Plataforma de Identificación, Autenticación y Firma

Documento de integración con la plataforma de identificación y autenticación para proveedores de servicios

Versión 31/12/2015

Madrid, 31 de diciembre de 2015

Elaborado por la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

© Ministerio de Hacienda y Administraciones Públicas

CONTROL DE CAMBIOS

Versión	Fecha	Descripción
01-00	30/05/2014	Creación del documento
01-01	09/06/2014	Modificaciones en la terminología usada para describir a los actores
01-02	31/03/2015	Añadidos y especificados los nuevos atributos y modificaciones del sistema actual
01-03	11/05/2015	Correcciones y ampliación en la especificación de los nuevos atributos
01-04	16/10/2015	Actualizada para explicar nuevas funcionalidades añadidas a la plataforma
01-05	31/12/2015	Se ha agregado nueva información y se han ampliado otras.

ÍNDICE

1. INTRODUCCIÓN 4

1.1 Objetivo del documento 4

1.2 El proyecto Cl@ve 4

1.3 Esquema general de la solución 4

1.4 Como se consigue la interoperabilidad 5

1.5 Datos disponibles 6

1.6 Nivel de calidad de la autenticación (QAA) 9

2. REQUISITOS TÉCNICOS DE INTEGRACIÓN 11

2.1 Esquema general de integración 11

2.2 Alta de proveedores de servicios en el sistema 12

3. INTERACCIÓN CON EL USUARIO 13

3.1 Esquema general de interacción 13

3.2 Enviar una petición a Cl@ve 14

3.3 Validar una respuesta SAML llegada desde un ciudadano 14

3.4 Interpretar la respuesta obtenida tras la validación del token 14

4. TIPO DE REGISTRO 17

5. FORZAR REAUTENTICACIÓN DEL USUARIO ¡ERROR! MARCADOR NO DEFINIDO.

6. FUNCIONALIDAD DE SEPARACIÓN DE APELLIDOS 19

7. IDENTIFICACIÓN CON CERTIFICADO DE PERSONA JURÍDICA 20

1. INTRODUCCIÓN

1.1 Objetivo del documento

El presente documento tiene como finalidad proporcionar una visión general de cómo se realiza la integración de los servicios de administración electrónica proporcionados por un determinado organismo, con la plataforma común de identificación y autenticación desarrollada en el proyecto Cl@ve.

1.2 El proyecto Cl@ve

El objetivo del proyecto Cl@ve es el de proporcionar una infraestructura para todas las Administraciones Públicas que provea de unos medios comunes para la autenticación y firma electrónica de los ciudadanos en los procedimientos de administración electrónica.

El diseño de dicha infraestructura se ha realizado basándose en los siguientes principios:

- Facilidad de uso para el ciudadano y homogeneidad en su relación con las Administraciones Públicas.
- Máxima seguridad en los sistemas de control de acceso y en la protección de las claves de firma de los ciudadanos.
- Alineamiento con los estándares internacionales y normas europeas, con el propósito final de que las firmas realizadas con este sistema puedan considerarse como firmas reconocidas.

El proyecto establece dos fases; una primera fase orientada a la provisión de mecanismos de identificación y autenticación, y una segunda fase, que se basa en lo desarrollado en la fase anterior, dedicada a los mecanismos de firma.

El presente documento se centra en la primera de esas fases, la relacionada con los mecanismos de identificación y autenticación.

1.3 Esquema general de la solución

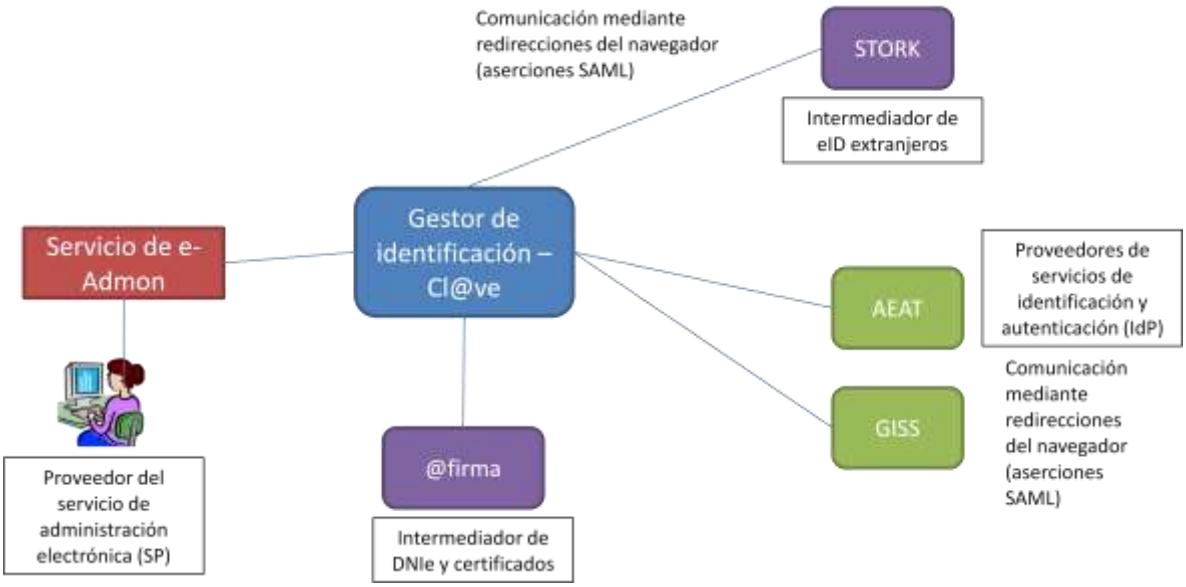
Como se ha comentado, el proyecto provee una plataforma común de identificación y autenticación, que puede ser utilizada por los servicios de administración electrónica para delegar el proceso de identificación y autenticación de los ciudadanos, y que además permite a estos elegir, de entre aquellos medios de identificación disponibles que se ajustan a los requisitos de seguridad establecidos por el servicio, el medio de identificación que les resulte más conveniente.

