European Commission

Communications Networks, Content and Technology
European Commission Directorate General

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 D3.3

Planning and design requirements for the group management and inter-operations standards and pilot implementation

European Commission

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

RedCLARA
+ Red + Ciencia

A project implemented by RedCLARA

Progress Report

MAGIC Deliverable: D3.3 Planning and design requirements for the group management and inter-operations standards and pilot implementation

Document Full Name	**D3.3 Planning and design requirements for the group management and inter-operations standards and pilot implementation**
Date	**18-01-2016**
Activity	**Cloud Provisioning and Groupware Standards**
Lead Partner	**CLARA**
Document status	**Final**
Classification Attribute	**Public**
Document link	

Abstract: This document contains the requirements for the Group Management in Federation (GMF) technologies and standards for the MAGIC project pilots. The document contains the results from the evaluation of the required use cases, and implementation candidates.

.

COPYRIGHT NOTICE

MAGIC (Middleware for collaborative Applications and Global virtual 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.

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	Gustavo García	CLARA	10-12-2015	CLARA
Revised by	Michal Procházka	CESNET	14-12-2015	CESNET
Revised by	Nicolas Liampotis	GRNET	14-12-2015	GRNET
Revised by	Carlos Gonzalez	CLARA	14-12-2015	CLARA
Revised by	Alejandro Lara	REUNA	08-01-2016	REUNA
Revised by	Chris Rohrer	UbuntuNet	20-01-2016	UbuntuNet
Approved by	Florencio I. Utreras	CLARA	25-01-2016	CLARA

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

RedCLARA + Red + Ciencia
A project implemented by RedCLARA

TABLE OF CONTENTS

1. INTRODUCTION

The MAGIC WP3 work team has been advancing in the evaluation of group management standards and existing technical solutions. Specifically, the team has identified the need for a Group Management solution that allows federated applications to provide authorized user access to certain resources based on group membership, as well as to share group membership information with applications in support of value-added collaboration features for groups. In this deliverable, the work package team has defined a set of requirements for the group management solution in terms of usability, security, privacy and provided functionality. The requirements particularly focus on implementing a standards-based pilot showcasing the group management capabilities in a federated environment. Among the technically feasible pilot applications we evaluated, two have been selected, namely the Docuwiki used in CESNET and the FileSender available at RENATER.

2. GROUP MANAGEMENT DESIGN REQUIREMENTS

This section describes the group management capabilities and features. It contains the functions and why they are needed, as well as classifing the functions by giving them a qualification of importance. As such, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this section are to be interpreted as described in RFC 2119[1].

Supported standards and protocols: The provided solution shall support multiple open standards and protocols that facilitate the integration with other organizations and solutions. The protocols requested will full support in the latest stable version:

1. VOOT for group management or authorization in federations.
2. SAML for attribute sharing and IdP/SP interaction.
3. Desirable SCIM for group management or authorization in federations.
4. Desirable OpenID Connect (OIDC) for commercial providers integration.

[1] http://tools.ietf.org/html/rfc2119

5. LDAP connectors for getting information of groups from legacy systems.
6. SQL connectors to gather users and group information from SQL databases.

Information gathering: The system shall be able to implement different trust relations with other federated organizations or resources. Having this as the first premise, the solution shall be capable of providing information that includes:

- An unique, persistent, non-reassignable group identifier that can be shared across other domains without conflicts.
- The group members to be used in specific applications like mailing lists.
- Activities and statistics about the group in order to track federated interactions and behaviour.
- Groups which a user belongs to. Information that will be used for authorization purposes.
- Roles of users within their groups (e.g. “admin”) for the same goal as the above.

The up-to-dateness of user information should be guaranteed through an on-demand and/or recurring verification process, e.g. to deal with changes in a person’s affiliation.

User management: The solution has to deal with getting users in. It must support at least these user enrollment workflows:

- Importing users from existing identity and group management systems via standard protocols. Import of the users can be on-time or recurrent.
- User enrollment based on an application form.
- Invitation of users into the group, e.g. via mail.

User ***interfaces and APIs***: The provided solution shall allow creating and updating group information in the host domain. This functionality shall be done through a management interfaces with different permission levels as follows:

A. The solution shall provide a graphical user interface for privileged users, i.e. administrators.
B. The solution shall provide a graphical user interface for end-users to see their memberships and allow updating their own information (e.g. affiliation).
C. The solution shall provide a REST API for allowing clients written in different programming languages to manage group information. Access tokens must be supported for authenticating API calls.

1. The graphical management interface should provide import and export functionality for group information.
2. Based on the type of the service the solution should be able to actively provision information about the groups to the services.
3. The graphical management interface should be easy to localise for target audiences that vary in region and/or language. Multilingual support should include English, Spanish, French and Portuguese in the implementation.
4. The graphical management interface should be user-friendly and intuitive.

Federated management: Integration to SAML2 protocol must be supported. The solution must allow sharing of group information using a SAML2 attribute authority. Support for LDAP- or SQL-based attribute authorities is recommended. This federated function must have the following capacities:

1. The manager must be able to restrict attribute release based on the targeted service provider.
2. The group management information must contain location and language

Secure & ***privacy-aware processing of data:*** Security and privacy are key requirements . The group management must be secure, and allow to define a set of permissions that guarantee group and users' information is not shared without consent. The main features that the solution must comply with are:

- The solution should satisfy the goals of security as listed in Chapter 2 of RFC 3552[2], most notably those under "Communication Security" (e.g. Confidentiality, Peer Entity Authentication). As such, X.509 certificates will be used for message signing, securing web service connections, and encrypting data where necessary. The use of certificates signed by public trusted CAs is recommended for all user browser-facing HTTPS connections.
- The solution must provide a mechanism to obtain user consent for sharing group data.
- Users must be able to revoke sharing permissions.
- The solution should allow users to inspect any personal information held. In addition, any user-asserted identity attributes (i.e. not provided by the Home Organisation / Group Manager) should be self-editable.

