

European Union's Horizon 2020 Programme
European Commission
Directorate General for Communications Networks, Content and Technology
eInfrastructure



Magic

Middleware for collaborative Applications
and Global virtual Communities

Deliverable 2.3
On line Training Material on AAI development for
Staff training

Periodical Progress Report

MAGIC Deliverable: D2.3 - On line Training Material on AAI development for Staff training (revised version)

Document Full Name	D2.3 - On line Training Material on AAI development for Staff training (revised version)
Date	30-09-2016
Activity	Platforms for mobility
Lead Partner	RNP
Document status	Final revised version
Classification Attribute	Public
Document link	

Abstract: This document describes and shows how the on line training material on AAI was developed and organized. This training was developed to be used on technical staff training of all NRENS members of MAGIC project. The material was developed to be used online only; there will be no printed material, although if the participant desire to use it in a in class course, it is possible as well.



COPYRIGHT NOTICE

Copyright © Members of the MAGIC Project October 2016.

MAGIC (Middleware for collaborative Applications and Global vrtual Communities – Project number: 654225) is a project co-funded by the European Commission within the Horizon 2020 Programme (H2020), Directorate General for Communications Networks, Content and Technology - eInfrastructure. MAGIC began on 1st May 2015 and will run for 24 months.

For more information on MAGIC, its partners and contributors please see <http://www.magic-project.eu>.

You are permitted to copy and distribute, for non-profit purposes, verbatim copies of this document containing this copyright notice. This includes the right to copy this document in whole or in part, but without modification, into other documents if you attach the following reference to the copied elements: "Copyright © Members of the MAGIC Project, 2015".

Using this document in a way and/or for purposes not foreseen in the paragraph above requires the prior written permission of the copyright holders.

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 MAGIC 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.



This project is co-funded by the Horizon 2020
Framework Programme of the European Union



A project implemented by RedCLARA



DELIVERABLE ROUTE

	Name	Member/Activity	Date	Responsible
From	Leandro Guimarães	WP2 Coordinator	29/09/2016	RNP
Revised by	Antônio Carlos Fernandes Nunes	RNP Project Coordinator	30/09/2016	RNP
Revised by	Florencio Utreras	RedCLARA(CEO	03/10/2016	RNP
Revised by				
Aproved by				



This project is co-funded by the Horizon 2020
Framework Programme of the European Union



A project implemented by RedCLARA



TABLE OF CONTENTS

COPYRIGHT NOTICE.....	3
DELIVERABLE ROUTE	4
1. Introduction.....	6
1.1. Purpose of the Document	6
2. Document Amendment Procedure	6
3. Glossary	6
4. Executive Summary.....	6
5.	6
6. TRAINING structure	7
7. TRAINING topics	9
8. Screenshots.....	11
Module 1	11
Module 2	12
Module 3	13
Module 4	14
9. Moodle usability	15
9.1. Reports	15
10. Conclusion.....	17



1. INTRODUCTION

1.1. PURPOSE OF THE DOCUMENT

The purpose of this document is to describe and show how the on line training material on AAI was developed and organized. This second version was necessary to include some changes suggested by evaluators in the first year review meeting. Using the same model applied in the ELCIA project, this training was developed to be used on technical staff training of all NRENs members of MAGIC project. Although the material was developed to be used online, it can be used to support a in class training.

2. DOCUMENT AMENDMENT PROCEDURE

All changes should be send to the author, with a copy to WP2 mailing list. The revisions shall be send to WP2 and MAGIC ALL mailing list, in order to allow to all members review the entire document, mainly their region chapter.

3. GLOSSARY

EC	European Commission
EU	European Union
EU-LAC	Europe, Latin America and the Caribbean

4. EXECUTIVE SUMMARY

This document reviews how the on line training material on AAI was developed and organized. This training was developed to be used on technical staff training of all NRENs members of MAGIC project. the material was developed to be used online only; there will be no printed material, although if the participant desire to use it in a in class course, it is possible as well.