El esquema general de la solución se describe en el gráfico siguiente, donde se identifica a los diferentes actores que participan en la misma:

- Proveedor de servicio de administración electrónica (SP): Entidad que proporciona servicios de administración electrónica y que utiliza la plataforma para la identificación y autenticación de ciudadanos.
- Proveedor de servicios de identificación y autenticación (IdP): Entidad que proporciona mecanismos de identificación y autenticación de los ciudadanos para ser utilizados como medios comunes por otras entidades. En el lanzamiento del proyecto únicamente se contempla la existencia de dos proveedores de servicios de identificación y autenticación, la Agencia Estatal de Administración Tributaria (AEAT), con su sistema de identificación PIN24H, y la Gerencia de Informática de la Seguridad Social (GISS), con su sistema de usuario y contraseña reforzado con claves de un solo uso por SMS,

aunque el diseño de la solución contempla la extensión a otros potenciales proveedores de servicios de identificación y autenticación.

- Gestor de identificación – Cl@ve: Plataforma común de identificación y autenticación, que posibilita el acceso por parte del SP a los IdP y a los sistemas intermediadores de identificación @firma y STORK.
- @firma: Suite de productos a disposición de las Administraciones Públicas que permite a los servicios de administración electrónica gestionar la identificación y firma mediante certificados electrónicos, entre ellos el DNIe.
- STORK: Plataforma de interoperabilidad que permite el reconocimiento transfronterizo de identidades electrónicas, desarrollada durante la ejecución de los proyectos STORK y STORK 2.0[1], y que servirá de base para la construcción del futuro sistema de reconocimiento de identidades electrónicas previsto en reglamento europeo de identificación electrónica y servicios de confianza (reglamento eIDAS).



Tal como se observa en el gráfico, el SP únicamente tiene que integrarse con el Gestor de Identificación (Cl@ve), encargándose este de establecer las relaciones pertinentes con los distintos sistemas de identificación. Para ello se establecen círculos de confianza entre los distintos actores que se integran entre sí, soportadas por el intercambio de certificados electrónicos y el envío de mensajes firmados entre ellos. Se trata, en definitiva, de crear una federación de sistemas de identificación electrónica, a los que se accede a través de un componente común.

1.4 Como se consigue la interoperabilidad

La creación de una federación de sistemas de identificación electrónica ha sido precisamente el objetivo del proyecto STORK. Para lograr la consecución de ese objetivo, varios miembros de la UE que participaron en el proyecto, entre ellos España, se han puesto de acuerdo en la especificación de una "capa de interoperabilidad" con la que los datos personales de los usuarios puedan intercambiarse entre estos países. Es por ello que la solución desarrollada

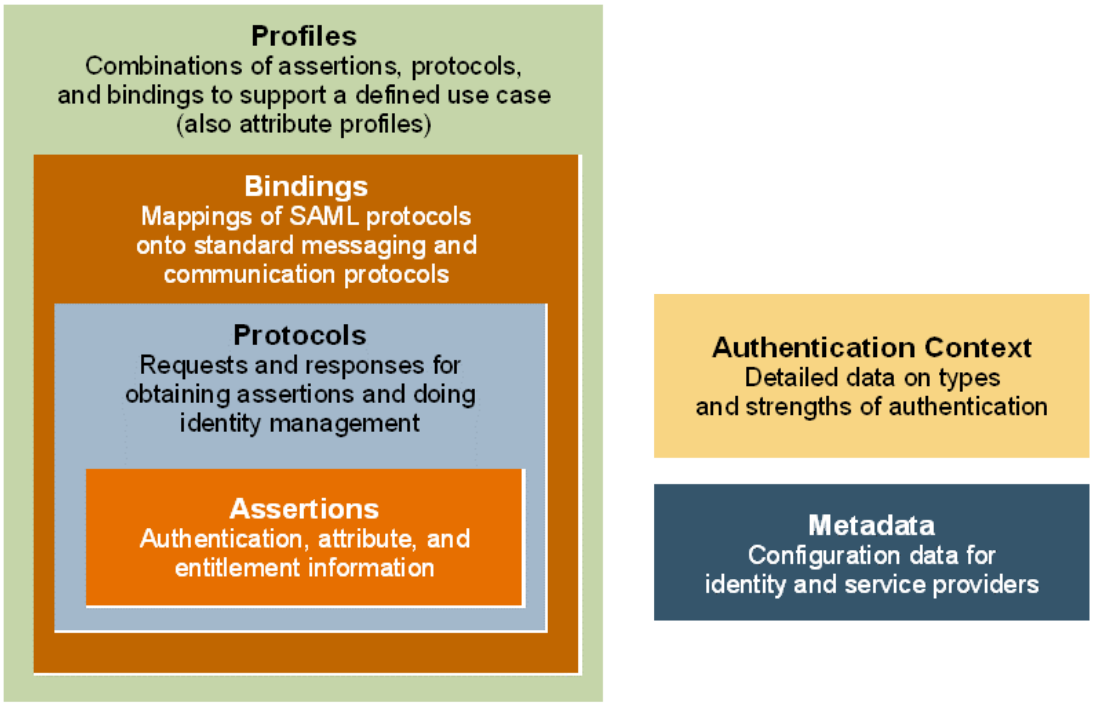
[1] *Se puede obtener más información de ambos proyectos en sus páginas web: http://www.eid-stork.eu/ y http://www.eid-stork2.eu/*

para Cl@ve se basa esencialmente en los resultados obtenidos por STORK, adaptándolos convenientemente a las necesidades del proyecto.

