PaNdata ODI 1st Open Workshop

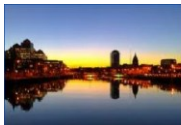Dublin 24-25/28th of March 2014

Co-located with the RDA 3rd plenary at Croke Park

https://indico.desy.de/event/1stow

Booklet of collected presentations

PART 2: UMBRELLA

Umbrella workshop at trinity college in Dublin 26th of March

Heinz Weyer:	Goal & Structure of Meeting
Björn Abt:	Address Updater: Proposed tools
Julien Savoyet:	Affiliation DB: ESRF tool
Mirjam van Daalen:	Affilliation DB: Minimal DB
Björn Abt:	Issue Handler
Alistair Mills:	ICAT integration
Mirjam van Daalen:	Moonshot (Switch)
Stefan Paetow:	Moonshot (DLS)
Mirjam van Daalen:	Memorandum of Understanding

Dublin Harmonisation Meeting
Umbrella and facilities

Intro (13:00-13:15)

13:00 [0]   Goal & Structure of the meeting   H.J. Weyer

Address updater (13:15-14:00)

13:15 [0]   Proposed tool   B. Abt
13:30 [0]   Discussion & decision   M. van Daalen

Affiliation db (14:00-14:50)

14:00 [0]   ESRF tool   J. Savoyet / D. Porte
14:15 [0]   Minimal db   M.van Daalen
14:30 [0]   Discussion & decision   M. van Daalen

Issue handler (14:50-15:30)

14:50 [0]   Proposed tool   B. Abt
15:10 [0]   Discussion & decision   M. van Daalen

New functionalities (15:30-16:05)

15:30 [0]   ICAT   A. Mills
15:45 [0]   Moonshot (SWITCH)   M. van Daalen
15:55 [0]   Moonshot (DIAMOND   S. Paetow

Coffee (16:05-16:20)

Umbrella future (16:20-17:00)

16:20 [0]   Operation scheme   R. Dimper
16:40 [0]   MoU   M. van Daalen

H2020 (17:00-18:00)

17:00 [0]   ESFRI, PaNSIG & Co   R. Dimper

- ❑ ***This is now the 6th meeting in this series***
  - ❖ Still more than 2 dozen participants, not bad

- ❑ ***Workshop sandwiched between a powerful application and a future project***
  - ❖ Indication of its role
  - ❖ No island or auto-centered tool
  - ❖ Meaningful only
    - o As basis of other tools
    - o As a federated system for European facilities

❑ *Umbrella already in operation at many sites*
  ❖ DESY
  ❖ DIAMOND
  ❖ Elettra
  ❖ ESRF
  ❖ ILL
  ❖ ISIS
  ❖ PSI

❑ *But still many open ends*
  ❖ Technical
    o See last December meeting
  ❖ Managerial
    o MoU
  ❖ Operational
    o Interplay users <-> user offices <-> IT support
  ❖ Strong need for action

Important issues

- ❑ **Closer contact between developers and practitioners**

- ❑ **Legal document**

- ❑ **Operational agreement**

- ❑ **Future issues**
  - ❖ short term
    - o Address updater
    - o Affiliation database
    - o Issue handler
  - ❖ mid-term
    - o ICAT
    - o Moonshot
  - ❖ Long-term
    - o H2020 actions

ESRF meeting

❑ *Intense discussion between IT people and UO representatives*

❑ *Detailed discussions, concept and(!) usability*
  ❖ Address updater 🙂
  ❖ Affiliation database 🙁
  ❖ Issue handler 🙂

❑ *Proposal to plenary meeting*
  ❖ Short presentation
  ❖ Decision

IT Experts vs. UO Experts

❑ *IT Experts:*
  - ❖ Highest priority: clean, attractive concept
  - ❖ Potential for *future* extensions

❑ *UO Experts:*
  - ❖ Highest priority: well defined and easy operation
  - ❖ Good performance *now*
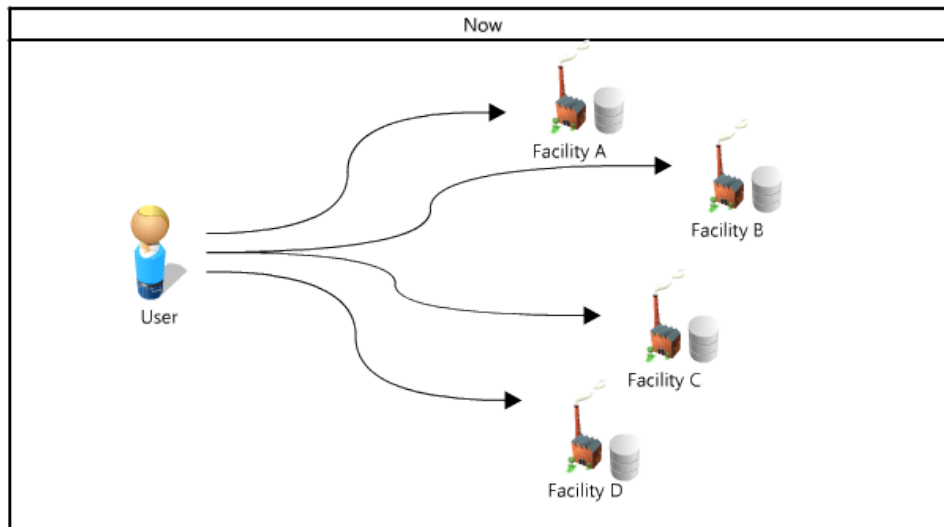
❑ *Goal:*
  - ❖ Combine both views

