European Commission

Communications Networks, Content and Technology
European Commission Directorate General

DG CONNECT

European Union's FP7 Programme
DG Connect
Directorate C: Excellence in Science
Unit C1: e-Infrastructure

elcira
Europe Latin America
Collaborative e-Infrastructure
for Research Activities

Deliverable D2.4

AAI Preparation

Assess the Identity Management of participating institutions

SEVENTH FRAMEWORK PROGRAMME
A project of the Seventh Framework Programme (FP7)

European Commission
This project is funded by the European Commission

RedCLARA + Red + Ciencia
A project implemented by RedCLARA

Periodical Progress Report

ELCIRA Deliverable: D.2.4 - AAI Preparation (Assess the Identity Management of participating institutions)

Document Full Name	**AAI Preparation (Assess the Identity Management of participating institutions)**
Date	**April, 2013**
Activity	**WP2 (Coordinated Actions for AAI between EU and LA)**
Lead Partner	**RNP**
Document status	**Final**
Classification Attribute	**Public**
Document link	

Abstract: This document contains all necessary information required for AAI Implementation at the two NRENs participating in the project. This document contains user information, schema adjustments and others.

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

COPYRIGHT NOTICE

ELCIRA (Europe Latin America Collaborative e-Infrastructure for Research Activities – Call (part) identifier: FP7-INFRASTRUCTURES-2012-1 – Project number: 313180) is a project co-funded by the European Commission within the Seventh Framework Programme (FP7), Infrastructures (DG Connect, Directorate C: Excellence in Science, Unit C1: e-Infrastructure). ELCIRA began on 1st June 2012 and will run for 24 months.

For more information on ELCIRA, its partners and contributors please see http://elcira.redclara.net (this website will be available in October 1st 2012).

The information contained in this document represents the views of the copyright holders as of the date such views were published.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED BY THE COPYRIGHT HOLDERS “AS IT IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE MEMBERS OF THE ELCIRA COLLABORATION, INCLUDING THE COPYRIGHT HOLDERS, OR THE EUROPEAN COMMISSION BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

DELIVERABLE ROUTE

	Name	Member/Activity	Date	Responsible
From	Camila Santos	WP2		RNP
Revised by	Leandro Guimarães	WP2		RNP
Revised by	Antônio Carlos Fernandes Nunes	WP2	24/05/2013	RNP
Approved by	Florencio Utreras	RedCLARA/Management	07/06/2013	RNP

TABLE OF CONTENTS

1.- INTRODUCTION

This document gives an overview on how to deploy a federation from scratch, considering technical and administrative aspects. It’s directed to NREN administrators that are willing to build a new federation and should read this document before putting federation deployment to practice.

2.- DOCUMENTS

Every federation should establish and publish a document that describes its policies, practices, and operation. It's best to refer to existing federation policy documents as a foundation and consider the own unique needs and legal restrictions of your jurisdiction and community. [1]

Another point to be considered is the integration with other federations by joining groups such as GÉANT eduGAIN service. If this is an intent, it’s worth a glimpse on what these groups require and build your own documents likewise, or at least care for not violating any of their pre-existent policies.

3.- TECHNICAL REQUIREMENTS

3.1 METADATA

Metadata provides the basis for all trust between providers in Shibboleth. The metadata doesn't configure the provider itself, but is used instead to identify and describe counterparties. When a Service Provider (SP) or an Identity Provider (IdP) receives a request from another provider, it needs to be able to verify that the remote provider is who it claims to be. This is done by comparing the declared name in the Security Assertion Markup Language (SAML) [2] message to the names the provider knows from the metadata. When there's a match, the remote provider must then present the credentials that are in that provider's metadata. Now that the remote provider has been positively identified, they can communicate. If there is no match, or the credentials presented are wrong, no attributes will be sent. [1]

The metadata file must be accessible from any IdP or SP in the federation. When managing metadata, the IdP and SP information can be stored in a single, manually-edited file, or can be unified using a metadata aggregator, which will collect information on the providers by their entityIDs.

3.2 DISCOVERY SERVICE

The Discovery Service (DS) is the tool that allows a user to choose the institution where his credentials are, and directs the Service Provider to the IdP where it can request user authentication. The Figure 1 below suggests the architecture for a federation; the technologies showed in this example are widely used, but there are several other options.

