML2 Service Provider software, e.g. mod\_shib2 (Apache) or SimpleSAMLphp (PHP), to be able to receive SAML2 attributes. Since the page should be accessible when no EAA-Session exists, the SAML2 isPassive value must be set.

### A1.3.5 “Single Sign-On” process

The “Single Sign-On” process consist basically of an extension to the SQL SELECT statement which, besides querying for username and password, also queries for the incoming EAAHash.

Following code snippet (red and bold) can be used to enhance this generic user query:

```
SELECT
    USERNAME
FROM
    USERS
WHERE
    (USERNAME='user' AND PASSWORD='changeit')
OR
    (EAAHASH= ' f5bba3c6-6240-4ccf-8048-13dbb3405192 ')
```

This query can also be split in two queries to better distinguish between the sources of the authentication request:

```
SELECT
    USERNAME
FROM
    USERS
WHERE
    (USERNAME='user' AND PASSWORD='changeit')
```

And a query for the incoming EAA-Session:

```
SELECT
    USERNAME
FROM
    USERS
WHERE
    (EAAHASH= ' f5bba3c6-6240-4ccf-8048-13dbb3405192 ')
```

### A1.3.6 “Match existing user” process

User Matching is necessary if there is an incoming EAA-Session but no WUO user registered with it. It's important to use the existing “Login” and “Create User” procedures



already installed at the facilities, so that no new procedures must be installed and approved.

There is a chance that the user already has an existing account at the WUO and that the user wants to bind those accounts together – then a WUO login is performed and if successful, the found user tuple is enhanced in the USERS table with the incoming EAAHash

```
UPDATE
    USERS
SET
    EAAHASH='f5bba3c6-6240-4ccf-8048-13dbb3405192'
WHERE
    USERID='foundID'
```

### A1.3.7 “Match new user” process

If the user has no existing account the WUO's user creation process is used to create a new WUO user. The EAAHash must then be appended to the created user.

```
INSERT INTO USERS
    (NAME,...,EAAHASH)
VALUES
    ('Muster',..., 'f5bba3c6-6240-4ccf-8048-13dbb3405192')
```

### A1.3.8 “Attribute Updater” process with challenge-response handshake

The attribute updater process involves a cryptographic check, where we can provide implementing classes in Java and PHP. The process involves a user lookup in the local database, where a key for that specific user is retrieved and used for the cryptographic check.

```
SELECT
    EAAKEY
FROM
    USERS
WHERE
    EAAHASH like 'f5bba3c6-6240-4ccf-8048-13dbb3405192'
```

This retrieved key is then used the respond to the Umbrella system and used for verification of the existence of the user at the WUO.

If verified the WUO receives the user information and should incorporate it into the local database.

```
UPDATE
  USERS
SET
  NAME='Muster', ...
WHERE
  USERID='foundID'
```

### **A1.3.9 “Coaching dispatcher” process**

This process will be part of the upcoming coaching system and mainly involves the registration of beamline experts at the coaching system, allowing coaches to dispatch users with questions being too facility specific to the respective beamline expert.

## **Appendix 2 Umbrella+**

To maintain user and facility interest, future applications must be built. The ecosystem should be extended in a way which fosters easiness of use and maintainability. Clearly a roadmap should be established.

Furthermore a team of facility and IT experts should be formed to support the ongoing process of establishing the umbrella system.

## **A2.1 Publication Database**

Publications are valuable assets for facilities or affiliations, serving as an efficiency statement of the scientific work. A publication database with reference to researcher and facility could help with the accessibility to publications for outsiders.

Of course the references should be linked with the existing user and affiliation database.

## **A2.2 Remote Data Access**

As newer generations of detectors accumulate petabytes of data it will become more and more impossible for researchers to take home their data on a hard disk. Therefore remote access to experiment data will become vital.

## **A2.3 Remote Experiment Access**

Long traveling distances can make it difficult for researchers to visit a specific facility. Remote access to parameters or spectrums of an experiment performed by co-researchers could allow better use of infrastructure. Still researchers need to be at-site.