[2] https://tools.ietf.org/html/rfc3552

- Users should be able to ask for their group membership information (i.e. personal data) to be deleted once that data is no longer necessary or they withdraw their consent.

Other functions:

- ***Mail to:*** A basic function when talking about using groups, is sending e-mails to the group members. This capability should be included in the model, either if provided by the group provider or by the service provider. If the group provider is going to have the e-mail capability, then a function to do that, must be provided. On the other hand, if the Service Provider is going to be able to do that, the Group Provider will have to provide the list of email addresses of the group members.

3. GMF PILOT REQUIREMENTS

There following are the application environments/markets that are candidates for a GMF pilot integration:

1. RedCLARA's Community Management System
2. RENATER's Sympa/Filesender
3. CESNET's Dokuwiki
    a. Docuwiki will be doing authorization based on the user's group membership. Membership will be expressed in eduPersonScopedEntitlement.
    b. eduPersonScopedEntitlement will be delivered from the SAML attribute authority.
    c. Registration of each SAML attribute authority is required.
    d. There will be created several pages on the Docuwiki which will be assigned to the groups. Groups can have read and/or write privilege.
    4. Docuwiki will be provided with a full support until the end of the MAGIC project.
5. Jitsi application
6. SURFmarket application market

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

RedCLARA + Red + Ciencia
A project implemented by RedCLARA

3.1. IMPLEMENTATION REQUIREMENTS

- Group management software must securely store the data.
- Service must require only minimum set of date (user attributes) which are required for proper service delivery.
- Access to the group management user interface and APIs must be protected by TLS using trusted X.509 certificate (e.g. TCS[3], Let's Encrypt[4], commercial CA).
- User interface must be at least in English language
- API of the group management software must be documented at least in English and the documentation must be publicly available.
- Group management software and services must be available at least to the end of the project.
- All the accesses to the user interfaces and API must be authenticated.
- Group management software and services should be available through the eduGAIN.
- In SAML protocol group information will be transferred in eduPersonScopedEntitlement attribute.

3.2. APPLICATION INTEGRATION REQUIREMENTS

a) The pilot implementation must include a use case:
   i) where group information is obtained in real-time from the federation, in this way, the service provider will get the most updated group membership/information available from the specific user.
   b) where group information is requested directly by the service, in this way, the services can have information about the group before the user access the service.

c) The service provider must contain a use case that covers one of the following scenarios:
   i) **Authorization**: The service provider provides access to an access controlled resource based on the group information.

   ii) **Group members action**: The service provider will obtain group members list from the federation, and execute an action (invite, share,

[3] https://www.terena.org/activities/tcs/

[4] https://letsencrypt.org/

etc) for each of its members. A clean example of this is the invitation for a conference to the members of a specific group.

iii) **Group mailing list**: The service provider will execute a notification action based on the mailing list address related to the group, and obtained through the standard group management protocol request.

d) In the pilot implementation, the service provider must use a standard protocol designed for group management in federations. The above excludes direct LDAP or SQL access implementations suited for local environments, and therefore can't be extended to multi-domain approaches.

3.1. ACTIVITIES DESCRIPTION

Activities are divided into groups. First is dedicated to setting up group management systems and the second one is dedicated to service configuration.

3.1.1 Group management systems involved

Perun
Responsible partner: CESNET
Instance dedicated to the pilot: https://perun.cesnet.cz/edugain/gui/
Authentication to the user interface: via eduGAIN
Authentication to the API: X.509, username/password, SAML
Attribute Authority: available through the eduGAIN

SYMPA
Responsible partner: RENATER
Instance dedicated to the pilot: https://groupes.renater.fr/
(The instance dedicated to the pilot could be: https://name.domain.tld/)
Authentication to the user interface: via eduGAIN
Authorization: based on the email user's groups
Group name: magic@groupes.renater.fr
(The group name could be: groupname@name.domain.tld)
Services already (automatically) integrated to Sympa:

- Survey tool for members of the group.
- Wiki for members of the group.
- Foodle for scheduling meeting between members of the group.

- Share documents between members of the group.

3.1.2 Services involved

Docuwiki
Responsible partner: CESNET
Instance dedicated to the pilot: https://docuwiki-magic.cesnet.cz
Authentication used: via eduGAIN
Authorization: based on the eduPersonScopedEntitlement containing user’s groups

Filesender
Responsible partner: RENATER
Instance dedicated to the pilot: https://filesender-premium.renater.fr/
(The instance dedicated to the pilot could be: https://name.domain.tld/ a little more work to do that)
Authentication used: via the French federation (could be via eduGAIN, needs to be discussed with RENATER)
Authorization: based on the “mail” and the “common name“

Colaboratorio Communities
Responsible partner: RedCLARA
Instance dedicated to the pilot: http://colaboratorio-dev.redclara.net
Authentication used: via Test IdP
Authorization: based on the eduPersonScopedEntitlement containing user’s groups

3.2. SCHEDULE OF MILESTONES

End of the January:

- Perun instance ready to support MAGIC users.
- Perun attribute authority ready to provide attributes to the pilot services.
- Docuwiki ready to accept groups from registered AAs.

Mid February

- Defined developers and integrators with implementation quote

End of the February:

- RedCLARA’s group manager installed

- Defined specific FileSender module modifications.
- FileSender instances in place

Mid March
- Testing Docuwiki's integration
- Defined specific FileSender module modifications.

End of the March:
- RedCLARA's group manager installed

End of the April:
- FileSender group pilot integrated
- Testing for Docuwiki and Filesender done