COFRe: Comunidad Federada REUNA

Reglas para el Registro de Metadatos

Versión 2.1 - 21/01/2021

RedUNA
Ciencia y Educación en Red

Tabla de Contenido

1. Definiciones y Terminología

Las palabras clave "DEBE(N)", "NO DEBE(N)", "OBLIGATORIO", "DEBERÁ(N)", "NO DEBERÁ(N)", "DEBERÍA(N)", "NO DEBERÍA(N)", "RECOMENDADO", "PUEDE(N)", y "OPCIONAL" utilizadas en este documento serán interpretadas según se describe en RFC 2119 [RFC2119].

Las siguientes definiciones serán usadas en este documento:

Federación	La Federación de Identidad. Una asociación de organizaciones que se reúnen para intercambiar información de manera segura, tanto de sus usuarios como de sus recursos, según sea convenido, con el fin de promover la colaboración y transacciones entre ellos.
Miembro de la Federación	Una organización que se ha unido a la Federación aceptando por escrito las Reglas de la Federación.
Operador de la Federación	Organización que provee de la infraestructura para la Autenticación y Autorización de los Miembros de la Federación.
Reglas de la Federación	Un documento que describe las obligaciones, los derechos y obligaciones tanto de los Miembros de la Federación como del Operador de la Federación.
Entidad	Un componente discreto que un Miembro de la Federación desea registrar y se describe en metadatos. Típicamente corresponde a un Proveedor de Identidad o a un Proveedor de Servicios.
Registro	Sistema utilizado por el Operador de la Federación para registrar los metadatos de una Entidad. Esto puede ser realizado por alguna herramienta de auto-servicio o a través de un proceso manual.
Representantes Registrados	Individuos autorizados para actuar en representación de un Miembro de la Federación. Estos pueden tener diferentes roles con diferentes derechos asociados.

2. Introducción y Aplicabilidad

Este documento describe las reglas para el registro de metadatos en COFRe, el cual tendrá efecto desde el 24 de abril de 2019. Todas las nuevas entidades registradas desde la fecha de publicación en adelante DEBERÁN someterse a lo descrito aquí hasta que este documento sea actualizado o reemplazado por revisión.

Este documento DEBERÁ ser publicado en el sitio web de la Federación https://www.reuna.cl/cofre/. Las actualizaciones realizadas a este documento DEBERÁN verse reflejadas con exactitud en los metadatos de la entidad.

Una entidad que no incluya una referencia a las reglas de registro DEBE ser asumida como una entidad registrada bajo un régimen anterior, sin reglas de registro. Los requerimientos para reevaluar una cierta entidad contra las Reglas Registro de Metadatos actuales PUEDEN ser solicitados al correo de contacto de la Federación cofre@reuna.cl.

3. Elegibilidad y Propiedad

Los Miembros de la Federación tienen el derecho de hacer uso del Registro del Operador de la Federación para registrar Entidades. Solicitudes de Registro desde otras fuentes NO DEBERÁN ser aceptadas.

El proceso para transformarse en un Miembro de la Federación está documentado en las Reglas de la Federación, disponibles en https://www.reuna.cl/cofre/.

Este proceso verifica que quien aplica tiene la capacidad legal para ello, y requiere que todos los miembros ingresen en una relación contractual con el Operador de la Federación, mediante el aceptar las Reglas de la Federación. El Operador de la Federación valida en base al nombre legal provisto por quien aplica. La validación es realizada de acuerdo a bases de datos oficiales, las que incluyen, pero no se limitan a:

- Portal Público de Datos del Gobierno de Chile: http://datos.gob.cl
- Registro de Compañías del Ministerio de Economía de Chile: http://www.registroempresas.cl
- Ministerio de Educación de Chile: https://www.mineduc.cl/

Este proceso busca también identificar y verificar a los Representantes Registrados (administrativos y técnicos), quienes están habilitados para actuar en nombre de la organización e interactuar con el Operador de la Federación. La verificación se realiza según la información provista durante el proceso de solicitud de
membresía.

Adicionalmente, el proceso establece un nombre canónico para el Miembro de la Federación, el cual PUEDE cambiar mientras la organización sea Miembro de la Federación, por ejemplo, como resultado de un cambio de nombre corporativo o por fusiones. El nombre canónico se publica en el elemento del metadato SAML v2.0 <md:OrganizationName> de la Entidad [SAML-Metadata-OS].

