



Junta de Andalucía

MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE

Guía para la Integración de Aplicaciones en Proxy-Clave

Versión: 0100

Fecha: 22/12/2020

[Proxy-Cl@ve X.Y.Z]

Queda prohibido cualquier tipo de explotación y, en particular, la reproducción, distribución, comunicación pública y/o transformación, total o parcial, por cualquier medio, de este documento sin el previo consentimiento expreso y por escrito de la Junta de Andalucía.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

HOJA DE CONTROL

Organismo	CONSEJERÍA DE HACIENDA INDUSTRIA Y ENERGIA - Dirección General de Transformación Digital		
Proyecto	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE		
Entregable	Guía para la Integración de Aplicaciones en Proxy-Clave		
Autor	Daniel García		
Versión/Edición	0100	Fecha Versión	22/12/2020
Aprobado por		Fecha Aprobación	DD/MM/AAAA
		Nº Total de Páginas	51

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
0100	Versión inicial	Daniel García	22/12/2020

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Daniel García



**MANTENIMIENTO Y SOPORTE DEL
COMPONENTE PROXY-CLAVE**
**Guía para la Integración de Aplicaciones
en Proxy-Clave**

**Servicio de Coordinación
y Desarrollo de Sistemas
Horizontales (SCDSH),
bajo la Dirección General
de Transformación
Digital (DGTD)**

ÍNDICE

1	Objetivo.....	5
1.1	Audiencia.....	5
1.2	Glosario y definiciones.....	5
1.3	Convenciones utilizadas en este documento.....	6
2	Introducción.....	7
2.1	¿Qué es Cl@ve?.....	7
2.2	Qué es Proxy-Clave.....	10
2.3	Conexión con Proxy-Clave.....	11
2.4	Qué Información proporciona Proxy-Clave.....	12
2.5	Qué puede mi sistema de información solicitar a Proxy-Clave.....	13
2.6	Cómo reconoce Proxy-Clave a su sistema de información.....	14
3	Caso de ejemplo utilizado en este documento.....	15
4	Introducción a SAML v2.....	16
4.1	Uso de SAML v2 en Proxy-Clave.....	16
4.2	Entidades roles y relaciones.....	16
4.3	Perfiles, bindings, protocolos y aserciones.....	18
5	Propósito y uso de metadatos SAML v2 en Proxy-Clave.....	29
5.1	¿Qué son los metadatos SAML v2?.....	29
5.2	¿Para qué se utilizan los metadatos SAML v2?.....	32
5.3	¿Qué contienen los metadatos SAML v2?.....	32
5.4	Que deben reflejar los metadatos SAML V2 para Proxy-Clave.....	34
5.5	Errores comunes en los metadatos.....	37
6	Modalidades de atributos de Proxy-Clave.....	38
6.1	Modo nativo Cl@ve 2 con protocolo Clave 2.0.....	38
6.2	Modo compatible Cl@ve 1 y Cl@ve 2.....	39
6.3	Modo nativo Cl@ve 2 con protocolo SAML.....	40
7	Kit de integración de aplicaciones J2EE.....	43
7.1	Aplicación de pruebas distribuida junto al kit.....	43

	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

7.2 Requisitos para la integración con Proxy-Clave.....	43
7.3 Procedimiento de configuración e integración.....	43
7.4 Verificación de la configuración.....	50
7.5 Invocar el proceso de autenticación y procesar la respuesta desde su aplicación.....	50

	<p style="text-align: center;">MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE</p> <p style="text-align: center;">Guía para la Integración de Aplicaciones en Proxy-Clave</p>	<p style="text-align: center;">Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)</p>
---	--	--

1 Objetivo

El objetivo del presente documento es servir de guía para el desarrollo de integraciones de aplicaciones J2EE que quieran hacer uso de las funcionalidades disponibles en el sistema Proxy-Clave.

1.1 Audiencia

El documento está dirigido a los desarrolladores de aplicaciones J2EE que requieran integrar en sus aplicaciones la autenticación vía Proxy-Clave.

1.2 Glosario y definiciones

- **SSO (Single Sign On).** Es un mecanismo de autenticación mediante el cual el usuario se autentica una vez propagando la identidad a las aplicaciones.
- **SAML.** Es un estándar basado en XML para el intercambio de mensajes de autenticación y autorización entre dominios de seguridad.
- **Federación de identidades.** La identidad federada es una de las soluciones para abordar la gestión de identidad en los sistemas de información. Su objetivo es obtener una gestión de usuarios eficiente, la sincronización de los datos identificativos, gestión de acceso, servicios de agrupación, servicios de directorio, auditoría e informes.
- **SP (Service Provider).** Es el elemento que consume la información de autenticación y autorización en la relación federada. Se puede equiparar a la aplicación de negocio a integrar.
- **IDP (Identity Provider).** Es el elemento que contiene la información de origen de la identidad en una relación federada.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	--

1.3 Convenciones utilizadas en este documento

Las siguientes convenciones tipográficas son utilizadas en este documento:

Cursiva

Indica nuevos términos, direcciones de correo, nombre de ficheros y extensiones de ficheros.

Ancho fijo con fondo gris

Se usa para listados de código, ficheros de configuración y para listados de directorios.

Ancho fijo

Se usa para indicar dentro de un párrafo elementos de programación como variables, nombres de funciones, bases de datos, tipo de datos, variables de entorno, declaraciones y palabras reservadas.

Ancho fijo negrita

Indica comandos que o otro texto que debe ser escrito literalmente por el usuario.

Ancho fijo cursiva

Indica texto que debe ser reemplazado por valores proporcionados por el usuario o valores determinados por el entorno

	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

2 Introducción

2.1 ¿Qué es Cl@ve?

Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Su objetivo principal es que el ciudadano pueda identificarse ante la Administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios.

Cl@ve complementa los actuales sistemas de acceso mediante DNI-e y certificado electrónico, y ofrece la posibilidad de realizar firma en la nube con certificados personales custodiados en servidores remotos.

Se trata de una plataforma común para la identificación, autenticación y firma electrónica, un sistema interoperable y horizontal que evita a las Administraciones Públicas tener que implementar y gestionar sus propios sistemas de identificación y firma, y a los ciudadanos tener que utilizar métodos de identificación diferentes para relacionarse electrónicamente con la Administración.

Cl@ve permite que las aplicaciones de administración electrónica puedan definir el nivel de aseguramiento en la calidad de la autenticación que desean, en base a los datos que tratan y a la clasificación de seguridad siguiendo las recomendaciones del Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica). El ciudadano usuario de los servicios de administración electrónica puede entonces escoger el identificador que desea usar entre los disponibles para el nivel de aseguramiento requerido por la aplicación.

El sistema Cl@ve fue aprobado por Acuerdo del Consejo de Ministros, en su reunión del 19 de septiembre de 2014, y sus condiciones de utilización son determinadas por la Dirección de Tecnologías de la Información y las Comunicaciones.

Más información disponible sobre Cl@ve en <http://clave.gob.es>

2.1.1 Niveles de calidad proporcionados por Cl@ve

Un elemento esencial en el marco de interoperabilidad del reglamento eIDAS es el nivel de seguridad de la autenticación. El nivel de seguridad caracteriza el grado de confianza de un medio de identificación electrónica para establecer la identidad de una persona, garantizando así que la persona que afirma poseer una identidad determinada la tiene.

	<p align="center">MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE</p> <p align="center">Guía para la Integración de Aplicaciones en Proxy-Clave</p>	<p align="center">Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)</p>
---	--	---

El nivel de seguridad depende del grado de confianza que aporte este medio de identificación electrónica sobre la identidad pretendida o declarada por una persona, teniendo en cuenta los procedimientos técnicos, (por ejemplo, prueba y verificación de la identidad, autenticación), los procedimientos de gestión (métodos utilizados por entidad para expedir la identidad electrónica) y los controles aplicados a todo el proceso.

El reglamento eIDAS establece los tres niveles de seguridad siguientes:

- El nivel de seguridad **bajo** se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un **grado limitado de confianza** en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es **reducir el riesgo de uso indebido o alteración de la identidad**;
- El nivel de seguridad **sustancial** se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un **grado sustancial de confianza** en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es **reducir sustancialmente el riesgo de uso indebido o alteración de la identidad**;
- El nivel de seguridad **alto** se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un **grado alto de confianza** en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial, y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, cuyo objetivo es **evitar el uso indebido o alteración de la identidad**.

	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

La siguiente tabla presenta un resumen de los niveles de seguridad.

Nivel en Cl@ve	Nivel de Registro	Modo de registro	Credencial	Nivel ENS
Bajo	Básico	Telemático a partir de datos conocidos, basado en CSV	Clave PIN Clave Permanente sin OTP	BAJO
	Fuerte	Presencial, telemático con certificado electrónico reconocido o sistemas equivalentes.	Clave Permanente sin OTP	
Sustancial	Fuerte	Presencial, telemático con certificado electrónico reconocido o sistemas equivalentes.	Clave PIN Clave Permanente reforzada con OTP (SMS al móvil) Certificado reconocido en soporte SW	MEDIO
Alto	Fuerte	Presencial, telemático con certificado electrónico reconocido o sistemas equivalentes.	DNI electrónico Otros certificados reconocidos en soporte HW, con la certificación de una entidad de certificación acreditada.	ALTO

Además, el reglamento eIDAS establece los siguientes datos a proporcionar para las **personas físicas**:

- Un conjunto de **3 datos obligatorios** que deben proporcionarse en todos los casos. Estos datos son:
 - **Identificador de unicidad**: Se trata de un identificador vinculado de manera única a una persona determinada, que permite asociar a la misma persona autenticaciones sucesivas. Se debe hacer notar que este identificador garantiza que no habrá dos personas con el mismo identificador, como es el caso del NIF español.
 - **Nombre** (en general uno o varios nombres)
 - **Apellido** (en general los apellidos del ciudadano)
- Un conjunto de **5 datos opcionales** que el emisor de la autenticación puede decidir proporcionar o no, en función de las características del esquema de identificación utilizado. El propósito de estos datos opcionales es facilitar la asociación de los datos de identificación del ciudadano en autenticaciones sucesivas. Estos datos opcionales son:

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	--

- Fecha de nacimiento
- Nombre al nacer
- Apellido al nacer
- Lugar de nacimiento
- Dirección actual
- Género

2.2 Qué es Proxy-Clave

De cara a gestionar la integración en Cl@ve de las distintas herramientas que la Administración de la Junta de Andalucía pone a disposición de la ciudadanía, la Dirección General de Política Digital ha decidido utilizar un componente centralizado que unifique a todos estos sistemas de cara a Cl@ve, actuando de manera virtual como si de un único sistema integrado se tratase. Se trataría del sistema Proxy-Clave.

Proxy-Clave debe permitir la integración multiprotocolo de múltiples sistemas de información de la Junta de Andalucía, realizando un login único entre ellos y actuando como proveedor de servicios en su relación con [Cl@ve](#). Los protocolos soportados por Proxy-Clave “de cara” a los sistemas de información de la Junta de Andalucía son SAML v2 y Cl@ve v2.