La interoperabilidad en STORK se consigue con la utilización del estándar SAML 2.0. SAML ha sido desarrollado por OASIS para ser usado en sistemas de federación de identidades, y en la actualidad es una tecnología madura que se utiliza ampliamente. Se trata de un framework basado en XML para reunir y organizar información de seguridad e identidad, e intercambiarla entre diferentes dominios, integrando tecnologías de seguridad ya existentes en lugar de inventar nuevas tecnologías. Sus perfiles ofrecen interoperabilidad para una variedad de casos de uso, pero pueden ser extendidos para casos adicionales, como así ha sido en STORK, que ha definido un perfil propio para satisfacer las necesidades derivadas del proyecto.

El significado de SAML es Security Assertion Markup Language, es decir, lenguaje de marcas para aserciones de seguridad, y como tal, permite gestionar el intercambio de aserciones sobre sujetos, relativas a procesos de gestión de la autenticación y derechos de acceso, y a la transferencia de atributos.

SAML 2.0 es la evolución más reciente de SAML e integra, además de SAML 1.0, las evoluciones de otras iniciativas de federación de identidades, Liberty Alliance y Shibboleth. Sus componentes fundamentales se describen en el gráfico que figura a continuación.



Dentro de los bindings, SAML 2.0 establece distintos tipos. STORK, y en consecuencia Cl@ve, utiliza dos de ellos, HTTP Redirect (GET) Binding y HTTP POST Binding, puesto que todas las interacciones con el sistema pasan a través del navegador del usuario que se comunica mediante HTTPS con los diferentes actores.

1.5 Datos disponibles

Las especificaciones de interoperabilidad definidas en STORK, y en las que se basa Cl@ve, contemplan no solamente el intercambio de información para la identificación y autenticación del usuario, sino también el intercambio de atributos. Es por ello que el modelo de datos

manejado por STORK (en STORK 2.0 se prevé ampliar el número de atributos disponibles) contempla los siguientes datos asociados a la identidad:

Atributo personal	Valores y comentario
eIdentifier	Identificador nacional de otros países.
givenName	Nombre del ciudadano
surname	Apellido(s) del ciudadano. inheritedFamilyName / adoptedFamilyName (cada país tendrá en el surname uno de estos casos como el apellido comúnmente usado)
inheritedFamilyName	Apellido de nacimiento
adoptedFamilyName	Apellido adoptado (para casos en que el apellido cambia al contraer matrimonio, por ejemplo)
gender	Género
nationalityCode	Código del país de nacionalidad
maritalStatus	Estado civil
dateOfBirth	Fecha de nacimiento
countryCodeOfBirth	Código del país de nacimiento
age	Edad
isAgeOver	¿Es mayor de X años?
textResidenceAddress	Dirección en varias líneas de texto de la dirección postal.
canonicalResidenceAddress	Dirección en formato canónico
residencePermit	Permiso de residencia
eMail	Correo electrónico
title	Título
pseudonym	Seudónimo
citizenQAAlevel	Nivel de calidad con el que se autenticó el usuario.
fiscalNumber	Número fiscal

En el caso de Cl@ve, de todos ellos solamente se utilizarán aquellos que pueden proporcionar los proveedores de servicios de identificación y autenticación integrados en la plataforma, que en principio son los siguientes:

- **eIdentifier**, que se asociará en un principio al DNI / NIE del ciudadano (ya que inicialmente el registro en el sistema exigirá el uso de estos identificadores), pero que en el futuro puede vincularse a otro tipo de identificador, como identificadores nacionales de otros países o número de pasaporte.
- **givenName,** que se vinculará al nombre del ciudadano[2].
- **surname,** que se asociará a los dos apellidos del ciudadano, en el caso de españoles vinculado al **inheritedFamilyName**
- **citizenQAAlevel,** que representa el nivel de calidad de la autenticación (QAA)

Aparte de los atributos heredados de STORK 2.0, el sistema ha incluido los siguientes que se describen a continuación:

- **isdnie**, que permitirá conocer si la identificación se ha realizado con un DNI Electrónico (DNIe).
- **allowLegalPerson**, que habilitará la posibilidad al usuario de autenticarse empleando un certificado de persona jurídica. Este atributo se envía como parámetro vía HTTP-POST, de la misma forma que es enviado el atributo idplist.
- **isLegalPerson**, que permitirá conocer si la identificación se ha realizado empleando un certificado de persona jurídica. Este atributo únicamente estará disponible si el proveedor de servicio ha permitido este tipo de certificado mediante **allowLegalPerson**. Este atributo se recibe como respuesta vía HTTP-POST.

Los atributos referentes al uso del DNIe y certificados de persona jurídica son válidos exclusivamente en @Firma.

