Everything You Always Wanted to Know About Umbrella

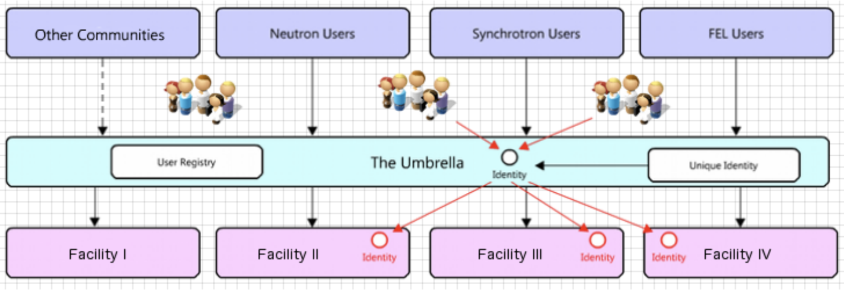
Version 1.1

The Umbrella Team

What is Umbrella (for users)

Umbrella is a *federated identity system* for the users of the (European) large neutron and photon facilities.
Identity system: Umbrella allows providing these users with a unique, *persistent* identity. That means that a user will be able to log in at any of the participating facilities and have access to the services offered. There will be only one person with this identity.
Persistent: Once defined, this identity will be valid for the rest of the academic life.
Federated: This identity is valid not only at one facility but holds at all partner facilities.

What is it good for?



Users of the photon and neutron facilities constitute a large community (with 30'000+ visiting scientists in Europe alone). At the moment the management of the experiments including identity management is performed locally on site via Web-based User Office (WUO) tools. However, users perform experiments increasingly at different facilities, about 30% on the average, in some research fields even up to 40%. They want to minimize the corresponding administration load and are interested in harmonized application surfaces. In addition, they need access to the data stored at the facilities and / or want to participate remotely in experiments. These trans-facility services need a federated identity management as provided by Umbrella. Furthermore, remote data analysis will become more important which again needs a federated identity management.

The direct advantage of the Umbrella environment for the user is that he/she has only one account for all partner facilities and once logged in he/she can access the services at these partner facilities without a need for a new identification (Single Sign On).

How can I use it?

Umbrella is built on top of the existing local IT infrastructures and it links its identity in a once-only action directly to the local identity at the respective facility. As this action is user-driven it avoids complex trust issues, which is a major complication for most other federated-identity systems.

This linking concept, however, implies that a user will get the new Umbrella identity but for the time being will still have the 'old' local identity at the local WUO, where, however, the remaining local account is seen only as backup. As a consequence of this structure, there are two ways of using Umbrella (for transparency, once-only registration and normal use are discussed separately):

Explicit registration (once-only): The user visits directly the Umbrella site (https://UmbrellaID.org) and registers for an Umbrella account. After that, goes to the respective WUO of choice, tells that he/she has an Umbrella account and logs in with the local WUO credentials. In this way, the user confirms to be the owner of this local account and from this moment on he/she has the right to access all related information (proposals, data etc.) also through Umbrella. This saves any complex trust procedures.

Implicit registration (once-only): The user logs in to a WUO of choice. Then on the website of a partner-WUO he/she will find the offer to umbrellify the account. If the user decides to do so, there is an implicit transfer to the Umbrella registration. There will be a minimum need for entering information; username is kept if possible (e.g. no duplication conflict, but because of security issues a password has to be entered).

Normal use: The user goes to the WUO of choice and logs in with the Umbrella credentials. If he / she decides to visit another WUO, no further login is needed (SSO functionality).

What has happened up to now?

Research at the European large photon and neutron facilities has been very successful as impressively demonstrated by the large number of high-profile publications and several Nobel prizes. However, there are developments within the experimental environment (e.g. novel detectors, need for remote experiment access, need for remote data access, access to new analysis techniques and tools) which call for an adaption of the experimental infrastructure. These requirements are quite similar for all facilities, thus a common approach appears to be highly advantageous. Giving the international user community access to these new developments requires a federated identity management on a higher and trans-facility level (i.e. at the moment European maybe later international).

As a reaction, the Umbrella project has been started as part of WP2 (work package 2) of the IRUVX-PP ESFRI (future EuroFEL; Free Electron Lasers of Europe) project. Soon it became clear that this need was going beyond the FEL user community and should be extended to the Photon and Neutron community at large, as the needs are very similar. Within WP2 of IRUVX-PP, functionality and architecture of Umbrella have been formulated and a prototype version has been produced. After that, work on Umbrella is being continued as part of the PaNdata ODI (WP3) and CRISP (WP16) EU FP7 programs. The development and implementation of Umbrella is carried through in close collaboration with other FP7 programs such as: CALIPSO (synchrotron facilities) and NMI3 (neutron facilities). In this way all European large facilities are represented as active partners or observers of the Umbrella project, thus covering with Umbrella as federated-identity system the whole photon / neutron large facility community with more than 30.000 users.