6. TRAINING STRUCTURE

The training was published in **virtual training platform** at:

<http://cursos.redclara.net>

Bienvenidos y bienvenidas a la plataforma de aprendizaje de RedCLARA. Esta plataforma es un recurso destinado al desarrollo de capacidades y competencias de los distintos actores que participan de nuestra organización. Es un espacio que permitirá la conexión de los participantes de las distintas áreas que nos conforman.

El propósito de esta herramienta es propiciar un proceso continuo de reflexión, ofrecer dispositivos y recursos de aprendizaje para la actualización de los profesionales y, en definitiva, aportar insumos que permitan instalar procesos de fortalecimiento a la Organización. Bajo esta plataforma se impartirán diversos cursos, diseñados según las necesidades del amplio abanico de actores que tienen funciones y responsabilidades en nuestra gran red.

Hoy en día, la gestión del conocimiento es una función estratégica para cualquier organización, ya que se requiere contar periódicamente con elementos de apoyo que permitan generar información de calidad, sistematizar experiencias y aprendizajes, consolidar conocimientos y difundir buenas prácticas. Pero, es importante señalar que la gestión de aprendizajes depende, principalmente, de la activa participación de sus usuarios. Una comunidad sin usuarios que se dispongan a compartir lo que saben, a analizar sus modos y prácticas y a incorporar nuevos conocimientos, no cumple con su propósito fundacional y se extingue. Por ello, entendemos la invitación a utilizar responsablemente estos recursos y generar, efectivamente, una comunidad que crece y aprende.

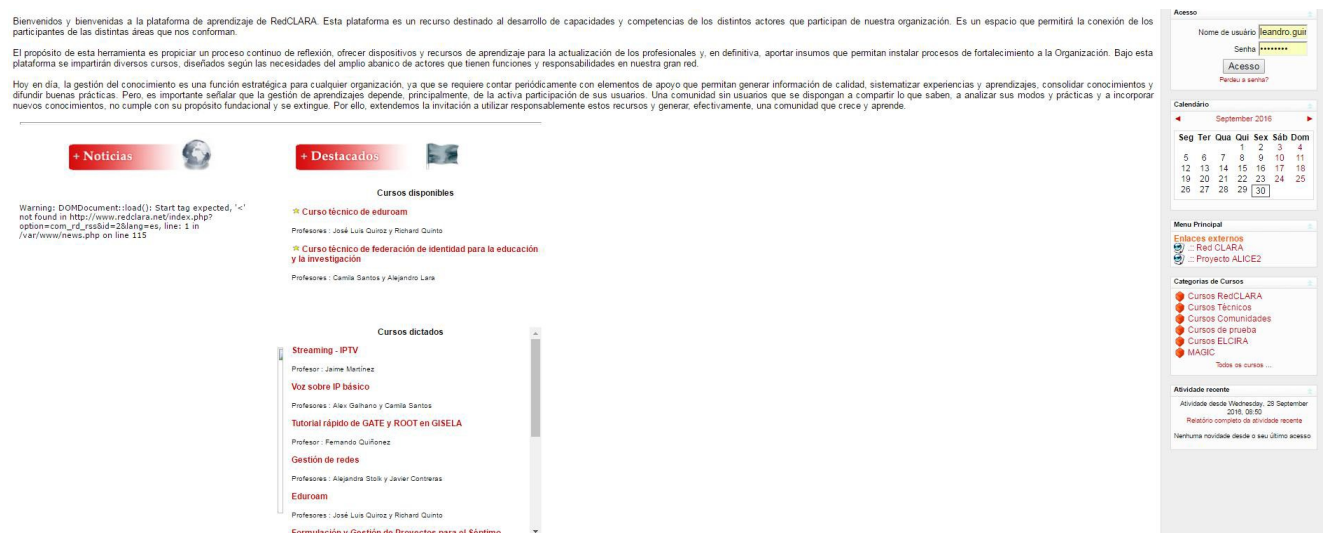


Figure 1: Main page of RedeCLARA's Moodle.