Thank you

Address Updater Proposed Concepts

Björn Abt

Address Updater Background:

- Let a user update his address just once
- Similar procedures on same data (changing addresses)
- Share resources and save time on a european scale
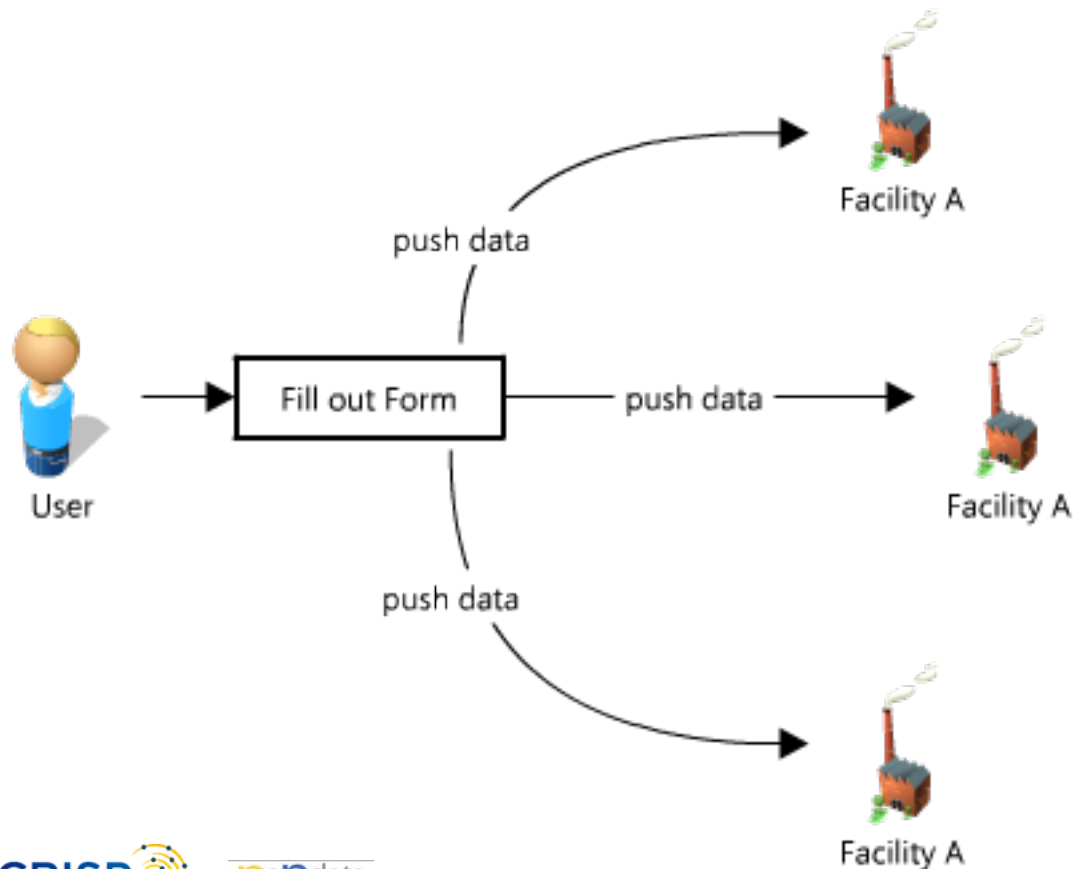- Do things once and not everywhere

User Address Update Now:

- Total Workload = W*N
- W = Workload for user for a single facility to complete task
- N = Number of facilities where the workload must be done

