

Memorandum of Understanding for the Umbrella Federated Identity System

by and between

Institut Max von Laue – Paul Langevin (ILL)

European Synchrotron Radiation Facility (ESRF)

Paul Scherrer Institut (PSI), CH 5232 Villigen PSI

ALBA Cells, xxx- Barcelona

Deutsches Elektronen-Synchrotron (DESY), D-22607 Hamburg

Sincrotrone Trieste S.C.p.A. (Elettra), I-34149 Basovizza, Trieste

European XFEL GmbH, D-22761 Hamburg

Helmholtz- Zentrum Berlin für Materialien und Energie GmbH (HZB),

D-14109 Berlin

Science and Technology Facilities Council, Swindon SN2 1SZ, UK

Diamond Light Source (DLS),

XXXXXX, xxxxx

(hereinafter referred to individually as the Party or
collectively as the **Parties**)

Preamble

RECOGNIZING

- That the Parties are operating and developing photon and neutron facilities with a user community of >30'000 + visiting scientists in Europe alone.
- That about 30 - 40% of these users perform experiments increasingly at different European facilities, which increases the need for transfacility services such as:
 1. Access to and management of experimental data.
 2. Remote experiment access
 3. Access to efficient data analysis tools.
 4. Remote file access.
 5. Harmonised proposal forms
 6. Harmonized application surfaces
- That unified access to these transfacility services needs a unique, persistent user identification in the form of a Federated Identity Management System.
- That a Federated Identity Management System ("Umbrella") was developed for this community.
- That Umbrella is a European wide, community overlapping system, developed within the frame of different EU FP7 projects, namely: EuroFEL, PaNdata Europe, PaNdata ODI, CRISP, NMI3, and CALIPSO.
- That the development of Umbrella was performed within the collaboration under the coordination of PSI.

BEING UNDERSTOOD

- That a close cooperation between the neutron and photon facilities on federated identity management is needed in order to meet the technological and scientific challenges of novel and rapidly developing technologies in the field of transfacility access and services.

WHEREAS the importance of a Federated Identity Management System for the Photon and Neutron community has been recognized and therefore work packages on Federated Identity Management were included within all of the following EU FP7 projects, namely: EuroFEL, PaNdata Europe, PaNdata ODI, CRISP, NMI3, and CALIPSO.

WHEREAS in the frame of the project listed above Umbrella was realized as a European wide, community overlapping Federated Identity Management System, developed for the Photon and Neutron community.

Therefore the Parties have agreed the following MoU:

The Purpose of this MoU is:

To establish, based on the developed UmbrellaID, an efficient long-term collaboration between the Parties, in order to facilitate authentication and authorization procedures to access transfacility user services.

The preamble and appendices x, and x are an integral part of the present MoU.

ARTICLE 1 – Purpose and Scope of the Umbrella Federated Identity System

The Parties have agreed to jointly further develop, implement and operate (details are agreed upon by the SC and described in ANNEX I) a common identity system (Umbrella). The identity system provides a unique and persistent identity for users of the European Analytical Facilities - the UmbrellaID (see article 9b).

The Umbrella system enables single sign on (SSO) access to Service Providers (SP's) in the Umbrella Federation. This is an answer to increased demand for transfacility services (see Article 5).

The Umbrella system enables the Parties to share services and divide associated workloads like developing appropriate tools and maintaining services.

ARTICLE 2 – Collaboration Membership

Membership of the Umbrella Collaboration is obtained via the signature of this MoU. In adhering to this MoU, each Party undertakes to contribute to the on-going development and operation of Umbrella for the mutual benefit of all the Parties of the collaboration.

As a second possibility Parties can enter the collaboration as Participants. They have the right to use the Umbrella services, without additional rights and obligations.

ARTICLE 3 – Entry into force, duration, new parties, and modification

This MoU will come into effect at the date of signature and will be renewed tacitly on a yearly basis.

Changes to the MoU will be agreed by the Steering Committee.

The Members are keen to welcome new Parties into the collaboration after the entry into force of this MoU. Adding or removing Parties from the collaboration shall require a unanimous decision by the other members of the Steering Committee (cf. Article 4).

Parties are free to leave the consortium at any point.

ARTICLE 4 – Collaboration Management

The Parties of this MoU form a consortium which is composed of a Steering Committee (SC) in charge of organizational and managerial decisions and a Technical Team (TT) in charge of the technical aspects of the project.

The Collaboration shall be governed by the SC. Each Party nominates one representative to the SC who can delegate the authority at their discretion. The SC shall be chaired by a representative elected by simple majority for a duration of one year renewable.

The Steering Committee shall make decisions unanimously.

