Integración de aplicaciones SAML 2.0 (ProxyCl@ve)

Manual de integración

Versión: 0100

[Versión del Producto]

HOJA DE CONTROL

Organismo	Sandetel		
Proyecto	ProxyCl@ve		
Entregable	Manual de integración		
Autor	Francisco Rodríguez Corredor		
Aprobado por		**Fecha aprobación**	15/02/2018
		Nº total de páginas	15

REGISTRO DE CAMBIOS

Versión	Causa del cambio	Responsable del cambio	Fecha del cambio
0300	Integración con el plugin spring-security-saml	Francisco Rodríguez Corredor	13/02/2018

CONTROL DE DISTRIBUCIÓN

Nombre y apellidos

ÍNDICE

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 ProxyCl@ve.

1.1 Audiencia

El documento está dirigido a los desarrolladores de aplicaciones J2EE que requieran integrar en sus aplicaciones la autenticación vía ProxyCl@ve.

1.2 Glosario y definiciones

- SSO (Single Sign On). Es un mecanismo de autenticación mediante el cuál 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, auditoria 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.

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, permitiendo que estos puedan identificarse ante la Administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios. Su funcionamiento se encuentra regulado por la Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

Cl@ve complementa los actuales sistemas de acceso mediante DNI-e y certificado electrónico, y está diseñado para ofrecer en un futuro 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 está preparada para incorporar en el futuro, conforme se vayan integrando en el sistema de reconocimiento transfronterizo de identidades electrónicas previsto en la legislación europea, mecanismos de identificación de otros países de la Unión Europea.

Mas información disponible sobre Cl@ve en http://clave.gob.es

2.2 Niveles de calidad proporcionados por Cl@ve.

Nivel calidad	Sistema de identificación	Nivel ENS	Proveedor de servicios de identificación y autenticación	Posibles ejemplos de uso
Nivel 4	• DNIe • Otros certificados reconocidos en soporte Hardware	ALTO	@firma	Acceso a datos de salud
Nivel 3	• Certificados electrónicos SW reconocidos • Claves concertadas de la Seguridad Social combinadas con mensaje SMS	MEDIO/ ALTO	@firma GISS	Acceso a expedientes con información personal con nivel de protección medio
Nivel 2	• PIN24H • Claves concertadas de la Seguridad Social sin SMS	BAJO	AEAT GISS	Acceso a expedientes con información personal con nivel de protección bajo

2.3 ¿Qué es ProxyCl@ve?

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 ProxyCl@ve.

ProxyCl@ve 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.

2.4 Conexión con ProxyCl@ve

Los sistemas de información de la Junta de Andalucía deben utilizar alguno de los protocolos con los que es compatible ProxyCl@ve para conectarse, aunque por norma general se requerirá el uso de SAML 2.

Para la conexión no se proporciona una librería específica para la conexión, ya que existen numerosas implementaciones de SAML 2 en componentes y librerías para cualquier tecnología. Por lo que se presenta en este documento una guía de integración para un sistema bajo tecnología Java utilizando la librería

spring-security-saml a modo de ejemplo. Antes de utilizar esta guía, debe analizarse si es la mejor solución para el sistema a integrar, puesto que el requisito es SAML 2 y no esta librería en concreto. Por lo tanto pueden utilizarse otros frameworks como OIOSAML o módulos ya desarrollados para la interoperación mediante SAML2 con la aplicación que se desea integrar.

3 PROCESO DE INTEGRACIÓN

3.1 Requisitos para la integración con ProxyCl@ve

3.1.1 Requisitos de integración

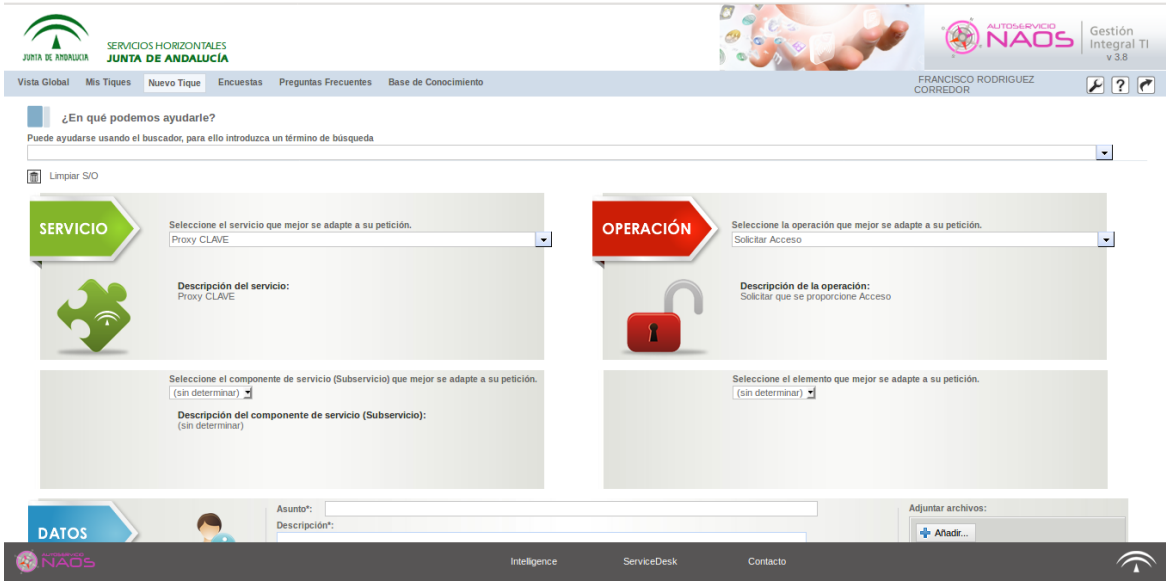
A continuación se enumeran los requisitos para la integración en el SP:

- Entorno JAVA[1]:
  - 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).

1

3.2 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 ticket del servicio “ProxyClave” y operación “Solicitar Acceso”



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 el Portal de Administración Electrónica de la CHAP: https://ws024.juntadeandalucia.es/ae/adminelec/areatecnica/clave

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

   ➔ Descomprima el archivador SAML2-SDK.zip descargado del Portal de Administración Electrónica de la CHAP: https://ws024.juntadeandalucia.es/ae/adminelec/areatecnica/clave

   ➔ Copie el contenido descomprimido en el WAR de la aplicación que desea integrar. Se recomienda realizar el copiado con un comparador de carpetas para resolver los conflictos de librerías que puedan surgir y para facilitar la mezcla de los ficheros web.xml y securityContext.xml que posiblemente ya existan el WAR de su aplicación

   ➔ El código fuente de la versión del plugin utilizada está disponible en https://github.com/spring-projects/spring-security-saml/releases/tag/1.0.2.RELEASE en formato Gradle, si lo desea puede acceder al su 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

3. 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 almacen de certificados configurado en el fichero securityContext.xml con el alias "apollo".

4. Edite en el fichero securityContext.xml la entrada <security:user name="admin" password="admin" authorities="ROLE_ADMIN"/> y cambie la password por la que se desee.

5. Edite el fichero securityContext.xml y descomente la configuración existente entre los comentarios *<!-- COMIENZO DEL BEAN DE CONFIGURACIÓN PARA UTILIZAR ProxyCl@ve -->* y *<!-- FIN DEL BEAN DE CONFIGURACIÓN PARA UTILIZAR ProxyCl@ve -->* .

6. Seleccione el entorno que quiere utilizar para la integración, para ello debe sustituir la cadena "*/metadata/ProxyCl@vePruebasQAA2.xml*" por el valor de la siguiente tabla que se corresponda con el entorno y nivel de calidad de la autenticación deseado:

Nivel de autenticación 2	Entorno de pruebas	/metadata/ProxyCl@vePruebasQAA2.xml
Nivel de autenticación 3	Entorno de pruebas	/metadata/ProxyCl@vePruebasQAA3.xml

Nivel de autenticación 4	Entorno de pruebas	/metadata/ProxyCl@vePruebasQAA4.xml
Nivel de autenticación 2	Entorno de producción	/metadata/ProxyCl@veProQAA2.xml
Nivel de autenticación 3	Entorno de producción	/metadata/ProxyCl@veProQAA3.xml
Nivel de autenticación 4	Entorno de producción	/metadata/ProxyCl@veProQAA4.xml

7. Reinicie el servidor de aplicaciones.
8. Acceda la URL http://<nombre_de_la_maquina>:<puerto>/<contexto>/saml/web/metadata y autentíquese en el formulario mostrado.
9. Pulse en el enlace "*Metadata Administration*" y posteriormente en el botón "*Generate new service provider metadata*".
10. Rellene los siguientes datos en el formulario:
    1. Store for the current session: No-
    2. Entity ID: saml.*<url_de_la_aplicación>* o *nombre identificativo de la misma.*
    3. Entity base URL: verificar que la URL generada tiene el nombre de dominio correcto para la aplicación.
    4. Entity alias: dejar vacío.
    5. Signing key: NO modificar este campo.
    6. Encription key: NO modificar este campo.
    7. Signature Security Profile: PKIX.
    8. Resto de valores: NO modificar este campo.
    9. En "Single sing-on bindings" marcar como "default" la opción "SSO HTTP-POST" y su checkbox es el único que debe quedar marcada en la columna "Included".
    10. En "Supported NameIDs" sólo marcar el checkbox "Transient".
    11. En "Enable IDP discovery profile" seleccionar "No".
11. 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:
    1. Store metadata content inside your achive at /WEB-

INF/classes/metadata/<*filename*>.xml.

