DELIVERABLE REPORT

WP8 JRA3 – Research on the e-infrastructure for data and information management

D8.3

Internal Test of the Information System

28 February 2017

M18

[illegible]

NFFA-Europe has received funding from the EU's H2020 framework programme for research and innovation under grant agreement n. 654360

nffa.eu

PROJECT DETAILS

PROJECT ACRONYM	PROJECT TITLE
NFFA-Europe	NANOSCIENCE FOUNDRIES AND FINE ANALYSIS - EUROPE
GRANT AGREEMENT NO:	FUNDING SCHEME
654360	RIA - Research and Innovation action
START DATE	
01/09/2015	

WP DETAILS

WORK PACKAGE ID	WORK PACKAGE TITLE
WP8	JRA3 – Research on the e-infrastructure for data and information management

WORK PACKAGE LEADER

Stefano Cozzini (CNR-IOM)

DELIVERABLE DETAILS

DELIVERABLE ID	DELIVERABLE TITLE
D8.3	Internal Test of the Information System

DELIVERABLE DESCRIPTION

The deliverable presents the internal test of the information system, including standard use cases.

EXPECTED DATE	ESTIMATED INDICATIVE PERSONMONTHS
M18 28/02/2017	6

AUTHOR(S)

Rossella Aversa (CNR-IOM), Stefano Cozzini(CNR-IOM)

PERSON RESPONSIBLE FOR THE DELIVERABLE

Stefano Cozzini(CNR-IOM)

NATURE

R - Report

DISSEMINATION LEVEL

☒ P - Public

☐ PP - Restricted to other programme participants & EC: (Specify)

☐ RE - Restricted to a group (Specify)

☐ CO - Confidential, only for members of the consortium

REPORT DETAILS

ACTUAL SUBMISSION DATE	NUMBER OF PAGES
23/02/2017	13

FOR MORE INFO PLEASE CONTACT

Rossella Aversa (CNR-IOM) Tel. +39-040-3787515 Email: aversa@iom.cnr.it

Version	Date	Author(s)	Description / Reason for modification	Status
0	10/02/2017	Rossella Aversa	First draft	Draft
1	14/02/2017	Stefano Cozzini	Second draft	Revision
2	22/02/2017	Rossella Aversa	Final version	Final

Contents

Executive Summary 4
1.Introduction 4
1.1 IDRP user description 4
2.Design specification and testing procedures 5
2.1 Creation of new IDRP user/First Login 5
2.2 First Login+1 6
2.3 Data/Metadata Access procedure 7
2.4 Publication through B2SHARE 8
3.Conclusions 9
Appendix APIs details 10
A.1 APIs exposed by the NFFA Portal 10
A.2 Interaction with the IDRP portal APIs 11
References 12

Executive Summary

This deliverable presents all the procedures and actions tested to provide a shared authentication mechanism across NFFA facilities.

The Authorization and Authentication Infrastructure (AAI) as described in deliverable D8.1 [1] has been implemented by KIT [2] and CNR-IOM [3] in collaboration with Promoscience srl [4]; procedures and mechanisms to link the information system to the NFFA Information and Data Repository Platform (IDRP) has been tested on the CNR-IOM OpenStack cloud infrastructure [5].

1. Introduction

This section acts as a short reminder on the main Authorization and Authentication concepts needed to introduce the design specifications of the implemented prototype. More details are available in the deliverable D8.1 [1].

The basic requirements the information system is asked to fulfill for the NFFA IDRP are the following:

- A primary entry point for the NFFA users, which is the NFFA portal, for registration/login/changes;
- A mechanism to associate/link/replace the local user authentication of each facility to an integrated and federated distributed Authorization and Authentication Infrastructure (AAI);
- A mechanism to allow NFFA users and external (not registered) users to directly browse the IDRP, without having to register on the NFFA portal.

1.1 IDRP user description

In this section, the possible scenarios that may arise when a user wants to access the IDRP are presented. The following user description may also be considered a glossary, which to refer to in this document.

The possible IDRP user scenarios are the following:

1. **Guest user**: Registration is not needed. The IDRP can be web browsed ([6] for the time being, only though a VPN) without any authentication. In this case, only the basic metadata associated to the proposal (PI, proposal ID, title) are visible.
2. **Registered user**: The user registers on the NFFA portal [7], and the user ID is communicated to the IDRP. In addition to the proposal basic metadata, in this case the user can see all the data and associated content metadata which are made public to the NFFA users by the PI of the proposal.
3. **Registered + associated user**: The user, who has already registered, is associated to the proposal by the PI. In this case, the user can see, access, and modify data related to even not-public measurements concerning the proposal s/he is associated to.