When user access the main page of RedCLARA's Moodle, it is possible to see all MAGIC courses available:



Figure 2: All MAGIC courses available (sept 2016).

Alternatively, if user knows the desired course address, he/she can access directly at:

<http://cursos.redclara.net/course/view.php?id=51>



This project is co-funded by the Horizon 2020
Framework Programme of the European Union



A project implemented by RedCLARA

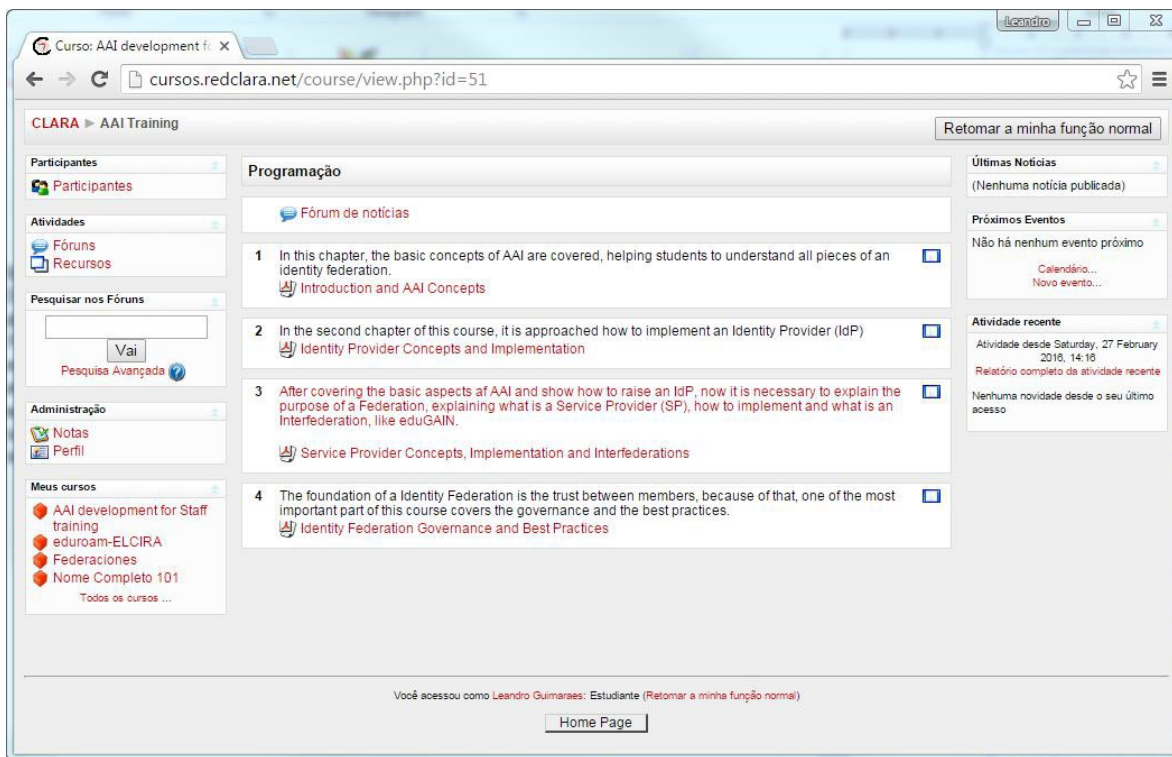


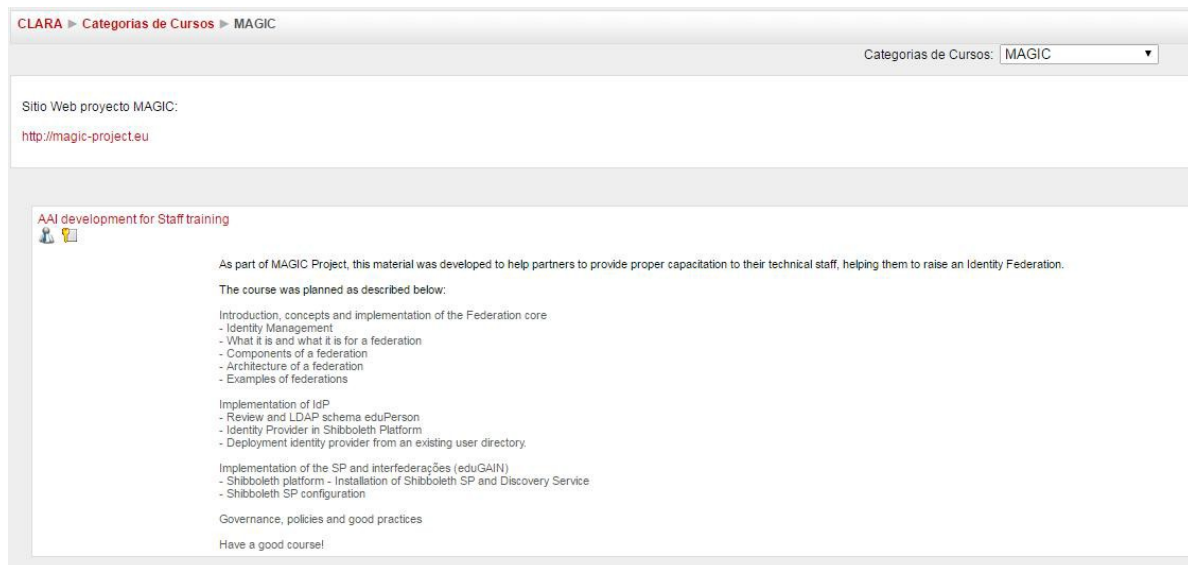
Figure 3: AAI course structure.



This project is co-funded by the Horizon 2020
Framework Programme of the European Union



A project implemented by RedCLARA



The screenshot shows a web browser interface for the CLARA project. At the top, there is a breadcrumb trail: "CLARA > Categorías de Cursos > MAGIC". To the right, there is a dropdown menu labeled "Categorías de Cursos:" with "MAGIC" selected. Below this, the text "Sitio Web proyecto MAGIC:" is followed by the URL "http://magic-project.eu". The main content area is titled "AAI development for Staff training" and contains the following text:

As part of MAGIC Project, this material was developed to help partners to provide proper capacitation to their technical staff, helping them to raise an Identity Federation.

The course was planned as described below:

- Introduction, concepts and implementation of the Federation core
 - Identity Management
 - What it is and what it is for a federation
 - Components of a federation
 - Architecture of a federation