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

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

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

    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 WAR de la aplicación que se desea integrar.

    2. Editar el fichero securityContext.xml ubicado en la carpeta WEB-INF del WAR de la aplicación que se desea integrar e incluir en el mismo el contenido del segundo textarea a continuación de la línea "<!--INSERTE A CONTINUACIÓN DE ESTA LÍNEA LA CONFIGURACIÓN DE LOS METADATOS GENERADOS -→".

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

3.3 Verificación de la configuración

Puede probar el funcionamiento de la integración accediendo a la siguiente URL: https://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:

Proxy Clave – QAA2	Entorno de pruebas	https://ws050.juntadeandalucia.es/ProxyCl@vepru/metadata/federation/production/ClaveSEQAA2
Proxy Clave – QAA3	Entorno de pruebas	https://ws050.juntadeandalucia.es/ProxyCl@vepru/metadata/federation/production/ClaveSEQAA3

Proxy Clave – QAA4	Entorno de pruebas	https://ws050.juntadeandalucia.es/ProxyCl@vepru/metadata/federation/production/ClaveSEQAA4
Proxy Clave – QAA2	Entorno de producción	https://ws050.juntadeandalucia.es/ProxyCl@veexp/metadata/federation/production/ClaveSEQAA2
Proxy Clave – QAA3	Entorno de producción	https://ws050.juntadeandalucia.es/ProxyCl@veexp/metadata/federation/production/ClaveSEQAA3
Proxy Clave – QAA4	Entorno de producción	https://ws050.juntadeandalucia.es/ProxyCl@veexp/metadata/federation/production/ClaveSEQAA4

3.4 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="${not empty
attribute.friendlyName}"> (<c:out value="${attribute.friendlyName}"/>)</c:if>
        </td>
        <td>
          <%
            Attribute a = (Attribute) pageContext.getAttribute("attribute");
            String[] attributeValues = credential.getAttributeAsStringArray(a.getName());
```

```
            pageContext.setAttribute("attributeValues", attributeValues);
          %>
          <c:forEach var="attributeValue" items="${attributeValues}">
            <c:out value="${attributeValue}"/> 
          </c:forEach>
        </td>
      </tr>
    </c:forEach>
```

Para más detalles consulte el fichero "*MyPage.jsp*" incluido en el fichero SAML2-SDK.zip

Una vez la aplicación ha pasado las pruebas pertinentes, se recomienda eliminar los siguientes ficheros del WAR que finalmente quedará desplegado: error.jsp, index.jsp, logout.jsp y MyPage.jsp

3.5 Publicación de aplicaciones para el acceso desde dentro y fuera de Red Corporativa de la Junta de Andalucía

Si se desea dar de alta una aplicación en ProxyCl@ve que será publicada tanto dentro como fuera de RCJA es necesario configurar en ella el protocolo SAML utilizando la URL de acceso externo de RCJA de forma que los metadatos generados expresen esta URL.

Una vez hecho esto los responsables de la aplicación integrada deberán solicitar a su Servicio de Producción (o similar) que los accesos internos (realizados desde dentro de RCJA) se atiendan siempre como Proxy Inverso sin realizar redirecciones al dominio interno.

3.6 Obtener datos adicionales del certificado electrónico utilizado para la autenticación

Si desea obtener **datos adicionales del certificado electrónico** utilizado en la autenticación de usuario puede hacer uso del atributo "**afirmaResponse**" contenido en el listado de atributos que se devuelve a la aplicación integrada.

El atributo "afirmaResponse" está **codificado en Base64** por lo que la aplicación integrada deberá decodificarlo para poder procesarlo. Este atributo, una vez decodificado, representa una cadena en formato XML del que pueden obtenerse todos los datos extraídos del certificado digital en el proceso de autenticación de usuario. **Utilizando estos datos podrá comprobar, entre otras cosas, si el certificado utilizado en la autenticación es de persona física o de representante de persona jurídica y obtener también información sobre esta identidad.**

4 Aplicación de ejemplo distribuida ya configurada

Para facilitar la integración se distribuye una aplicación de pruebas ya configurada y operativa contra el entorno de pruebas de ProxyCl@ve. Puede descargar este WAR del Portal de Administración Electrónica de la CHAP: https://ws024.juntadeandalucia.es/ae/adminelec/areatecnica/clave

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 ProxyCl@ve accediendo en un navegador web a la URL http://samlintegration.sandetel.int:8080/SpringSAMLIntegrationExample/MyLogin.jsp y pulsar en el enlace "Autenticación contra ProxyCl@ve en el entorno de pruebas".