Además de los datos personales anteriores, el sistema permite gestionar información adicional de interés para el proveedor de servicio de administración electrónica y el proveedor de servicios de identificación y autenticación:

- En el caso del proveedor del servicio de administración electrónica, este define
  - Qué proveedores de servicios de identificación y autenticación deben ser intermediados por Cl@ve.
  - El nivel de calidad de la credencial (QAA) que se debe usar para autenticarse en su servicio.
  - Permitir o denegar la autenticación si se usa un certificado de persona jurídica.

  Y recibe como respuesta
  - El resultado del proceso de autenticación (OK, KO)
  - Datos de identidad: identificador (DNI), nombre y apellidos
  - Datos del proceso de autenticación: QAA, proveedor de servicios de identificación y autenticación, tipo de certificado (persona jurídica o no) y su OID.

[2] *En función de la disponibilidad del servicio SVDI de la Dirección General de la Policía para su integración con las aplicaciones de registro, del que los IdP obtienen los datos de identidad, es posible que haya un periodo transitorio en el que en el campo givenName se envíen conjuntamente el nombre y los dos apellidos..*

- En el caso del proveedor de servicios de identificación y autenticación, recibe datos de identificación del proveedor del servicio de administración electrónica: País, sector, proveedor de servicio, aplicación del proveedor

1.6 Nivel de calidad de la autenticación (QAA)

Tal como se ha mencionado, el proyecto Cl@ve contempla la utilización de varios mecanismos de identificación. La existencia de esta diversidad se justifica por la necesidad de conciliar la seguridad en la identificación con la facilidad de uso. Lo que se pretende es que, de acuerdo con el principio de proporcionalidad, los servicios electrónicos de la administración puedan decidir el nivel de seguridad en la identificación que requieren, conforme a la clasificación del sistema definida en el Esquema Nacional de Seguridad (ENS). Y que el usuario/ciudadano pueda escoger de entre aquellos mecanismos con el nivel de seguridad requerido los que le resulten más convenientes, bajo el principio de que se permitirá el acceso siempre que el nivel de seguridad del mecanismo de identificación usado por el ciudadano sea igual o superior al exigido.

Para la gestión de estos niveles de seguridad, Cl@ve se apoya de nuevo en los desarrollos realizados en STORK. En concreto, utiliza el marco conceptual de STORK, basado en el modelo de QAA (Quality of Authentication Assurance) de calidad en el aseguramiento de la autenticación[3]. Dicho marco de niveles de aseguramiento de la autenticación es la base que toma el reglamento eIDAS, que establece que se deberán tener en cuenta los niveles 2, 3 y 4 de STORK para definir las características de los niveles de aseguramiento bajo, sustancial y alto previstos en el reglamento.

El modelo QAA de STORK establece cuatro niveles, que se mencionan a continuación junto con una descripción genérica de su significado.

- Nivel 1: Ningún o mínimo aseguramiento. No hay ninguna, o hay una confianza mínima, en la identidad alegada. Las credenciales de identidad se aceptan sin ningún tipo de verificación.
- Nivel 2: Bajo aseguramiento. Hay una validación de que las identidades corresponden a personas reales, y los tokens de identificación se entregan con ciertas garantías
- Nivel 3: Aseguramiento sustancial. El registro de la identidad se realiza con métodos que proporcionan una alta certeza sobre la identidad de la persona que la declara, y las credenciales electrónicas son robustas.
- Nivel 4: Alto aseguramiento. Se requiere un registro presencial al menos una vez, y la credencial electrónica se entrega como certificado hardware criptográfico.

Para la asignación de un determinado nivel a un mecanismo de identificación, el modelo establece una serie de requisitos asociados a 5 factores, de forma que el nivel global de QAA se determina a partir de la combinación de los niveles individuales de cada factor, usando el principio de que el nivel global es igual al nivel más bajo de todos los factores que intervienen.

Estos 5 factores se agrupan en dos categorías: factores asociados al proceso de registro y entrega de la credencial, y factores asociados al proceso de autenticación electrónica con dicha credencial.

Los factores asociados al proceso de registro son:

[3] *El modelo QAA completo de STORK se puede consultar en el siguiente enlace: https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577*

- Nivel de calidad del proceso de identificación durante el registro (ID): Este nivel depende de la presencia física o no de la persona en el momento de la identificación, la calidad de la aserción sobre la identidad (si los datos identifican de forma única a la persona y pueden contrastarse en un registro oficial o no) y la validación de la aserción (si se presenta un documento oficial que puede ser contrastado, un certificado digital, etc.).
- Nivel de calidad del proceso de entrega de la credencial (IC): Este nivel depende de si la credencial se entrega de manera presencial, se envía por correo electrónico o por correo postal, se descarga de una página web, etc.
- Nivel de calidad de la entidad que entrega la credencial (IE): Depende de la naturaleza del emisor (si es una entidad gubernamental o privada, y en este caso, del tipo de supervisión) y de los procedimientos para la retención de información acerca del registro para auditoría.

Respecto a los factores asociados al proceso de autenticación electrónica, estos son:

- El tipo y la robustez de la credencial electrónica (RC): Usuario y contraseña, lista de contraseñas, dispositivos de contraseñas de un solo uso, certificados electrónicos, etc.
- Seguridad del mecanismo de autenticación (AM): Relacionado con la protección que ofrece frente a los ataques de suplantación de identidad.