User Address Update Harmonised:
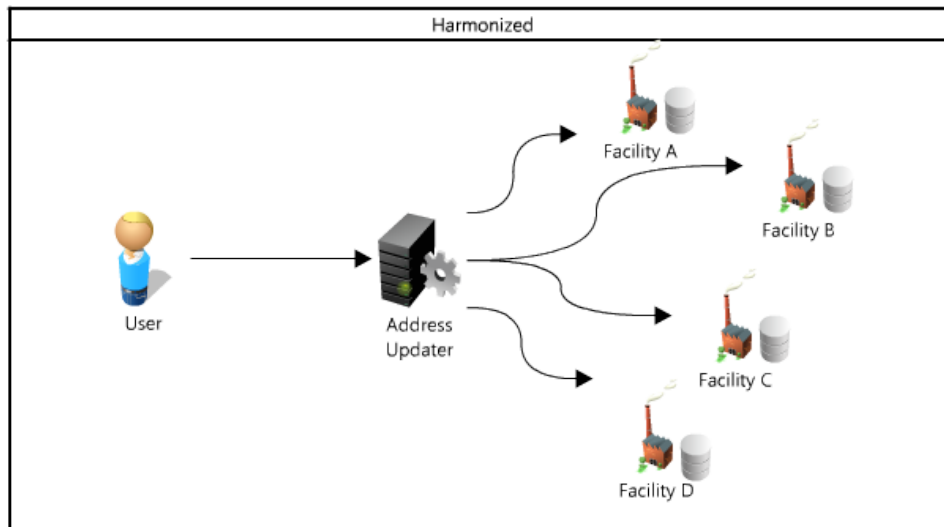
- Total Workload = W
- W = Workload for user for a single facility to complete task
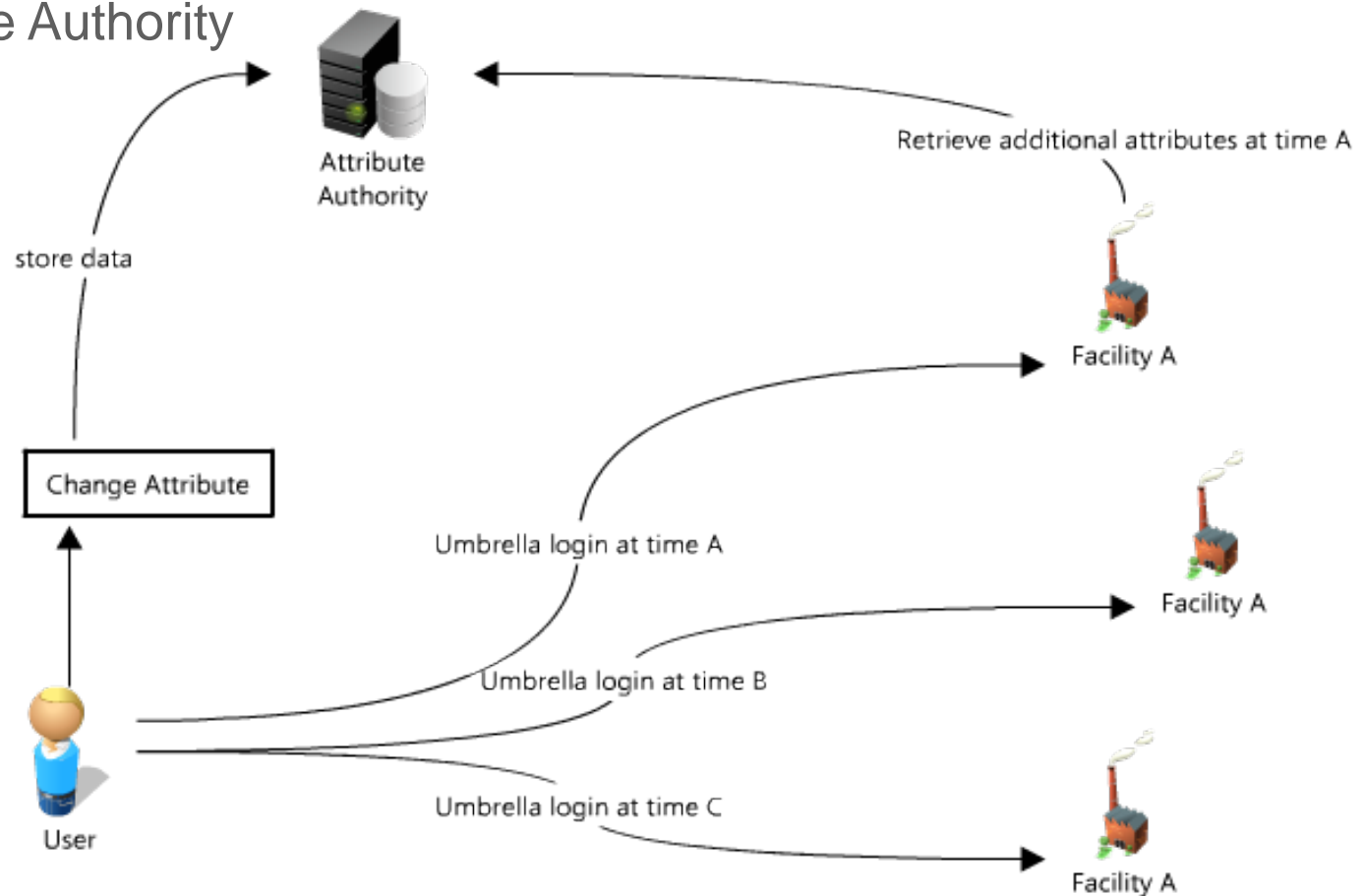
Attribute Distribution

Attribute Distribution

- The user fills out a form with his changed attributes and submits it
- The data is pushed to facilities which can integrate the changes in the local databases
- The data is not permanently stored at the Umbrella

Attribute Authority

Attribute Authority

- The user changes his attributes at an external source
- The attributes are persisted
- When login in to a service, the service can fetch additional attributes from an attribute authority

Thank you for your attention!

