Consejo Nacional de Ciencia y Tecnología
"CONACyT"
Fondo de Cooperación Internacional en Ciencia y Tecnología "FONCICYT"

Unión Europea Programa Horizonte 2020
Comisión Europea
Dirección General para las Redes de Comunicación, Contenido y Tecnología
e-Infraestructura

Magic
Middleware for collaborative Applications and Global vIrtual Communities

WP3 Aprovisionamiento en la Nube

Entregable E3.1

Reporte: Reunión de Trabajo Presencial MAGIC WP3

Viena, Austria, marzo 2016

Proyecto Apoyado por FONCICYT

Proyecto co-financiado en el Marco del Programa Horizonte 2020 de la Unión Europea

Proyecto Implementado en México por CUDI

Proyecto implementado por RedCLARA

Reporte de Progreso

Entregable MAGIC: E3.1 Reporte MAGIC Gestor de Grupos Viena, Austria

Nombre completo del Documento	Reporte: Reunión de Trabajo para definir la arquitectura del gestor de grupos que implementarán las RNIES, participantes en el proyecto MAGIC)
Fecha	**10 y 11-03-2016**
Actividad	**WP3 / Aprovisionamiento en la Nube** T3.2 **–** Reunión de líderes técnicos para establecer la arquitectuta para la integración del gestor de grupos
Líder del WP	**RedCLARA**
Estatus del Documento	**borrador**
Atributos	**Público**

Proyecto Apoyado por FONCICYT

Proyecto co-financiado en el Marco del Programa Horizonte 2020 de la Unión Europea

Proyecto Implementado en México por CUDI

Proyecto implementado por RedCLARA

Resumen: En marzo 2016 se llevó a cabo una reunión del WP3, que tuvo lugar en Viena, Austria. En esta sesión , se definió la arquitectura que utilizará el manejador de grupos que se integrará con los protocolo SAML y VOOT, utilizará las aplicaciones SYMPA (RENATER) y PERUN (CESNET) para implementar el gestor de grupo que será utilizado por las RNIE´s que participan en MAGIC.

El gestor de grupo será diseñado para la implementación y uso de las herramientas desarrolladas por RedCLARA, para sus miembros:

1. Colaboratorio
2. enVío
3. SIVIC
4. Dokuwiki

CESNET la Red Nacional de Investigación y Educación (RNIE) de Checoslovaquia, la RNIE de Francia RENATER y RedCLARA serán las redes que participarán en el piloto que implementará el gestor de grupos.

CONACYT
Consejo Nacional de Ciencia y Tecnología
Proyecto Apoyado por FONCICYT

European Commission
Proyecto co-financiado en el Marco del Programa Horizonte 2020 de la Unión Europea

cudi
Proyecto Implementado en México por CUDI

RedCLARA
+ Red + Ciencia
Proyecto implementado por RedCLARA

RUTA DEL ENTREGABLE

	Nombre	Institución / WP-Actividad	Fecha	Responsable
De	Martha Ávila / Rafael Morales	CUDI / WP3/T2.2 Reunión de Trabajo para definir la infraestructura del gestor de grupos que implementarán las RNIES participantes en el proyecto MAGIC	28/06/16	Martha Ávila
Revisado por	Rocío Cos	CUDI / Administración del Proyecto	06/07/2016	
Revisado por				
Revisado por				
Aprobado por	Rocio Cos	CUDI / Administración del Proyecto	22/07/2016	

TABLA DE CONTENIDOS

1. INTRODUCCIÓN

En el marco del Proyecto denominado "Aprovisionamiento en la Nube", que tiene como principal objetivo establecer acuerdos entre Europa, América Latina y otras regiones participantes, para completar el middleware necesario en el mercado de infraestructura de cómputo avanzado, servicios y aplicaciones en tiempo real para los grupos de investigación internacionales e intercontinentales con la finalidad de facilitar su movilidad y el trabajo colaborativo, se desarrollarán pilotos en las RNIE´s participantes, facilitando así la movilidad y el trabajo de las Comunidades Globales de Ciencia.