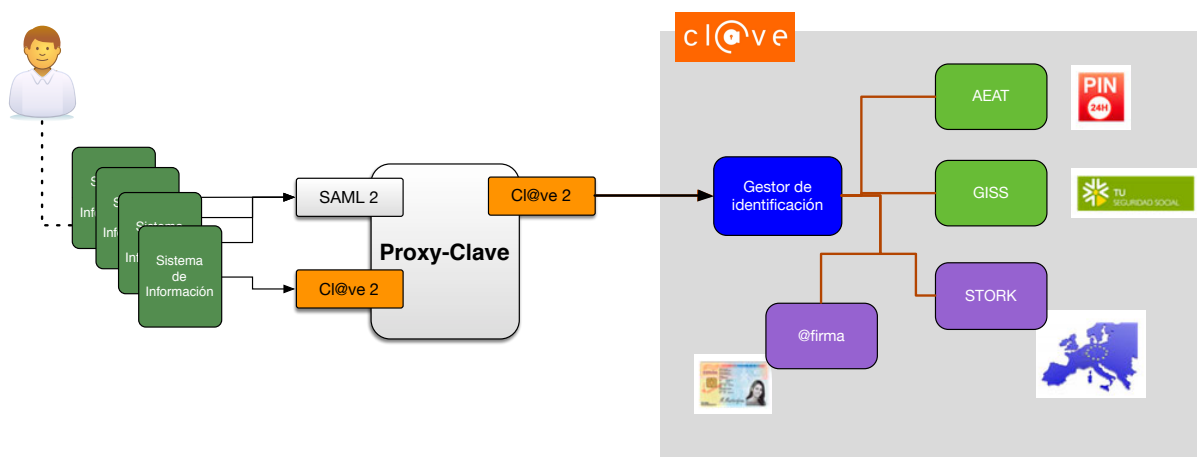
Proxy-Clave, por tanto, es un servicio que actúa como representante de los sistemas de información de la Junta de Andalucía ante Cl@ve v2. De forma que los citados sistemas de información, es a Proxy-Clave a quien solicitan la identificación de los ciudadanos, y es de Proxy-Clave de quien obtienen respuesta.

Proxy-Clave, para proporcionar respuesta a cerca de la identidad de los ciudadanos (como consecuencia de las peticiones de los sistemas de información) realizará la petición de autenticación a Cl@ve, obteniendo una respuesta con el resultado de la autenticación. Respuesta la cual es tratada y enviada al sistema de información que originalmente solicitó a Proxy-Clave la identificación.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

2.2.1 Diagrama lógico del sistema Proxy-Clave

El sistema Proxy-Clave es por tanto un intermediario o representante de los sistemas de información de la Junta de Andalucía ante [Cl@ve](#). Tal como puede observarse en el siguiente diagrama.



2.3 Conexión con Proxy-Clave

Los sistemas de información de la Junta de Andalucía deben como “protocolos” de SSO SAML v2 ó el propio protocolo Cl@ve v2.

La norma es realizar la conexión de los sistemas de información mediante el protocolo SAML v2.

Sólo se permitirá la conexión por medio del protocolo Cl@ve v2, cuando el sistema de información a conectar sea un desarrollo del que no se disponen los fuentes y ya implemente el protocolo Cl@ve v2.

Para la conexión mediante SAML v2, no se proporciona una librería específica, ya que existen numerosas implementaciones de SAML 2 en componentes y librerías para cualquier tecnología. Siendo el propósito de esta guía la descripción del proceso de integración en Proxy-Clave siguiendo el estándar SAML v2, en vez de una implementación concreta del mismo.

Debe considerar, por tanto, el protocolo SAML v2 como un mecanismo que permite interoperar a su sistema de información con Proxy-Clave, en todos aquellos aspectos relativos a la identificación de los ciudadanos que desean tener acceso al mismo.

EL objetivo de este mecanismo de interoperabilidad es proporcionar a su sistema de información los suficientes detalles sobre la identidad del cada ciudadano que trata de acceder a su sistema.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

2.4 Qué Información proporciona Proxy-Clave

Proxy-Clave proporciona datos a cerca de la identidad de los ciudadanos, así como información sobre el proceso de identificación que ha seguido el ciudadano para identificarse, esto es, que método de autenticación de los disponibles en Cl@ve ha utilizado, como Certificado Digital, Pin 24, Clave Permanente o si se ha identificado en su país de origen, para ciudadanos europeos.

Aunque el conjunto de datos sobre la identidad de los ciudadanos se detalla en el punto [6. Modalidades de atributos de Proxy-Clave](#), a continuación se muestra un listado con los mismos.

- <http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName>. Contiene el nombre del usuario. Se puede recibir tanto un nombre simple como uno compuesto. Es un atributo personal obligatorio que se recibirá siempre.
- <http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName>. Contiene los apellidos del usuario. Es un atributo personal obligatorio que se recibirá siempre.
- <http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier>. Contiene el identificador único (NIF) del Usuario. Es un atributo personal obligatorio que se recibirá siempre.
- <http://es.minhafp.clave/SelectedIdP>. Identifica el proveedor de identidades utilizado para la identificación. Este atributo puede poseer alguno de los siguientes valores:
 - AFIRMA. IdP “Certificado electrónico”.
 - EIDAS. IdP “Credencial europea”.
 - SEGSOC. IdP “Clave permanente”.
 - PIN24H. IdP “PIN24H”.

No obstante, y con carácter opcional, podrán ser retornados además los siguientes atributos

- <http://es.minhafp.clave/PartialAfirma>. Contiene la respuesta parcial de @firma en Base64, en la que se incluyen el mapeo de campos extraídos del certificado presentado para la identificación.
- Otros datos proporcionados sobre la persona identificada por el proveedor de identidades, para los que esta otorgo su consentimiento consulta y/o comunicación.

La lista de atributos aquí expuesta no es exhaustiva, dado que Proxy-Clave permite la entrega de los atributos de la identidad del ciudadano en diferentes modalidades, las cuales se detallan en el punto [6. Modalidades de atributos de Proxy-Clave](#)

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

2.5 Qué puede mi sistema de información solicitar a Proxy-Clave

Los sistemas de información integrados con Proxy-Clave pueden solicitar la identificación de los ciudadanos, por medio de peticiones de autenticación SAML. Obteniendo como respuesta el resultado de la autenticación que el ciudadano realice en Cl@ve y un conjunto de atributos que determinan la identidad del mismo.

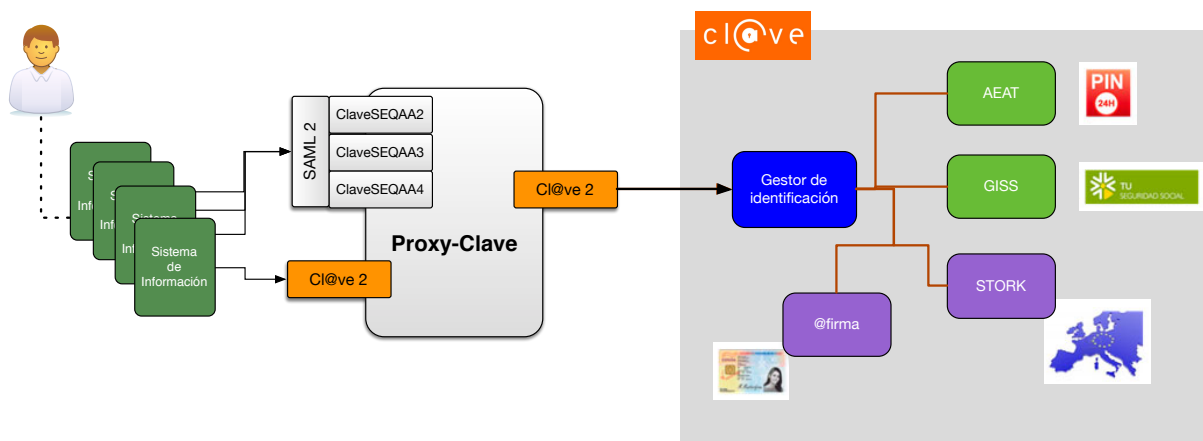
Dentro del contexto de la solicitud de de la identidad de un ciudadano, los sistemas de información pueden solicitar un determinado nivel de calidad de la credencial (LoA), esto es pueden solicitar el nivel de seguridad de la autenticación (véase punto [2.1.1. Niveles de calidad proporcionados por Cl@ve](#)).

La forma en la que se pueden solicitar estos niveles es remitiendo la petición de autenticación SAML v2 al proveedor de identidad SAML v2 de Proxy-Clave que represente el nivel solicitado.

En Proxy-Clave estos proveedores de identidad SAML v2 se identifican como

- ClaveSEQAA2. Implementa el nivel de seguridad Cl@ve **bajo**
- ClaveSEQAA3. Implementa el nivel de seguridad Cl@ve **sustancial**
- ClaveSEQAA4. Implementa el nivel de seguridad Cl@ve **alto**

De esta forma de modelar los niveles de seguridad Cl@ve en Proxy-Clave se puede observar por tanto que Proxy-Clave actúa como una federación de identidad SAML v2, donde los sistemas de información son las aplicaciones o proveedores de servicio de la citada federación y los proveedores de identidad que representan los tres niveles de seguridad de la autenticación en Cl@ve los distintos proveedores de identidad de la federación.



 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	--

2.6 Cómo reconoce Proxy-Clave a su sistema de información

Para que Proxy-Clave reconozca las peticiones de identificación de ciudadanos, emitidas por un sistema de información, primero se debe establecer una relación de confianza entre ambos, esto es, entre Proxy-Clave y el sistema de información.

Esta relación de confianza se establece mediante el intercambio de metadatos SAML v2, los cuales consisten en un documento XML donde se detalla cómo debe realizarse la comunicación entre ambos, así como los certificados, correspondientes a las claves privadas utilizadas para firmar los mensajes tanto de petición de autenticación SAML v2 (emitidos por el sistema de información) como las respuestas SAML v2 (emitidas por Proxy-Clave).

En los metadatos, también figura información sobre del organismo bajo el que se encuentra el sistema de información, así como datos de contacto de las personas responsables, del sistema de información, bien sea su responsabilidad de gestión, técnica, etc.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	--

3 Caso de ejemplo utilizado en este documento


Con el objeto de no proporcionar únicamente descripciones abstractas en este documento, se presenta el un caso de ejemplo, basado en la integración en Proxy-Clave de un sistema de información ficticio.

Este sistema de información ficticio se identificará como “la aplicación”.

El sistema de información identificado como “la aplicación”, hará uso de una biblioteca software que implementa el estándar SAML v2, la cual se identificará como “el conector”, dado que es la biblioteca la que realiza la conexión entre “la aplicación” y Proxy-Clave.