SMIS & ICAT & European Affiliation Database

Presented by D.Porte & J. Savoyet

Several projects at the ESRF in the scope of the Umbrella

Where are we now?

-SMIS in the Umbrella (Stefan Schulze)

-ICAT implementation (Nicola Bessone, Christophe Cleva, Alistair Mills, Julien Savoyet)

- European Affiliation Database (Julien Savoyet, Dominique Porte)

-DOI specification and implementation (Julien Savoyet, Dominique Porte)

Umbrella (Stefan Schulze)

Link your Account

- Login to my ESRF User Portal (SMIS) account

NEW You can now login through the Umbrella.

Account name : [ ] Password : [ ] Login

Please note: If you are an ESRF staff member you should use your site login and password!

Umbrella Login

- Login to my ESRF User Portal (SMIS) account

If you want to use your Umbrella account you need to log in first with your local account!

Account name : schulze Password : ●●●●●●●● Login

Please note: If you are an ESRF staff member you should use your site login and password!

UP Login
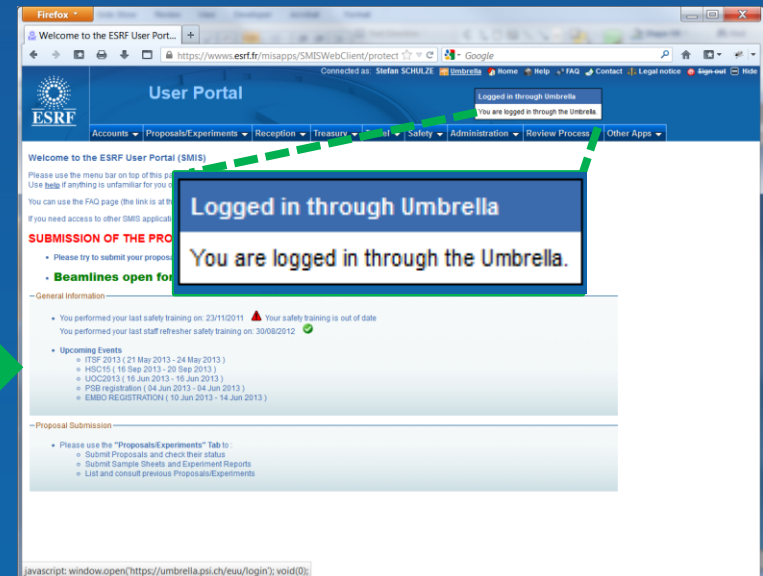
Link

Do you want to link your local User Portal account to the **Umbrella** account which you are currently logged in to ?

If yes, for future visits you only need to login to the Umbrella. If you select the User Portal while being logged into Umbrella you will not need to re-authenticate anymore.

Yes   No

Done

Logged in through Umbrella

You are logged in through the Umbrella.

