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 D3.2

Assessment of the existing Group Management Standards and Value Services for Global Communities

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: D3.2 Assessment of Group Management Standards, NREN tools and value services

Document Full Name	**MAGIC WP3 D3.2 Assessment of group management standards, NREN tools and value services for global communities**
Date	**19-10-2015**
Activity	**Cloud Provisioning and Groupware Standards**
Lead Partner	**CLARA**
Document status	**Final**
Classification Attribute	**Public**
Document link	

Abstract: The Group Management in Federation (GMF) technologies and standards was the focus of this deliverable. The document contains the results from the research on the existing technologies like Openconext, Perun, Sympa, Oauth, SAML2, among others. This work will be the base for the terms of reference in order to advance in the MAGIC WP3 goals.

.

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

DELIVERABLE ROUTE

	Name	Member/Activit y	Date	Responsible
From	Gustavo García	CLARA	10-9-2015	CLARA
From	Michal Procházka	CESNET	10-09-2015	CESNET
Contribution by	Soňa Mastráková	CESNET	14-09-2105	CESNET
Contribution by	Michal Procházka	CESNET	14-09-2015	CESNET
Contribution by	Nicolas Liampotis	GRNET	12-10-2015	GRNET
Contribution by	Ognjen Prnjat	GRNET	12-10-2015	GRNET
Contribution by	Christos Kanellopoulos	GRNET	12-10-2015	GRNET
Contribution by	Niels Van Dijk	SURNET	15-10-2015	SURFNET
Contribution by	Ricardo Makino	RNP	16-10-2015	RNP
Contribution by	Carlos Gonzalez	CLARA	16-10-2015	CLARA
Contribution by	Michal Procházka	CESNET	22-10-2015	CESNET
Approved by	Florencio Utreras	CLARA/CEO	23-10-2015	CLARA

TABLE OF CONTENTS

1. INTRODUCTION

The MAGIC project stands for defining a Group Management in Federations (GMF) solution to foster sharing applications and resources in the community. The focus of GMF is in maintain group information in a central and secure location, and providing the capacity to share digital resources with other organizations or domains. For instance, the NRENs will be capable of handling the authorization based on group ownership. The NREN users could share resources with a complete group, access to specific functions or applications depending on their role, among others. Standards and technologies to handle GMF in a domain scope already exists, and there are initiatives of protocols to share this information like VOOT or Grouper, under the concept of virtual organizations. The MAGIC group will select a solution to be implemented in one application market, and establish a pilot with other one sharing group details in two applications. The first step towards this goal is to compare and evaluate the possible solution. This document presents the evaluation of the most advanced solutions in the area, and it will serve as the base ground to build requirements and advance to the committed pilot implementations.

KEY FUNCTIONS AND CAPABILITIES

We can reveal the GMF importance through the exposure of some use cases commonly seen in the collaboration environment. For the MAGIC group, the GMF should address cases like:

> *Authorization*: An application in one service provider domain has a user connected to it. When the user wants to use an specific feature, the GMF should check if he belongs to an specific group or role, and allow or deny the access. All of this shall be done in a federated approach, and the user group information could be anywhere in its home institution.
>
> *Share information about groups*: Some user applications could require or need to share its information to other domains. For instance, A specific group in Biology can benefit from having its existing public to the global community, and be able to use it in a remote application. This information can include: Global group type classification, Participants in the group, among others.

Single Management interface (create and update group information): Nowadays, the organizations have to create groups and manage then in almost every application. The above leads to a highly redundant information, and complexity in its administration. A single domain shall have a single repository, and administration interface for its groups.

Federated management: Is the simplest and central capacity that GMF will fulfill. The groups information must be always up to date, and this requires management at the source. Every institution shall have the capacity to handle their groups information, and make it available to the entire community with the options to segment access or customize privacy features.

2. DESCRIPTION OF TECHNOLOGIES AND STANDARDS

In the following section, the WP3 working group describe the group management technologies available and their characteristics. The listed solutions have been deployed in several organizations across the academic community. The evaluation of the technologies is focused on their features, and how it can be used in a multi-virtual-organization environment.

