F E N I X

Technology Profile Annex Fenix

Authors	Fernando Aranda Gabriel Cruz
Last Modification	June 5, 2017
Version	1.0
Date	June 5, 2017

Copyright

The research conducted by CUDI and leading to these results has received funding from FONCICYT, under Agreement 4 / II / 2014, which authorized the allocation of resources to support the Second Call for registration of pre-proposals CONACYT Horizon2020 and through Agreement number 15/IVE/2015, of the Technical and Administration Committee of "FONCICYT", authorizing the transfer of resources in favor of CUDI for the development of the project called "**M**iddleware for Collaborative **A**pplications and **G**lobal V**I**rtual Communities". It is based on the results obtained from the financing granted by the Seventh Framework Program (FP7 2007-2013) of the European Community, under Grant Agreement No. 238875 (GÉANT).

Table of Contents

1 Definitions

Attribute	Piece of information describing the End User their properties and/or their roles within an Organization.
Attributes Authority	The organization responsible to administering additional attributes for an End User in an Organization.
Authentication	Process by which the identity of a previously registered End User is verified.
Authorization	Process to allow or deny the right of access to a service for previously authenticated End User.
Digital Identity	A set of information attributable to an End User. This information is issued and administered by an Identity Provider Organization based on prior End User Authentication.
Discovery Service	Service administered by the Federation Operator for Federation Members acting as Service Providers which provides a list of the Identity Provider Organizations of the Federation.
Federation	The Identity Federation. An association of organizations that unite to exchange information of their users and their resources, in order to allow collaboration and transactions.
Identity Management	Process of issuing and managing the digital identities of the End Users.
Identity Provider or IdP	Organization with which the End User is affiliated. This is responsible for authenticating the End User and managing the data of the Digital Identity of its End Users.
Interfederation	Voluntary Collaboration of two or more Identity Federations to enable End Users in an Identity Federation to access to Service Providers of another Identity Federation.
Member of the Federation	An organization that has joined the Federation by accepting in writing the Federation Policies. Within the framework of the Federation a Member may act as an Identity Provider and/or a Service Provider.
Metadata	File in SAML / XML format that contains information regarding Federation Members.
NREN	National Research and Educations Network (Also known as NREN)
Service Provider or SP	Organization responsible to offering the End User the service it intends to use. The Service Providers can rely on the results of the authentication and attributes that the Identity Providers validate from their End Users.
Operator of the Federation	Organization which provide the infrastructure for the Authentication and Authorization of the Members of the Federation.
Technological profile	One type of Federation Technology, e.g. WebSSO, eduroam.

2 Introduction

This document establishes the technical specifications that organizations interested in joining the Federation as an Identity Provider must comply with and is an annex to the Federation Policies.

3 Protocol

The protocol used by the Federation for the exchange of information between its members is SAML version 2.0

4 Deployment Application

The Federation establishes as a standard application for the deployment of a SimpleSAMLphp IdP (https://simplesamlphp.org/), it is an open source tool, developed in php and based on the SAML protocol.

SimpleSAMLphp has a large installed base, the project is led by UNINETT and is found in many Identity Federations around the world.

5 Operating System

The Federation offers support, as a standard implementation of an IdP, for Linux operating systems, in its Debian distributions in version 7 or higher and Ubuntu in version 12 or higher, other operating systems may be used, but there will be no support from the from the Federation to them.

6 Certificates

The Federation Identity Providers must generate the certificates they will use, with at least the following characteristics:

- Full domain name (FQDN)
- The certificate must be within the validity period, not be revoked and have the correct certification path.
- The key size must be 2048 or 4096 bit RSA and the RSA signing algorithm with SHA-2 hash must be included.

7 Metadata

The Federation's metadata must be in SAML 2.0 format according to **SAML V2.0 Metadata Interoperability Profile.**

8 Attributes

The attributes are a fundamental part of the authorization of users, they show the information inherent to the user and his link with the institution to which he belongs.

The minimum attributes that a Federation Identity Provider must be able to release are:

Attribute	**Description**	**Format**
eduPersonPrincipalName	User name, NetID type (e.g. user@domain)	user@institution.edu.mx
Cn	User Name	User
Sn	User Nickname	Last name
Mail	e-mail address of the user	user@institution.edu.mx
eduPersonScopedAffiliation	User link with the institution	student@institution.edu.mx
eduOrg	Name of the Organization	University Name

In addition to these attributes, Service Providers (SP) may request additional attributes, this will depend on the service offered and the agreements between IdP and SP.