What is the present status?

As soon as Umbrella is installed and federated identity management is available, many trans-facility services are possible, which at present are still under development. The concept of the Umbrella project is not to deliver a closed box but rather this loosely coupled bundle of tools with a new component published as soon as it is ready. This concept also allows components to be defined in a flexible way in collaboration with the final users and according to the available resources. Instead of waiting until all functionalities are available, it has was decided to offer them to the users at the moment they are ready and provide a road map for the further developments.

Umbrella interacts closely with the local WUO systems at the individual facilities and the implementation / deployment follows a conservative procedure, in order to keep problems at a minimum. From the over a dozen facilities three have volunteered to participate in the first-wave (ESRF, ILL, PSI) implementation. The other facilities will follow in fall 2013.

Initially, these implementation phases cover only the basic functionalities of Umbrella (Login, personal information update, access to the local user office systems). During the whole process direct feedback by the users is extremely important as only in this way it will be possible to develop a system which complies with the real needs of the users.

What will be the future? What is the roadmap?

An important component of the Umbrella is the affiliation database, which is an essential element for allowing for a user- and facility-friendly management of user accounts. Development of this component is ongoing (ESRF) and will be concluded within the coming months.

As for every trans-facility system, there are legal issues to be solved as e.g. access rights, responsibilities. By design, Umbrella has been set up, that these resulting legal requirements are minimal and it is expected that they are resolved within a few months. There is no need for a time-zero for setting Umbrella into operation and facilities are free to decide when to switch to the Umbrella. Thus, facilities will be able to start the system till end of 2012.

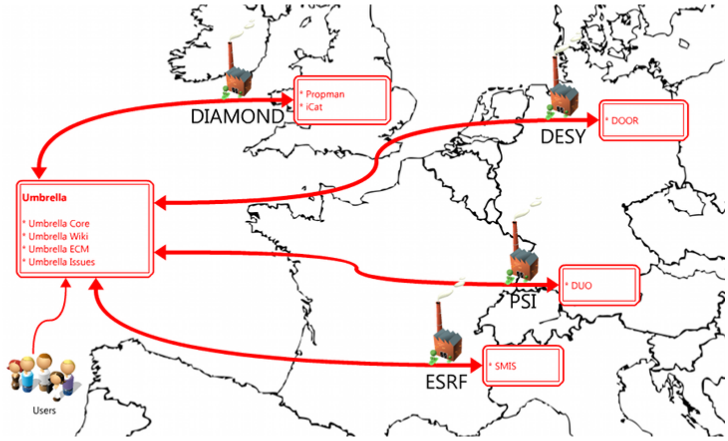
As soon as Umbrella is deployed, many novel user services will be possible like remote data access (e.g. ICAT/TopCat), remote experiment access (e.g. Moonshot), software catalog, conference services, publication service and many more. As resources are limited in close contact with the users a priority list will be established.

As soon as Umbrella is installed, one of the first options available will be to log in from the Umbrella to the local WUO. Remote experimental data access (ICAT/TopCat) is an ongoing topic of the CRISP and PaNdata EU projects and will be available within the next years. There are also concrete plans (Moonshot) for non-web remote access to experiments (passive: spectra and active: control).

What is Umbrella (for IT experts)

Characteristic properties of Umbrella:

- Umbrella is not yet another identification system, but it is built on top (= umbrella) of the already existing Web-based User Office (WUO) systems of the participating large scale facilities with the additional functionality to enable a unique user identification.



- In order to guarantee uniqueness, Umbrella has only one (1) identity provider (IdP).
- User information is stored in a hybrid database system, where the central part contains the information (e.g. username + password) for user identification. All other authentication information and all authorization information remain at the local WUO systems.
- Umbrella is a bottom-up system. Authentication information is provided and updated via self-service by the user with optional confirmation loops with authorities. Supervision is provided by the user office staff. This avoids complex trust structures and procedures.
- Umbrella communication is based on SAML, which is state of the art, and is designed by industry experts like e.g. EMC, Hewlett Packard, IBM, Microsoft, Nokia, Oracle, SAP, Boeing. It is also used by national federations in the (higher) education sector.
- The Umbrella user identity is persistent. It is not fixed to the home affiliation of the user which permits a permanent link of a user to a team or a dataset or document, also in case of an affiliation change.
- Umbrella is web-based and supports single sign on (SSO) functionality.
- Physically this one IdP is not be realized via only one central Umbrella server; there is a replication system, based on ldap replication and geoDNS technologies, in order to increase the uptime of the system and also to reflect the federal character of the system.