2.1. SAML2

The Security Assertion Markup Language 2.0 (SAML2) is an open standard and one of the key technologies for federated identity. It enables single sign-on (SSO), which is used to decouple authentication and authorization process from application. It means that a user can use a single credential to access multiple applications. User's credentials are not stored in these applications, they are stored in trusted attribute authorities, which handle authentication and authorization processes by themselves. SAML2 is used to exchange these authentication and authorization data, called assertions. Assertions are in XML format. One assertion represents a set of information about an identity, made by SAML authority (e.g. SAML server). Assertions are exchanged between identity provider, an entity which is able to verify user's credentials and service provider, an entity which needs identity provider to verify user's credentials.
According to this request-reply model, there are 3 kinds of assertions: authentication assertion, attribute assertion and authorization assertion. Authentication assertion serves to assert, that the identity was authenticated by authentication mechanism at a certain time. Attribute assertion serves to assert,

that the identity was associated with the specified attributes (name, surname, etc.). Authorization assertion contains a proof, that the identity has been authorized to access specific resource with specific rights.
Groups information can be carried by SAML2 in two ways:

1. Attributes: In this scenario, the group information is carried as SAML attributes as part of the Authentication statement. Many attributes in the commonly used eduPerson schema actually represent groups:
   a. eduPerson{Scoped}Affiliation provides a fixed naming scheme for labaling people into groups like student, faculty, member, etc
   b. eduPersonEntitlement is used to express roles and rights and may represent groups of people.
   c. eduMember IsMemberOf is commonly used to express group memeberships

   In addition SAML allows arbitrary attributes to be used to express group membership.
   Note that in this scenario the information is only available when a user logs in. This may therefor not serve all use-cases
2. SAML Attribute Query: This protocol provides a back channel for querying attribute- and thus also group- information from an SAML Attribute Authority.
   Note that authorisation management between the SAML Attribute Authority and the requestion Services is based on the same mechanisms as between Identity Providers and Service Providers (SAML metadata). This mechanism is rather course, and may therefor not serve all use-cases.

Finally, it should be noted that SAML supports a variety of security mechanisms at transport- and message-level, namely SSL 3.0 or TLS 1.0 for transport-level security and XML Signature and XML Encryption for message-level security.

For more information about SAML2, please see https://www.oasis-open.org/standards#samlv2.0.

2.2. OAUTH2

The OAuth 2.0 authorisation framework (OAuth2[1]) is an open standard that enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. Instead of requiring the resource owner to share their credentials with the third party, OAuth allows issuing a different set of credentials than those of the resource owner when a client requests access to

[1] Hardt, D., “The OAuth 2.0 Authorization Framework”, RFC 6749: https://tools.ietf.org/html/rfc6749

resources controlled by the resource owner and hosted by the resource server. More specifically, the client obtains an access token, i.e. a string denoting a specific scope, lifetime, and other access attributes, which can then be used to access the protected resources hosted by the resource server. Thereby, OAuth separates the role of the client from that of the resource owner and provides the following advantages over the traditional client-server authentication/authorisation model:

a) Third-party applications are not required to store the resource owner's credentials, typically their password in clear-text.
b) Servers are not required to support password authentication
c) Resource owners have the ability to restrict duration of access and/or provide access to only a limited subset of resources.
d) Resource owners can revoke access to an individual third party without revoking access to all third parties.

OAuth is commonly used to allow users to sign into third party websites using their Google, Facebook or Twitter accounts without exposing their password.
It should be noted that the 2.0 specification replaces and is not backward-compatible with the original OAuth 1.0[2] protocol described in RFC 5849. OAuth 1.0 was vulnerable[3] to session fixation attacks. OAuth 2.0 does not support native encryption capabilities, thus it relies on the SSL/TLS protocol to provide encryption of the sensitive data being exchanged between parties.