Las actividades a desarrollar fueron:

Section 1 Welcome

- **Meeting welcome** and introduction (15 minutes)
- -**MAGIC WP3** Summary, goals and results to date.- Gustavo García (RedCLARA)
- -**Goals and use cases on Group Management**.-Gustavo García (RedCLARA) | presentación
- **VOOT.- Michal Procházka (CESNET)** | presentación
- **SCIM.- Carlos Gonzáles (RedCLARA)**
- **Sympa**
- **Perun.- Michal Procházka (CESNET)** | presentación
- **Definition of the selection methodology (**90 minutes)

Section 2: Methodology and for GMF definitions

- **Evaluation** of existing alternatives (60 min)
- **Use cases enclosed in each proposed alternatives** (60 min)
- I**nitial comments and arguments** (60 min)

Section 3: Architecture Definition

- **Definition** (120 min)
- **Architecture elements evaluation and definition** (120)

Section 4: Pilot implementation elements

- **Pilot Implementation definitions**
- **Final comments or suggestions** (20 minutes)

En este contexto, una de las actividades inmediatas del WP3 es desarrollar un modelo mundial para la interoperación entre mercados de aplicaciones en la nube, herramientas de colaboración y servicios de las RNIEs

En esta ocasión el personal de CUDI responsable de estas actividades ha participado en la reunión de trabajo para definir la arquitectura del gestor de grupos en la ciudad de **Viena en Austria, los días 10 y 11 de marzo del 2016**.

2. REFERENCIAS

[R1]	Sitio Web MAGIC	http://www.magic-project.eu
[R2]	Sitio Web CUDI	http://www.cudi.edu.mx/noticia/resultados-de-la-reunion-presencial-del-wp3-del-proyecto-magic
[R3]	Sitio Web CUDI-MAGIC	http://www.cudi.edu.mx/content/magic
[R4]	Sitio Web CUDI	http://www.cudi.edu.mx/noticia/reunion-magic-wp3
[R5]	Sitio Web CUDI	http://www.cudi.edu.mx/eventos/reunión-presencial-del-wp3-del-proyecto-magic
[R6]	CESNET. (2016).	Perun | Identity and Access Management System. Recuperado el 11 de julio de 2016, a partir de https://perun.cesnet.cz/web/
[R7]	GÉANT. (s/f).	VOOT: An extensible protocol for dynamic exchange of group and authorization data. Recuperado el 11 de julio de 2016, a partir de http://openvoot.org/
[R8]	IETF. (s/f). SCIM	System for Cross-domain Identity Management. Recuperado el 11 de julio de 2016, a partir de http://www.simplecloud.info/
[R9]	RENATER. (2016, junio 17).	Sympa mailing list server. Recuperado el 11 de julio de 2016, a partir de http://www.sympa.org/

3. PROCESO DE ENMIENDA DE DOCUMENTO

Las solicitudes de enmiendas a este documento se deberán hacer a los autores (Martha Avila (CUDI), cudi@cudi.edu.mx y Rafael Morales, rmorales@suv.udg.mx), con copia al Administrador del proyecto MAGIC-CUDI (María del Rocío Cos – WP1 Administración del Proyecto, rcos@cudi.edu.mx).

4. GLOSARIO

EC	European Commission
EU	European Union
EU-LAC	Europe, Latin America and the Caribbean
RedCLARA	Red de Cooperación Latino Americana de Redes Avanzadas
CONACYT	Consejo Nacional de Ciencia y Tecnología
FONCICYT	Fondos de Cooperación Internacional en Ciencia y Tecnología
CUDI	Corporación Universitaria para el Desarrollo de Internet
MAGIC	Middleware for collaborative Applications and Global vIrtual Communities
SimpleSAMLphp	Mediante el protocolo estándar SAML2, proporciona una infraestructura de autenticación distribuida que permite la autenticación en múltiples entornos mediante un proceso de autenticación único. Esto quiere decir que el usuario sólo tiene que introducir sus credenciales una única vez lo que implica al mismo tiempo, que no existe redundancia de datos de autenticación, ni por otra parte, inconsistencia de datos por duplicación de la información de un mismo usuario.
Shibboleth	El Shibboleth Internet2 middleware iniciativa creó una implementación de la arquitectura y de código abierto para la gestión de la identidad y la identidad federada basada en la autenticación y la autorización (o control de acceso) infraestructura basada en aserción de seguridad Markup Language (SAML).
RNIE	Red Nacional de Investigación y Educación
eduGAIN	Es un servicio que interconecta a las federaciones de identidades en todo el mundo, simplificando el acceso a contenidos, servicios y recursos de la comunidad científica y la educación global. Permite el intercambio fiable de información relacionada con la identidad, la autenticación y autorización (AAI).
AAI	Infraestructura de Autenticación y Autorización (Authentication and Authorization Infrastructure)
Autenticación	Proceso mediante el que se verifica la identidad de un Usuario Final previamente registrado.
Autorización	Proceso de permitir o denegar el derecho de acceso a un servicio, para un Usuario Final previamente autenticado.
Federación	Asociación de organizaciones que se unen para intercambiar información de sus usuarios como de sus recursos, con la finalidad de permitir la colaboración y transacciones.
Perun	Identity and access management system
VOOT	An extensible protocol for dynamic exchange of group and authorization data
SCIM	System for Cross-domain Identity Management. Sympa: A mailing list server with support for LDAP, multiple authentication protocols and API for integration with other systems
Proveedor de Servicio o SP	Organización responsable de ofrecer al Usuario Final el servicio que este pretende usar. Los Proveedores de Servicio pueden confiar en el resultado de la autenticación y atributos que los Proveedores de Identidad validan de sus Usuarios Finales.
Proveedora de Identidad o IdP	Organización con la cual el Usuario Final está afiliado. Esta es responsable de autenticar al Usuario Final y de administrar los datos de la Identidad Digital de sus Usuarios Finales.