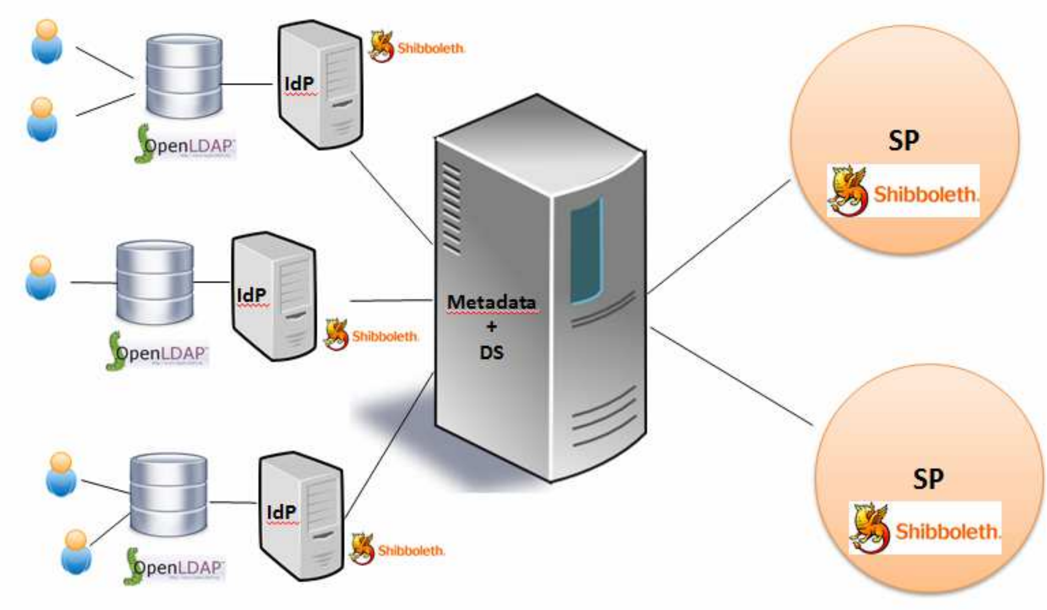
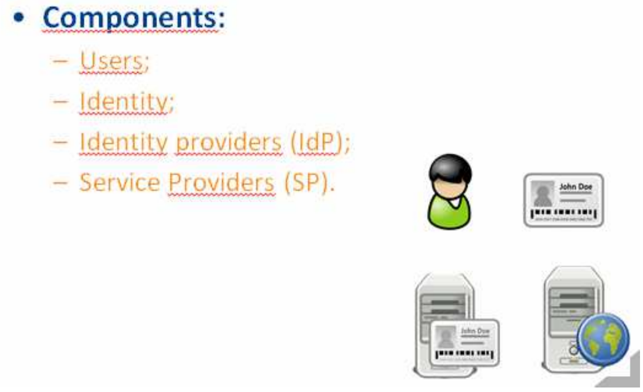


Figure 1 – Architecture for a federation.

3.3 AUTHENTICATION PROCESS THROUGH A FEDERATION

The Figure 2 presents the authentication process through an identity federation.



- **Components:**
  - Users;
  - Identity;
  - Identity providers (IdP);
  - Service Providers (SP).

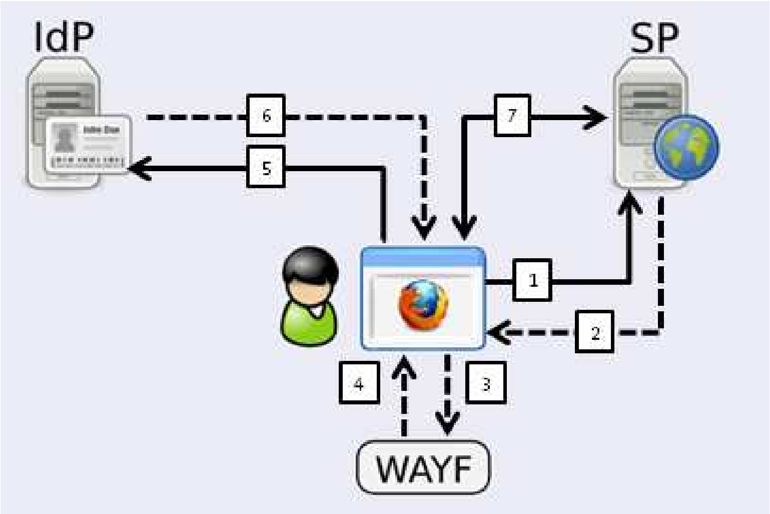


Figure 2 – Authentication process [3].