Para concretar el caso de ejemplo se proporciona la siguiente información sobre la aplicación:

- FQDN del host donde se ejecuta: www.example.com
- Datos de la persona que solicita el alta de la aplicación en Proxy-Clave
 - Nombre: Juan
 - Apellidos: Nadie
 - NIF: 99999999X
 - Teléfono: 123456789
 - Correo electrónico: juan.nadie@example.com
 - Organismo: Organismo de ejemplo
 - Puesto de trabajo/Cargo: Cargo del solicitante
- Datos del sistema de información o aplicación cliente
 - Nombre y acrónimo: “La aplicación” LA_APP
 - Descripción: Aplicación de para modelar un caso de ejemplo en la guía para la integración de aplicaciones en Proxy-Cl@ve
 - Órgano: “El organismo”
- Datos de responsable técnico
 - Nombre: Antonio
 - Apellidos: Técnico
 - NIF: 88888888Y
 - Teléfono: 987654321
 - Correo electrónico: antonio.tecnicoe@example.com
 - Puesto de trabajo/Cargo: Técnico_Responsalbe

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	--

4 Introducción a SAML v2

Si el lector ya es conocedor del estándar SAML v2 puede dirigirse directamente al punto [5. Propósito y uso de metadatos SAML v2 en Proxy-Clave](#)

Según wikipedia [...] El Lenguaje de Marcado para Confirmaciones de Seguridad, conocido como SAML, (pronunciado como "sam-el") es un estándar abierto que define un esquema XML para el intercambio de datos de autenticación y autorización[...] Por lo que se puede definir de forma más sencilla como un marco de trabajo basado en XML para intercambiar información sobre autenticaciones, derechos, información sobre atributos y otro tipo de información, que debido a su capacidad de extensión, se desee intercambiar.

Muchas veces se hace referencia a SAML como un protocolo, aunque no deja de ser un estándar, el cual está descrito en los siguientes 8 documentos.

- [Assertions and Protocols \[SAMLCore\]](#)
- [Bindings \[SAMLBind\]](#)
- [Profiles \[SAMLProf\]](#)
- [Metadata \[SAMLMeta\]](#)
- [Authentication Context](#)
- [Conformance Requirements](#)
- [Security and Privacy Considerations](#)
- [Glossary](#)

A parte de la especificación definida en los documentos anteriores también existen Un [resumen ejecutivo](#) y un [resumen técnico](#).

4.1 Uso de SAML v2 en Proxy-Clave

Se hace uso del perfil Web SSO del estándar SAML v2, por lo que los sistemas de aplicación serán proveedores de servicio dentro de un Single Sign On, y Proxy-Clave desempeña el rol de Proveedor de Identidad.

4.2 Entidades roles y relaciones

SAML v2 hace uso de una terminología un tanto confusa cuando trata de identificar a las diferentes entidades que actúan como participantes en el intercambio de información, los roles que desempeñan y la información necesaria para establecer relaciones de confianza entre ellas.

Los términos utilizados para identificar a las entidades y una sencilla aclaración

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

sobre los mismos:

- **Subject:** Entidad que puede ser autenticada o identificada
 - Normalmente es una persona, pero también puede serlo una aplicación o una parte de ésta
- **Relying Party:** Entidad que actúa en base a información de otra entidad
 - Normalmente es una aplicación que confía en la información que emite otra entidad, a cerca de un **subject**
- **Aserting Party:** Entidad que emite aserciones SAML
 - Normalmente es una aplicación que emite información sobre un **subject** y en la cual confían las aplicaciones que actúan como **relying party**

Realizando una adaptación al servicio Proxy-Clave la correspondencia de las entidades SAML y los participantes en el servicio Proxy-Clave sería la siguiente:

- **Subject:** Ciudadano que puede ser identificado por Proxy-Clave
- **Relying Party:** Aplicaciones que se conectan con Proxy-Clave para solicitar la identificación de los ciudadanos y que confían en la información que sobre ellos le proporciona Proxy.Clave
- **Aserting Party:** Proxy-Clave

Una vez descritas las entidades SAML, podemos pasar a describir los **roles** que estas entidades desempeñan dentro del perfil SSO Web Broser, que es el utilizado por Proxy-Clave.

- **Service Provider:** Este es el rol que desempeñan las aplicaciones de Proxy-Clave, y se define por el uso de las aserciones para realizar el control de acceso a los servicios que estas aplicaciones proporcionan a los ciudadanos.
- **Identity Provider:** Es es el rol que desempeñá Proxy-Clave, y se define por la emisión de aserciones sobre los ciudadanos para que sean utilizadas por los proveedores de servicio.

Por último mencionar que la información necesaria para establecer relaciones de confianza entre la aserting party, esto es Proxy-Clave y las relying parties, esto es, las aplicaciones, se conoce como **metadatos**, y se puede definir como:

Información y datos de configuración para los proveedores de identidad (IdP) y para los proveedores de servicios (SP), que son intercambiados entre ambos.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

4.3 Perfiles, bindings, protocolos y aserciones

El estándar SAML, siguiendo un aproximación *top-botton*, define un conjunto de diferentes “casos de usos”, para los que presenta una solución.

A estos casos de uso los denomina **perfiles**, siendo los utilizados en Proxy-Clave **SSO Web Browser** y **Single Logout**.

Los perfiles esquematizan un conjunto de reglas, definiendo como “añadir” y “extraer” aserciones SAML en y de un protocolo.

Por ejemplo un perfil SOAP de SAML describe como se pueden añadir las aserciones SAML a los mensajes SOAP, como se ven afectadas las cabeceras SOAP por las aserciones SAML, y como reflejar los errores de estado SAML en los mensajes SOAP.

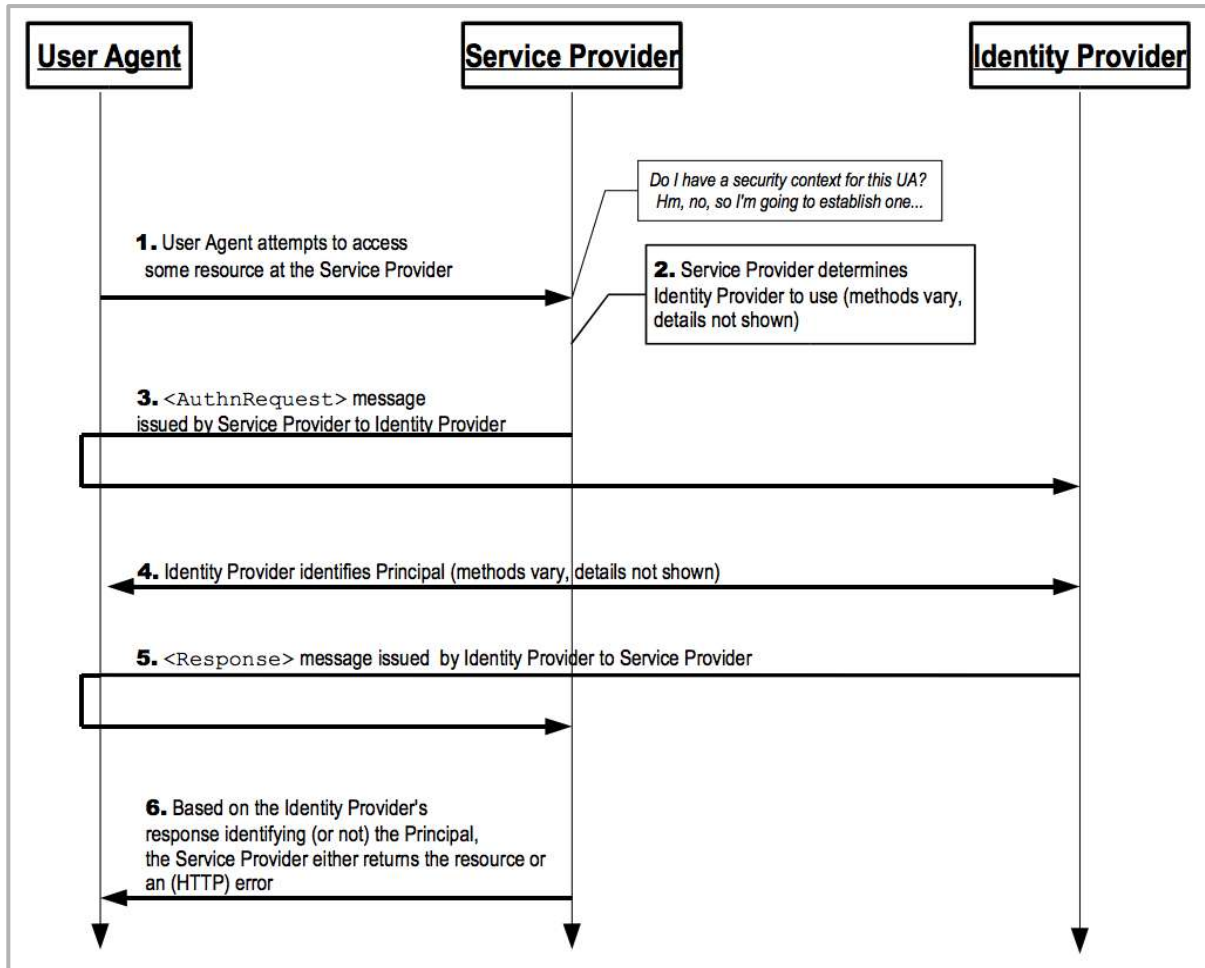


4.3.1 Perfil SSO Web Browser

El perfil **SSO Web Browser**, define como debe realizarse la autenticación de un sujeto (ciudadano) por medio de un proveedor de identidad (Proxy-Clave) a petición de un proveedor de servicio (aplicación). Donde todos los mensajes que se intercambian entre el proveedor de identidad y el proveedor de servicio son *user centric*, esto es, centrados en el usuario, lo que en última instancia significa que todos los mensajes deben ser enviados y recibidos por el agente web (navegador web) del ciudadano.

El siguiente diagrama de secuencia detalla¹ el paso de mensajes entre las entidades SAML, identificadas por el rol que desempeñan. Téngase en cuenta que el *user agent* puede ser considerado, de forma abstracta, como el ciudadano.

1 Para una completa explicación del diagrama de secuencia véase [Profiles for the OASIS Security Assertion Markup Language \(SAML\) V2.0](#). Epígrafe 4.1.2 Profile Overview. Pág. 15



Fuente: [Profiles for the OASIS Security Assertion Markup Language \(SAML\) V2.0](#). Epígrafe 4.1.2 Profile Overview. Pág. 15

Este perfil hace uso de dos mensajes SAML **<AuthRequest>** y **<Response>** que forman parte del protocolo *Authentication Request Protocol*

- El mensaje **<AuthRequest>** es emitido desde el proveedor de servicio o aplicación hacia el proveedor de identidad o Proxy-Clave, solicitándole que identifique al ciudadano que lo transporta.
- El mensaje **<Response>** ó “artefacto” devuelto desde el proveedor de identidad o Proxy-Clave hacia el proveedor de servicio o aplicación, conteniendo la aserción sobre si el ciudadano, que lo transporta, es quien dice ser y aquella información de identidad y autenticación de la que disponga el IdP sobre el ciudadano.

