confía

Informe técnico

Preparado para: Comité CONFIA

Versión: 1.1

05 ene 2010

Número de referencia: P-174-INF-09-11115

Rioja 5 - 1ª planta
41001 Sevilla Spain
admon@yaco.es
www.yaco.es
T 954 500 057
F 954 500 929

Control de Versiones del Documento			
Versión	**Fecha**	**Descripción del Cambio**	**Autor**
1	27/10/09	Versión inicial	Ernesto Revilla
1.1	05/01/10	Añadido obligatoriedad de firmar todos los mensajes SAML2 y cifrar aserciones.	Ernesto Revilla

ÍNDICE DE CONTENIDO

1.- PROTOCOLO

La federación CONFIA utiliza el protocolo SAML 2.0, tanto para el intercambio de datos como para la definición de los metadatos, de acuerdo con las especificaciones de OASIS y de las reglas específicas descritas en este documento.

Los siguientes apartados detallan el uso de estos protocolos en los diferentes escenarios contemplados por la federación, así como en lo necesario para establecer los lazos de confianza entre sus componentes.

El uso de los términos “DEBEN”, “PUEDEN”, “se RECOMIENDA”, usados en este documento se corresponden con los significados de sus equivalentes en inglés MUST, MAY, SHOULD, según el BCP14/RFC2119 de IETF.

1.1.- Perfil básico para acceso Web

Este perfil es de aplicación cuando los usuarios intenten acceder cualquier recurso que ofrezca una interfaz Web estándar (por medio de HTTP y HTTPS) empleando un navegador Web. Las interacciones de acuerdo a este perfil se ajustan a los procedimientos descritos para los perfiles Single Sign-On de SAML 2.0 en [SAML2Prof] y los bindings definidos por [SAML2Bind], de acuerdo con las siguientes reglas:

- Los SPs DEBEN soportar y usar el binding HTTP Redirect. Excepcionalmente, los SPs PUEDEN emplear el binding HTTP POST cuando el tamaño de la AuthenticationRequest exceda los límites prácticos de la codificación en URLs y si se ha recibido el visto bueno del comité técnico de CONFIA.
- Los IdPs DEBEN emplear en sus respuestas el binding HTTP POST.
- Todos los mensajes emitidos por SPs, IdPs y el WAYF DEBEN estar digitalmente firmados mediante el algoritmo RSA-SHA1 o al menos DSA-SHA1, según lo indicado en [XML-DSIG].
- Los IdPs y SPs DEBEN validar la firma digital de todos los mensajes recibidos.
- Los IdPs DEBEN cifrar las aserciones SAML2 emitidas para evitar la captura de datos privados.

1.2.- Otros perfiles

De momento no se consideran otros perfiles.

1.3.- Formato de metadatos

El modelo de información de metadatos de la federación está definido según las especificaciones de metadatos de SAML 2.0 [SAML2Meta], y es utilizado para describir los elementos que interactúan dentro de la federación de una manera formalizada. Esta información se usa principalmente con dos propósitos:

- Identificar los elementos válidos en la federación, así como los interfaces de los mismos, en coordinación con el esquema de confianza de la federación.
- Localizar los componentes capaces de satisfacer una determinada petición de datos de identidad.

Los metadatos de la federación se pueden acceder de manera conjunta como un solo documento XML conteniendo como elemento raíz EntitiesDescriptor, donde cada una de las instituciones participantes está representado por un elemento EntityDescriptor. En función de los diferentes mecanismos de acceso a los metadatos, también es posible acceder a elementos EntityDescriptor individuales o a elementos EntitiesDescriptor que incluyan un conjunto de entidades de un mismo tipo (IdP, SP) representadas cada una por un elemento EntityDescriptor.

Adicionalmente, los productores de metadatos DEBEN cumplir lo indicado en [SAML2MetadataIOP] al generar los metadatos.

Para CONFIA se impone la siguiente restricción adicional:

- Los elementos EntityDescriptor DEBEN tener un atributo entityID que contiene una URL accesible y cuyo resultado es el conjunto de metadatos que definen la entidad.
- Los elementos EntitiesDescriptor emitido por el agregador de la federación DEBEN indicar en el atributo Name la URL desde donde obtener metadatos.