Link your Account
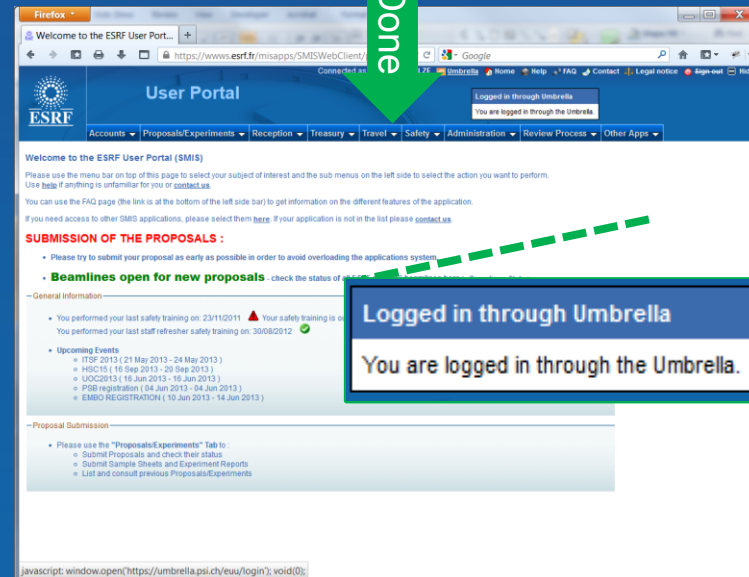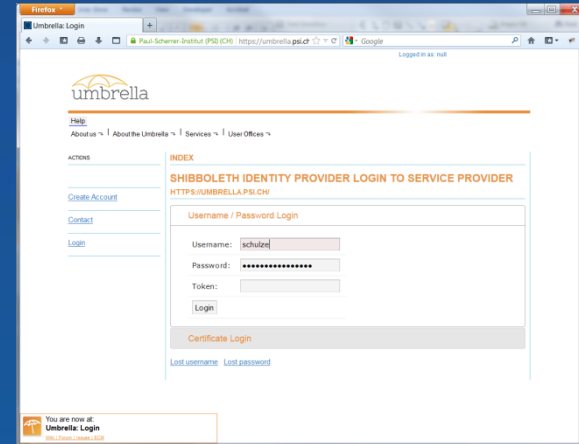
You still keep the possibility to log in locally
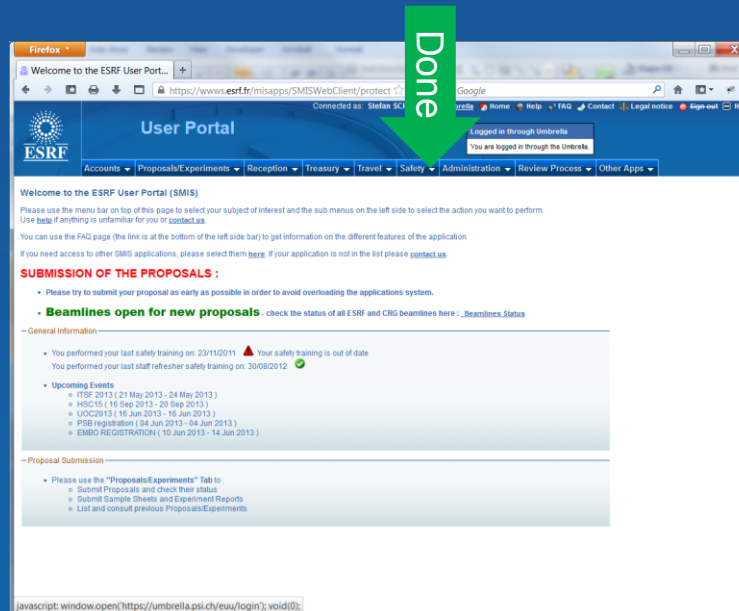
ICAT

-ICAT is installed

-Nicola Bessone customized ICAT to collect data from a beam line (id19),
-Christophe Cleva is continuing the implementation

-Data is collected from SMIS & TomoDB

-ESRF is in the "service verification" game

DOI (Digital Object Identifier) is a persistent identifier that allows referring uniquely any item of intellectual property on digital networks. In research, DOIs are alrea

European Synchrotron Radiation Facility

WP7 - Preservation

-Long-term data preservation

-DOI

DOI (Digital Object Identifier) is a persistent identifier that allows referring uniquely any item of intellectual property on digital networks. In research, DOIs are already used for a wide variety of scientific data: texts, images, sounds, videos, datasets, raw files, software...

European Affiliation Database

https://wwws.esrf.fr/ead/preprod/EvuoFront/mockup/login/
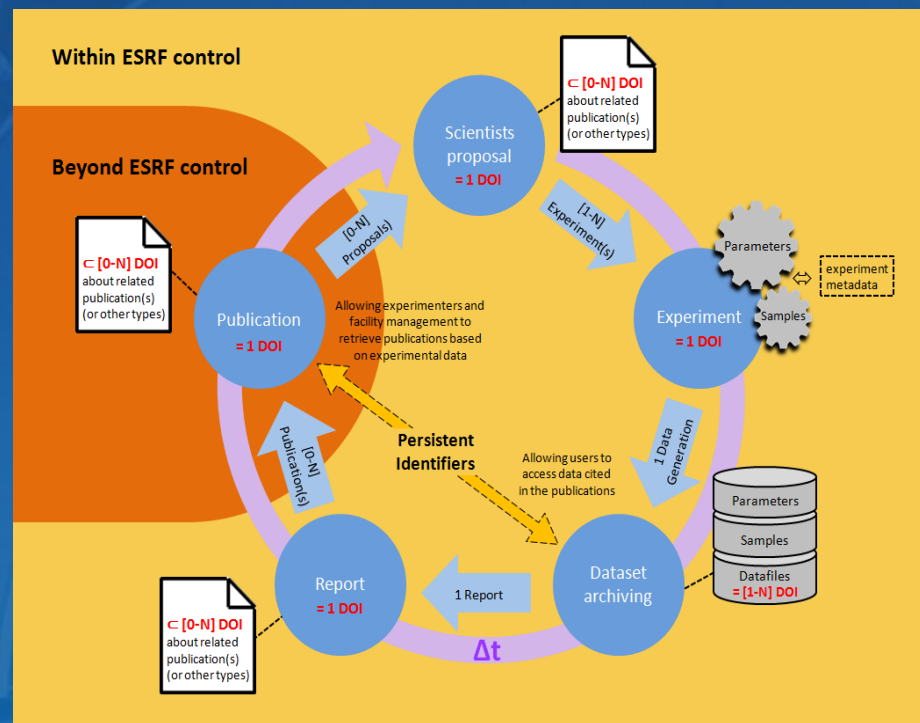
- 2011 - first specification