1) The user try to access a service provided a Federation’s (or through eduGAIN) Service Provider;
2) The Service Provider redirects the user’s request to WAYF (Where Are You From?);
3) The user select his home Identity Provider (IdP);
4) The WAYF redirect the user’s request to his home Identity Provider;
5) The user send his Identity (login and password) to his home IdP;
6) In case of authentication success, the IdP redirect the user’s request, with authentication success back to the Service Provider;

7) The Service Provider grants access to the user.

3.4 ATTRIBUTE DEFINITION AND HANDLING [1]

The final part of an exchange between providers that may be facilitated by a federation is the definition of attributes that would be of common interest to federation members. This provides a common language for expressing and interpreting data about users so that access is properly controlled.

Attribute names in SAML, and by extension Shibboleth, are generally expressed as URIs. Section 8.2 of SAML 2.0 Profiles recommends that all LDAP attributes be expressed as URIs through transformation of the OID identifier, e.g. urn: oid:1.3.6.1.4.1.5923.1.1.1.5. Attributes may also be named through other URN namespaces, or by using URLs, which could be resolved to yield a controlled vocabulary, synonyms, and other information. It's very important that proper attribute naming etiquette be followed and that you don't define attributes in namespaces you don't control.

Proliferation in attributes and misappropriation of attributes are two countervailing forces that need to be balanced as you decide which attributes to use. A large number of attributes has already been defined and named (e.g. eduPerson and x.520), and in any situation where a pre-existing attribute meets your needs, it should be used. However, controlled vocabularies and specific definitions must be followed. Use your best judgment in deciding whether to create a new attribute definition.

Attribute definitions should be written in appropriately normative language and assigned at least a SAML-based name. This information should be made available to all providers in your federation and referenced by or included in your federation's policy statement.

3.5 SCHEMA DEFINITION

A federation can define its own schema, containing attributes that aren't standardized in other federations but would be widely used in its context. In order to ensure interoperability, it's recommended that this schema be derived from another already known by other federations as eduPerson, and that these new attributes be associated with OIDs that aren't already in use.

3.5.1 Hardware requirements

The infrastructure of federation depends on the size and the amount of users and its attributes provided in the federation schema.

As with every other professionally-operated service though, you should keep in mind that service uptime is paramount, and plan your procurement accordingly. Examples:

- In the case of virtual machines, use an underlying infrastructure which enables you to migrate machines without VM downtime, if possible.
- In the case of physical machines, use hot-pluggable parts where possible; and ideally, keep either spare hardware parts at hand or a set up a decent service contract.

3.6 INTERFEDERATION – EDUGAIN

If the federation opts in joining a larger group, it is required that they share metadata information. Taking eduGAIN as an example, presented in the Figure 3, the federation metadata must be accessed by eduGAIN and will be merged into their Metadata Distribution Service (MDS). The IdPs and SPs that wish to be available inside the interfederation must consume MDS metadata file, which should be made available by the federation, alongside with the previously configured metadata.

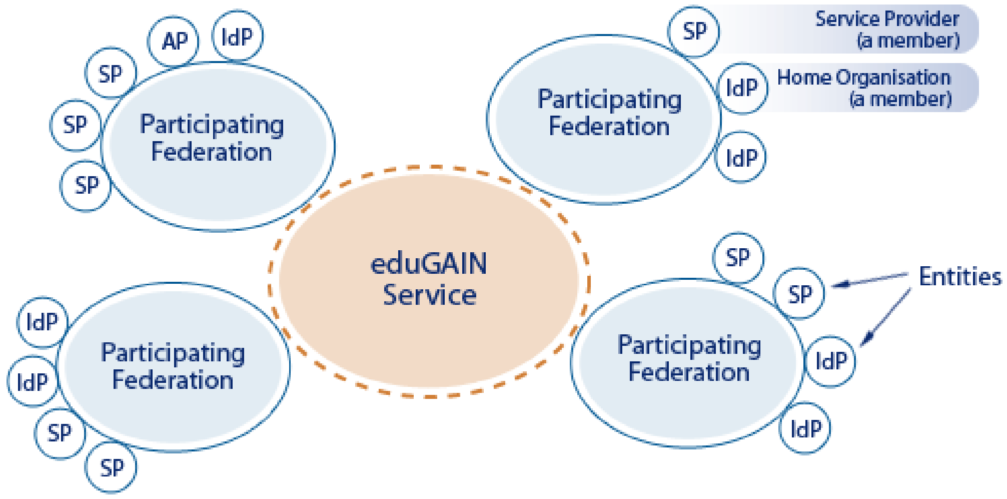


Figure 3 - eduGAIN structure[4].