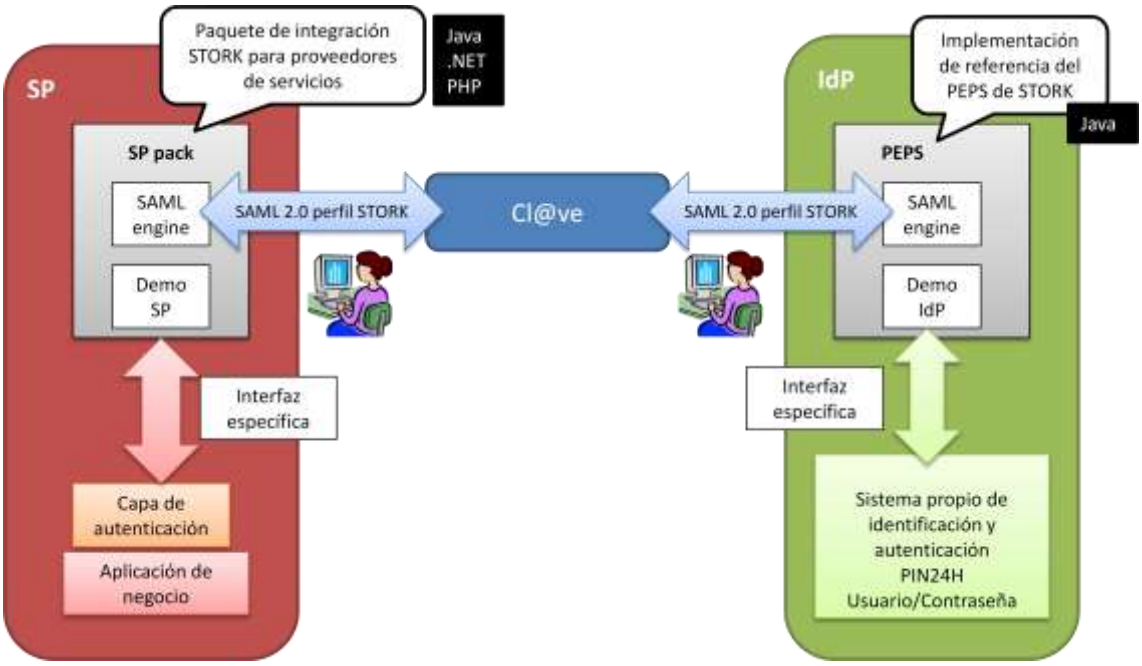
El sistema Cl@ve manejará sistemas de identificación de los niveles 2, 3 y 4 de QAA de STORK. Aunque la clasificación de los sistemas de identificación gestionados no se ha terminado de definir completamente, la asignación de niveles con la que se trabaja en la actualidad es la siguiente:

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. REQUISITOS TÉCNICOS DE INTEGRACIÓN

2.1 Esquema general de integración

Tal como se ha mencionado, el proyecto Cl@ve se basa en la utilización del perfil SAML 2.0 definido por STORK. Este perfil se utilizará tanto para la integración entre Cl@ve y el proveedor de servicios de administración electrónica, como para la integración entre Cl@ve y el proveedor de servicios de identificación y autenticación, tal como se observa en la siguiente figura:



En la figura anterior aparecen también las utilidades que se desarrollarán en el proyecto, a partir del código obtenido en STORK, para facilitar la integración de SP e IdP en el sistema.

En el caso particular de los proveedores de servicios de administración electrónica, para interactuar con la plataforma Cl@ve, un SP debe tener por tanto la capacidad de crear tokens SAML. Para la generación de estos tokens, el paquete de integración para SP prevé el suministro de un motor SAML, el STORKSAMLEngine, que debe ser integrado en la capa de autenticación de la lógica de negocio del SP.

El paquete de integración se completa con un Servidor de Aplicaciones Demo (SP-DEMO) que integra el motor de creación de tokens SAML y facilita el desarrollo de los métodos de invocación de las funciones de envío y recepción de tokens del motor SAML.

Este paquete de integración está previsto que se proporcione para su utilización en tres diferentes plataformas tecnológicas de uso habitual en administración electrónica: Java, .NET y PHP.

En cuanto a los requisitos técnicos para utilizar el paquete de integración estos son:

- Para el Servidor de Aplicaciones Demo:
  - Tomcat 5.5 / JBoss 5 ó 7 / GlassFish versión 3
  - Instalación de la versión 1.6+ del SDK de Java.
  - Conexión a Internet.

- Para el Motor STORKSAMLEngine:
  - Tomcat 5.5 / JBoss 5 ó 7 / GlassFish versión 3.
  - Instalación de la versión 1.6+ del SDK de Java.
  - En el caso de .Net, se requiere la versión 4.5+.
  - En el caso de PHP se requiere la versión 5.5+.
  - Librería OpenSAML.
  - Instalación de un Certificado para firmar los token SAML.
  - Certificados públicos en los que confiar, de los otros sistemas que intervienen en el proceso.
  - En caso de utilizar claves largas, es necesario instalar el paquete de desbloqueo de Java, llamado JCE (Java Cryptography Extension).

Una vez configurados los entornos se tendrán dos ficheros de configuración: los que afectan al SP-DEMO (fichero sp.properties) y los que afectan al STORKSAMLEngine (fichero SignModuleSP.xml), que habrá que modificar con los parámetros adecuados para el servicio en cuestión.