Dentro de un elemento EntityDescriptor, al menos uno de los siguientes elementos RoleDescriptor ha de estar presente:

- IDPSSODescriptor, para la interfaz del IdP, capaz de responder peticiones de autenticación que incluyan información relativa a atributos.
- SPSSODescriptor, para la interfaz del SP.

Opcionalmente, también puede aparecer un RoleDescriptor del tipo AttributeAuthorityDescriptor, para la interfaz del IdP capaz de responder peticiones adicionales de atributos.

Para cada entidad descrita en los metadatos también han de incluirse datos de gestión:

- Definición de la institución, incluyendo su dominio y el método de autenticación que utilizan sus usuarios.
- Persona(s) de contacto, responsable(s) de mantener la información de la institución en el modelo de información de metadatos.

1.4.- Perfiles de atributos

Los SPs DEBEN soportar los siguientes protocolos de provisión de atributos [SAML2Prof]:

- Basic
- X.500/LDAP

Se RECOMIENDA que todas las entidades trabajen con el perfil Basic. Las entidades PUEDEN implementar [SAML2AttrExt] para poder determinar el origen de un atributo.

1.5.- Transmisión y procesamiento de metadatos

Las entidades de la federación han de cumplir lo indicado en la Política de confianza y en [SAML2MetadataIOP].

2.- OTRAS OBLIGACIONES TÉCNICAS

2.1.- IdP: Disponibilidad de cuenta de usuario para vigilancia del estado del servicio

En caso de integrarse como Proveedor de Identidad, CONFIA requiere la existencia de una cuenta de usuario para monitorizar el estado de de la conexión.

2.2.- Descarga periódica de metadatos

Se RECOMIENDA que todos los miembros descarguen los metadatos al menos una vez al día con el objetivo de evitar que problema de seguridad en la plataforma central de CONFIA se propaguen a las diferentes entidades de la federación. Los IdPs y SPs DEBEN descargar estos metadatos al menos una vez a la semana.

Antes la primera sincronización se proporcionará el certificado usado para la firma de los metadatos por canales de comunicación alternativos.

3.- REFERENCIAS

- RFC2119 BCP 14/RFC2119 S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", March 1997.
- EDUGAIN eduGAIN Profiles and Implementation Guidelines 1.0
- EDUPERSON EduPerson? Object Class Specification 200806
- REC IRISEDUPERSON
- RFC1630 RFC 1630 - Universal Resource Identifiers in WWW: A Unifying Syntax for the Expression of Names and Addresses of Objects on the Network as used in the World-Wide Web
- RFC1867 RFC 1867 - Form-based File Upload in HTML
- RFC2527 RFC 2527 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC2798 RFC 2798 - Definition of the inetOrgPerson LDAP Object Class
- RFC3280 RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC3377 RFC 3377 - Lightweight Directory Access Protocol (v3): Technical Specification
- RFC3548 RFC 3548 - The Base16, Base32, and Base64 Data Encodings
- SAML2AttrExt SAML V2.0 Attribute Extensions Version 1.0
- SAML2Bind Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0
- SAML2Core Assertions and Protocols for the OASIS Security Assertion Markup

Language (SAML) V2.0

- SAML2Prof Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0
- SAML2Meta Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0
- SAML2MetadataIOP SAML V2.0 Metadata Interoperability Profile Version 1.0
- SCHAC SCHAC Attribute Definitions For Individual Data 1.4
- SCHIRIS IRIS LDAP Schema. Generic objects for the IRIS community
- [PKCS1] RFC 2437 - PKCS #1: RSA Cryptography Specifications
- [SHA1] RFC 3174 - US Secure Hash Algorithm 1 (SHA1)
- [X500] The Directory: Overview of concepts, models and services
- [X501] The Directory: Models
- [X509] The Directory: Authentication framework
- [XML-DSIG] XML Signature Syntax and Processing (Second Edition)