Introducción a los servicios paneuropeos de identificación electrónica para aplicaciones de las AAPP

Resumen: Esta es una introducción a la plataforma STORK para proveedores de servicio, que puedan tener interés en aceptar credenciales extranjeras en su portal. También integradores de sistemas se pueden beneficiar de esta introducción.

Historia

Versión	*Fecha*	*Causa modificación*	*Modificado por*
0.1	15/09/2011	Versión inicial	
0.2	17/10/2011	Modificaciones varias	
1.0	30/01/2012	Inclusión de Validación de certificados, varias mejoras	

Índice

HISTORIA **2**
ÍNDICE **3**
1 QUE ES A STORK **4**
1.1 EL PROYECTO STORK 4
1.2 ¿CÓMO SE CONSIGUE ESTA INTEROPERABILIDAD? 4
1.3 ¿CÓMO FUNCIONA ESTA INTEROPERABILIDAD? 4
1.4 QAA 11
1.5 PAÍSES CONECTADOS A STORK 12
1.6 CONTROL POR EL USUARIO 13
1.7 SERVICIOS DISPONIBLES 13
1.8 EL NODO DE STORK EN SU ENTORNO 14
1.9 SAML2.0 15
2 CONECTARSE A STORK **17**
2.1 DISEÑO DE LA INTEGRACIÓN 17
2.2 DATOS DISPONIBLES QUE MANEJA LA PLATAFORMA 17
2.2.1 EIDENTIFIER 18
2.2.2 SURNAME Y GIVENNAME 19
2.2.3 PAÍSES 19
2.2.4 ISAGEOVER 19
2.2.5 RESIDENCEADDRESS 19
2.3 DATOS OBLIGATORIOS Y OPCIONALES 20
2.4 PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y SEGURIDAD 20
2.5 PROCEDIMIENTO 21
3 PAQUETE DE INTEGRACIÓN DE STORK PARA PROVEEDORES DE SERVICIOS **22**
3.1 UN PAQUETE SOFTWARE 22
3.2 UN DOCUMENTO DE INSTALACIÓN, CONFIGURACIÓN E INTEGRACIÓN 22
3.3 KIT DE HERRAMIENTAS 22
4 PREGUNTAS FRECUENTES **23**
5 ANEXO: PETICIÓN DE ALTA COMO PROVEEDOR DE SERVICIOS CON ACCESO A LA PLATAFORMA STORK **25**

1 Que es a STORK

1.1 El proyecto STORK

El proyecto STORK (Secure idenTity acrOss boRders linKed), o traducido "cigüeña", por ser el pájaro migratorio por excelencia, fue realizado por un consorcio de 29 participantes de 17 países europeos, con la misión de establecer una plataforma de interoperabilidad para las identidades electrónicas existentes en Europa. El proyecto fue co-financiado por la Comisión Europea.

Esta plataforma permite a los ciudadanos europeos establecer nuevas relaciones electrónicas con gobiernos extranjeros, usando sus credenciales nacionales.

De la misma manera, aplicaciones de administración electrónica españolas, pueden ofrecer sus servicios a ciudadanos de otros países europeos, al permitirse la identificación electrónica completa y fehaciente de los mismos, a través de la plataforma STORK.

Originalmente los servicios de administración electrónica que permitían esta identificación fueron definidos como pilotos, pero desde mediados del 2011 también se permite la conexión con otros proveedores de servicio que pueden ya beneficiarse de la identificación electrónica de ciudadanos extranjeros de los países Europeos.

1.2 ¿Cómo se consigue esta interoperabilidad?

Ya que existen más de 110 tipos de credenciales diferentes, todos los países participantes han acordado una capa de interoperabilidad que permite el intercambio de datos personales de identidad entre estos países en un nivel de abstracción mayor de lo que sería en las propias credenciales. Esta capa de interoperabilidad está implementada entre todos los nodos nacionales de los países conectados, que a su vez conectan con sus proveedores de servicio así como los proveedores de identidades y atributos adicionales.

Estos nodos de la plataforma STORK también son llamados PEPS, Pan European Proxy Service. Este PEPS tiene dos objetivos importantes:

1) esconde toda la infraestructura nacional para todos los demás países. En esta infraestructura de incluyen los tipos de credenciales, todos los proveedores de servicios de identidades (IDP's), posibles proveedores de atributos (AP), así como toda la colección de administraciones públicas o proveedores de servicios (SPs).
2) forma un punto de confianza que permite elevar el circulo de confianza nacional a niveles europeos

Mediante este nodo, una administración pública sólo necesita pedir credenciales de extranjeros a un único nodo, y recibirá la respuesta también del mismo. Este PEPS a su vez realizará peticiones a su homólogo del país del usuario para que obtenga sus datos de identidad.