4. **PI of the project**: S/he is the reference person for the accepted proposal. Information about his/her identity and his/her privileged role is one of the basic metadata associated to the proposal, contained in the JSON file sent by the NFFA portal to the IDRP when a proposal is accepted.

2. Design specification and testing procedures

In this section, the possible actions implemented according to the information system design [1] are described. All these procedure has been tested on the prototype deployed on the CNR-IOM Openstack cloud [5].

2.1 Creation of new IDRP user/First Login

This action is the first one needed to access the IDRP as (at least) registered user. The steps of the designed procedure, depicted in Figure 1, follows:

- The user accesses the IDRP webpage and finds a login button
- The user is redirected to the NFFA portal where s/he can register an account
- After successful login, the portal creates a unique and temporary authentication Token, and locally saves it. Then, the portal redirects (by a POST request) the user to the IDRP including userId and authentication Token in the body of the request
- The IDRP queries the NFFA portal to check the validity of the token:
    - Success: A new IDRP user with the provided userId is created and the logged in user is stored in the session
    - Failure: No IDRP user is created, the user is redirected to an error page
- Once the proposal is approved, a JSON file with all the relevant proposal metadata is exchanged
- The proposal JSON document received by the IDRP contains the PI as authorized NFFA user. The IDRP has then to create a "preliminary" user for this PI in order to assign proper permissions

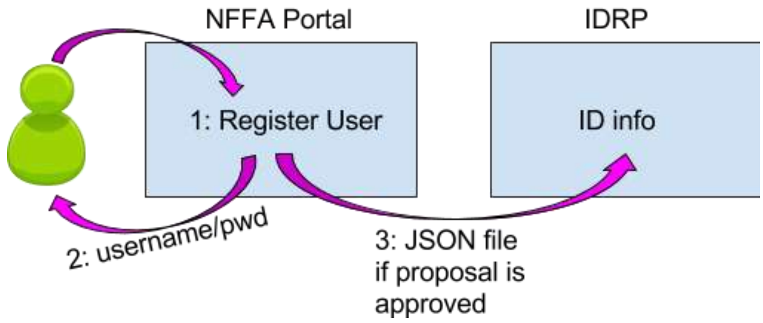


Figure 1: Schematic view of the user registration on the NFFA portal

This procedure has been implemented and tested, and a RESTful interface (described in details in Appendix) has been developed by Promoscience srl [4].

2.2 First Login+1

This action, illustrated in detail in Figure 2, pertains to an already registered user, who wants to login to the IDRP. This can be done either via the IDRP user interface [6] or via the NFFA portal [7]. This procedure has been tested and validated.

Via the IDRP, the steps are the following:

- The user clicks the login button and gets redirected to the NFFA portal login web page
- The user provides username+password
- The IDRP validates the token and the existence of the user by its id:
    - Success: The logged in user is stored in the session
    - Failure: The user is redirected to an error page

Via the NFFA portal, the steps are the following:

- The user logs in directly at the NFFA portal
- The user provides username+password
- The portal checks credentials and allows/denies login
- The portal provides a link to the IDRP that mimics the redirect for the “first login” case, if the user wants to go to the IDRP keeping her/his session