5. RESUMEN EJECUTIVO

Este documento tiene como objeto presentar un reporte del trabajo desarrollado durante la reunión presencial del WP3, realizada en Viena, Austria, los días 10 y 11 de marzo de 2016, para definir la arquitectura del gestor de grupos que utilizarán las RNIES que participan en el proyecto MAGIC.

A continuación se describen los datos generales de la reunión, los participantes, el objetivo y el desglose de actividades, así como los resultados obtenidos y beneficios, los próximos pasos y las conclusiones del trabajo desarrollado.

5.1. DATOS GENERALES

Nombre : Reunión de Trabajo del WP3

Lugar: Austria Viena.

Fecha: del 10 al 11 de marzo 2016

Participantes:

Yousef Torman (ASREN)
Annass Chablí (RENATER)
Michal Prochazca (CEZNET)
Ongjen Prnjat (GRNET)
Christos Kanellopoulos (GRNET)
Eriko Porto (CKLN)
Martha Avila (CUDI)
Rafael Morales (UDG)
Gustavo García (RedCLARA)
Carlos Gonzalez (RedCLARA)

5.2. OBJETIVO

El objetivo principal de esta reunión fue llegar a acuerdos sobre cómo implementar la función de administración de grupos entre las federaciones. El tema fue discutido en

reuniones anteriores, y a partir trabajo realizado en la reunión de Viena, quedó establecida la arquitectura utilizando una entidad de gestión de grupos vinculada a una autoridad de atributo SAML (AA) .

5.3.DESGLOSE DE ACTIVIDADES

Durante la reunión se pudo observar que el trabajo del proyecto MAGIC tiene como antecedentes trabajos previos en el área de gestión de grupos para atender necesidades específicas, resaltando los productos VOOT (GÉANT), SCIM (IETF), SYMPA (RENATER) y Perun (CESNET).

SCIM: Un sistema para la gestión de identidades a través de distintos dominios.

VOOT: Un protocolo para intercambiar información sobre grupos y autorizaciones basadas en pertenencia a grupos.

Sympa: Un sistema para manejo de listas de correo electrónico con varios métodos de autentificación (basada en estándares) y API para la integración con otros sistemas.

Perun: Un sistema integral para gestión de identidades, grupos, servicios y recursos.

Mientras que SCIM y VOOT ofrecen tecnologías horizontales para gestión de identidades y grupos, Sympa y Perun ofrecen tecnologías verticales para la provisión de servicios de más alto nivel (intercambio de mensajes entre miembros de grupos y gestión de servicios y recursos), para lo cual han tenido que integrar, necesariamente, tecnologías similares a las ofrecidas por SCIM y VOOT.

La intención del grupo es integrar las funcionalidades de los cuatro productos, de la mejor manera y con el menor esfuerzo posible, de modo que la reunión consistió en la presentación de cada uno de los productos y negociar su integración en una arquitectura común, la cual se delineó en términos de decisiones de diseño y especificación de restricciones.