2.3. OPENID CONNECT

OpenID Connect[4] is a new emerging standard for single sign-on and identity provision, published in 2014. It adds an identity layer on top of the OAuth 2.0 protocol, thereby allowing clients to verify the identity of an end-user based on the authentication performed by an authorisation server, as well as to obtain profile information about the end-user. Compared to other popular federation approaches, such as SAML and OpenID 1.0/2.0, its main strengths include usability and simplicity. In OpenID Connect, client applications receive the user’s identity encoded in a secure JSON Web Token (JWT), called ID token. Apart from being portable, such ID tokens support a wide range of signature and encryption algorithms. In this context, the ID token resembles the concept of an identity card,

[2] Hammer-Lahav, E., “The OAuth 1.0 Protocol”, RFC 5849: https://tools.ietf.org/html/rfc5849

[3] OAuth Security Advisory: 2009.1: http://oauth.net/advisories/2009-1/

[4] Sakimura, N., Bradley, J, Jones, M., de Medeiros, B., Mortimore, C., “OpenID Connect Core 1.0”, http://openid.net/specs/openid-connect-core-1_0.html

in a standard JWT format, which is signed by the OpenID Provider (OP). To obtain one, the client needs to send the user to their OP with an authentication request. The returned token asserts the identity of the user, called subject in OpenID (sub). Each token specifies both the issuing authority (iss) and the particular audience, i.e. client (aud), for which it was generated. It may specify when (auth_time) and how, in terms of strength (acr), the user was authenticated. It may include additional requested details about the subject, such as their name and email address. Being digitally signed, it can be verified by the intended recipients. It may optionally be encrypted for confidentiality. The ID token statements, or claims, are packaged in simple JSON objects, thus supporting web applications, as well as native / mobile apps.

The OpenID Connect specification defines a set of standard scope values to request the above information to be made available as claim values (e.g. "sub", "name", "email" - see Standard Claims section[5]) from the UserInfo Endpoint. In order to carry group information, OpenID Connect allows additional scope values to be defined and used. For instance the "memberOf" scope is commonly used to get all the groups that the user is member of.

Although SAML had levels of flexibility, security and reliability much greater than OpenID, OAuth or any combination of those two standards, the latest versions of OpenID Connect and OAuth 2.0 provide most, if not all, the benefits that SAML has to offer. For example, from a security perspective, OpenID Connect can provide ISO/IEC 29115 Level of Assurance 1 to 4, through the use of cryptographic and other techniques. Thus, while OpenID Connect is most commonly known for its adoption by Social Media sites for sign-in purposes, it is also gaining traction in enterprise-targeted services, such as Windows Azure Active Directory (WAAD), Ping Federate and PingAccess. There are also mature deployments underway by Deutsche Telecom, AOL, and Salesforce. OpenID connect can also be integrated with provisioning protocols such as System for Cross-domain Identity Management (SCIM) (see below). Finally, it is worth mentioning that while OpenID Connect has many architectural similarities to OpenID 2.0, the identifier format is different and thus Relying Parties need to migrate[6] those user identifiers to continue serving these users.

[5] http://openid.net/specs/openid-connect-basic-1_0-28.html#StandardClaims

[6] Sakimura, N., Bradley, J., Agarwal, N., Jay, E., "OpenID 2.0 to OpenID Connect Migration 1.0", http://openid.net/specs/openid-connect-migration-1_0.html

2.4. SCIM

The System for Cross-domain Identity Management (SCIM) open standard provides a a platform-neutral schema and extension model for representing users and groups in JSON format.The SCIM standard can be used to automatically add/delete users from systems or to share information about user attributes, group attributes, attribute schema. SCIM is suitable for cloud-based applications and services, because it is simpler than other existing standards and builds on prior standards. SCIM model consists of the main object, called Resource. Each SCIM Resource is a JSON object. All other objects are derived from the Resource. First derived object is ServiceProviderConfig[7], which enables service provider to discover SCIM specification features in a standardized form, as well as provide additional implementation details to clients. Second derived object is Schema, which specifies metadata about Resource. Third derived object is CoreResource. There are user and group data contained in the CoreResource object, within their own objects User and Group. More specifically, each user is member of a set of groups (may be empty). For each group that the user is member of, the membership is represented with the existence of an membership object. The membership object has no required properties, but a set of optional properties.
For good manipulation with resources, SCIM provides REST API. It is possible to create, update, delete, search, read, replace or bulk resources. Data for the API can be formatted in JSON or XML.