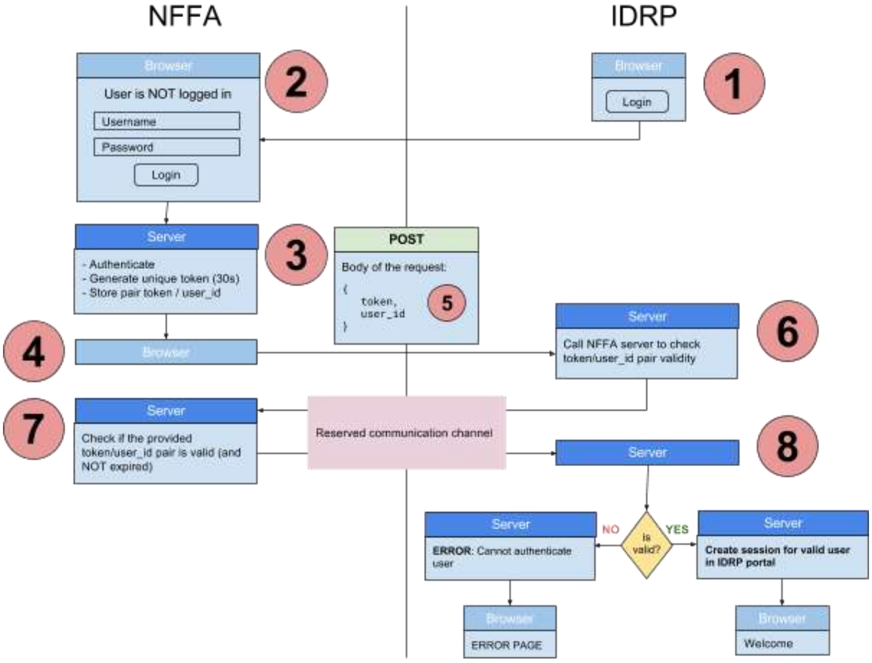
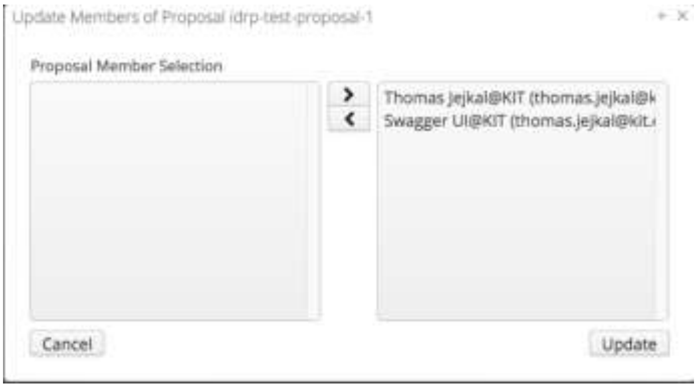

NFFA
IDRP
Browser
Login
1
Browser
User is NOT logged in
Username
Password
Login
2
Server
- Authenticate
- Generate unique token (30s)
- Store pair token / user_id
3
POST
Body of the request:
{
token,
user_id
}
5
4
Browser
Server
Call NFFA server to check token/user_id pair validity
6
7
Server
Check if the provided token/user_id pair is valid (and NOT expired)
Reserved communication channel
Server
8
Server
ERROR: Cannot authenticate user
NO
Is valid?
YES
Server
Create session for valid user in IDRP portal
Browser
ERROR PAGE
Browser
Welcome

Figure 2: Schematic view of the login+1 procedure

2.3 Data/Metadata Access procedure

Registered users can now access the basic metadata of project, proposals and experiments. Thus, the prerequisite to access data/metadata in the IDRP is a successful “First Login” or “First Login+1”. Depending on permissions, access to published measurements and datasets can also be possible if the prerequisite is not fulfilled.

Access to measurement metadata and data assets of a given proposasl is restricted to PIs and all registered+associated users nominated by the PI. This procedure has been tested on the IDRP user interface [6], and is shown in Figure 3.

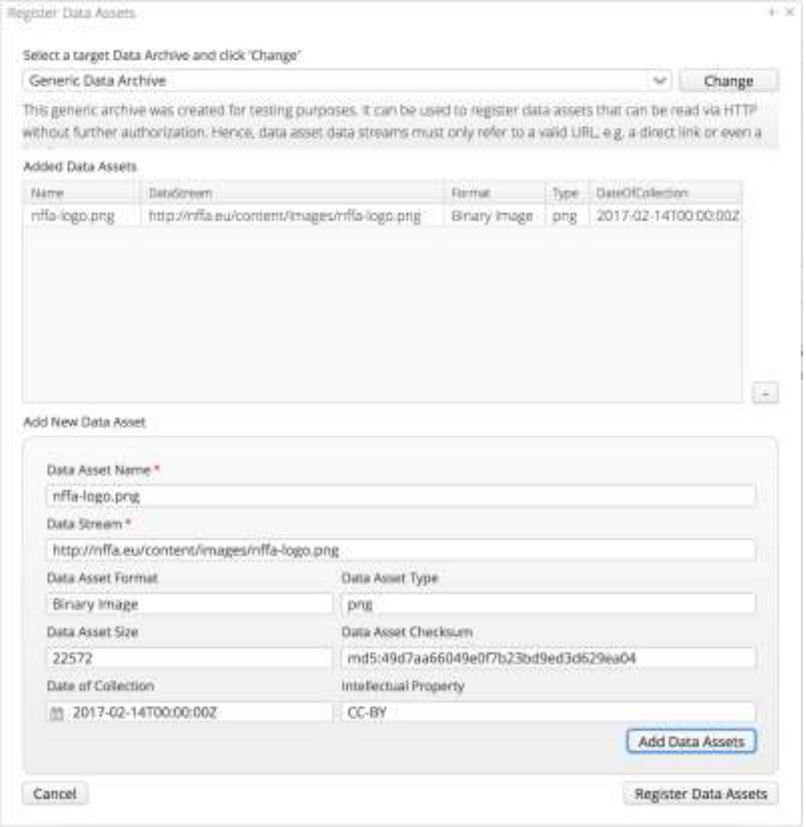

Update Members of Proposal idrp-test-proposal-1

Proposal Member Selection

Thomas Jejkal@KIT (thomas.jejkal@k
Swagger UI@KIT (thomas.jejkal@kit.

