Corporación Universitaria para el Desarrollo de Internet A.C.
Internet 2 - México

Federación Nacional de Identidades Mexicanas

F E N I X

Especificaciones Técnicas Para Incorporación Como Proveedor de Identidad (IdP)

Autores	Fernando Aranda Gabriel Cruz
Última modificación	05 de junio 2017
Versión	1.0
Fecha	05 de junio de 2017

Copyright

La investigación realizada por CUDI y que lleva a estos resultados ha recibido financiamiento de FONCICYT, bajo el Acuerdo 4/II/2014 con el que se autorizó la asignación de recursos para apoyar la Segunda Convocatoria para el registro de pre-propuestas CONACYT Horizon2020 y mediante acuerdo número 15/IVE/2015, del Comité Técnico y de Administración del "FONCICYT", autorizando la canalización de recursos a favor de CUDI para el desarrollo del proyecto denominado "**M**iddleware for Collaborative **A**pplications and **G**lobal V**I**rtual **C**ommunities". A su vez se fundamenta en los resultados obtenidos del financiamiento otorgado por el Séptimo Programa Marco (FP7 2007-2013) de la Comunidad Europea, bajo el Acuerdo de Subvención No. 238875 (GÉANT).

Tabla de Contenidos

1 Definiciones

Administración de la Identidad	Proceso de emitir y administrar las identidades digitales de los Usuarios Finales.
Atributo	Pieza de información que describe al Usuario Final, sus propiedades y/o sus roles dentro de una Organización.
Autenticación	Proceso mediante el que se verifica la identidad de un Usuario Final previamenteregistrado.
Autorización	Proceso de permitir o denegar el derecho de acceso a un servicio, para un Usuario Final previamente autenticado.
Federación	La Federación de Identidad. Una asociación de organizaciones que se unen para inter cambiar información de sus usuarios como de sus recursos, con la finalidad de permitir la colaboración y transacciones.
Identidad Digital	Conjunto de información atribuible a un Usuario Final. Esta información es emitida y administrada por una Organización Proveedora de Identidad basándose en la previa Autenticación del Usuario Final.
Interfederación	Colaboración voluntaria de dos o más Federaciones de Identidad para habilitar a los Usuarios Finales en una Federación de Identidad para acceder a Proveedores de Servicio en otra Federación de Identidad.
Metadato	Archivo en formato SAML/XML que contiene información respecto de los Miembros de la Federación.
Miembro de la Federación	Una organización que se ha unido a la Federación aceptando por escrito las Políticas de la Federación. Dentro del marco de la Federación, un Miembro puede actuar como un Proveedor de Identidad y/o un Proveedor de Servicio.
Operador de la Federación	Organización que provee la Infraestructura para la Autenticación y Autorización de lo los Miembros de la Federación.
Proveedora de Identidad o IdP	Organización con la cual el Usuario Final está afiliado. Esta es responsable de autenticar al Usuario Final y de administrarlos datos de la Identidad Digital de sus Usuarios Finales.
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.
RNEI	Red Nacional de Educación e Investigación (También conocida como RNIE)
Servicio de Descubrimiento	Servicio administrado por el Operador de la Federación para los Miembros de la Federación que actúan como Proveedores de Servicio el que ofrece una lista de las Organizaciones Proveedoras de Identidad de la Federación.
Usuario Final	Cualquier persona afiliada a una Organización Proveedora de Identidad, ej. un empleado, investigador, profesor o estudiante, haciendo uso de los servicios de un Proveedor de Servicio.

2 Introducción

Este documento establece las especificaciones técnicas que las organizaciones interesados en adherirse a la Federación como Proveedor de Identidad deben cumplir y es un anexo de las Políticas de la Federación.

3 Protocolo

El protocolo utilizado por la Federación para el intercambio de información entre sus miembros es SAML versión 2.0

4 Aplicación de despliegue

La Federación establece como aplicación estándar para el despliegue de un IdP **SimpleSAMLphp** (**https://simplesamlphp.org/**), es una herramienta de código libre, desarrollada en php y se basa en el protocolo SAML.

SimpleSAMLphp tiene una gran base instalada, el proyecto está dirigido por UNINETT y se encuentra en muchas Federaciones de Identidad en el mundo.

5 Sistema Operativo

La Federación ofrece soporte, como implementación estándar de un IdP, para los sistemas operativos Linux, en sus distribuciones Debian en su versión 7 o superior y Ubuntu en su versión 12 o superior, otros sistemas operativos podrán ser utilizados, pero no habrá soporte por parte de la Federación hacia ellos.

6 Certificados

Los Proveedores de Identidad de la Federación, deberán generar los certificados que utilizarán, con al menos las siguientes características:

- Nombre completo del dominio (FQDN)
- El certificado debe estar dentro del periodo de validez, no estar revocado y tener la ruta de certificación correcta.
- El tamaño de la clave debe ser de RSA de 2048 o 4096 bits y se debe incluir el algoritmo de firma RSA con hash SHA-2.

7 Metadatos

Los metadatos de la Federación deberán en formato SAML 2.0 de acuerdo al **SAML V2.0 Metadata Interoperability Profile**.

8 Atributos

Los atributos son parte fundamental de la autorización de usuarios, en ellos se muestra la información inherente al usuario y su vínculo con la institución a la que pertenece.

Lo atributos mínimos que un Proveedor de Identidad de la Federación debe ser capaz de liberar son:

Atributo	Descripción	Formato
eduPersonPrincipalName	Nombre del usuario, tipo NetID (ej usuario@dominio)	usuario@institucion.edu.mx
Cn	Nombre de Usuario	Usuario
Sn	Alias o sobrenombre de usuario	Apellido
Mail	Dirección de correo del usuario	**usuario@institucion.edu.mx**
eduPersonScopedAffiliation	Vínculo del usuario con la institución	alum@institucion.edu.mx
eduOrg	Nombre de la Organización	Universidad de XXXXXX

Adicionalmente a estos atributos, los Proveedores de Servicio (SP) podrían solicitar atributos adicionales, esto dependerá del servicio ofrecido y de los acuerdos entre IdP y SP.