- Test period to collect very last feedback

- User Office role

- Content based on ESRF affiliation database

| Harmonization Meeting Hamburg / 21 January 2013 | PaNdata Meeting Lund / 12 March 2013 | Harmonization Meeting Berlin / June 2013 |

| EAD Project Specification | EAD Database Design | EAD Database implementation | EAD Web Forms Mock-up | EAD "Ergonomic Interface" Mock-up | EAD developments | EAD "Trial Prototype" launch | Umbrella Integration & EAD Maintenance |

End Of Developments
ESRF / July 2013
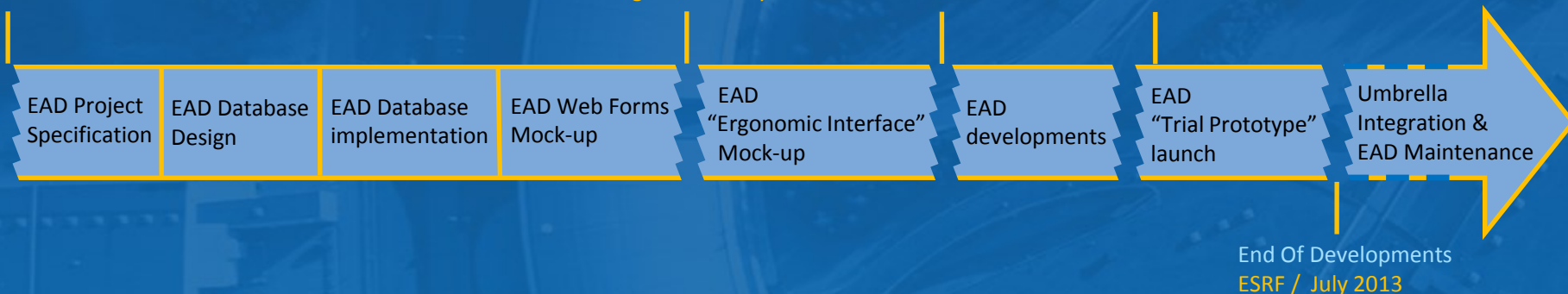
European Affiliation Database

The work done by ESRF can be used in different ways:

- Common European Affiliation database shared by facilities (initial goal).

- EAD included in the Umbrella portal

-Replacement of a local AD system by the EAD software application.

European Affiliation Database

-demonstration

Umbrella AAI next steps..

Mirjam van Daalen

Todays discussions:

Part 1: Adress updater

Part 2: Issue handler

Part 3: Affiliation data base

Part 4: MoU

Discussion address updater:

- Was accepted and proposed to the plenary meeting today (ESRF meeting Jan. 2014).
- Harmonised list of fields that are merged is documented in the holy list.
- Facilities who have more entries than the harmonised list have to fill in the entries manually.

Action: Implementation address merger within extension PaNdata project until Sept. 2014

Meeting 20.01.2014 @ ESRF

- Discussion on usefulness of a central affiliation data base.
- User offices made clear that it is not easy to update affiliations in the local database.
- Attempt was made at ESRF, mission impossible.
- Main problem is the merge of all different databases.
- Is a EU AFD feasible?

Umbrella affiliation data base

Conclusions ESRF meeting Jan 2014

- Keep local data data bases as they are (minimalistic approach)?

Why do we need a common AFD?

- Database is necessary for statistics, statistics is the main reason for having it, the better the database the better the statistics.

- Address updater would be easier.

- Lobbying funding agencies.

Next steps proposed

- Divide postal address from department or room number.

- Create extra column, if it is used by more facilties, the weight of the affiliation is increased.

- Create small working group?

Umbrella issue handler

Discussion issue handler:

- Was accepted and proposed to the plenary meeting today (ESRF meeting Jan. 2014).

- User offices can answer questions themselves or forward them to the issue handler.

- Implementation issue handler within extension PaNdata project until Sept. 2014

Umbrella MoU

Status and actions

- MoU should be signed ASAP
- Copy on Indico site harmonisation meeting.
- Version by editorial group is status November 2013, meeting at ESRF.
- How is the situation at the different facilities?
- Is everyone ready to sign?

Action: Feedback from legal offices until mid of June 2014.