4. Formato del Metadato

Los metadatos para las Entidades registradas por el Operador de la Federación DEBERÁN hacer uso de la extensión [SAML-Metadata-RPI-V1.0] para indicar que el Operador de la Federación es quien registra la Entidad y para detallar la versión de Reglas Registro de Metadatos que aplican a la Entidad. El siguiente es un ejemplo de esto:

```
<mdrpi:RegistrationInfo
egistrationAuthority=http://cofre.reuna.cl
registrationInstant="2016-11-29T13:39:41Z">
        <mdrpi:RegistrationPolicyxml:lang="es">
              http://cofre.reuna.cl/index.php/es/reglas-federacion
        </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>

<mdrpi:RegistrationInfo
registrationAuthority=http://cofre.reuna.cl
registrationInstant="2016-11-29T13:39:41Z">
        <mdrpi:RegistrationPolicyxml:lang="en">
              http://cofre.reuna.cl/index.php/en/federation-rules
        </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5. Elegibilidad de una Entidad y Validación

5.1 Registro de Entidad

El proceso mediante el cual un Miembro de la Federación puede registrar una Entidad se describe en https://www.reuna.cl/cofre/.

El Operador de la Federación DEBERÁ validar que el Miembro de la Federación tiene el derecho de usar ciertos nombres de dominio, en base a los atributos de su identificador de Entidad (entityID de aquí en adelante) y, para Entidades Proveedoras de Identidad, cualquier nombre dominio que identifique a sus usuarios (scope en inglés).

El derecho a usar un cierto nombre de dominio DEBERÁ ser establecido de una de las siguientes formas:

- Un nombre canónico que calce con la información registrada que aparece en el servicio WHOIS.
- Un miembro PUEDE recibir los derechos de uso de un nombre de dominio específico, mediante un permiso por escrito extendido por el dueño del nombre de dominio en base a la Entidad. Este permiso NO DEBERÁ ser considerado como autorización para usar subdominios.

5.2 Formato del EntityID

El atributo entityID a registrar DEBE corresponder a una URI que utilice uno de los siguientes esquemas; HTTP, HTTPS o URN.

El esquema de URI HTTPS es RECOMENDADO para todos los Miembros de la Federación.

Los esquemas de URIs HTTP y HTTPS utilizados para el entityID DEBEN contener una componente de nombre de dominio, cuyo valor corresponde a un dominio tipo DNS.

5.3 Formato de Nombre de Dominio de Usuario

Para entidades Proveedoras de Identidad, el nombre de dominio de usuario DEBE pertenecer al espacio de nombre de dominio DNS y expresado en letras minúsculas. Se permiten múltiples nombres de dominio de usuario.

5.4 Validación de la Entidad

Durante el registro de la Entidad, el Operador de la Federación DEBERÁ llevar a cabo validaciones de la misma. Estas validaciones incluyen:

- Asegurar que toda la información requerida se encuentre en el metadato;
- Asegurar que el metadato tiene el formato correcto;
- Asegurar que las URI HTTPS definidas por el protocolo (o protocol endpoints en inglés) se encuentran debidamente protegidas con certificados TLS / SSL.

6. Gestión de la Entidad

Una vez que la organización sea un Miembro de la Federación, este PUEDE agregar, modificar o eliminar la cantidad de entidades que desee.

6.1 Solicitud de Modificación de Entidad

Cualquier solicitud de agregar, cambiar o quitar una entidad desde un Miembro de la Federación necesita de la previa información y confirmación por parte de los respectivos Representantes Registrados.

La información de cambios se realizará a través de email a cofre@reuna.cl.

6.2 Modificación de Entidad No Solicitado

El Operador de la Federación puede enmendar o modificar los Metadatos de la Federación en cualquier momento, de manera de:

- Garantizar la seguridad e integridad de los metadatos;
- Cumplir con acuerdos de Interfederación;
- Mejorar la interoperabilidad;
- Agregar valor a los metadatos.

Estos cambios serán comunicados a los Representantes Registrados de la entidad.

7. Referencias

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[SAML-Metadata-RPI-V1.0]	SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0. 03 April 2012. OASIS Committee Specification 01. http://docs.oasisopen.org/security/saml/Post2.0/saml-metadatarpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html.
[SAML-Metadata-OS]	OASIS Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasisopen.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.