### **A2.3.1 Remote Experimenting**

Complete remote experimenting would allow parameters to be set from off-site, allowing

researchers to perform experiments with on-site facility-staff from almost everywhere.

## Glossary

- 1 Account  
A user account allows user to authenticate to system services and be granted authorisation to access them; however, authentication does not imply authorisation.
- 2 Authentication  
Authentication is the act of confirming the truth of an identity of a person. Who am I; the goal of the umbrella system is to identify a person uniquely europe-wide.
- 3 Authorisation  
Authorisation is the function of specifying access rights to resources. Which roles (i.e. Rights) do I have (e.g. facility access, computer resources), what is my function.
- 4 CAPTCHA  
***Completely Automated Public Turing test to tell Computers and Humans Apart***
- 5 Challenge-response mechanism  
A challenge-response mechanism is a set of protocols in which one party presents a question ("challenge") and another party must provide a valid answer ("response").
- 6 DNS name  
The *Domain Name System* (DNS) is a hierarchical naming system built on a distributed database which translates names meaningful to humans (e.g. [www.google.com](http://www.google.com)) into numerical identifiers associated with networking equipment.
- 7 DUO  
The *Digital User Office* (DUO) is the PSI Web User Office (WUO)
- 8 EAAHash  
The EAAHash is an internal unique identifier for an account in the umbrella system. It is mainly used by software components to identify users.
- 9 Email verification  
Email verification is a mechanism to verify the existence and legitimacy of an email address associated with an account. An email will be sent to the specified address containing a unique code. After entering this code an account can be enabled. The reason is to prevent fraud.
- 10 Failover  
Failover is the capability to switch over automatically to a redundant or standby computer system upon the failure or abnormal termination of a previously active application. The reasons are high availability and a high degree of reliability.

|                   |  |
|-------------------|--|
| 11 Federation     | A federation is a virtual assembly of web applications and user accounts which represents a whole community which can collaborate.   |
| 12 Java           | Java is an object oriented programming language released in 1995. The language derives much of its syntax from C and C++. Java is currently one of the most popular programming languages in use.                              |
| 13 LaTeX          | LaTeX is a document markup language and document preparation system. LaTeX is widely used in academia.   |
| 14 LDAP           | The <i>Lightweight Directory Access Protocol</i> is an application protocol for reading and editing directories over a network. A directory in this sense is an organised set of records.                                      |
| 15 Load balancing | Load balancing is a computer network methodology to distribute workload across multiple resources, to achieve optimal resource utilisation, maximise throughput, minimise response time and avoid overload.                    |
| 16 OpenID         | OpenID is an open standard that describes how users can be authenticated in a decentralised manner. The OpenID protocol does not rely on a central authority to authenticate a user's identity.                                |
| 17 PHP            | PHP is a general-purpose scripting language originally designed for web development to produce dynamic web pages. PHP stands for " <i>PHP: Hypertext Preprocessor</i> ".   |
| 18 PSI            | Paul Scherrer Institut   |
| 19 SAML2          | <i>Security Assertion Markup Language 2.0</i> is a version of the SAML OASIS standard for exchanging authentication and authorisation data between security domains. SAML 2.0 was ratified as an OASIS Standard in March 2005. |
| 20 SAML2-SP       | SAML2-Service Providers provide functionality to let users authenticate against an identity provider and to fetch the released metadata for providing the attributes to an application.  |
| 21 Shibboleth     | Shibboleth is a project that has created an architecture and open-source implementation for federated identity-based authentication and authorisation based on Security Assertion Markup                                       |

Language.

22 Single sign-on (SSO)

Single sign-on is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them.

23 SQL statement

The *structured query language* is a database computer language designed for managing data in relational database management systems.

24 Umbrella

The term umbrella describes the whole system planned, including authentication system and web applications.

25 VMware

VMware is an independent software vendor specialised in virtualisation technologies.

26 WUO

*Web-based User Office*, the application that supports a local user office in managing user-related issues (e.g. proposal handling, on-site user issues).