Thank you for your attention!

Umbrella Support Workflow

Björn Abt

Umbrella Support Workflow:

- Support Roles
- Support Workflow
- Ticketing System
- Release Planning

Support Roles

- Roles are important for an efficient routing of tickets
- A ticket is always assigned to a role not a person
- The abstraction from a specific person is useful to make persons interchangeable

Roles List

Name of Role	Description of Role	Escalation
User	Umbrella Enduser	↓
Service Provider	The Entity responsible for running a specific service	↓↑
Local IT	The local IT department at a specific facility	↓↑
Umbrella IdP Team	The Umbrella IdP consist of SAML experts from facilities who are responsible to run physical nodes of the logical IdP	↓↑
NREN	National Research and Education Networks are responsible for running the National Federations, e.g. Switch, Janet, et. al.. They do have a long record of running SAML federations and are willing to give specific SAML support.	↑

Support Workflow
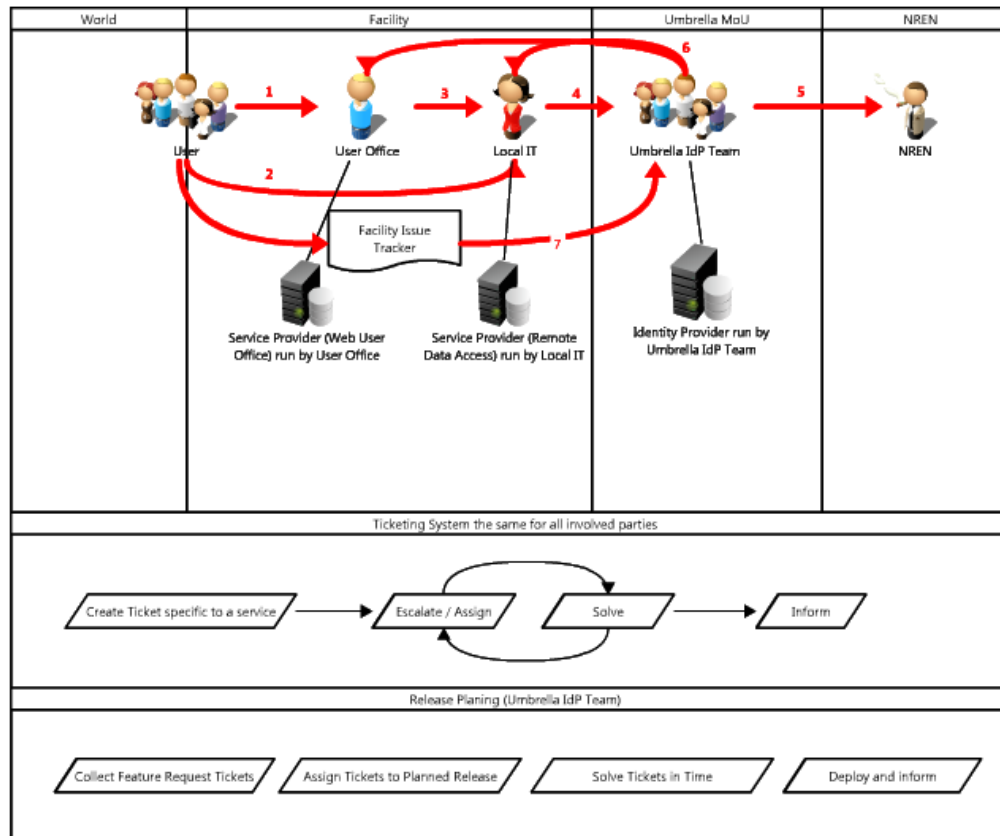
Support Workflow

Nr.	Description
1	The user contacts the user office regarding a problem with the WUO. At this point the user might be asked to create a ticket for his issue. The user office might be able to solve this issue independently and close the ticket.
2	The user contacts the local IT regarding a problem with a service run by the local IT. The user might be asked to create a ticket for his issue. The local IT might be able to solve this issue independently and close the ticket.
3	The user office escalates a problem to the local IT when it is unable to solve this problem independently. The local IT might be able to solve this problem and close the ticket.
4	The local IT escalates a problem to the Umbrella IdP Team when it is either unable to solve it or if the source of the problem resides at the IdP level.
5	If the Umbrella IdP Team is unable to solve a problem because it requires to deep SAML knowledge it can contact a NREN.
6	In certain cases the root of the problem doesn't reside on the IdP and therefore the issue is assigned either to the user office or the local IT.
7	The user can also use the local facility issue tracker to submit a ticket there and let the local IT escalate to the IdP Support Team if necessary.