The SC shall meet regularly, at least once per year, to review progress achieved and discuss/decide upon strategic matters. Urgent matters can be decided between meetings by written procedure (via e-mail) by the SC. If a Party does not respond to a written procedure within reasonable time consent will be assumed. Technical issues will be delegated by the SC to the Technical Team (TT). Each Party nominates one representative to the TT who can delegate the authority at their discretion. The TT shall be chaired by a representative elected by simple majority for a duration of one year renewable.

ARTICLE 5 – Related infrastructure and services

Accounts

Anyone interested in any of the services offered by the Umbrella collaboration may register for an account at UmbrellaID.org. Registering for an account implies acknowledging the privacy policy and the terms of use published on UmbrellaID.org.

Identity System

The identity system is realized as a federated network, it is based on the existing user office systems of the analytical facilities. Authentication is provided by an additional central layer (Umbrella), which guarantees the uniqueness of the user identity. Authorisation of the users remains fully under the control of the local user offices.

The identity system consists of a distributed network of identity provider instances (IdP) and a federation of service providers (SP). The distributed infrastructure makes the Umbrella extremely robust. Even in the very unlikely event that the entire Umbrella system breaks down, the most essential services will remain fully functional irrespective of the status of the Umbrella system.

Services

The most essential services like proposal and beamtime handling are provided by the individual facilities web user offices (WUO), which implement the interface between the users and the facilities. A user once authenticated on UmbrellaID.org can use any of the WUOs he has registered to without the need to login again.

As another example some Parties store scientific data in archives accessible through local data catalogues. Through the federation of the data catalogues under the Umbrella a user will be able to access, transfer and manage his/her own data or share data with colleagues inside or outside a scientific collaboration irrespective of the physical location of the data and irrespective of the instrument or facility utilized to generate these data.

A number of additional services will become available in due course offering a rich eco-system accessible with a single sign-on.

Each Party can run any number of services and responsibility and rights for the service rely entirely on the Party providing that service. All services will be available to all users, but are subject to authorization, which is exclusively determined by the local SP and hence by the Party offering the service. For example, any user might implicitly be authorized on an open access scientific database or a software catalogue. On the other hand, the web user offices will always require a local registration and in some cases certain documents like a passport before granting access to beamlines or facilities.

ARTICLE 6 – Costs

Each Party shall be responsible for managing their own costs for the development and operation of the Umbrella system.

ARTICLE 7 – Responsibilities for performance of work

Each Party shall ensure that suitable staff is available to perform the activities covered under the present MoU.

ARTICLE 8 – Security

The TT will define and the SC will approve appropriate measures for protection against external and internal misuse of the Umbrella system. Each Party is responsible for making sure that their own security policy is not compromised by Umbrella services. The TT will be responsible for defining the security measures required for making this possible.

Granting or denying access to local services remains the responsibility of the individual Party. Every SP has the right to define his/her own rules

ARTICLE 9 – Umbrella account opening

The creation of an Umbrella account generates an Umbrella-ID which is immediately valid for authentication to access services provided by the Umbrella system. Umbrella account is only valid in combination with a local account.

ARTICLE 10 – Intellectual Property and Publications

The Parties agree that developments within the Umbrella collaboration will be released under the open source licence XXX (...to be discussed and written in the MoU).

Article 10a – Management of UmbrellaID.org

UmbrellaID.org is managed by the Umbrella collaboration, all corresponding certificates and registrations irrespective of the actual registrar shall be used only for purposes of the Umbrella collaboration.

ARTICLE 11 – Data Confidentiality

The amount of personal information stored in the Umbrella system will be kept at the strict minimum. Personal information shall not be used by any of the parties for any other purpose than described in article 1.

ARTICLE 12 – Validity

The Parties acknowledge that this MOU shall only be construed as an expression of their desire to accomplish the objectives described herein, recognizing that it is not intended to constitute a legally binding document. Therefore, any other specific activities must be negotiated in a form mutually acceptable to the Parties, in order to establish the respective rights and responsibilities in regard to such matters as rights in information and intellectual property (including inventions and discoveries, patents, copyrights and technical data), confidentiality, liability for injuries, damages, and other technical, legal, and/or administrative (including financial, where applicable) requirements or other commitments.

For ILL:

Mr. Andrew HARRISON
Director

&

Mr. Manuel RODRIGUEZ-CASTELLANO
Head of Administration Division

Signature

Signature

Date

For ESRF:

Signature

Date

For PSI:

Signature

Date

For DESY:

Signature

Date

For Alba-Cells:

Signature

Date

For HZB:

Signature

Date

For DLS:

Signature

Date