 - Examples of federations
- Implementation of IdP
 - Review and LDAP schema eduPerson
 - Identity Provider in Shibboleth Platform
 - Deployment identity provider from an existing user directory.
- Implementation of the SP and interfederaciones (eduGAIN)
 - Shibboleth platform - Installation of Shibboleth SP and Discovery Service
 - Shibboleth SP configuration
- Governance, policies and good practices

Have a good course!

Figure 4: AAI course structure.

7. TRAINING TOPICS

Module 1: Introduction, concepts and implementation of the Federation core:

In this chapter, the basic concepts of AAI are covered, helping students to understand all pieces of an identity federation:

- Identity Management;
- What it is and what it is for a federation;
- Components of a federation;
- Architecture of a federation;
- Examples of federations.

Module 2: Implementation of IdP:

In the second chapter of this course, it is approached how to implement an Identity Provider (IdP):

- Review and LDAP schema eduPerson;
- Identity Provider in Shibboleth Platform;
- Deployment identity provider from an existing user directory.





Module 3: Implementation of the SP and interfederações (eduGAIN):

After covering the basic aspects of AAI and show how to raise an IdP, now it is necessary to explain the purpose of a Federation, explaining what is a Service Provider (SP), how to implement and what is an Interfederation, like eduGAIN:

- Shibboleth platform - Installation of Shibboleth SP and Discovery Service;
- Shibboleth SP configuration.