For more information about SCIM, please see http://www.simplecloud.info/.

2.5. VOOT

Virtual Organisation Orthogonal Technology (VOOT) standard extends SCIM to exchange information about groups and its members in federated environment. Old version 1.0, which is currently used in some products (Perun, OpenConext, Grouper, COmanage), is not compatible with the new one. Version 1.0[8] defines a protocol for read-only access to information about users' group membership within an organisation or aggregated across organisations and their role in these groups. VOOT 1.0 provides REST API, which supports 2 calls: retrieve a list of groups the user is member of and retrieve the list of people that are members of a group the user is also member of. Only JSON data format is supported.

[7] "draft-ietf-scim-core-schema-22 - System for Cross-Domain ..." 2012. 31 Aug. 2015 <https://tools.ietf.org/html/draft-ietf-scim-core-schema>

[8] "Old version - VOOT." 2014. 1 Sep. 2015 <http://openvoot.org/v1/>

Current version 2.0 defines a protocol and a data model. Protocol provides information about groups and roles. All requests towards VOOT provider have to be authenticated with an OAuth2.0 Bearer Token. Information about authorization can be found here https://tools.ietf.org/html/rfc6750. Protocol can work very well also with OpenID Connect. Data model extends SCIM model with membership object and group types object, so it has four entities: user, membership, group and group type. Group type can be chosen according to the situation, there is no detailed specification in core itself about group types, so it is up to communities to standardize it. Thanks to these 2 additional entities, comparing to SCIM, it is possible to build more flexible environment using VOOT 2.0 data model. For example, when user wants to belong to one group and have 2 different roles in this group, it is possible now with the membership entity, which is a big advantage.

For more information about VOOT, please see http://openvoot.org/.

3. EXISTING GROUP MANAGEMENT SYSTEMS

3.1. HEXAA

HEXAA is an External Attribute Authority (EAP) based on SAML2 that can manage Virtual Organisations with fine-grained role management requirements, as well as user profile management to share common data with multiple Service Providers. It is also possible to handle user consent (aligned to the EC data protection directives) and implement custom provisioning hooks.

License: Open source
Current deployments: Hungarian Identity Federation (EDUID), NIFI NREN HPC, e-Science gateway
Modes of deployment:
Sustainability model: Project runs until March 2015, MTA SZTAKI and NIIFI will maintain it after it.

3.2. OPENCONEXT

OpenConext is an open source collaboration management platform. It provides a SAML2 proxy for identity federation, a group proxy for group management and built-in tools for the management of the service registry and of group providers. OpenConext is an infrastructure that enables groups, teams or organizations to bring together a set of federated tools such as wiki's, mailing lists, or video conference software for use in a collaboration. More specifically, OpenConext comprises two core components:

a) Engine is a SAML2.0 (SAML2Int WebSSO profile) compliant authentication proxy capable of acting as an IdP or SP. Apart from the authentication proxy, it also provides a "Where Are You From" (WAYF) service. Moreover, an interface allowing users to express their consent regarding the release of their identity attributes is available. Finally, the OpenConext Engine includes an interface enabling users to view and manage profile and group membership information.

b) API: Serves as the group proxy, also providing a management tool, named Manage. It supports both the Grouper API and VOOT with either OAuth (2.0) or Basic Auth authentication.

All other components are provided by 'third parties', including SPs, IdPs and group providers.