Figure 3: View of the procedure to associate registered members to the proposal

To register data assets (still only available at the repository where they have been stored by the user) to a measurement, the Pi of the proposal has to manually provide any valid URL as a data asset's data stream. An example of the data asset registration procedure is shown in Figure 4. In the future, this process is planned to be automated.



Select a target Data Archive and click 'Change'

Generic Data Archive

This generic archive was created for testing purposes. It can be used to register data assets that can be read via HTTP without further authorization. Hence, data asset data streams must only refer to a valid URL, e.g. a direct link or even a

Added Data Assets

Name	DataStream	Format	Type	DateOfCollection
nffa-logo.png	http://nffa.eu/content/images/nffa-logo.png	Binary Image	png	2017-02-14T00:00:00Z

Add New Data Asset

Data Asset Name *: nffa-logo.png

Data Stream *: http://nffa.eu/content/images/nffa-logo.png

Data Asset Format: Binary Image

Data Asset Type: png

Data Asset Size: 22572

Data Asset Checksum: md5:49d7aa66049e0f7b23bd9ed3d629ea04

Date of Collection: 2017-02-14T00:00:00Z

Intellectual Property: CC-BY

Figure 4: IDRP procedure for registering data assets to a measurement

2.4 Publication through B2SHARE

Only registered+associated users can publish a measurement. Thus, the prerequisite for this action is a successful "First Login" or "First Login+1".

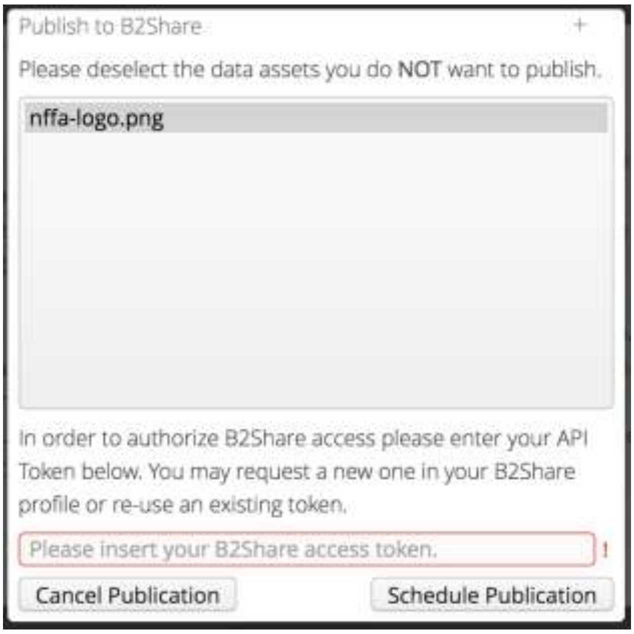
B2Share [10] is an external service provided by the EUDAT [11] project. In order to publish to B2Share, the PI of the proposal must be registered at B2Share in order to authorize the access to the service.

S/he should also provide an access token for B2Share, which can be created in the user profile when logged in to the B2Share web user interface.

When the IDRP publishes the measurement, the steps of the procedure are the following:

- A B2SHARE deposit is created
- The data assets are transferred (through a download from the original repository and an upload to B2SHARE)
- The deposit is committed in the NFFA domain with the NFFA metadata schema
- The PID is stored.

The procedure to publish a measurement to B2Share has been tested and validated, and an example is shown in Figure 5.



Publish to B2Share

Please deselect the data assets you do **NOT** want to publish.

nffa-logo.png

In order to authorize B2Share access please enter your API Token below. You may request a new one in your B2Share profile or re-use an existing token.

Please insert your B2Share access token.

Figure 5: IDRP procedure for publishing a measurement to B2Share.

3. Conclusions

This document presents the procedures implemented to provide a shared authentication mechanism on the first NFFA prototype, deployed on the CNR-IOM OpenStack cloud, following the design described in the deliverable D8.1 [1]. The tests and the validations of the AAI are also reported.

The possible IDRP users and login procedures have been described, as well as the main actions that can be performed on the IDRP.

Appendix APIs details

This section presents the APIs for the management of the communication between the IDRP and the NFFA Portal, developed by Promoscience.