El paquete de integración incluye también el código fuente de la aplicación, para su utilización en el entorno de desarrollo. En el caso de Java, se incluye un fichero POM para maven.

2.2 Alta de proveedores de servicios en el sistema

Como se ha comentado anteriormente, el funcionamiento del sistema se basa en el establecimiento de un círculo de confianza entre el proveedor de servicios de administración electrónica y la plataforma Cl@ve. Para ello será necesario que el proveedor de servicios obtenga un certificado para la firma de los token SAML que intercambiará con Cl@ve, cuya parte pública remitirá a la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (DGMAPIAE), como gestora de la plataforma de identificación y autenticación. En la petición se adjuntará el nombre de la institución, nombre e email del responsable del servicio y del responsable técnico.

Por su parte, la DGMAPIAE proporcionará al proveedor de servicios el identificador SP_ID, que le servirá para identificarse en el sistema (y que deberá usar en los ficheros de configuración del STORKSAMLEngine), así como la parte pública del certificado usado por Cl@ve para la firma de los token SAML intercambiados con el SP.

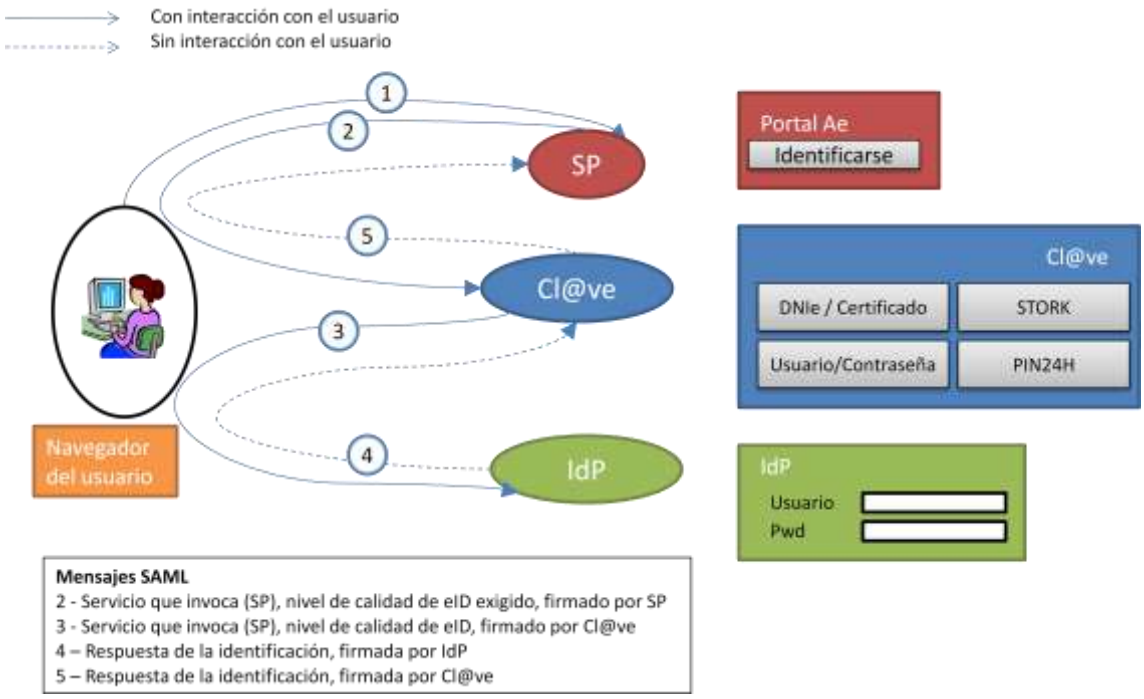
Adicionalmente, la DGMAPIAE proporcionará las URL a las cuales se debe enviar las peticiones del entorno de pruebas, para que el SP pueda realizar todas las pruebas de conexión necesarias antes del paso a producción, cuya URL también se facilitará.

3. INTERACCIÓN CON EL USUARIO

3.1 Esquema general de interacción

Toda comunicación con un componente de la plataforma Cl@ve se realiza a través del intercambio de tokens que pasan previamente por el navegador del ciudadano. De esta manera cada proveedor de servicios de identificación y autenticación sólo responde al ciudadano desde el que ha recibido una petición de autenticación.

Esta comunicación se refleja en el gráfico siguiente:



En este caso genérico vemos que el SP no interactúa directamente con ningún IdP, sino que lo hace exclusivamente a través del navegador del ciudadano.

Los pasos de la interacción son los siguientes:

1. El ciudadano accede a un servicio de administración electrónica integrado con Cl@ve que requiere que se identifique.
2. El ciudadano es redirigido a Cl@ve, que le presenta una pantalla en la que debe seleccionar el método de identificación que quiere utilizar. Las opciones activas en la pantalla vienen condicionadas por los parámetros que el SP ha indicado en el mensaje que ha enviado a Cl@ve relativos a los IdP y niveles QAA permitidos.
3. El ciudadano selecciona el método de identificación y es redirigido al IdP correspondiente.
4. El ciudadano se autentica en el IdP seleccionado y es redirigido de nuevo a Cl@ve
5. De forma transparente, sin que sea necesario interacción, el ciudadano es redirigido de nuevo al SP.

En la información que viaja a través del ciudadano siempre existe un token SAML, y es en la creación y validación de esos tokens donde se produce la comunicación indirecta de los distintos componentes del sistema.