To ease OpenConext deployment, several sample implementations of these components can be installed as part of the OpenConext VM. These include: i) Teams, a federated self-service GUI for managing collaboration groups which uses Internet2's Grouper as its back-end; ii) Mujina, a mock SAML2 IdP and SP, and iii) Profile, an SP that displays profile, groups and application information to end-users. A MySQL database is shared among OpenConext components for storing configuration data.
The remainder of this section focuses on Teams and Grouper, which serve as the basis for the group management capabilities of OpenConext. More specifically, besides serving as an authentication proxy, OpenConext can be configured as a Group proxy. In this context, it allows Group providers to be connected using the Grouper API or the VOOT API. When an SP submits a query to the Group API, all available group information of a given user can be combined taking into account the access control list(s) and attribute release policy in effect for that particular SP. The default OpenConext installation contains the Teams application for managing groups. This provides an easy to use interface for end-users to self-manage groups after login into the application via an IdP. Teams allows an authorised end-user to: create teams; invite and re-invite other team members via email; manage team members; assign basic roles like admin, manager and member; combine groups from connected group providers into new (virtual) teams; search for publicly available teams; request membership information of existing teams. Finally, OpenConext exposes the OpenSocial/VOOT API for the exchange of user and group information using a standardised REST API. The OpenSocial/VOOT API

only implements People and Group REST API calls, it is thus a partial OpenSocial[9] Container implementation. For authorisation purposes, the REST API uses OAuth 2.0 (preferred) and optionally OAuth v1 (deprecated, though still functional).

License: Apache License Version 2.0
Current deployments: SURFnet (SURFconext), AARnet, Dutch Hacker Space, TraIT; see https://www.openconext.org/showcases
Modes of deployment: as a VM
Sustainability model: Maintained by SURFnet and the open source community. It also relies on external open source projects, such as Janus, Grouper, simpleSAMLphp, Shibboleth

3.3. PERUN

Perun is an identity and access management system. It covers management of the whole user life cycle, including user registration, expiration or suspension of the user. It is a tool, whose key features are virtual organisation management, user management, group management, resource management and service management. The system can be customized for various use cases. Perun has been designed to work in distributed environments like identity federations and grids.

Perun does not manage primary user identities; users have to come with some existing identity like federated identity, social identity or digital certificate. Users can link those identities, so they will be recognized properly even if they use different identities. Users does not need to create any additional credentials, because Perun can publish linked identities to the end services.

Because user communities usually already have some local user/group management system which cannot by simply connected to the federated services, Perun supports import/export of existing users/groups. Currently, there is support for communication with external sources using VOOT, SAML2, LDAP, VOMS, SQL (MySQL, Oracle, SQLite) or import data from XML and CSV files. Synchronization can work in both ways.

[9] OpenSocial Specification: http://opensocial.github.io/spec/trunk/OpenSocial-Specification.xml

Basic component for group management is virtual organisation (VO), this concept has been adapted from computational grid environments. Every VO can have several groups and each group can be nested like a tree, so it can have its own subgroup, where the access rights are inherited in the same way. Users be in several VOs as well in any number of groups. Each VO and each group has its own VO/group managers. VO can have not only groups but also resources which represent services to which VO members can have an access. Actually, access management in Perun is done on group level. Every group can have an access to VO's resources. The responsibility for the group management can be delegated from VO manager to the group manager. The group manager can be specific user from the VO or other exiting group in VO. Those group administrators obtain permissions to handle the access to resource/service via group membership, so the VO manager is not the only responsible person and does not have to handle all permission/membership issues in the VO.

Perun is specific for its push mechanism which is used for delivering data about users and groups (authorization data) to the end services. Access management for federated services is supported by attribute authority (managed by Perun), but the services which need to know about the user in advance (e.g. videoconferencing systems, reservation systems, computational resources) cannot use attributes about the users from identity federation, because they come when the user logs in. Perun is able to push the information about users/groups to those services via various communication channels.

Perun provides its functions and components via various APIs. The basic API is REST-like API, using JSON as a data container. In case some external system wants to use Perun's functions and components and does not want to use REST-like API, there is possibility to connect via Java library, JavaScript library, PERL library or PHP library. Perun pushes also information to the LDAP which is then used by Attribute Authority or Identity Provider, so information stored in Perun can be used in identity federation world.

Perun has several production deployments where manages tens of thousands users, hundreds of virtual organizations and manages access to nearly 2000 services.