Module 4: Governance, policies and good practices

The foundation of a Identity Federation is the trust between members, because of that, one of the most important part of this course covers the governance and the bestpractices.



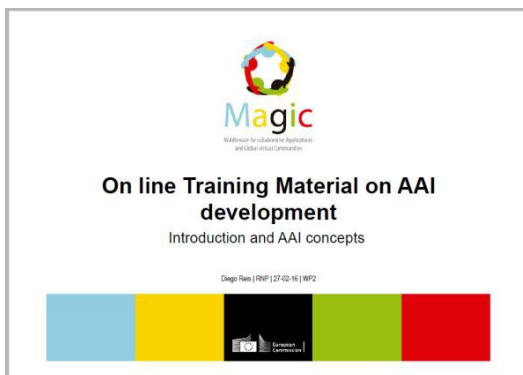
This project is co-funded by the Horizon 2020
Framework Programme of the European Union



A project implemented by RedCLARA

8. SCREENSHOTS

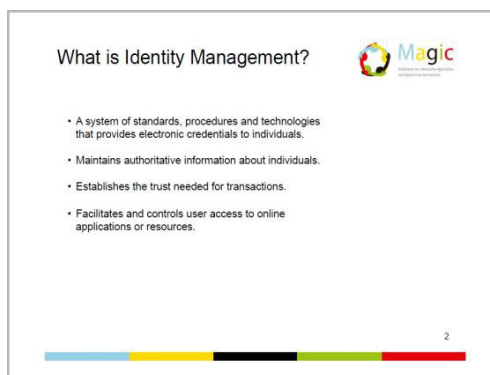
MODULE 1:



MAGIC
Middleware for collaborative Applications
and Global Virtual Communities

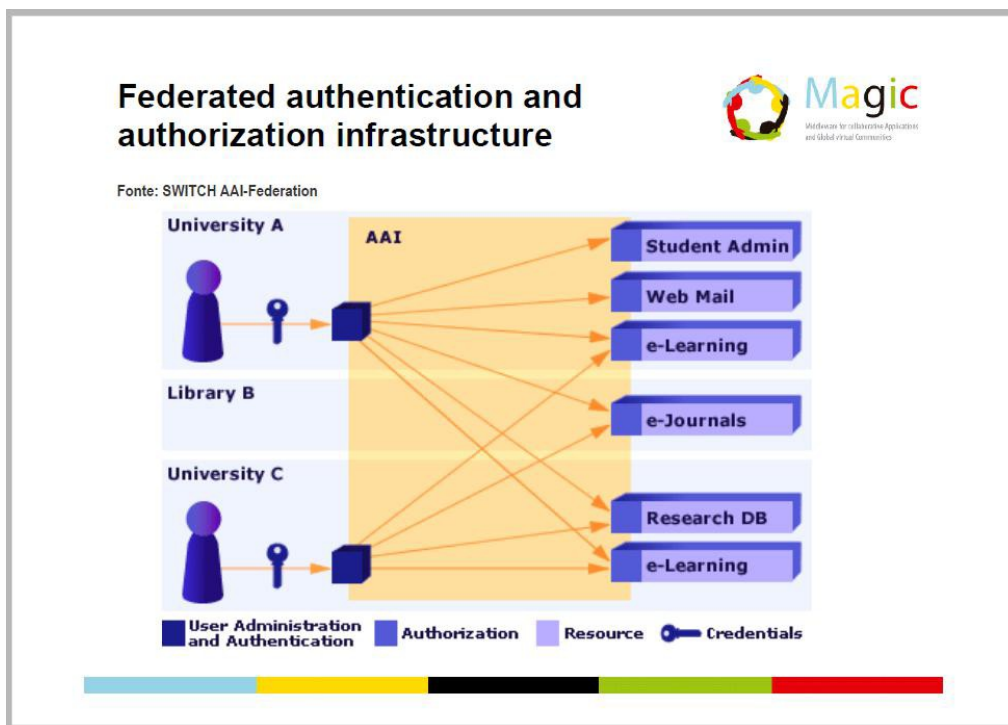
**On line Training Material on AAI
development**
Introduction and AAI concepts

Diego Soto | RNP | 27-02-16 | WP2



What is Identity Management?