Además de la integración de una arquitectura a partir de los productos comentados previamente, otro de los problemas más importantes discutidos en la sesión fue la protección de la privacidad de los usuarios y la reglamentación de la Unión Europea a ese respecto, que imponen restricciones importantes en la manera en que se solicita información sobre la pertenencia de un usuario a uno o varios grupos (ej. soluciones

fáciles, como proveer la lista de grupos a los que pertenece un usuario, proporcionan más información de la necesaria sobre el usuario y violan su privacidad).

DAY 1

The introductory session begin at 08:30am

Gustavo makes an introduction to WP3 objectives, the meeting goal and background of GMF

Carlos Gonzalez asks wether the federation of GMF will run on or parallel to the identity federation. Gustavo says it's going to be decided on this meeting.

The group discusses about the three regions needed to reach the "3 world regions incorporated in the pilot" indicator. Eriko tells it could be difficult for Caribnet as there' not technical people in the NRENs committed to the project and thinks to deploy some GMF components other way than from the NREN

Yousef tells that if we help communities can help NRENs become interested in deploy services for their users.

Carlos tells RedCLARA started delivering services to LA users and after then, NRENs became engaged deploying services or identity providers.

Yousef also tells two technical people left their group and it could be difficult to join middle east to the objectives

We agreed to start talking with APAN, WACREN and Caren.
Michal shows the presentation about VOOT.
Carlos shows the presentation about SCIM.

A question about what what VOOT vs SCIM raises and Michal and Carlos tell Voot is best (simplest) to retrieve information about users and groups and has attributes that SCIM doesn't (as information about inactive users or no-longer belongings) SCIM, on the other hand, allows write users and groups information between systems (not only read this information)

Anass shows the presentation about Sympa

In sympa EEPN is used as the user identifier, so a user can have multiple Emails.

The session for presentations finish by 11:50.

The session to discuss the architecture starts at 12:10

We define we're going to review the requirements, and so, think what technologies are required and the architecture of the solution.

It's mentioned that a Agreement where a user accept to share his or her information is required. It could be one for each VO.

In order to think about the requirements, we'll have to think three use cases:
- To know if a user belongs to a group
- To know what groups a user belongs to
- To get the list of user of a group

Two additional scenarios were evaluated:
- Using an Attribute Authority pass info about what groups the user belong
- An users goes to a SP and the SP needs to know if the user is member of a group in another domain

The group discusses three ways of manage group information:
- A SP using only a group manager
- A SP connecting to a group proxy
- A SP connecting only to a group manager exchanging info with other or others group manager

After the discussion, the following schema (related to option 3) is proposed:

- The Group Provider will have an AttAuthority, a VOOT server and a proxy (cache) to store information about groups in other GP

- The AttAuthority should release the list of groups a member belongs to
-
- The VOOT Server should release information about the groups (as list of members of group A)

- The proxy should harvest information about other groups and keep it locally in order

to response to the SP

The session ends at 16:50

Things to discuss tomorrow about:
. How to authorize a group to access a resource
. Administrative offline authorizing groups in the SP
. Send the groups or groups managers through the
. GM integrated as an AA in current federation, perhaps using a DS, however, using only SAML is not possible because functions like getthig the list of users of a group wont be available,so using VOOT or SCIM

DAY 2

- Session starts at 09:00
-

The group establishes the requirements to implement the architecture. The Group Manager MUST:

- To implement an Attribute Authority able to release the list of groups a member belongs to

- To implement a VOOT interface able to release information about groups (list of members of a group, role of a member in the group, etc.

- The AA and the VOOT system must be on the same endpoint

- Be able to show to the user what groups her belongs to

- Have a self-service group management interface (that could be or not deployed)

- Allow import users from legacy systems through standard protocols (SQL, LDAP...)

- Have audit logs that provides information to tracking

The group mentioned the responsibility to deploy the procedures of removing a user from a group, should be carried by any service, because there are different needs based

on any specific service.

The process of join a user to a group needs to have a disclaimer or must inform the user that his email can be shared to other services provided by partners

The group agreed not to define a Unique global group identifier. This decision was taken because groups would not need anything to be unique on each instance. The above due to the fact that systems groups reference is done by group name, and the source where it came from.

The group review the deliverables list and agree that it will work on the Services Catalogue. We review the GEANT Cloud Catalogue, that could be used as a model.

5.4.RESULTADOS OBTENIDOS, BENEFICIOS

En la reunión se discutieron los siguientes casos de uso:

1. Un usuario en el dominio A tiene que ser autorizados a acceder a un recurso de SP en el dominio B. Cuando esto sucede, el SP en el dominio B puede solicitar a la autoridad de atributo de dominio B (a través de SAML) qué grupos pertenece el usuario. La autoridad atributo de tener la capacidad, y ya tienen un atributo estándar SAML para ello.