License: FreeBSD License
Current deployments: Czech eInfrastructure, EGI, ELIXIR, SAGRID, Masaryk University
Modes of deployment: as a service or as a VM

Sustainability model: Maintained by CESNET and Masaryk University

3.4. SYMPA

Sympa is not only the more complete opensource mailing-list manager. Sympa wears in its genes group management since 18 years, with a userfriendly web interface. In Sympa, the groups can be provisionned by multiple protocols : VOOT, LDAP, SQL, flat files, SMTP, SOAP and other Sympas. In Sympa the groups membership can be requested by various protocols : VOOT, SAML2, SQL. Sympa proposes 4 different roles. Sympa accepts various authentication method : Federation (SAML2), LDAP, X509. Sympa is scalable for big VOs (with more than 1.000.000 members).

At RENATER (the service is called Universalistes) we have linked Sympa with ther tools so that each VO hosted at RENATER can benefit, in one clic, from mailing list, wiki (with public and private pages), foodles, limesurveys filesenders. We also have copled Sympa with an Attribute Authority in order to permit Sympa group authorizations on any external Services Providers using SAML protocol. The RENATER's Sympa infrastructure is used by more than 1600 VOs with up to 300000 members, but there are biggest deployments in the world.

Licence: Free Software distributed under GNU General Public License, version 2
Current deployments: All over the world, here are some of the well known organizations that use Sympa
Modes of deployment: As a Service in Universalistes or as a Software
Sustainability model: maintained by RENATER and the OpenSource community

3.5. UNITY

Unity is a complete solution for identity, federation and inter-federation management. Unity allows its administrators to enable authentication using various protocols, with different configurations for many relaying parties. The actual authentication can be performed using the built-in, feature-rich users database or can be delegated to one of supported upstream identity providers (IdPs). The information obtained from upstream IdPs can be flexibly translated and merged with the local database (if needed) and re-exported using other protocols.

License: BSD
Current deployments: EUDAT (Work in progress)
Modes of deployment:
Sustainability model:

4. FUNCTIONS COMPARATIVE

Possibilities of interoperability:
Does system support import/export of its data?
If yes, please explain briefly in the *comment*.

Systems	Yes / No	Comment
Hexaa	yes	
OpenConext	yes	SAML2 Metadata import/export in XML is possible in the Janus Service Registry
Perun	yes	Import of users/groups is possible via LDAP, SQL, XML, CSV, VOOT interfaces
Sympa	yes	
Unity	no	

Supported standard protocols:
Does system support standard protocols like SAML2, OAuth, VOOT, SCIM, …?
If yes, please specify which ones in the *comment*.

Systems	Yes / No	Comment
Hexaa	yes	Hexaa currently supports REST API and SAML2 AA.
OpenConext	yes	OpenConext currently supports VOOT and SAML2 AA. OpenID 2 support is under development.
Perun	yes	Perun currently supports VOOT, SAML2 and REST API. OpenID Connect support is under development.
Sympa	yes	Sympa currently supports VOOT, SAML2 and SOAP.

Unity	yes	Unity currently supports SAML2 AA and SAML2 IdP. OpenID Connect and OpenID 2 support is under development.

Multilingual support:
Can system talk to the end-users using different languages?
If yes, please specify which ones in the *comment*.

Systems	Yes / No	Comment
Hexaa		
OpenConext	yes	Metadata is stored in multiple languages. The interfaces support multiple languages.
Perun	yes	English is a default. Notifications and application forms are multilingual.
Sympa	yes	23 languages(English,French,Spanish,Deutsch,Italiano,Nederlands,Portugues,Romana,Català,Cesky,Eesti,Suomi,Turkce “Arabic-in progress”...)
Unity		

Federation and inter-federation support:
Is system able to be connected to the identity federations?
If yes, please explain briefly in the *comment*.

Systems	Yes / No	Comment
Hexaa	yes	
OpenConext	yes	SALM2int and eduGAIN complient.
Perun	yes	
Sympa	yes	
Unity	yes	

External/homeless identity management:
Does system provide registration of homeless or external (Google, Facebook) identities?
If yes, please specify which ones in the *comment*.