4.- RECOMMENDED PERSONNEL

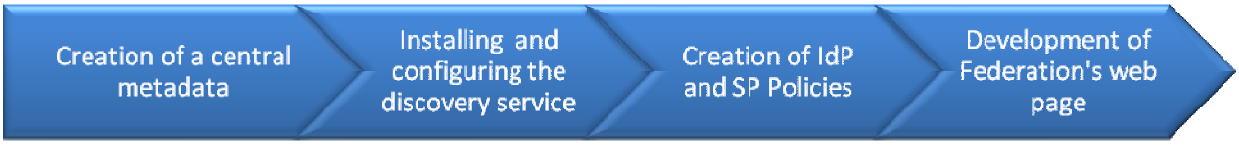
With a fully operational federation, comes the necessity of client support. When dealing with IdPs and SPs, the support team must be prepared to guide users on questions about how to set up the provider's rules for authorization and authentication, translation of attributes, attribute collection from different kinds of basis, deployment of new services and many others. This includes knowledge not only of the IdP or SP itself, but also of the available tools that could be used to fulfill the provider's necessities and development possibilities inside the federation.

4.- SCHEDULES

In this chapter is described the phases to implement a national federation for research and education, implement a Identity Provider and to join eduGAIN.

The time to run all these phases depends largely of the effort of National Research and Education team; because of this the schedules consider only tasks, not dates.

4.1 STEP 1: CREATION OF A NATIONAL FEDERATION



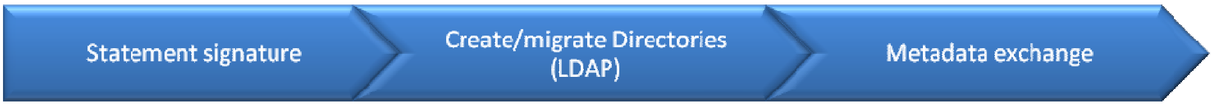
Creation of a central metadata

Installing and configuring the discovery service

Creation of IdP and SP Policies

Development of Federation's web page

4.2 STEP 2: CREATION OF AN IDENTITY PROVIDER (IDP)

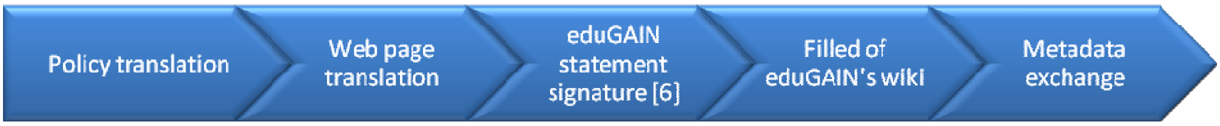


Statement signature

Create/migrate Directories (LDAP)

Metadata exchange

4.3 STEP 3: JOIN EDUGAIN [5]



Policy translation

Web page translation

eduGAIN statement signature [6]

Filled of eduGAIN's wiki

Metadata exchange

5.- REFERENCES

[1] Shibboleth Wiki – Build a Federation, accessed in 24th May 2013 – https://wiki.shibboleth.net/confluence/display/SHIB2/BuildAFederation.

[2] Security Assertion Markup Language (SAML) v2.0, accessed in 24th May 2013 – https://www.oasis-open.org/standards#samlv2.0.

[3] GT-STCFed – Serviços para transposição de credenciais e autenticação federadas UFSC, IFSC e UNIVALI, accessed in 24th May 2013 - http://www.rnp.br/_arquivo/gt/2010/GT-STCFed_fase2.pdf.

[4] How eduGAIN Works, accessed in 24th May 2013 – http://www.geant.net/service/eduGAIN/about_edugain/how_eduGAIN_works/Pages/home.aspx.

[5] eduGAIN Joining checklist, accessed in 24th May 2013 - http://www.edugain.org/technical/joining_checklist.php.

[6] eduGAIN statement, accessed in 24th May 2013 - http://www.geant.net/service/edugain/resources/Documents/eduGAIN%20declaration.pdf.