- A system of standards, procedures and technologies that provides electronic credentials to individuals.
- Maintains authoritative information about individuals.
- Establishes the trust needed for transactions.
- Facilitates and controls user access to online applications or resources.




Federated authentication and authorization infrastructure

Fonte: SWITCH AAI-Federation



The diagram illustrates a federated authentication and authorization infrastructure. On the left, three entities are shown: University A, Library B, and University C. Each entity has a user icon and a key icon representing credentials. These entities are connected to a central AAI (Authentication, Authorization, and Accounting) infrastructure. The AAI infrastructure is represented by a large orange box. From the AAI infrastructure, arrows point to various resources: Student Admin, Web Mail, e-Learning, e-Journals, Research DB, and e-Learning. A legend at the bottom identifies the components: User Administration and Authentication (blue square), Authorization (blue square), Resource (purple square), and Credentials (key icon).



MODULE 2:


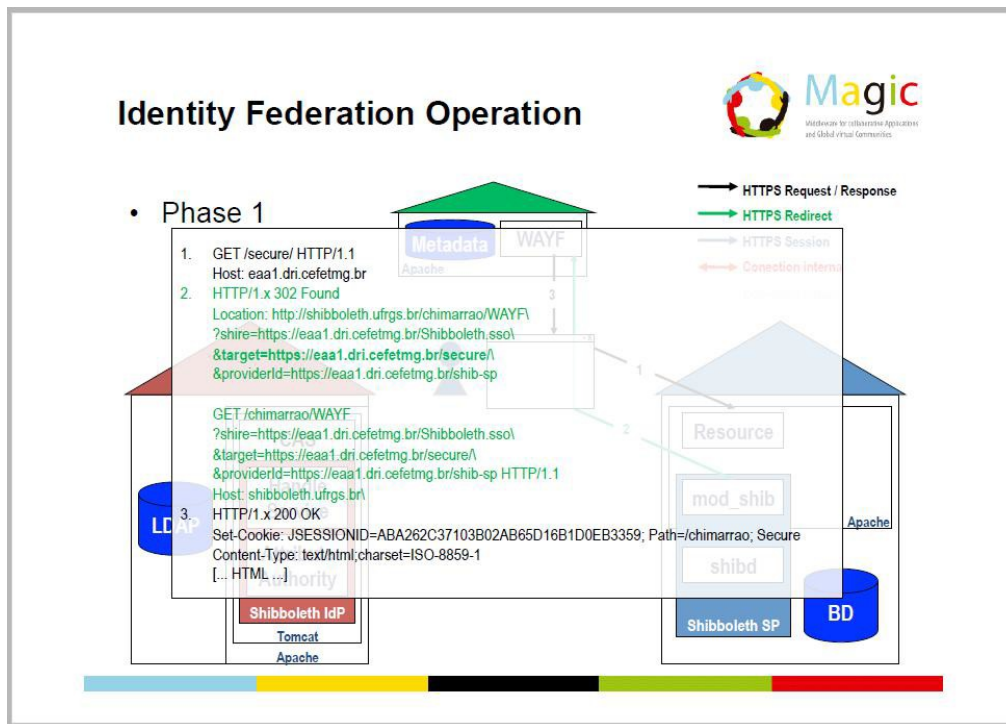


**On line Training Material on AAI
development**
Identity Provider Concepts and
Implementation
Luciano Fernandes Rocha / Francisco Leonardo Mota | RFP | 27-02-16 | WP2





Shibboleth


- What is Shibboleth?
 - Middleware project from Internet2
 - SAML (Security Assertion Markup Language)
 - Standard defined by OASIS (Organization for the Advancement of Structured Information Standards)
 - Federated access
 - Authentication
 - Authorization
 - SSO (Single Sign-On)

MODULE 3:





**On line Training Material on AAI
 development**
 Service Provider Concepts, Implementation
 and Interfederations
Francisco Leonardo Muñoz (FP7 (27-02-16) / WP2)



Service Providers (SP)


A Service Provider enables web applications written with any programming language or framework integrating natively with a web server.