 Junta de Andalucía	<p align="center">MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE</p> <p align="center">Guía para la Integración de Aplicaciones en Proxy-Clave</p>	<p align="center">Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)</p>
---	--	---

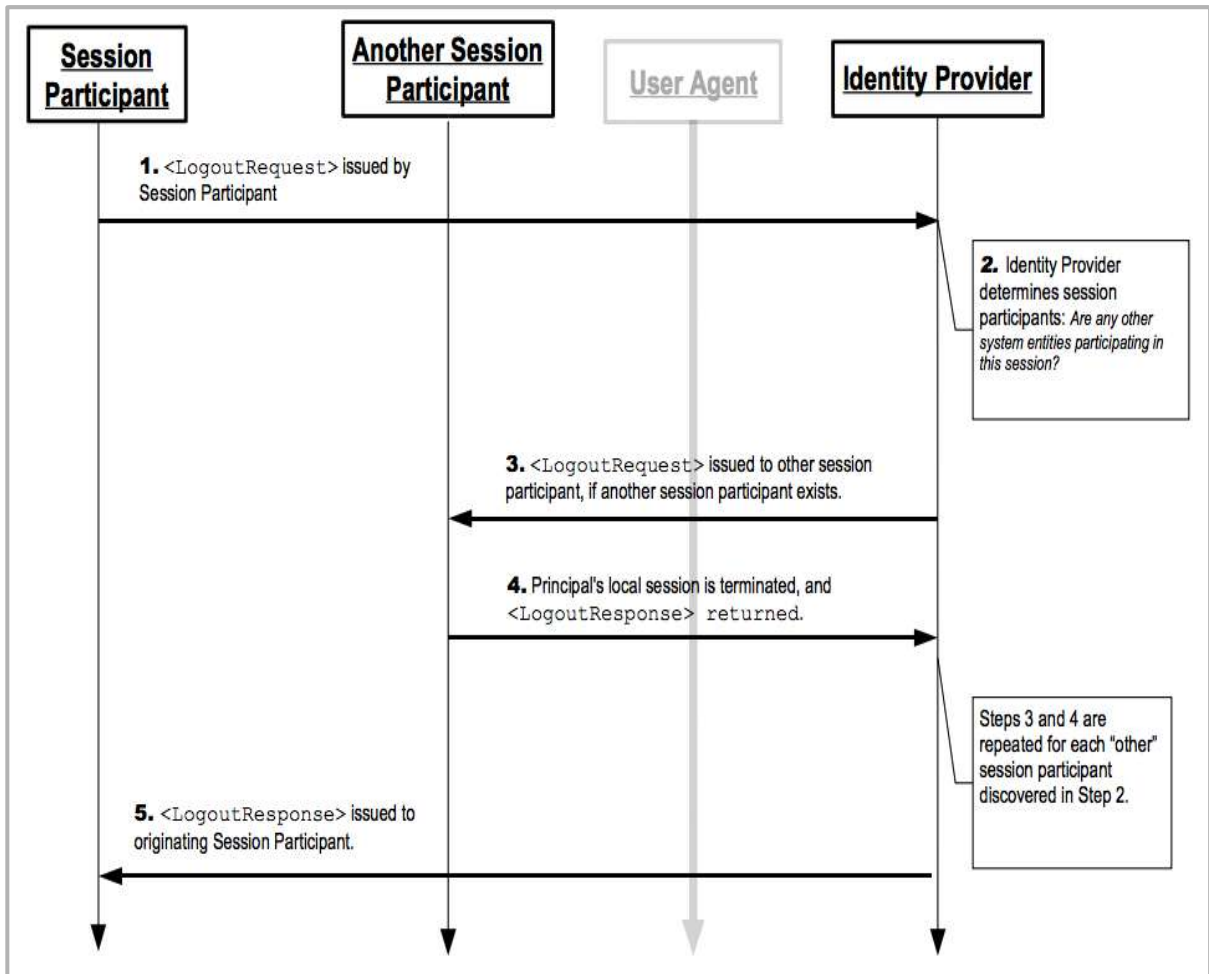
4.3.2 Perfil Single Logout

El perfil **Single Logout**, define como debe realizarse el cierre de sesión desde un *session participant* o aplicación en la que un ciudadano tiene una sesión abierta, hacia un proveedor de identidad (Proxy-Clave), y como este debe solicitar a todos aquellos otros *session participants* en los que el ciudadano tuviese otra sesión abierta, antes del informar al *session participant*, que inició el procedimiento de que se ha producido el cierre de la sesión que el ciudadano disponía en el Single Sign On.

Al igual que en el perfil SSO Web Browser, todos los mensajes que se intercambian entre el proveedor de identidad y el proveedor de servicio **pueden ser** *user centric*, esto es, centrados en el usuario, lo que en última instancia significa que todos los mensajes deben ser enviados y recibidos por el agente web (navegador web) del ciudadano. O pueden ser intercambiados en *backchannel*, esto es, directamente entre el proveedor de identidad (Proxy-Clave) y el resto de *session participants* (aplicaciones en las que el ciudadano tuviese una sesión abierta).

El siguiente diagrama de secuencia detalla² el paso de mensajes entre las entidades SAML, identificadas por el rol que desempeñan. Téngase en cuenta que aquí el *user agent* puede estar presente o no como el encargado de enviar y recibir los mensajes, es por ello que se muestra sombreado.

2 Para una completa explicación del diagrama de secuencia véase [Profiles for the OASIS Security Assertion Markup Language \(SAML\) V2.0](#). Epígrafe 4.4.2 Profile Overview. Pág. 33




Fuente: [Profiles for the OASIS Security Assertion Markup Language \(SAML\) V2.0. Epígrafe 4.1.2 Profile Overview. Pág. 15](#)

Este perfil hace uso de dos mensajes SAML **<LogoutRequest>** y **<LogoutResponse>** que forman parte del protocolo *Authentication Request Protocol*

- El mensaje **<LogoutRequest>** es emitido desde el proveedor de servicio o aplicación hacia el proveedor de identidad o Proxy-Clave; o desde el proveedor de identidad hacia un proveedor de servicio.

El mensaje puede ser emitido de forma síncrona, por medio del binding SOAP (backchannel), o asíncrona, por medio del binding HTTP-Redirect (user centric).

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

- El mensaje <LogoutResponse> ó “artefacto” devuelto desde el proveedor de identidad (Proxy-Clave), o desde un proveedor de servicio (otras aplicaciones donde el ciudadano tuviese sesión abierta) hacia el proveedor de servicio (aplicación) o hacia el proveedor de identidad (Proxy-Clave), indicando se la sesión se ha cerrado satisfactoriamente o no.

Como se ha podido observar, los **perfiles** hacen uso de los **bindings**, para intercambiar o transportar los mensajes, los cuales son definidos junto a su semántica en los **protocolos**, y que estos mensajes contienen como resultado de la identificación de los sujetos o ciudadanos **aserciones** sobre la identidad y el proceso de autenticación que han realizado en el proveedor de identidad.

4.3.3 Bindings

La correspondencia entre el intercambio de mensajes de petición y respuesta SAML en mensajes estándares o protocolos de comunicación se conoce en SAML como SAML protocol bindings o sólo bindings.

Por ejemplo el Binding SOAP describe como se intercambian peticiones y respuestas SAML dentro de mensajes SOAP.

Se puede, por tanto, concluir que los bindings en SAML son la capa de transporte del estándar. Y que cuando se hace referencia a ellos lo que se está indicando es cómo una entidad debe transportar un mensaje SAML (ya sea de petición o de respuesta) hacia la entidad de destino del mismo.

En el perfil **SSO Web Browser** se pueden hacer uso de los bindings **HTTP-Redirect**, **HTTP POST** y **HTTP Artifact**, mientras que en el perfil **Single Logout** se puede hacer uso de los bindings **SOAP**, **HTTP-Redirect**, **HTTP POST** y **HTTP Artifact**.

Aunque en Proxy-Clave solo se permite el uso de los bindings **HTTP-Redirect** y **HTTP POST**.

4.3.3.1 Binding HTTP-Redirect

El binding HTTP-Redirect consiste en enviar los mensajes como parámetros de peticiones HTTP GET y hacer uso de respuestas HTTP con código de estado 302, esto es, por medio de redirecciones.

Los mensajes SAML se definen mediante XML, por lo que deben ser codificados para poder transportarlos como parte de una URL en la petición HTTP.

El tamaño de una petición HTTP GET no está restringido por definición del protocolo HTTP en el [RFC-7231](#),³ pero en la práctica esto no es real, puesto que el

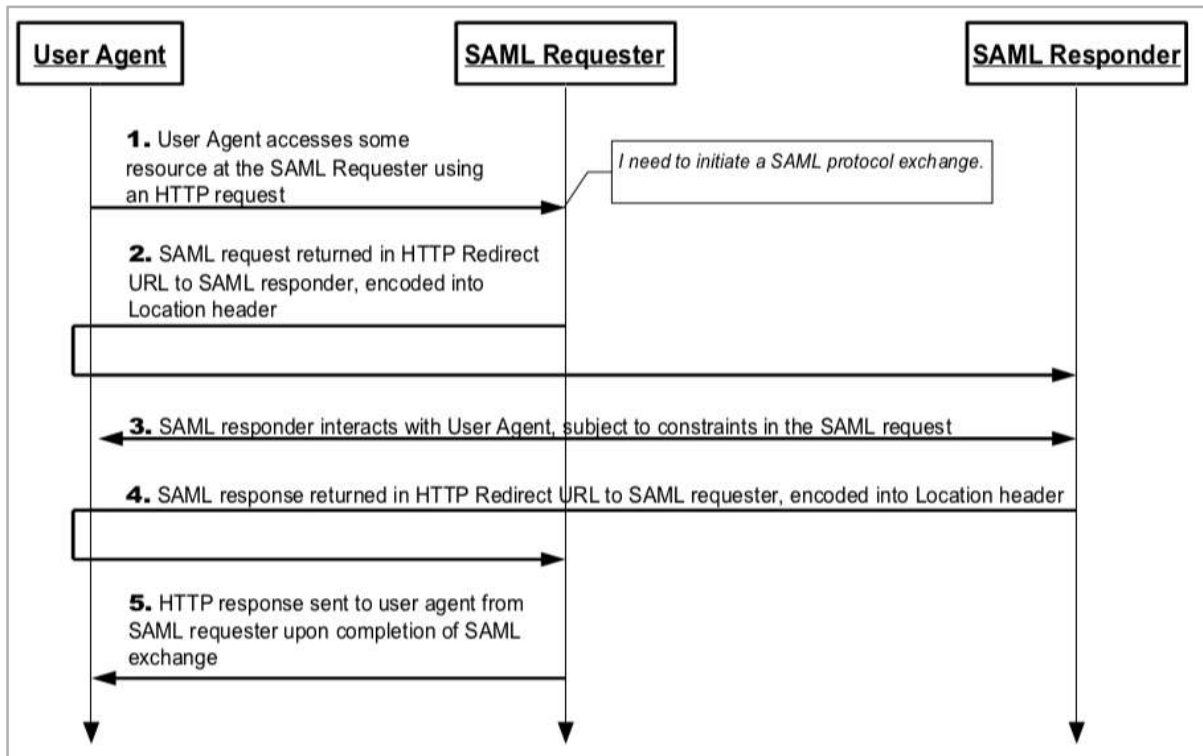
3 [Hypertext Transfer Protocol \(HTTP/1.1\): Semantics and Content](#)

 <p>Junta de Andalucía</p>	<p align="center">MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE</p> <p align="center">Guía para la Integración de Aplicaciones en Proxy-Clave</p>	<p align="center">Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)</p>
---	--	---

tamaño dependerá del agente de usuario o navegador web. Es por esto que los mensajes de mayor tamaño o más complejos se suelen dejar para bindings como HTTP-POST o HTTP Artifact.