Support Workflow

- Creating ticket
- Solving issue
- Escalating issue
- Assigning issue
- Preventing deadlocks and endless loops
- Informing involved parties

Ticketing System

- The ticketing software to be used must still be defined
- A certain amount of data must be gathered for a ticket to be resolved:
  - Title
  - Description
  - Reporter
  - Assignee
  - Type
  - Status
  - Role
  - History

Ticketing System Types and Status

Type List
Issue
Feature Request
Feature

Status List
New
Reopened
Assigned
InProgress
Feedback
Resolved
Testing
Deployment
Closed
Rejected

Release planing

- Releases should happen in a periodical way.
- Release numbers consist of
  - Major number – Release all 2 years
  - Minor number – Release all 0.5 years
  - Subminor number – Bugfixes and Patches

  - Example: Version 3.2.6

Release planing

- Issues can be converted to feature requests
- Feature requests are collected and assigned to a specific release number
- Releases must be tested. Procedures still to be defined.
- After testing a release it must be deployed. Procedures still to be defined.

Thank you for your attention!

Piloting with Umbrella

Ann Harding, SWITCH

Mirjam van Daalen, PSI

Umbrella Harmonsiation Meeting

Dublin March 2014

connect • communicate • collaborate

A Quick Recap – GN3plus Pilots
Helping communities benefit from federated identity

Collaborate with international user communities to increase usage of AAI infrastructure.

Act as an expert partner for large pan-European projects with AAI requirements.

Coordinate a set of two or three projects between GÉANT and user communities addressing their federated-identity concerns.

Umbrella selected as one of the key projects in Y1

connect • communicate • collaborate

GN3plus Overview of Pilots
User Community Pilots

Make ELIXIR services available on a pan European basis
Investigate requirements for LoA

Bridge between the "Umbrella" persistent federated identity and eduGAIN
Pilot non web access

Make DARIAH DE services available via eduGAIN
Encourage attribute release based on GÉANT CoCo

Umbrella Pilot in Detail

eduGAIN Bridging

- Evaluation of Lasso found the application not suitable
- Alternative approach developed
- Architecture designed
- Successful proof of concept carried out on test server
- Includes WAYF to find the right Identity Provider
- Valuable learning experience for Umbrella and GÉANT

Moonshot

- Implementation of IdP, radius infrastructure, SSH server underway
- On target to complete a little ahead of schedule
- Explore doing international demo early?
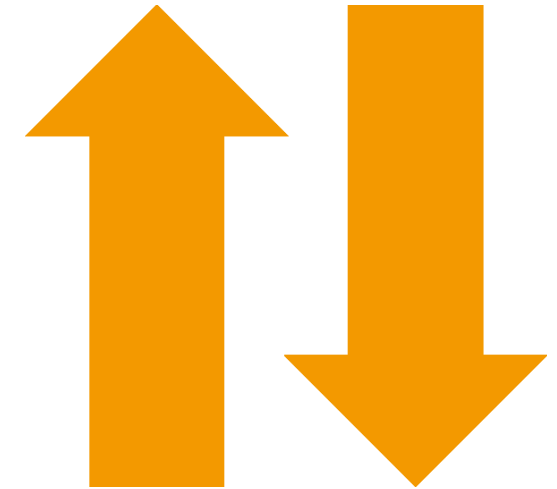
Moonshot + Umbrella

Using Moonshot with Umbrella at Diamond

What is...?

- Moonshot
  - JANET initiative for federating non-web authentication
  - Now an IETF RFC (RFC4462/7055-7057).

- eduroam
  - World-wide RADIUS authentication infrastructure for educational orgs (for free Internet)

- Umbrella
  - Everyone here knows what it is

What have Diamond done so far?

- Connected Moonshot PoC with eduroam authentication (June '13)

- Added Umbrella as additional authentication source to PoC (late Aug '13)

- Published Jasig CAS ABFAB authenticator on Maven Central (Nov '13)

- Built Shibboleth ECP client together with DARIAH-DE (Dec '13/Jan '14)
  - Used indirectly in new iCat Shib2Local authenticator

- Launched pilot beamline with Moonshot + Umbrella using above (Mar '14)

How does it work?

- RADIUS uses username@realm for authentication

- Umbrella IDs become 'UmbrellaUser@umbrellaid.org'

- 'umbrellaid.org' realm tells RADIUS which server to use
    - Returns EAAHash as Chargeable-User-Identity attribute
    - Moonshot can make Umbrella return proper SAML over RADIUS
    - To be extended as part of GÉANT part of Moonshot

What next?

- Continue to work with JANET on Moonshot
    - Stefan moving to JANET in April to continue liaison role from there

- Extend Umbrella-over-RADIUS
    - Use freeradius-pysaml2 to obtain SAML assertions dynamically from Umbrella IdP
    - Work with Björn et al to extend this

- Demo to Diamond management + interested parties
    - Moonshot + Umbrella + eduroam **works**

Demo + Questions?

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   &   Mr. Manuel RODRIGUEZ-CASTELLANO
Director   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