In a federation, it relies on a trusted Identity Provider (IdP) for authentication and authorization.

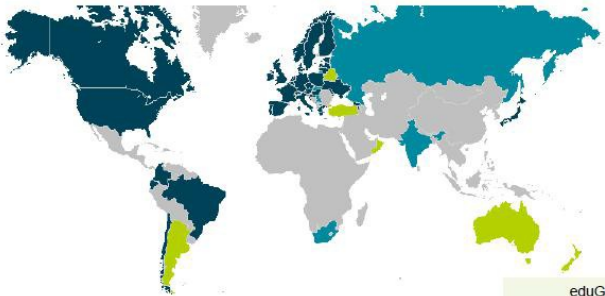



eduGAIN status*

- <https://technical.edugain.org/status>




Global



■ eduGAIN
 ■ Voting only
 ■ Candidate

* Feb, 16th, 2016



eduGAIN numbers

Federations:	37
All entities:	3.099
IdPs:	1.993
SPs:	1.107
Standalone AAs:	3




This project is co-funded by the Horizon 2020 Framework Programme of the European Union




A project implemented by RedCLARA


MODULE 4:





**On line Training Material on AAI
development**
Identity Federation Governance and Best
Practices
Ricard Mikiel | RNP | 27-02-16 | WP2




**Identity Federation Governance
and Best Practices**




- Given its complexity, breadth, implications and importance, the phrase “don’t attempt this at home” might well apply to federation identity management deployment.
- Although best practice federation identity management is a desirable goal, it is a status that can realistically be achieved only in stages.



**Identity Federation Services
Architecture**



- Federated services architecture generally conforms to multiple desired characteristics, including:
 - Service oriented
 - Standards based
 - Flexible and interoperable
 - Loosely coupled
 - Secure
 - Appropriately redundant
 - Scalable
 - Efficient





9. MOODLE USABILITY

All courses published in the Moodle can be monitored using the system functionalities, like:



9.1. REPORTS

Follows below some examples of information that is possible to obtain in the system:

AAI development for Staff training: All participants, Friday, 30 September 2016 (America/Sao_Paulo)

AAI development for Staff training ▾ All participants ▾ Today, 30 September 2016 ▾ All activities ▾ Display on page ▾ Get these logs

Displaying 30 records

Time	IP Address	Full name	Action	Information
Fri 30 September 2016, 10:40 AM	200.143.100.131	Leandro Guimarães	course report log	AAI development for Staff training
Fri 30 September 2016, 10:40 AM	200.143.100.131	Leandro Guimarães	resource view	Introduction and AAI Concepts
Fri 30 September 2016, 10:40 AM	200.143.100.131	Leandro Guimarães	course view	AAI development for Staff training
Fri 30 September 2016, 10:40 AM	200.143.100.131	Leandro Guimarães	resource update	Introduction and AAI Concepts
Fri 30 September 2016, 10:40 AM	200.143.100.131	Leandro Guimarães	course update mod	resource SSP
Fri 30 September 2016, 10:39 AM	200.143.100.131	Leandro Guimarães	resource view	Introduction and AAI Concepts
Fri 30 September 2016, 10:39 AM	200.143.100.131	Leandro Guimarães	course view	AAI development for Staff training
Fri 30 September 2016, 10:39 AM	200.143.100.131	Leandro Guimarães	course extraction	1
Fri 30 September 2016, 10:39 AM	200.143.100.131	Leandro Guimarães	course view	AAI development for Staff training
Fri 30 September 2016, 10:39 AM	200.143.100.131	Leandro Guimarães	course report log	AAI development for Staff training
Fri 30 September 2016, 10:38 AM	200.143.100.131	Leandro Guimarães	resource view	Service Provider Concepts, Implementation and Interfederations
Fri 30 September 2016, 10:38 AM	200.143.100.131	Leandro Guimarães	course report log	AAI development for Staff training
Fri 30 September 2016, 10:38 AM	200.143.100.131	Leandro Guimarães	resource view	Service Provider Concepts, Implementation and Interfederations
Fri 30 September 2016, 10:38 AM	200.143.100.131	Leandro Guimarães	course view	AAI development for Staff training
Fri 30 September 2016, 10:38 AM	200.143.100.131	Leandro Guimarães	course report log	AAI development for Staff training

Figure 5: Usage log.