El uso del este binding, se suele restringir al envío de los mensajes que se corresponden con petición de autenticación.

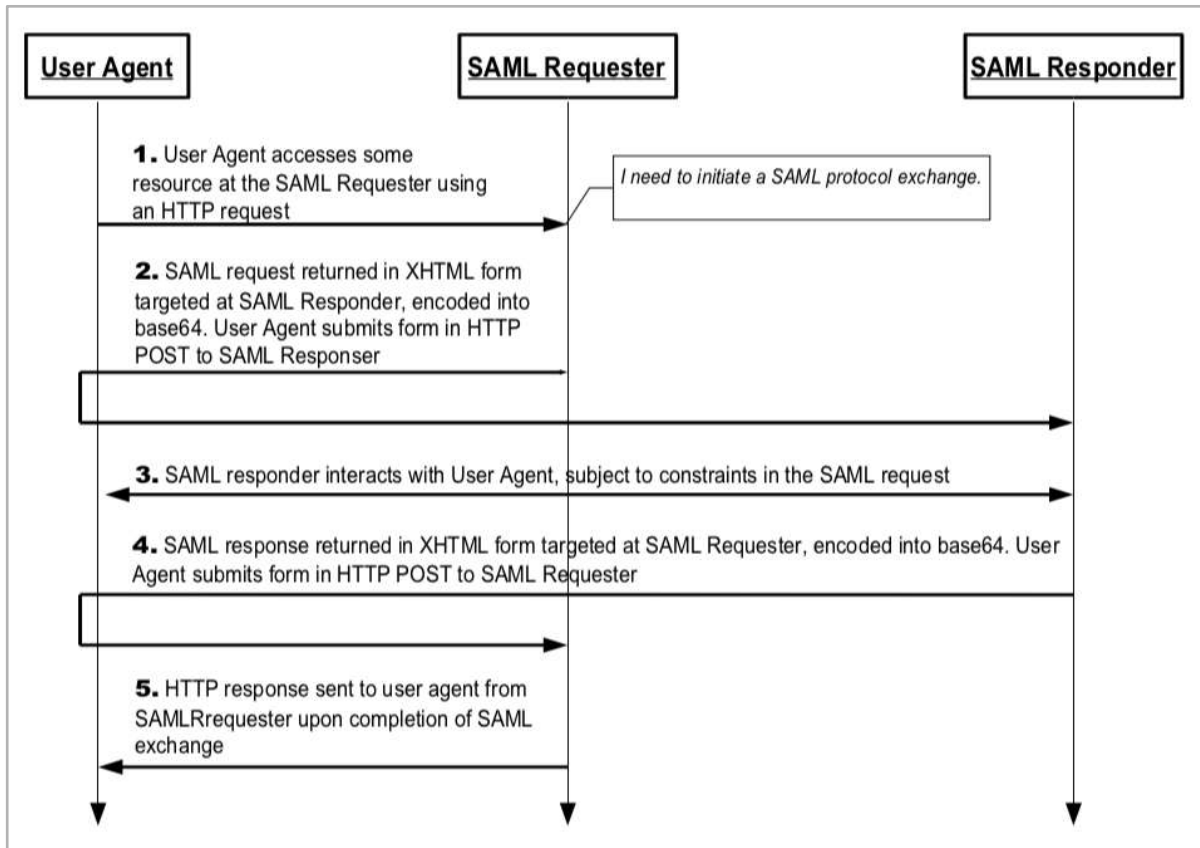
El siguiente diagrama de secuencia describe de forma visual el binding HTTP-Redirect.



4.3.3.2 Binding HTTP POST

El binding HTTP POST consiste en enviar los mensajes dentro del contenido de un formulario HTML, codificados en base64. Se utiliza cuando nos encontramos en un escenario “user centric”, es decir, todo el contenido de los mensajes pasa por el agente web del usuario.

El siguiente diagrama de secuencia describe de forma visual el binding HTTP Post.




4.3.4 Protocolos

Los mensajes de los protocolos SAML pueden ser generados e intercambiados usando diferentes protocolos, como se puede observar hablamos de protocolos SAML y protocolos de transporte, siendo estos últimos los bindings SAML.

La mejor forma de presentar este hecho es mediante la propia definición del estándar.

SAML protocol messages can be generated and exchanged using a variety of protocols. The SAML bindings specification [SAMLBind] describes specific means of **transporting protocol** messages using existing widely deployed transport protocols.

Por tanto es importante no confundir protocolos SAML con protocolos de transporte como pueden ser HTTP, SOAP, etc.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

Los protocolos definidos por SAML “hacen” las siguientes acciones

- Devuelven una o más aserciones solicitadas
- “Disparan” la autenticación tras una petición y devuelven la aserción correspondiente
- Registran un “name identifier” o eliminan su registro
- Obtienen un mensaje de un protocolo que ha sido solicitado por medio de un artefacto
- “Disparan” un cierre de sesión, etc.

4.3.4.1 Protocolo Authentication Request

El protocolo *Autenticación Request* es utilizado por un un *principal*⁴ o un **agente** (navegador web) en representación de este para obtener una **aserción** con una **declaración de autenticación** (identificación), que permita **establecer un contexto de seguridad** (crear una sesión de usuario) en uno o más proveedores de servicios (aplicaciones).

Por medio de este protocolo se envían los mensajes <AuthnRequest> a un proveedor de identidad (Proxy-Clave) requiriendo que devuelva un mensaje <Response>.

El mensaje de petición de autenticación, esto es, el elemento xml <AuthnRequest> debe (SHOULD) ser firmado, o en caso de que no lo sea, la privacidad e integridad del mismo debe ser proporcionada mediante el binding usado (HTTP sobre TLS, en el caso del binding HTTP-GET).

El mensaje de respuesta de autenticación, esto es, el elemento xml <Response> depende del **perfil** y el **binding** utilizado.

4.3.4.2 Protocolo Single Logout

El protocolo *Single Logout* proporciona los mensajes para que todos los proveedores de servicio (aplicaciones) con sesión en un proveedor de identidad (Proxy-Clave) la cierren **casi simultáneamente**. Para ello el sujeto (ciudadano) puede provocar el cierre de la sesión bien en un proveedor de servicio, o bien en el proveedor de identidad. El protocolo además permite identificar el motivo por el que se solicita el cierre de la sesión.

4 Es la forma en la que en SAML se denomina a una entidad de sistema que puede ser autenticada, según se extrae de Security Frameworks for Open Systems: Authentication Framework. ITU-T Recommendation X.811 (1995 E), ISO/IEC 10181-2:1996(E). See <http://www.itu.int/itudoc/itu-t/rec/x/x500up/x811.html>.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

Cuando el sujeto (ciudadano) solicita un cierre de sesión a un proveedor de servicio, éste debe (MUST) enviar un mensaje <LogoutRequest> al proveedor de identidad, obligando a este último a responder con un mensaje <LogoutResponse>.

Más adelante en este documento se volverá a hacer mención al cierre de sesión en Proxy-Clave y las implicaciones que conlleva dentro de su entorno, además de aspectos relativos a como es implementado el cierre de sesión por las bibliotecas software.

4.3.5 Aserciones

Una aserción es una afirmación hecha por alguien (*asserting party*, proveedor de identidad o Proxy-Clave) a cerca de alguien (sujeto o ciudadano).

Los proveedores de servicio (aplicaciones) usan aserciones sobre sujetos para realizar el control de acceso y proveer servicios personalizados.

SAML v2 define tres tipos diferentes de declaración de aserciones, donde todos están asociadas con un sujeto o ciudadano.

- **Autenticación:** El sujeto fue autenticado por un método concreto a una hora concreta

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  ID="_e15361b0-72d4-11e8-8011-616263646566"
  Version="2.0"
  IssueInstant="2018-06-18T08:52:07Z">
...
</saml:Assertion>
```

- **Atributo:** El sujeto está asociado con los atributos suministrados

```
<saml:Assertion
...
  <saml:Attribute
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    Name="PartialAfirma"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml:AttributeValue
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xsi:type="xs:string">
      PD94gdmVy ... c21vbj0iMS4wIbmNv=
    </saml:AttributeValue>
  </saml:Attribute>
...

```

- **Decisión de Autorización:** Una petición para permitir al sujeto acceder al recurso especificado a sido concedida o denegada. Este último tipo no está

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

en uso en Proxy-Clave.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

5 Propósito y uso de metadatos SAML v2 en Proxy-Clave

Los metadatos en SAML v2 es información que se deben intercambiar los proveedores de servicio y el proveedor de identidad, esto es, entre las aplicaciones y Proxy-Clave. Esto es así debido a que los perfiles SAML requieren que se realicen *acuerdos* sobre identificadores, bindings soportados, *endpoints*⁵, certificados y claves, etc, entre las entidades del sistema.

En pocas palabras podría decirse que las entidades que forman el sistema deben saber:

- Dónde preguntar por la identidad de los ciudadano y dónde responder a las preguntas
- Cómo preguntar y cómo responder
- Qué preguntar qué responder

Y es para esto para lo que se usan y se usan y se intercambian los metadatos.

Como se ha descrito en el punto [4. Introducción a SAML v2](#) el servicio Proxy-Clave hace uso del perfil SSO Web Browser, esto es, forma junto con las aplicaciones un sistema Single Sing On.

Por lo que en dicho Single Sign On será necesario que el proveedor de identidad que es Proxy-Clave sepa, o mejor dicho conozca, a los proveedores de servicio que son las aplicaciones, las cuales le van a solicitar autenticaciones de ciudadano y por tanto a las que debe responder a cerca de los ciudadanos.

En el caso de los proveedores de servicios, las aplicaciones, necesitan saber dónde escucha el Proxy-Clave, esto es sus *endpionts* y que bindings soporta, para poder enviar los mensajes SAML con la seguridad de que serán atendidos.

Ambas partes, tantos aplicaciones com Proxy-Clave, deben intercambiarse certificados para realizar operaciones de firma y cifrado de los mensajes SAML o de las aserciones SAML.

Y como es lógico, también deben poder identificarse mutuamente, por lo que tendrán que intercambiar sus identificadores como entidades SAML.

5.1 ¿Qué son los metadatos SAML v2?

Los metadatos SAML v2 son un documento XML que contienen de forma ordenada, concreta y bien definida, la información descrita anteriormente.

Los metadatos SAML v2 están diseñados para ser entendidos por aplicaciones, aunque con el suficiente entrenamiento, se pueden manejar y comprender sin

⁵ Puede considerarse un *endpoint* como la URL final a la que se debe enviar un mensaje SAML.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

muchas dificultades, no dejan de ser un documento XML.

Los metadatos suelen firmarse digitalmente con el propósito de su integridad y reconocer a la identidad la entidad que los emite o genera. Si bien no obligatorio formarlos, es una práctica recomendada.

Los metadatos SAML v2 tienen el siguiente aspecto.



Junta de Andalucía

MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE

Guía para la Integración de Aplicaciones en Proxy-Clave

Servicio de Coordinación y Desarrollo de
Sistemas Horizontales (SCDSH), bajo la
Dirección General de Transformación
Digital (DGTD)

```
<?xml version="1.0" encoding="utf-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://ws050.juntadeandalucia.es/proxyclavepru/SAML2/">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDYDCCAkgCCQDSiwcV2...0XH723ItINbmGLw0iI57v0ew0NpyYA==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDYDCCAkgCCQD/SiwcV2...0XH723ItINbmGLw0iI57v0ew0NpyYA==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://ws050.juntadeandalucia.es/proxyclavepru/SAML2/SLOService.php"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://ws050.juntadeandalucia.es/proxyclavepru/SAML2/SSOService.php"/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://ws050.juntadeandalucia.es/proxyclavepru/SAML2/SSOService.php"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

5.2 ¿Para qué se utilizan los metadatos SAML v2?

