confía

Política de confianza

Preparado para: Comité CONFIA

Versión: 3

01 dic 2009

Número de referencia: P-174-INF-09-09-64

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	15/09/09	Versión inicial	Ernesto Revilla
2	24/09/09	Inclusión del apartado 6. acerca de la gestión, publicación y uso de los metadatos.	Ernesto Revilla
3	01/12/09	Quitar detalles de los certificados en 4.	Ernesto Revilla

ÍNDICE DE CONTENIDO

1.- OBJETO DEL DOCUMENTO

El presente documento describe la política de confianza con respecto a procedimientos, protocolos y certificados a aplicar por parte de los miembros de la federación de identidades (CONFIA) de la Asociación de Universidades Públicas de Andalucía (AUPA), así como otras entidades que desean actuar como proveedores de servicios para esta federación.

2.- ABREVIATURAS Y ACRÓNIMOS

- CA: Autoridad de Certificación
- CRL: Certificate Revocation List (Lista de certificados revocados)
- DN: Distinguished Name (Nombre unívoco reconocido mundialmente)
- IdP: Identity Provider (Proveedor de Identidad)
- PKCS: Public Key Cryptography Standard
- PKI: Public Key Infrastructure (Infraestructura de clave/criptografía pública)
- PKIX: Public Key Infrastructure extendida para uso en Internet
- SP: Service Provider (Proveedor de Servicio)
- SSL: Secure Socket Layer
- TLS: Transport Layer Security (Seguridad a nivel de capa de transporte)
- URL: Uniform Resource Locator (Localizador de recurso uniforme)

3.- PRINCIPIOS

La federación requiere un modelo de confianza que permita a sus componentes garantizar la privacidad, integridad y autenticidad de los mensajes intercambiados. Se aplican los siguientes mecanismos:

- Conexiones seguras
- Firma digital de documentos y su validación
- Cifrado de mensajes, cuando sea necesario

Toda la confianza residirá en una Infraestructura de Clave Pública (PKI), basada en certificados X.509, que está formada por una serie de Autoridades de Certificación (CA) validadas para el esquema de confianza. De esta forma, se establecerá un procedimiento mediante el cual una CA podrá ser admitida dentro del esquema de confianza. La federación distribuirá por métodos fuera de línea (correo electrónico digitalmente firmado, repositorio fiable basado en la tecnología TACAR, etc.) las raíces de confianza correspondientes a las CAs reconocidas.

4.- CERTIFICADOS Y AUTORIDADES DE CERTIFICACIÓN (CAS)

4.1.- Perfiles de los certificados

Todos los certificados emitidos por cualquier CA válida en el esquema de confianza de la federación se ajustarán al perfil PKI para Internet (PKIX) de certificados X.509v3 [RFC3280]. En función de las posibilidades, se emplearán certificados emitidos por autoridades de certificación reconocidos nativamente por los navegadores más populares. Los certificados serán de servidor SSL y tendrán al menos los usos *digitalSignature* y *nonRepudiation*. Las CAs DEBEN publicar CRLs en formato X.509v2.

Cada entidad tendrá un único Distinguished Name (DN) en todos los certificados emitidos para ella por su correspondiente CA. El DN estará estructurado tal como se define en [X501].

4.2.- Política de certificación y declaración de prácticas de certificación

Todas las CAs aceptadas en la federación andaluza deberán disponer de una Política de Certificación (CP) y una Declaración de Prácticas de Certificación (CPS), acordes a [RFC2527] y aceptadas formalmente por el órgano rector de la federación.

5.- PROTOCOLO DE CONEXIÓN PARA INTERCAMBIO DE DATOS

A menos que se indique lo contrario en la especificación del perfil correspondiente, toda conexión entre dos componentes de la federación se realizarán usando SSL3 [SSL3] o TLS v1.0 [RFC2446] o posterior con validación mutua de los certificados usados en dicha conexión, tanto del que la inicia como del que responde.

6.- GESTIÓN, PUBLICACIÓN Y COMPROBACIÓN DE LOS METADATOS DE LA FEDERACIÓN

La entidad en que CONFIA delega la gestión se responsabiliza de publicar los metadatos actualizados de la federación consistentes en la unión de los metadatos de cada uno de los IdPs y SPs. Para ello se habilitará y autorizará una o varias URLs de la que todas la entidades descargarán estos datos periódicamente empleando una conexión segura según el apartado anterior.

Los IdPs y SPs han de emplear sólo las URLs de descarga autorizadas por la federación.

Los metadatos están digitalmente firmados y el receptor sólo aceptará los nuevos datos recibidos si la firma es válida y ha sido realizada mediante un certificado con huella reconocida o firmado por una CA admitida a tal propósito.

Diariamente se comprobarán los certificados de todas las entidades participantes y se eliminarán aquellas cuya validación del certificado resulte negativa. De esta manera, las entidades recibirán los metadatos sólo de aquellas otras que dispongan de certificado válido. En caso de detección de fecha de expiración cercanas, certificados caducados o revocados, se enviarán notificaciones a los administradores de las entidades afectadas.

La validación de los certificados se realizará en base a:

- Fecha de validez del certificado
- Firma del certificado por una entidad de autorización reconocida en la federación
- No revocación del certificado

7.- FIRMA Y VALIDACIÓN DE DOCUMENTOS XML

La entidades participantes en la federación, es decir IdPs y SPs, crearán y verificarán firmas XML para las siguientes construcciones SAML2:

- Aserciones que contengan una declaración de autenticación SAML (`AuthenticationStatement`) y, opcionalmente, diferentes declaraciones de atributo (`AttributeStatement`) en respuesta a cualquier tipo de petición de autenticación, ya sea directa por XML, por medio de redirección Web o por cualquier otro procedimiento.

Se recomienda crear y verificar firmas XML para las siguientes construcciones SAML:

- Aserciones que contengan una declaración de atributo SAML (`AttributeStatement`) en respuesta a una petición de atributos (`AttributeRequest`).

Los documentos XML intercambiados entre miembros de la federación sólo serán aceptados si han sido firmados mediante certificados incluidos en los metadatos. (Ver apartado anterior.)

8.- REFERENCIAS

- [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
- [SSL3] The SSL Protocol Version 3.0: http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt
- [RFC2246] RFC 2246 - The TLS Protocol 1.0
- [X501] The Directory: Models
- [X509] The Directory: Authentication framework