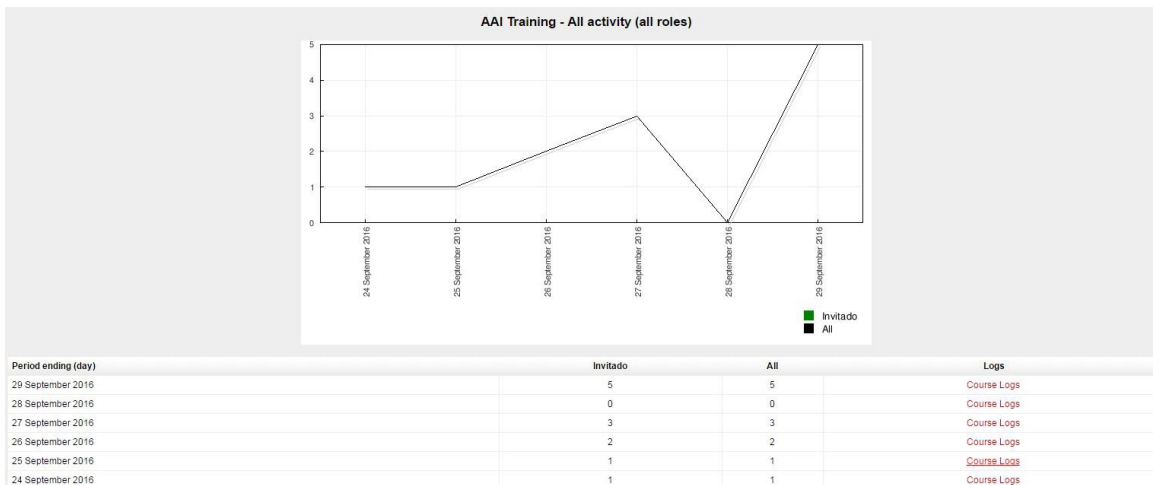


Figure 6: Usage statistics.

References

- [R1] MAGIC Website <http://www.magic-project.eu>
- Module Part1-AAI- <https://wiki.geant.org/pages/viewpage.action?pageId=50399132>
1 Fundamentals
- Module LDAP protocol <https://tools.ietf.org/html/rfc4511#page-3>
1
- Module Service Providers <https://wiki.refeds.org/dosearchsite.action?queryString=service+provider>
3
- Module Service Providers https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#overview
3
- Module Service Providers <https://wiki.shibboleth.net/confluence>
3
- Module Service Providers <https://shibboleth.net/products/service-provider.html>
3
- Module Interfederatoin www.edugain.org
3
- Module Identity https://www.suse.com/docrep/documents/fdoi5xvzef/4622078_en.pdf
4 Management
Planning: Best
Practices, Insights





and
Recommendations -
Novell technical
white paper.

Module REFEDS Federation <https://wiki.refeds.org/display/FBP/Federation-Best-Practice+Home>
4 Best Practice Wiki

Module InCommon https://spaces.internet2.edu/download/attachments/16548332/Federated_IdM_Checklist.pdf
4 Federated Identity Management Checklist

10. CONCLUSION

After providing this material, initially in English, all Magic members can capacitate their technical staff in order to raise federations in their regions.

The second phase that started now is the translation activities, to have this material translated to Russian, Spanish, French and Portuguese. Doing this it is expected to reach the WP2 milestones in federation, having at the end of the project, pilot federations deployed in at least 4 countries.