Principalmente se utilizan para establecer la relación de confianza entre un proveedor de servicio y el proveedor de identidad. Una vez establecida la citada relación de confianza, tanto el proveedor de servicio como el proveedor de identidad sabrán cómo y a dónde deben enviarse los mensajes SAML.

Siguiendo el ejemplo de los metadatos mostrados en el punto anterior, se puede saber que los metadatos mostrados se corresponden con un proveedor de identidad, cuyo identificador de entidad es <https://ws050.juntadeandalucia.es/proxyclavepru/SAML2/> que dispone de dos certificados, uno para firmar y otro para cifrar, y que ofrece dos servicios, uno de Single Sign On y otro de single Logout; que el primero se puede consumir por medio de los binding HTTP Post y HTTP-Redirect en la url <https://ws050.juntadeandalucia.es/proxyclavepru/SAML2/SSOService.php> y que el segundo se puede consumir por medio del binding HTTP-Redirect en la url <https://ws050.juntadeandalucia.es/proxyclavepru/SAML2/SLOService.php>.

Por tanto los metadatos son imprescindibles para que las diferentes entidades puedan comunicarse entre ellas.

5.3 ¿Qué contienen los metadatos SAML v2?


Los metadatos contienen la siguiente información reflejada en el punto anterior así como otros aspectos necesarios para organizar el Single Sign On.

Los elementos XML más relevantes son los siguientes:

- **<EntitiesDescriptor>** Este elemento contiene la lista de descriptores de entidades que forman parte de los metadatos. Lo normal, en el ámbito de Proxy-Clave es que las aplicaciones no lo utilicen, dado que sus metadatos sólo contienen un descriptor de entidad, el de la propia aplicación. Pero los metadatos de Proxy-Clave disponibles en la siguiente url <https://ws050.juntadeandalucia.es/proxyclaveexp/metadata/federation/production> contienen tres descriptores de identidad.
- **<EntityDescriptor>** Este elemento es el que contiene la información en sí de cada aplicación o proveedor de identidad. Como atributo del mismo se proporciona el identificador de cada entidad, en el atributo **entityID**. El los metadatos de Proxy-Clave se encuentran tres elementos **<EntityDescriptor>**, cada uno de ellos con su **entityId** correspondiente:
 - `<md:EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://ws050.juntadeandalucia.es/proxyclaveexp/metadata/federation/production/ClaveSEQAA2">`

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

- `<md:EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://ws050.juntadeandalucia.es/proxyclaveexp/metadata/federation/production/ClaveSEQAA3">`
- `<md:EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://ws050.juntadeandalucia.es/proxyclaveexp/metadata/federation/production/ClaveSEQAA4">`
- **<IDPSSODescriptor>** Este elemento indica el rol de la entidad SAML. En este caso es un proveedor de identidad. Dentro de él estarán contenido el resto de elementos que definen el comportamiento de este proveedor de identidad. Como
 - **<KeyDescriptor>** Información sobre el certificado digital de este proveedor de identidad. En el elemento, por medio del atributo **use** se indica si es usado para firmar **signing** o para cifrar **encryption**
 - **<SingleSignOnService>** Elemento que describe la URL donde espera recibir las peticiones de autenticación mediante el atributo **Location** y el **binding** que se ha de utilizar
 - **<SingleLogoutService>** Elemento que describe la URL donde espera recibir las peticiones de logout mediante el atributo **Location** y el **binding** que se ha de utilizar
- **<SPSSODescriptor>** Este elemento indica el rol de la entidad SAML. En este caso es un proveedor de servicio. Dentro de él estarán contenido el resto de elementos que definen el comportamiento de este proveedor de servicio. Como
 - **<KeyDescriptor>** Información sobre el certificado digital de este proveedor de servicio. En el elemento, por medio del atributo **use** se indica si es usado para firmar **signing** o para cifrar **encryption**
 - **<SingleLogoutService>** Elemento que describe la URL donde espera recibir los mensajes de logout mediante el atributo **Location** y el **binding** que se ha de utilizar
 - **<AssertionConsumerService>** Elemento que describe la URL donde espera recibir las aserciones SAML enviadas como mensajes de respuesta de autenticación mediante el atributo **Location** y el **binding** que se ha de utilizar
- **<Organization>** Este elemento proporciona información básica sobre la organización responsable de las entidades SAML. Trasladado al ámbito de Proxy-Clave, se corresponde con el organismo bajo el cual se encuentra la aplicación a integrar en Proxy-Clave. Es en sus elementos hijos donde se deben reflejar los detalles del organismo
 - **<OrganizationName>** Nombre del organismo

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

- <OrganizationDisplayName> Nombre del organismo que se le mostrará a los ciudadanos
- <OrganizationURL> URI de la organización
- <ContactPerson> Este elemento proporciona información sobre una persona responsable en alguna manera de una entidad SAML. Se puede indicar que tipo de responsable es, por medio del atributo **contactType** cuyos posibles valores son: **technical**, **support**, **administrative**, **billing**, y **other**. Es en sus elementos hijos donde se deben reflejar los detalles del contacto
 - <Company> Nombre de la empresa de la persona de contacto
 - <GivenName> Nombre de la persona de contacto
 - <SurName> Apellido de la persona de contacto
 - <EmailAddress> Dirección de correo de la persona de contacto
 - <TelephoneNumber> Número de teléfono de la persona de contacto

5.4 Que deben reflejar los metadatos SAML V2 para Proxy-Clave

Los metadatos SAML v2 de una aplicación o sistema de información deben cumplir una serie de requisitos antes de ser enviados al técnico responsable de Proxy-Clave.

Para detallar estos requisitos, y construir un ejemplo de documento xml de metadatos se seguirá la información de la aplicación de ejemplo del punto [3. Caso de ejemplo utilizado en este documento](#)

Antes de continuar, tenga en cuenta que la biblioteca SAML que utilice su aplicación será la encargada de generar el documento XML por usted, y que su responsabilidad es la de indicarle la información necesaria para tal fin. Y que es sobre la información necesaria a reflejar en los metadatos lo que se explica a continuación.

Identificador de entidad o entityID es el “nombre” con el cual será conocida su aplicación como entidad SAML v 2 en Proxy-Clave. Generalmente, las bibliotecas software generan el identificador de forma automática, a partir de la URL de la propia aplicación. No es obligatorio que el valor del atributo **entityID** del elemento **EntityDescriptor** de sus metadatos sea una URL.

Para el caso de ejemplo que nos ocupa nuestra biblioteca SAML ha generado el siguiente identificador <https://www.example.com/laapliccion> de forma que el elemento XML **EntityDescriptor** queda como se muestra a continuación

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_877873b6766cafcd94dff9add1f5ec00b4922173"
entityID="https://www.example.com/laapliccion">
```

Certificado digital será necesario utilizar uno para firmar las peticiones de autenticación, aunque realmente la operación criptográfica de firma se realiza con la clave privada, por lo que la biblioteca SAML necesitará que se le proporcione un certificado.

Este certificado puede ser autofirmado, no tiene por qué ser un certificado para autenticar servidores web, basta con que entre sus capacidades se encuentren realizar firmas y cifrados. Para ello es necesario que estén activos los usos de la clave *digitalSignature*⁶, *keyEncipherment*⁷.

Una vez que la biblioteca SAML dispone del certificado y la clave privada, suponiendo que sólo lo utilizará para firmar genera el elemento XML `KeyDescriptor` como se muestra a continuación⁸

```
<md:KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>
      <ds:X509Certificate>
        MIIDUjCCAjqgAwIBAgIEUOLIQTBgkqhkbH ... wSoBy5hLPNALaEUoa5zPDwlixwRjFQ=
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>
```

URL del servicio de consumo de aserciones es la URL a la cual Proxy-Clave enviará los mensajes SAML de respuesta de autenticación. Generalmente, las bibliotecas software generan el identificador de forma automática, a partir de la URL de la propia aplicación.

Para el caso de ejemplo que nos ocupa nuestra biblioteca SAML ha generado la siguiente URL de forma que el elemento XML `AssertionConsumerService` queda como se muestra a continuación

```
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://https://www.example.com/laapliccion/saml/SSO" index="0"
isDefault="true"/>
```

URL del servicio de logout es la URL a la cual Proxy-Clave enviará los mensajes SAML de logout (peticiones o respuestas) de cierre de sesión. Generalmente, las bibliotecas software generan el identificador de forma automática, a partir de la

6 Para más información véase <https://tools.ietf.org/html/rfc5280#section-4.2.1.3>

7 Para más información véase <https://tools.ietf.org/html/rfc5280#section-4.2.1.3>

8 Debido al tamaño del certificado la cadena que lo describe se ha acortado

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

URL de la propia aplicación.

Para el caso de ejemplo que nos ocupa nuestra biblioteca SAML ha generado la siguiente URL de forma que el elemento XML `SingleLogoutService` queda como se muestra a continuación

```
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://https://www.example.com/laapliccion/saml/SingleLogout"/>
```

Información del organismo son los datos del organismo bajo el cual se encuentra la aplicación. No todas las bibliotecas SAML permiten, de una forma intuitiva, cumplimentar esta información. Información que en el estándar SAML es opcional, pero que en Proxy-Clave es de obligado cumplimiento.

Para el caso de ejemplo que nos ocupa nuestra biblioteca SAML ha generado la los siguientes elementos XML quedando como se muestra a continuación

```
<md:Organization>
  <md:OrganizationName xml:lang="es">El &#xF3;rganismo</md:OrganizationName>
  <md:OrganizationDisplayName xml:lang="es">El &#xF3;rganismo</md:OrganizationDisplayName>
  <md:OrganizationURL xml:lang="en">http://www.elorganismo.org</md:OrganizationURL>
</md:Organization>
```

Datos de contacto del responsable administrativo son los datos del responsable administrativo de la aplicación. No todas las bibliotecas SAML permiten, de una forma intuitiva, cumplimentar esta información. Información que en el estándar SAML es opcional, pero que en Proxy-Clave es de obligado cumplimiento.

Para el caso de ejemplo que nos ocupa nuestra biblioteca SAML ha generado la los siguientes elementos XML quedando como se muestra a continuación