A.1 APIs exposed by the NFFA Portal

1. User profile by ID

```
GET
www.nffa.eu:[port]/api/user/id/{userId}
{
  "userAffiliation": string,
  "userEmail": string,
  "userName": string (LASTNAME FIRSTNAME),
  "userId": GUID
}
```

2. User profile by email

```
POST
{
  "Email": string
}
www.nffa.eu:[port]/api/user/email/
{
  "userAffiliation": string,
  "userEmail": string,
  "userName": string (LASTNAME FIRSTNAME),
  "userId": GUID
}
```

3. Proposal info by ID

```
GET
www.nffa.eu:[port]/api/proposal/{proposalId}
```

4. List of all User profiles with status “sent” (not received by idrp server)

```
GET
www.nffa.eu:[port]/api/user/not_received
```

5. List of user profiles:

```
{
  "userAffiliation": string,
  "userEmail": string,
  "userName": string (LASTNAME FIRSTNAME),
  "userId": GUID
}
```

6. List of all Proposal with status “sent” (not received by IDRP server)

```
GET
```

www.nffa.eu:[port]/api/proposal/not_received

7. List of proposals:

```
{
  "projectId": null,
  "proposalId": GUID,
  "proposalDescription": JSON
}
```

8. Verify Token
POST
www.nffa.eu:[port]/api/token/verify

This endpoint must be called by the IDRP server to verify the validity of a pair userId/token. To be sure about the origin of the request, the NFFA portal will check and make sure the IP that originated the request is the IP of the IDRP Server. The request must be of type POST and must have the following body:

```
{
   Token: GUID,
   UserId: GUID
}
```

9. Authentication Url
GET
http://www.nffa.eu/ar/Account/LogOn?IdrpLogin=true

Once the token is created by the NFFA Portal (upon successful login), a POST request will be sent to a url [IDRP_SERVER_URL]/idrp-ui, putting the following token information in the body of the request:

```
{
   "Token": GUID,
   "UserId": GUID
}
```

A.2 Interaction with the IDRP portal APIs

All these APIs will be available for the NFFA portal only. Access will be restricted by IP.

1. PUT /proposals

```
{
  "proposalData": JSON (all proposal data)
}
```

A proposal is sent to IDRP server when one of these conditions are met:

- The proposal status changes to APPROVED (= ACCEPTED)
- The proposal status changes from APPROVED to any other status.

Results:

201: Successfully created proposal.
400: Invalid request, e.g. proposal data format invalid.
401: Unauthorized
403: Forbidden
409: Conflict, e.g. there is already a proposal with the provided unique id.
500: Internal server error

2. POST /portal/users

```
{
  "userAffiliation": string (OPTIONAL),
  "userEmail": string,
  "userName": string (LASTNAME FIRSTNAME),
  "userId": GUID
}
```

This endpoint will be called every time a user is created in the NFFA Portal.

Results:

201: Successfully created user.
400: Invalid request, e.g. userName, userEmail or userIdentifier is missing.
401: Unauthorized
403: Forbidden
409: Conflict, e.g. there is already a user with the provided unique id or email.
500: Internal server error

3. PUT /portal/users/{userId}

```
{
  "userAffiliation": string (OPTIONAL),
  "userEmail": string (OPTIONAL),
  "userName": string (LASTNAME FIRSTNAME) (OPTIONAL),
}
```

This endpoint will be called every time a user is updated in the NFFA Portal.

Results:

200: Successfully updated existing user.
201: Successfully created new user.
401: Unauthorized
403: Forbidden
404: User with id uniqueIdentifier not found.
409: Conflict, e.g. there is already a user with the same email or userId.
500: Internal server error

References

[1] Stefano Cozzini, "Design of Trusted authentication source for NFFA-EUROPE services", http://intranet.nffa.eu/DocumentRepository

[2] Karlsruhe Institute of Technology website, https://www.kit.edu/english/

[3]: CNR-IOM website, https://www.iom.cnr.it/

[4] Promoscience srl website, http://promoscience.com/

[5] CNR Openstack cloud, http://nimbo.escience-lab.org/dashboard/auth/login/

[6] IDRP User Interface, http://147.122.7.215:8080/idrp-ui/

[7] NFFA portal, http://nffa.eu/

[8] Thomas Jejkal, "NFFA Information and Data Repository Platform", http://ipelsdf1.lsdf.kit.edu/nffa/idrp/manual/index.html

[9] Thomas Jejkal, "Information and Data Repository Platform - RESTful API", http://ipelsdf1.lsdf.kit.edu/nffa/idrp/api/index.html

[10] B2Share website, https://b2share.eudat.eu/

[11] EUDAT website, https://www.eudat.eu/