Systems	Yes / No	Comment
Hexaa	No	
OpenConext	yes	Google, Facebook, Twitter, LinkedIn (via simpleSAMLphp proxy)
Perun	yes	Google. Facebook, LinkedIn (via Social bridge IdP)
Sympa	yes	Native registration of sympa+ Google,Facebook..(via proxy)
Unity	Will	It is under development

User-life cycle management:
Does system care about user enrollment/expiration/suspension?
If yes, please explain briefly in the *comment*.

Systems	Yes / No	Comment
Hexaa	No	
OpenConext	No	This is a responsibility for the IDP
Perun	yes	User can have different status within different virtual organisations (valid/invalid/suspended/expired/disabled). Expiration of user membership are per virtual organization.
Sympa	yes	Care about user enrollment/expiration/suspension Care about enrollment/expiration/suspension of a group of users Enrollment also possible from multiple databases (SQL,LDAP)
Unity		

Delegated administration:
Does system provide capabilities to delegate administration of groups?
If yes, please explain briefly in the *comment*.

Systems	Yes / No	Comment
Hexaa	No	
OpenConext	yes	Serves as the group proxy, also providing a

		management tool, named Manage. It supports both the Grouper API and VOOT with either OAuth (2.0) or Basic Auth authentication.
Perun	yes	
Sympa	yes	
Unity		

5. NREN TOOLS AND SERVICES FOR GMF PILOT

The WP3 working group suggested the following tools as the possible candidates for a pilot implementation in GMF:

A. ***Colaboratorio***: Developed and shared by RedCLARA, the Colaboratorio is a space to share applications and manage communities. The Colaboratorio integrates services like Webconference, Wiki, and FileSender around a community. The GMF functions in the Colaboratio could be oriented to share communities associated with a user, so other services can take access decisions on it. For instance: a) a user wants to use Foodl to invite all people in a Astronomy community for a meeting, b) a user wants to share an article about Cancer to the medicine related groups, etc.

B. ***Webconference (MCONF/Jitsi)***: Webconferencing is an application that usually handle groups. It is really common to invite people in a group to attend to meeting or online event. RedCLARA already do this using the communities in scheduling application (SIVIC) in Colaboratorio. With MAGIC, this feature could become an inter-domain feature.

C. ***Shared cloud storage***: Systems like ownCloud allows people in the community to store files in the Cloud. Experience have shown that public clouds are not a safe place for highly sensitive information because of the privacy guarantee. Several NRENs are working on implementing secure cloud storage for its communities. When this environment is in place, a method to share and authorize access to this resources will be required.

D. ***Zimbra***: Is a corporate class email, calendar and social platform with a free version for the communities. This kind of solutions will be a good pilot for academic institutions.

E. ***Wiki***: Collaborative edition of online published content is the main value of any wiki solution. This feature requires permission management, that in most cases is handled within an authentication domain, or just providing full read and write permissions to everyone that is authenticated. A GMF could add value to the wikies by improving its security, and providing a method to provide the right permission to the right people/group.

F. ***eLearning***: Learning Management Systems (LMS) or Massive Open Online Course (MOOC) platforms are one of the most used elements across the academic and research communities. Facilitate course sharing and diffusion could be a great advantage of including GMF in this solutions.

6. CONCLUSIONS

Group Management in Federations (GMF) is taken a lot of interest and attention in the community. We can saw this by the solutions, standards and development involved in this area. The MAGIC work package 3 have studied the solutions available and found that OpenConext, Perun, Sympa, SCIM, and Unity could potentially fulfill the need to manage working groups. There are technologies like OpenConext that has the advantage of the support and the architecture itself that brings together the whole elements for identity and group management. On the other side, solutions focused specifically in the group management and authorization part like Perun or Sympa can be easier to be integrated to the current Latin-American applications market of RedCLARA because less architectural changes would be required. It is foreseen that a standard like OAuth2.0/OpenID Connect or VOOT would be directly or indirectly involved in the integration. Further research in testing and integration results shall be done. The next step in the MAGIC path is to evaluate the define a set of requirements for the GMF solution, and from there taking the next step in adopting one of the evaluated technologies.