```
<md:ContactPerson contactType="administrative">
  <md:GivenName>Juan</md:GivenName>
  <md:SurName>Nadie</md:SurName>
  <md:EmailAddress>mailto:juan.nadie@example.com</md:EmailAddress>
  <md:TelephoneNumber>123456789</md:TelephoneNumber>
</md:ContactPerson>
```

Datos de contacto del responsable técnico son los datos del responsable técnico o de soporte de la aplicación. No todas las bibliotecas SAML permiten, de una forma intuitiva, cumplimentar esta información. Información que en el estándar SAML es opcional, pero que en Proxy-Clave es de obligado cumplimiento.

Para el caso de ejemplo que nos ocupa nuestra biblioteca SAML ha generado la los siguientes elementos XML quedando como se muestra a continuación

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	--

```
<md:ContactPerson contactType="technical">
  <md:GivenName>Antonio</md:GivenName>
  <md:SurName>Tecnico</md:SurName>
  <md:EmailAddress>mailto:antonio.tecnico@example.com</md:EmailAddress>
  <md:TelephoneNumber>987654321</md:TelephoneNumber>
</md:ContactPerson>
```

5.5 Errores comunes en los metadatos

Hay dos errores concretos que se suelen producir con asiduidad en la integración de aplicaciones en Proxy-Clave, cuando el equipo de trabajo que hay detrás de ellas es desconocedor del estándar SAML.

Estos errores siempre se derivan de la modificación “a mano” del documento XML de metadatos que generan las bibliotecas SAML. Por lo que la regla base con los metadatos es **no modificarlos nunca a mano**, dado que esto significa que Proxy-Clave trabaje con metaformación de la biblioteca SAML falsa y hace muy difícil de depurar las integraciones.

La primera recomendación consiste en no modificar metadatos firmado digitalmente, dado que una la modificación altera el contenido del documento XML y provoca que Proxy-Clave no los acepte al no poder validar la firma digital de los mismos.

La segunda recomendación es no modifique el atributo `entityID` de su aplicación, esto puede dar lugar a confusiones en su aplicación cuando Proxy-Clave le haga llegar un mensaje SAML de respuesta de autenticación emitido para una entidad que no es la que su biblioteca SAML espera, provocando que pueda descartarlo o generar error.

La tercera recomendación es no modifique ninguna URL de ningún atributo `Location` puesto que provocará que Proxy-Clave envíe los mensajes SAML de respuesta de autenticación a una URL donde su biblioteca SAML no los está esperando.

En resumen, **no modifique los metadatos**, sino **modifique la configuración de su biblioteca SAML** para que esta lo refleje en sus metadatos.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

6 Modalidades de atributos de Proxy-Clave

Proxy-Clave dispone de tres modalidades de entrega de atributos a los sistemas de información.

Se define un modo de entrega de atributos como a) el conjunto de atributos que lo forman, b) los identificadores de estos atributos y c) el formato de los valores de los atributos.

Estas modalidades se derivan de la evolución que ha sufrido el servicio desde la versión 1 de Clave hacia la versión 2, junto con la necesidad de ofrecer a las aplicaciones [Cl@ve 2](#) nativas⁹

Estas modalidades se conocen como

- Modo nativo Cl@ve 2 con
- Modo compatible [Cl@ve 1](#)
- Modo nativo Cl@ve 2 con protocolo SAML v2

y pueden ser solicitadas en el proceso de integración en Proxy-Clave

6.1 Modo nativo Cl@ve 2 con protocolo Clave 2.0

Esta modalidad es la utilizada por las aplicaciones Cl@ve 2 nativa y se caracteriza por el siguiente conjunto de atributos, identificadores y formatos:

Identificador	Valor ¹⁰	Formato/Observación
http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName	Ficticio Activo	Se puede recibir tanto un nombre simple como uno compuesto. Es un atributo personal obligatorio que se recibirá siempre
http://eidas.europa.eu/attributes/naturalperson/GivenName	Ciudadano	Es un atributo personal obligatorio que se recibirá siempre.
http://es.minhafp.clave/FirstSurname	Ficticio	Contiene el identificador único (NIF) del Usuario. Es un atributo personal obligatorio

⁹ Se considera aplicación nativa Cl@ve 2 a aquella que ha sido desarrollada para conectar directamente con Cl@ve 2 y por lo tanto “habla” de forma nativa dicho protocolo. Debido a esto estas aplicaciones esperan como resultado de las autenticaciones, los atributos tal y como los provee Cl@ve 2, esto es, sin adaptaciones.

¹⁰ Los valores se han obtenido de una autenticación de pruebas a partir de un certificado de autenticación del Kit de pruebas del DNIE. Por lo que los valores son ficticios, pero permiten observar el formato de los mismos

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

Identificador	Valor	Formato/Observación
http://es.minhafp.clave/PartialAfirma	PhcnRpYXxfQW...	que se recibirá siempre. Contiene la respuesta parcial de @firma en Base64. Este atributo solo está disponible cuando el ciudadano se autentica con un certificado digital
http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier	99999018D	Contiene el identificador único (NIF) del Usuario. Es un atributo personal obligatorio que se recibirá siempre
http://es.minhafp.clave/RelayState	_ddffa1dfd5d1222c49b359ea63a288f808c9a5	Contiene el mismo valor enviado en la petición
http://es.minhafp.clave/SelectedIdP	AFIRMA	Identifica el proveedor de identidades utilizado para la identificación. Este atributo puede poseer alguno de los siguientes valores: AFIRMA, EIDAS, SEGSOC o PIN24H
http://es.minhafp.clave/RegisterType	-	No esta presente durante esta autenticación. tipo de registro que el ciudadano realizó para crear su identidad en el Proveedor de Identidad. Posibles valores: <ul style="list-style-type: none"> • 0: Sin datos • 1: Presencial • 2: Carta invitación • 3: Certificado • 4: Presencial + certificado

6.2 Modo compatible Cl@ve 1 y Cl@ve 2

Esta modalidad es la utilizada por las aplicaciones integradas en Proxy-Clave durante el periodo de tiempo que estuvo funcionando la versión 1 de Cl@ve.

Debido a cambios en los atributos devueltos desde Cl@ve 2, Proxy-Clave genera los antiguos atributos y valores de Cl@ve 1, permitiendo que la migración de la versión de 1 a la 2 fuese transparente para las aplicaciones.

Esta modalidad se caracteriza por el siguiente conjunto de atributos, identificadores y formatos:

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

Identificador	Valor	Formato/Observación
afirmaResponse	PbhcnRpYWxfQW...	Contiene la respuesta parcial de @firma en Base64. Este atributo solo está disponible cuando el ciudadano se autentica con un certificado digital
citizenQAALevel	3	Nivel de calidad de la autenticación. Posibles valores de 2 a 4.
eIdentifier	ES/ES/99999018D	Código identificador legal del ciudadano, bajo el formato XX/YY/12345678Q, donde XX es el código del país de origen del identificador (por ejemplo ES), YY es el del país de destino (por ejemplo ES) y 12345678Q es el código identificador legal del ciudadano.
givenName	Ciudadano	Nombre del ciudadano
InheritedFamilyName	Ficticio	inheritedFamilyName
isLegalPerson	false	Valor "true" o "false" para indicar si el usuario se autenticó utilizando un certificado de representación de persona jurídica
isdnie	true	Valor "true" o "false" para indicar si el usuario se autenticó utilizando el DNI-e
RegisterType	3	Tipo de registro que el ciudadano realizó para crear su identidad en el Proveedor de Identidad. Posibles valores: <ul style="list-style-type: none"> • 0: Sin datos • 1: Presencial • 2: Carta invitación • 3: Certificado • 4: Presencial + certificado
surname	Ficticio Activo	Apellidos del ciudadano

6.3 Modo nativo Cl@ve 2 con protocolo SAML

Esta modalidad es la utilizada por las aplicaciones Cl@ve 2 nativa y se caracteriza por el siguiente conjunto de atributos, identificadores y formatos:

Identificador	Valor ¹¹	Formato/Observación
---------------	---------------------	---------------------

¹¹ Los valores se han obtenido de una autenticación de pruebas a partir de un certificado de autenticación del Kit de pruebas del DNIE. Por lo que los valores son ficticios, pero permiten observar el formato de los mismos

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

FamilyName	Ficticio Activo	Se puede recibir tanto un nombre simple como uno compuesto. Es un atributo personal obligatorio que se recibirá siempre
GivenName	Ciudadano	Es un atributo personal obligatorio que se recibirá siempre.
FirstSurname	Ficticio	Contiene el identificador único (NIF) del Usuario. Es un atributo personal obligatorio que se recibirá siempre.
PartialAfirma	PhcnRpyWxfQW...	Contiene la respuesta parcial de @firma en Base64. Este atributo solo está disponible cuando el ciudadano se autentica con un certificado digital
PersonIdentifier	99999018D	Contiene el identificador único (NIF) del Usuario. Es un atributo personal obligatorio que se recibirá siempre
RelayState	_ddffa1dfded5d1222c49b359ea63a288f808c9a5	Contiene el mismo valor enviado en la petición
SelectedIdP	AFIRMA	Identifica el proveedor de identidades utilizado para la identificación. Este atributo puede poseer alguno de los siguientes valores: AFIRMA, EIDAS, SEGSOC o PIN24H
RegisterType	-	No esta presente durante esta autenticación. tipo de registro que el ciudadano realizó para crear su identidad en el Proveedor de Identidad. Posibles valores: <ul style="list-style-type: none"> • 0: Sin datos • 1: Presencial • 2: Carta invitación • 3: Certificado • 4: Presencial + certificado

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

Kits de integración de aplicaciones

Los kits de integración de aplicaciones son ejemplo de elaborados con bibliotecas software concretas para diferentes tecnologías como Java, PHP y .Net.

Estos kits de integraciones se han creado, no para servir de referencia para cada tecnología, sino como un ejemplo práctico que permita entender y observar en comportamiento de una aplicación integrada en Proxy-Clave.

Cada kit va acompañado de una guía para la integración de una aplicación por medio de la biblioteca software utilizada por dicho kit.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

7 Kit de integración de aplicaciones J2EE

7.1 Aplicación de pruebas distribuida junto al kit

Para facilitar la integración se distribuye una aplicación de pruebas ya configurada y operativa contra el entorno de integración de Proxy-Clave. Puede descargar este WAR de la red profesional.

<https://redprofesional.juntadeandalucia.es/file/view/33599286/aplicacion-j2ee-de-pruebas-de-integracion-con-proxy-clve>

Para que el WAR funcione debe añadir la siguiente línea al fichero */etc/hosts* de la máquina en que vaya a desplegarlo:

```
127.0.0.1 samlintegration.sandetel.int
```

Una vez añadida la línea en el fichero */etc/hosts* y desplegado el WAR en un servidor de aplicaciones puede probar la autenticación contra Proxy-Clave accediendo en un navegador web a la URL

<http://samlintegration.sandetel.int:8080/SpringSAMLIntegrationExample/MyLogin.jsp>

y pulsar en el enlace “Autenticación contra Proxy-Clave en el entorno de pruebas”.

7.2 Requisitos para la integración con Proxy-Clave

A continuación se enumeran los requisitos para la integración en el SP:

- Entorno JAVA:
 - JDK: **versiones 1.6, 1.7 y 1.8**
 - Servidor de aplicaciones J2EE
- Permisos para reiniciar el servidor de aplicaciones.
- El servidor debe tener configurada y operativa la resolución por DNS (FQDN).

7.3 Procedimiento de configuración e integración

1. **Solicitar el alta de la aplicación en NAOS.** Acceda al Portal de Usuario de **NAOSv3** y solicite el alta mediante un ticket¹² del servicio “Servicios

¹² Si no tuviera visibilidad de alguna de las categorías anteriores, puede solicitarla a

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

TIC”, operación “Realizar petición”, componente “Otros”, elemento “Proxy CLAVE - Integración de nuevo sistema en Pruebas” o “Proxy CLAVE - Integración de nuevo sistema en Producción” según aplique.

Al ticket NAOS deberá adjuntar el fichero de metadatos que el plugin de SAML generará de forma automática una vez ejecute el punto 11 de este mismo apartado.

También debe adjuntarse al ticket NAOS el formulario de solicitud cumplimentado y firmado digitalmente disponible en la red profesional: <https://redprofesional.juntadeandalucia.es/file/view/33598716/formulario-de-integracion-de-aplicaciones>

2. Integración de los ficheros y recursos necesarios en el WAR de la aplicación a integrar:

2.1. Descomprima el archivador *SAML2-SDK.zip* descargado de la red profesional:

<https://redprofesional.juntadeandalucia.es/file/view/33599456/recursos-asociados-al-kit-de-integracion-con-proxy-clve-para-j2ee>

2.2. Dependiendo del entorno de Proxy-Clave contra el que se desee configurar la aplicación (explotación, integración o pruebas) se deben copiar todos los ficheros *xml* de la ruta:

DIRECTORIO_TRABAJO/plantillas/metadatos/proxyclave/ENTORNO

a la ruta

DIRECTORIO_TRABAJO/war/WEB-INF/classes/metadata/

2.3. Se deben añadir el contenido de los ficheros *txt* de la ruta:

DIRECTORIO_TRABAJO/plantillas/securityContext/proxyclave/ENTORNO

al fichero

DIRECTORIO_TRABAJO/war/WEB-INF/securityContext.xml

entre las líneas comentadas:

```
<!-- COMIENZO DEL BEAN DE CONFIGURACIÓN PARA UTILIZAR PROXYCLAVE -->
```

y

```
<!-- FIN DEL BEAN DE CONFIGURACIÓN PARA UTILIZAR PROXYCLAVE -->
```

2.4. El código fuente de la versión del plugin utilizada en este WAR está disponible en

<https://github.com/spring-projects/spring-security-saml/releases/tag/1.0.10.RELEASE> en formato *Gradle*, si lo desea puede acceder al su

través de un correo a ceis.soporte.cehap@juntadeandalucia.es, desde donde le darán más instrucciones.

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	--

código fuente para consultar las dependencias de librerías e incorporarlas en su fichero *pom.xml* o incluso incorporar todo el código fuente del plugin a su proyecto

- Si desea utilizar un certificado no autogenerado por la aplicación para cifrar las peticiones SAML recurra al apartado "8.1 Key management" de la Guía oficial del plugin *spring-security-saml* (<https://docs.spring.io/spring-security-saml/docs/current/reference/html/security.html>).

Los certificados autogenerados por la aplicación son útiles para entornos de desarrollo pero **no deben ser utilizados en entornos productivos**.

En caso de configurar un certificado distinto al autogenerado debe seguir estando registrado en el almacén de certificados configurado en el fichero *securityContext.xml* con el alias *apollo*

- Edite en el fichero *./war/WEB-INF/securityContext.xml* la entrada

```
<security:user name="admin" password="admin" authorities="ROLE_ADMIN"/>
```

y cambie la password por la que se desee.
- Genere el WAR de la aplicación con la nueva configuración, para ello desde el directorio *DIRECTORIO_TRABAJO/war* ejecute:

```
jar cvf ../SpringSAMLIntegration.war
```
- Copie el fichero WAR resultante al servidor de aplicaciones y despliegue la aplicación en su contenedor J2EE.
- Acceda la URL http://nombre_de_la_maquina:puerto/contexto/saml/web/metadata y auténtíquese en el formulario mostrado
- Pulse en el enlace "Metadata Administration" y posteriormente en el botón "Generate new service provider metadata"
- Rellene los siguientes datos en el formulario:



MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE
Guía para la Integración de Aplicaciones en Proxy-Clave

Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)

SAML Login **Metadata Administration**

Metadata generation

Generates new metadata for service provider. Output can be used to configure your securityContext.xml descriptor.

<< Back

Store for the current session:

When set to true the generated metadata will be stored in the local metadata manager. The value will be available only until restart of the application server.

Entity ID:

Entity ID is a unique identifier for an identity or service provider. Value is included in the generated metadata.

Entity base URL:

Base to generate URLs for this server. For example: https://myServer:443/saml-app. The public address your server will be accessed from should be used here.

Entity alias:

Alias is an internal mechanism allowing collocating multiple service providers on one server. When set, alias must be unique.

Signing key:

Key used for digital signatures of SAML messages. Public key will be included in the metadata.



MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE
Guía para la Integración de Aplicaciones en Proxy-Clave

Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)

Encryption key:

apollo (apollo) ▾

Key used for digital encryption of SAML messages. Public key will be included in the metadata.

Signature security profile:

MetalOP ▾

Security profile determines how is trust of digital signatures handled:

- In MetalOP mode certificate is deemed valid when it's declared in the metadata or extended metadata of the peer entity. No validation of the certificate is performed (e.g. revocation) and no certificate chains are evaluated. The value is recommended as a default.
- PKIX profile verifies credentials against a set of trust anchors. Certificates present in the metadata or extended metadata of the peer entity are treated as trust anchors, together with all keys in the keystore. Certificate chains are verified in this mode.

SSL/TLS security profile:

PKIX ▾

SSL/TLS Security profile determines how is trust of peer's SSL/TLS certificate (e.g. during Artifact resolution) handled:

- PKIX profile verifies peer's certificate against a set of trust anchors. All certificates defined in metadata, extended metadata or present in the keystore are considered as trusted anchors (certification authorities) for PKIX validation.
- In MetalOP mode server's SSL/TLS certificate is trusted when it's explicitly declared in metadata or extended metadata of the peer.

SSL/TLS hostname verification:

Standard hostname verifier ▾

Algorithm for verification of match between hostname in URL and hostname in the presented certificate.

SSL/TLS client authentication:

None ▾

Key used to authenticate this instance for SSL/TLS connections.

Sign metadata:

None ▾

If true the generated metadata will be digitally signed using the specified signature key.

Signing algorithm:

None ▾

Algorithm used for creation of digital signature on metadata. Typical values are "http://www.w3.org/2000/09/xmldsig#rsa-sha1", "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" and "http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"



MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE
Guía para la Integración de Aplicaciones en Proxy-Clave

Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)

Sign sent AuthNRequests: ▾

Require signed authentication Assertion: ▾

Require signed LogoutRequest: ▾

Require signed LogoutResponse: ▾

Require signed ArtifactResolve: ▾

	Default	Included	Name
Single sign-on bindings:	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	SSO HTTP-POST
	<input type="radio"/>	<input type="checkbox"/>	SSO Artifact
	<input type="radio"/>	<input type="checkbox"/>	SSO PAOS
	<input type="radio"/>	<input type="checkbox"/>	HoK SSO Artifact
	<input type="radio"/>	<input type="checkbox"/>	HoK SSO HTTP-POST
Supported NameIDs:	<input type="checkbox"/>	<input type="checkbox"/>	E-Mail
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Transient
	<input type="checkbox"/>	<input type="checkbox"/>	Persistent
	<input type="checkbox"/>	<input type="checkbox"/>	Unspecified
	<input type="checkbox"/>	<input type="checkbox"/>	X509 Subject

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

Enable IDP discovery profile:

Discovery profile enables service provider to determine which identity provider should be used for a particular user. Spring Security SAML contains it's own discovery service which presents user with an IDP list to select from.

Custom URL for IDP discovery:

When not set local IDP discovery URL is automatically generated when IDP discovery is enabled.

Include IDP discovery extension in metadata:

10. Tras esto pulse en "Generate metadata" y siga las instrucciones que se indican en la página de resultado para configurar los metadatos y que serán del tipo:

10.1. Store metadata content inside your achive at
`/WEB-INF/classes/metadata/filename.xml`

10.2. Make sure to update your identity provider(s) with the generated metadata.

10.3. Modify bean "metadata" in your securityContext.xml and include content from the configuration above.

11. Básicamente los subapartados del punto anterior indican que lo que hay que hacer es:

11.1. Copiar el contenido del *textarea metadata* y almacenarlo en un fichero xml llamado *filename.xml* dentro de la carpeta `/WEB-INF/classes/metadata` del contenedor J2EE de la aplicación que se desea integrar

11.2. Editar el fichero `/WEB-INF/securityContext.xml` de la aplicación que se ha desplegado he inserte el contenido del segundo *textarea* entre las líneas:

```
<!-- INSERTE A CONTINUACIÓN DE ESTA LINEA LA CONFIGURACIÓN DE LOS METADATOS GENERADOS -->
```

```
<!-- FIN DE METADATOS GENERADOS -->
```

12. Una vez hecho lo anterior, reinicie el servidor de aplicaciones

 Junta de Andalucía	MANTENIMIENTO Y SOPORTE DEL COMPONENTE PROXY-CLAVE Guía para la Integración de Aplicaciones en Proxy-Clave	Servicio de Coordinación y Desarrollo de Sistemas Horizontales (SCDSH), bajo la Dirección General de Transformación Digital (DGTD)
---	---	---

7.4 Verificación de la configuración

Puede probar el funcionamiento de la integración accediendo a la siguiente URL

<http://fqdn:puerto/contexto/saml/login?idp=selectedidp>

Donde debe sustituir:

- fqdn: nombre de dominio asociado a la aplicación integrada.
- puerto: puerto en el que se presta el servicio en la aplicación integrada.
- contexto: contexto en el que se encuentra desplegada la aplicación integrada.
- selectedidp: identificador del proveedor de identidades contra el que se desea realizar la autenticación. Deberá seleccionar su valor de la siguiente tabla en función del entorno y del nivel de calidad en la autenticación que desea utilizar

7.5 Invocar el proceso de autenticación y procesar la respuesta desde su aplicación

Para invocar el proceso de autenticación desde su aplicación basta con que incluya un enlace con una url con el formato descrito en el apartado anterior.

Mediante las siguientes instrucciones pueden recuperarse los atributos relativos a la identidad del usuario autenticado:

```
<%
Authentication authentication = SecurityContextHolder.getContext().getAuthentication();
if (authentication != null) {
    SAMLCredential credential = (SAMLCredential) authentication.getCredentials();
    pageContext.setAttribute("authentication", authentication);
    pageContext.setAttribute("credential", credential);
    pageContext.setAttribute(
        "assertion",
        XMLHelper.nodeToString(
            SAMLUtil.marshallMessage(credential.getAuthenticationAssertion())
        )
    );
}
%>
[.....]
<c:forEach var="attribute" items="${credential.attributes}">
  <tr>
    <td width="200">
      <strong>
        <c:out value="${attribute.name}"/>
      </strong>
      <c:if test="${not empty attribute.friendlyName}">
```