Todos los tokens van firmados por la entidad emisora y el que esa firma sea validada por el componente destinatario depende de que exista confianza entre los certificados de firma de ambos componentes. Así pues, en el almacén de certificados que maneja el STORKSAMLEngine del SP siempre debe estar incluido el de Cl@ve, y el certificado con el que firma el SP también debe ser conocido por Cl@ve.

3.2 Enviar una petición a Cl@ve

Para generar una petición de autenticación desde el SP (token SAML que es enviado al browser del ciudadano para ser redirigido a Cl@ve) son suficientes los siguientes requisitos:

- Haber sido dado de Alta como proveedor de servicios de administración electrónica con acceso a la plataforma.
- Tener integrado el componente STORKSAMLEngine en la lógica de negocio
- Haber configurado correctamente los ficheros de configuración del STORKSAMLEngine incluyendo el certificado de firma

Una vez cumplidos todos estos requisitos desde la lógica de negocio del SP se utilizará el interfaz del STORKSAMLEngine: **generateSTORKAuthnRequest**.

Adicionalmente, y fuera del token SAML, pero dentro del mensaje HTTP, el SP tiene la opción de incluir parámetros vía POST donde podrá indicar los proveedores de servicios de identificación y autenticación excluidos en su servicio. Para ello, hay que enviar un parámetro con nombre “excludedIdPList” que contenga los valores “aFirma", "Stork”, "SS” y/o "AEAT" (separados por comas). Por compatibilidad hacia atrás la pasarela también entiende los valores “PIN24H”, “AFIRMA” y “SEGSOC”. En caso de no querer aplicar este filtro se debe enviar un valor “none” o vacío.

Es posible forzar un IdP en concreto por parte del SP enviando de forma análoga a la lista de excluidos, un parámetro llamado “forcedIdP” que contenga el identificador del IdP que se va a forzar. Éste parámetro tiene prioridad sobre la lista de excluidos.

3.3 Validar una respuesta SAML llegada desde un ciudadano

Para validar una respuesta SAML son suficientes los siguientes requisitos:

- Haber enviado una petición SAML (SAML Authentication Request) a la que esa respuesta se refiere.
- Tener integrado el componente STORKSAMLEngine en la lógica de negocio
- Haber configurado correctamente los ficheros de configuración del STORKSAMLEngine incluyendo el certificado público de Cl@ve (con el que irá firmada la respuesta que ha llegado del ciudadano)

Una vez cumplidos todos estos requisitos desde la lógica de negocio del SP se utilizará el interfaz del STORKSAMLEngine: **validateSTORKAuthnResponse**.

3.4 Interpretar la respuesta obtenida tras la validación del token

Tras validar una respuesta SAML se ha obtenido un objeto STORKAuthnResponse.

En este objeto los datos importantes a tener en cuenta son:

- statusCode → Si la autenticación se produjo positivamente este campo tendrá el valor “success”. En caso contrario detallará el tipo de error producido.
- inResponseTo → ID de la petición a la que se contesta.

- Issuer → IdP que provee la identidad del ciudadano. Puede valer lo siguiente:
  - AFIRMA .- Autenticación mediante DNIe/certificado.
  - STORK-XX .- Autenticación a nivel europeo. XX es el código del país.
  - SEGSOC.- Autenticación mediante clave permanente.
  - PIN24H.- Autenticación mediante Cl@ve PIN
- personalAttributeList → Contiene una lista con todos los atributos personales obtenidos y sus correspondientes valores.
  - name → nombre del atributo
  - value → valor del atributo
  - status → Available (atributo disponible) / notAvailable (atributo no disponible)

En cuanto a los atributos personales los valores que se pueden obtener, para los atributos manejados inicialmente en el proyecto, son:

Atributo personal	Tipo	Valores y comentario
eIdentifier	String	CP/CP/xxxxxxxxxx…. (CP=Código de país, el primero será el del país de origen del identificador, el segundo el del país de destino) En el caso de identificación de ciudadanos españoles o extranjeros residentes, el formato será por tanto ES/ES/[DNI o NIE]
givenName	String	
surname	String	
inheritedFamilyName	String	
adoptedFamilyName	String	
afirmaResponse	String	
isdnie	String	[true,false]
registerType	Number	[0,1,2,3,4]
citizenQAAlevel	Number	[2,3,4][4]

No obstante, puesto que la interfaz de STORK lo soporta, podrían estar disponibles también el resto de atributos personales previstos en STORK, en el caso de que los proveedores de

[4] *Aunque el nivel 1 está definido en el modelo QAA de STORK, y está soportado por la interfaz, este valor no se utilizará en Cl@ve al no contemplarse proveedores de servicios de identificación y autenticación que autentiquen con credenciales de ese nivel.*

servicios de identificación y autenticación (o potenciales proveedores de atributos con los que se integrase la plataforma) pudieran proporcionarlos.

4. TIPO DE REGISTRO

Actualmente, para utilizar los proveedores de identidad de la agencia tributaria y seguridad social es necesario que el ciudadano se dé de alta previamente. Este proceso de alta puede ser realizado de varias maneras, cada cual con sus peculiaridades y su nivel de seguridad. Se ha ampliado el esquema SAML para que un proveedor de servicios pueda preguntar al proveedor de identidad sobre el tipo de registro que hizo el ciudadano, y para que el SP marque un requisito de seguridad sobre el tipo de registro al IdP, de forma análoga a como se hace con el nivel QAA.

