YAMI

Práctica de registro de metadatos

Enero 2025

1 Tabla de Contenidos

1. Práctica de registro de metadatos 3
1.1 Alcances 3
1.2 Elegibilidad y propiedad de los miembros 3
1.3 Formato de metadatos 3
1.4 Elegibilidad y validación de la entidad 3
1.4.1 Registro de la entidad 3
1.4.2 Formato EntityID 4
1.4.3 Formato de alcance 4
1.4.4 Validación de entidades 4
1.5 Gestión de entidades 4
1.5.1 Solicitudes de cambio de entidad 5
1.5.2 Cambios de entidad no solicitados 5
2. Referencias 5

1. Práctica de registro de metadatos

1.1 Alcances

Las presentes Prácticas de Registro de Metadatos del Operador de la Comunidad afectará a todo los registro de nuevas entidades u organizaciones que sea realizada en o después de la fecha de firma del presente documento. Este documento y sus reformas serán publicadas en el sitio web de la Comunidad en:

https://www.redconare.ac.cr/yami/.

Las actualizaciones de la documentación deberán ser reflejadas con precisión en los metadatos ingresados por cada entidad. Las inclusiones que no incluyan referencia a una política de registro serán asumidas como simple registro histórico indocumentado. Las solicitudes para reevaluar una entidad determinada con respecto a un MRPS actual deberán dirigirse al servicio de asistencia de la Comunidad.

1.2 Elegibilidad y propiedad de los miembros

Los miembros de la Comunidad serán elegibles para hacer uso del registro de Operadores de la Comunidad para registrar entidades. No se aceptarán solicitudes de registro de otras fuentes. La identidad será verificada a través de una conversación en vivo y en tiempo real.

El proceso establecerá un nombre para el miembro de la Comunidad que podrá cambiar durante el período de membresía, como resultado de cambios de nombre corporativo o fusiones, por ejemplo. El nombre del miembro se revela en el elemento [SAML-Metadata-OS] <md:OrganizationName> de la entidad.

1.3 Formato de metadatos

Cuadro de texto: <mdrpi:RegistrationInfo registrationAuthority="urn:mace:mds.redclara.net"

registrationInstant="2021-07-01T11:28:03Z"> <mdrpi:RegistrationPolicy xml:lang="en">

https://www.redclara.net/index.php/en/servicios-rc/federaciones-de-identidad
</mdrpi:RegistrationPolicy>
<mdrpi:RegistrationPolicy xml:lang="es">

https://www.redclara.net/index.php/es/servicios-rc/federaciones-de-identidad
</mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>

Los metadatos para todas las entidades registradas por el operador de Comunidad deberán hacer uso de la extensión de metadatos [SAML-Metadata-RPI-V1.0] para indicar que el operador de Comunidad es el registrador de la entidad y para detallar la versión de la declaración MRPS que se aplica a la entidad.

1.4 Elegibilidad y validación de la entidad

1.4.1 Registro de la entidad

El proceso mediante el cual un miembro de la Comunidad puede registrar una entidad será publicado en forma permanente en la dirección:

https://www.redconare.ac.cr/miembros/

El Operador de la Comunidad verificará el derecho del miembro a usar nombres de dominio particulares en relación con los atributos entityID. El derecho a utilizar un nombre de dominio SE establecerá de una de las siguientes maneras:

- El nombre del miembro deberá coincidir con la información del registrante que se muestra en la herramienta WHOIS para consultar el registro DNS.
- A un miembro se le puede otorgar el derecho de hacer uso de un nombre de dominio específico a través de una carta de permiso del propietario del dominio por entidad. No se considerará que el permiso incluya permiso para el uso de subdominios.

1.4.2 Formato EntityID

Los valores del atributo entityID registrado deben ser un URL absoluto utilizando los esquemas http, https o urn. Los URI de esquema https se recomiendan a todos los miembros. Los URL http-scheme y https-scheme utilizados para los valores entityID deben contener una parte host cuyo valor sea un dominio DNS.

1.4.3 Formato de alcance

Para las entidades que tengan la función de Proveedor de Identidades, los ámbitos deben estar enraizados en el espacio de nombres de dominio DNS, expresado en minúsculas. Se permiten múltiples ámbitos.

Se puede usar expresiones regulares que representen múltiples ámbitos, pero todos los dominios DNS cubiertos por la expresión se incluirán las comprobaciones por parte del Operador de la Comunidad para el derecho del miembro a usar esos dominios. Para que estas comprobaciones sean alcanzables por el operador de Comunidad, el conjunto de dominios DNS cubiertos por la expresión regular debe terminar con un dominio bajo un sufijo público, es decir, un literal '.', seguido de al menos dos etiquetas DNS separadas por literal '.' s (que representa un dominio que se validará como "propiedad" del propietario de la entidad) y que termina con un ancla '$' (por ejemplo, (foo|bar)\.example\.com$).

1.4.4 Validación de entidades

Para el registro de la entidad, el Operador de la Comunidad llevará a cabo verificaciones de validaciones de entidades. Estas comprobaciones incluyen:

- Asegurarse de que los metadatos tienen el formato correcto;
- Garantizar que los puntos finales del protocolo estén correctamente protegidos con certificados TLS / SSL;
- Asegurarse de que toda la información requerida esté presente en los metadatos.

1.5 Gestión de entidades

Una vez que un miembro se ha unido a la Comunidad, cualquier número de entidades puede ser agregado, modificado o eliminado por la organización.

1.5.1 Solicitudes de cambio de entidad

Cualquier solicitud de adición, cambio o remoción de entidades de los miembros de la Comunidad debe ser comunicada o confirmada por sus respectivos Representantes Registrados. La comunicación del cambio deberá ser realizada mediante el correo electrónico: yami@conare.ac.cr.

1.5.2 Cambios de entidad no solicitados

El Operador de la Comunidad puede enmendar o modificar los metadatos de la Comunidad en cualquier momento para:

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

Los cambios se comunicarán a los Representantes Registrados de la entidad.

2. 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.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/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.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.