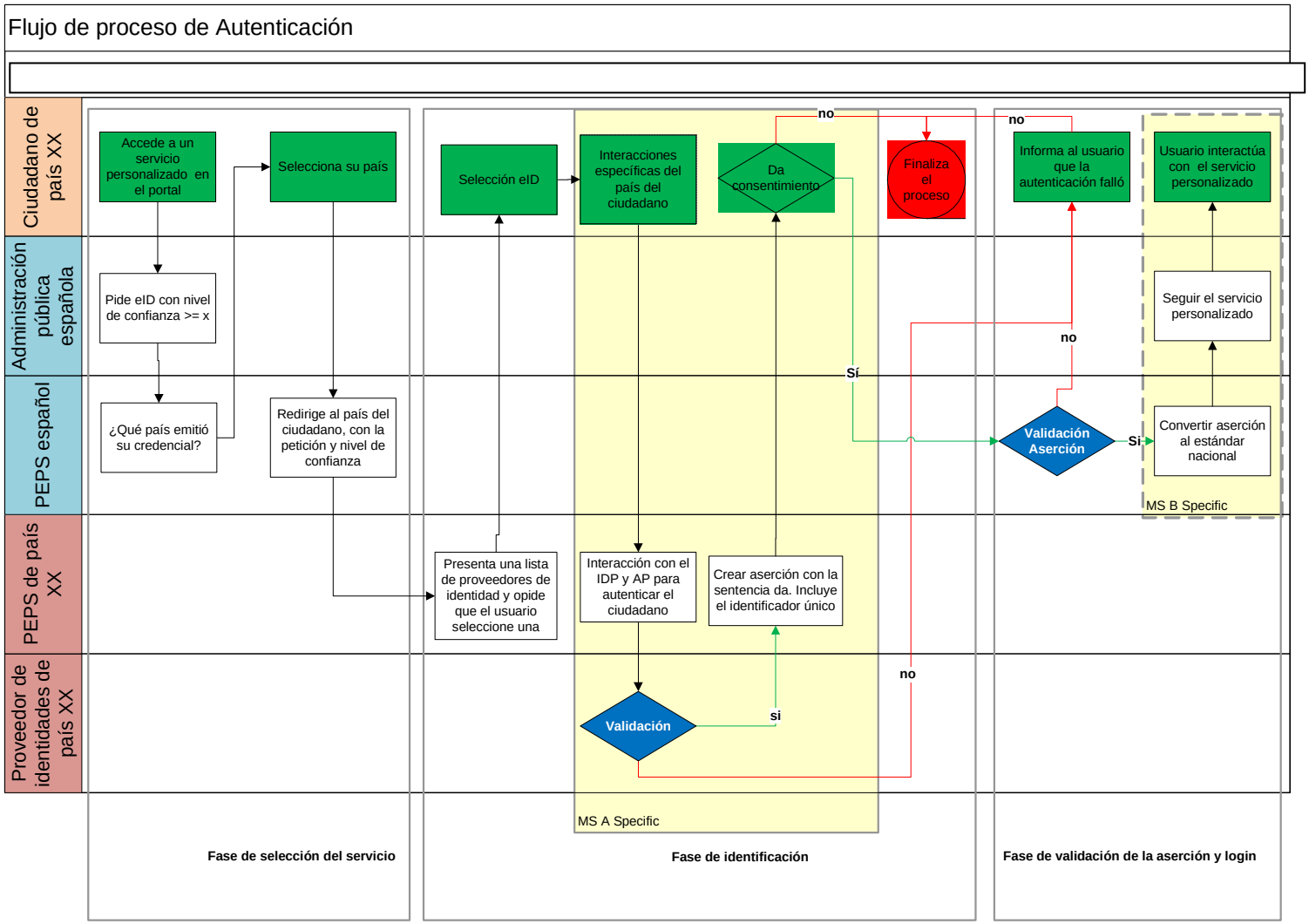
El nodo español PEPS que conecta a España a la federación de identidades y servicios asociados de STORK, es explotado y mantenido por la Dirección General de Modernización Administrativa, Procedimientos e Impulso a la Administración Electrónica, del Ministerio de Hacienda y Administraciones Públicas.