Para ello, se ha creado el atributo “registerType”, cuyo valor puede ser un número entero. Los valores son los siguientes:

- Tipo 0 Sin datos
- Tipo 1 Presencial
- Tipo 2 Carta invitación
- Tipo 3 Certificado
- Tipo 4 Presencial + certificado

5. SINGLE SIGN ON

La pasarela cuenta con un sistema de Single Sign On para que el usuario no tenga que re-autenticarse continuamente si va a realizar varias peticiones en un breve lapso de tiempo. Actualmente, si el tiempo entre peticiones es inferior a una hora el sistema reutilizará los datos que tiene almacenados en sesión relativos a ese usuario en lugar de obligarle a repetir todo el proceso de identificación.

En todo caso el sistema Cl@ve solicitará una nueva autenticación cuando se requiera un nivel QAA superior al nivel para el que el usuario ha sido autenticado previamente o cuando el SP fuerce un Proveedor de Identificación diferente.

Integración de la desconexión

El proceso de SSO es automático por parte de la pasarela, el SP no tiene que hacer nada para disponer de SSO. Sin embargo, el SP debe integrar el botón de desconexión o logout de su página con la desconexión del sistema cl@ve para cerrar la sesión en ambos entornos. Cerrar la sesión solamente en la página del SP realmente no desconecta al usuario ya que la conexión es automática a través de la pasarela Cl@ve y en ésta la sesión seguiría abierta. En el SP Demo se ofrece un ejemplo de cómo integrar la desconexión de la página con la desconexión en Cl@ve.

Forzar la autenticación

En caso de que el Proveedor de Servicios quiera obligar al usuario a que se identifique siguiendo el proceso completo al margen de que ya tuviese una sesión previa (y vigente) en la pasarela, el SP debe mandar el atributo “forceAuthN” con el valor “true” en la SAMLRequest que se le envía a la pasarela. De esta forma la pasarela ignorará la sesión previa del usuario y le forzará a realizar el proceso de autenticación como si fuese la primera vez que accede a la plataforma.

Forzar la autenticación tiene el efecto de reiniciar la sesión SSO. Ello significa que para los SP que no fuercen la autenticación la sesión SSO seguirá disponible.

6. FUNCIONALIDAD DE SEPARACIÓN DE APELLIDOS

Esta funcionalidad permite al SP conocer cuál es el primer apellido y cuál es el segundo (en caso de que el usuario tenga segundo apellido) a partir de la respuesta del IdP.

Los SP en caso de que quieran ser capaces de distinguir el primer apellido del segundo tendrán que indicarlo explícitamente en la petición SAML que envíen a la pasarela. Para ello lo único que tendrán que hacer será solicitar (adicionalmente al resto de atributos) el atributo “inheritedFamilyName”, que puede ser opcional u obligatorio, y el “surname”, para poder posteriormente realizar la separación de los apellidos. La respuesta que le llegará de vuelta al SP contendrá en el atributo “inheritedFamilyName” el primer apellido del usuario autenticado, y en el atributo “surname” estarán los dos apellidos. De esta forma, al procesar la respuesta el SP sólo tendrá que comparar esos dos atributos para saber cuál es el segundo apellido (el primero lo puede obtener directamente del valor del atributo “inheritedFamilyName”).

En los casos en los que el usuario sólo tenga un apellido (por ejemplo en el caso de usuarios extranjeros) los atributos “inheritedFamilyName” y “surname” tendrán el mismo valor, por lo que al hacer el procesamiento para obtener el segundo apellido el resultado será una cadena de texto vacía.

7. IDENTIFICACIÓN CON CERTIFICADO DE PERSONA JURÍDICA

Actualmente la pasarela permite al usuario identificarse con un certificado de persona jurídica en lugar de uno de persona física en caso de que el Proveedor de Servicio lo permita.

Para permitir este tipo de identificación el SP tiene que enviar a la pasarela en su petición, junto al resto de parámetros, un parámetro POST con nombre “allowLegalPerson” y valor “true” en caso de que se admita (en caso de que no se admita puede o bien enviar el valor “false” o bien no enviar el parámetro). Es importante señalar que los certificados de persona jurídica sólo son compatibles con los atributos “eIdentifier” y “givenName”, dentro de los cuales devolverán el Identificador Electrónico asociado a ese certificado de persona jurídica y el Nombre. Por ello, en caso de querer solicitar más atributos en la petición, es conveniente que sean como opcionales para que la petición no falle en caso de que el usuario decida autenticarse con un certificado de persona jurídica en lugar de con uno de persona física. En este sentido, recomendamos solicitar los apellidos como un valor opcional, ya que si fueran obligatorios, al no poder ser devueltos por la plataforma (el ciudadano se autenticó como persona jurídica) fallará el proceso de autenticación.

Adicionalmente a la respuesta SAML que se le envíe de vuelta al SP, también llegarán dos parámetros POST:

- isLegalPerson: Este parámetro sólo se envía en caso de que el SP haya enviado el parámetro “allowLegalPerson=true”. El parámetro indicará (con un “true” o un “false”) si el certificado que se ha usado en la identificación es de persona jurídica (true) o de persona física (false).
- oid: Este parámetro sólo se envía en caso de que el SP haya enviado el parámetro “allowLegalPerson=true” y sólo tendrá valor en caso de que la identificación se haya llevado a cabo con un certificado de persona jurídica (“isLegalPerson=true”). El parámetro indica el OID del certificado de persona jurídica.