2. Un usuario en el dominio A entra en un servicio en el dominio B, y desea utilizar la lista de usuarios en un grupo en el dominio A. Para este caso, el usuario debe ser miembro del grupo está tratando de usar. En este sentido, el proveedor de servicios en el dominio B consultará su propio gestor de grupo. El gestor del grupo B tendrá una lista local del grupo que se ha sincronizado previamente usando un protocolo de petición Voot al administrador del grupo A.

A partir de la reunión se definió:

1. La implementación de la administración del grupo, estará formado por tres componentes:
a) una autoridad de atributo SAML (AA) ,
b) un administrador de grupo (GM aplicación), y
c) un servidor proxy de gestión de grupo (GMP) .

2. El protocolo de información de grupo de cambio será Voot. Voot es una adaptación del protocolo SCIM , para las necesidades de la NREN.

3. La pertenencia a un grupo se validó utilizando atributos SAML estándar.

4. Con el fin de garantizar la velocidad y la fiabilidad, la información de los miembros del grupo se sincronizará periódicamente entre los administradores de grupo.

5. Para el piloto, las aplicaciones de Dokuwiki en Perun, Colaboratorio en RedCLARA , y una aplicación FileSender en RENATER .

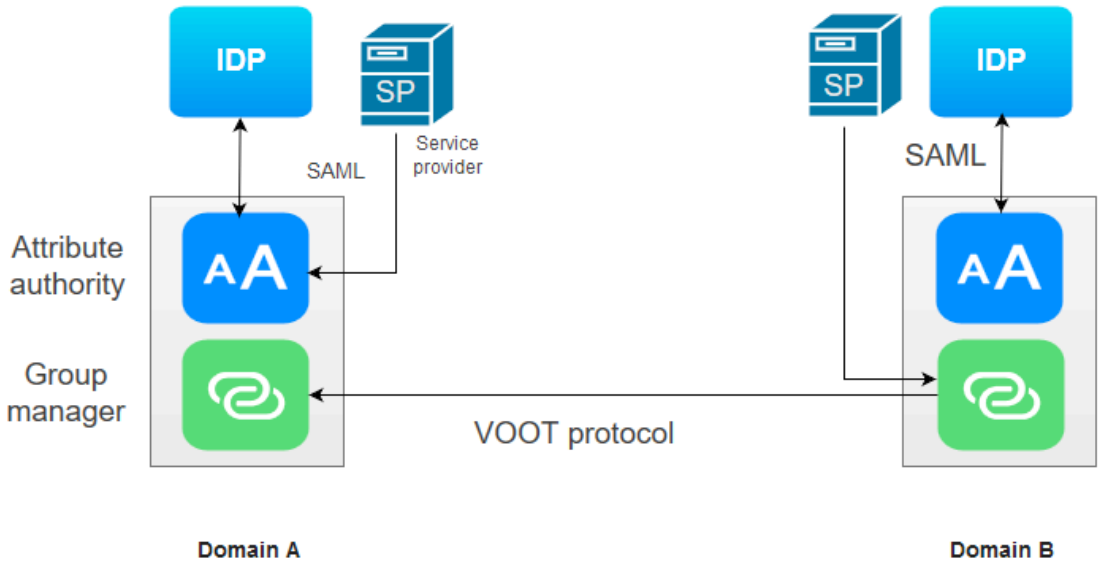
6. Se requiere 1 tercera región del mundo para ser parte del piloto . Esta región haría es probable que sea debido a África y Oriente Medio Caribe tiene algunas limitaciones de recursos en esta etapa .

5.5.PRÓXIMOS PASOS

El equipo de expertos del WP3 está trabajando en implementar el piloto del gestor de grupo y la integración de varias herramientas que requieren administración de grupos en el portal Colaboratorio.

5.6.CONCLUSIÓN

La arquitectura que se definió se ejemplifica en la siguiente imagen



El grupo acordó que los administradores pueden ser una entidad independiente que reside en la autoridad de atributos, así que no hay relación de confianza adicional y esta tendría que ser con configuración.

La única conexión que aún debe ser acordada por los proveedores, es entre los administradores de grupo a través del protocolo Voot.