1.3 ¿Cómo funciona esta interoperabilidad?

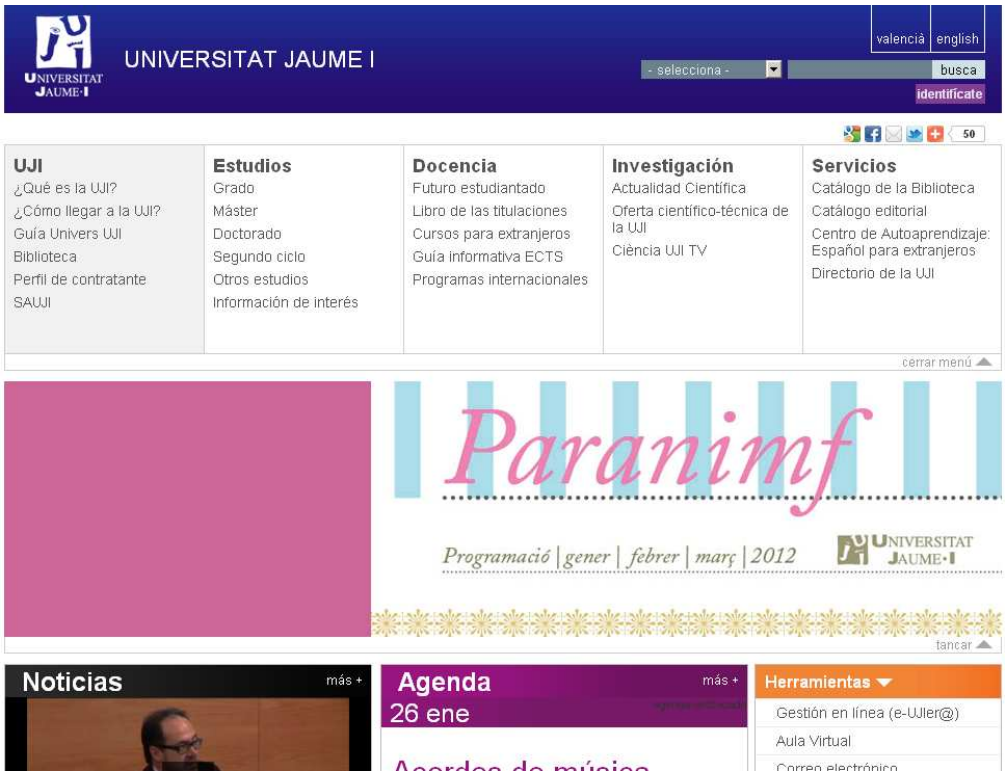
Cuando un usuario accede a la parte personalizada del portal de un proveedor de servicio español, este pide los datos personales de identidad que necesita, redirigiendo el usuario al PEPS español. Este nodo redirigirá el usuario al nodo de su propio país, que le permitirá identificarse en los

proveedores de identidad (IDP) homologados con él. En la medida de necesitar datos complementarios que estén disponibles en proveedores de atributos adicionales, accederá a los mismos. El camino de la vuelta es justo el inverso: el PEPS extranjero redirige el usuario al PEPS español, que le redirige al portal de administración electrónica. Esta comunicación sigue el esquema presentado a continuación.

Proveedores de servicio se pueden fiar de los datos recibidos, puesto que el gobierno extranjero garantiza que son datos reales, y que son trazables a un personal real.


Flujo de proceso de Autenticación
Ciudadano de país XX
Administración pública española
PEPS español
PEPS de país XX
Proveedor de identidades de país XX
Accede a un servicio personalizado en el portal
Selecciona su país
Pide eID con nivel de confianza >= x
¿Qué país emitió su credencial?
Redirige al país del ciudadano, con la petición y nivel de confianza
Selección eID
Presenta una lista de proveedores de identidad y opide que el usuario seleccione una
Interacciones específicas del país del ciudadano
Interacción con el IDP y AP para autenticar el ciudadano
Validación
Da consentimiento
Crear aserción con la sentencia da. Incluye el identificador único
Finaliza el proceso
Informa al usuario que la autenticación falló
Validación Aserción
Usuario interactúa con el servicio personalizado
Seguir el servicio personalizado
Convertir aserción al estándar nacional
MS B Specific
MS A Specific
no
Sí
si
Fase de selección del servicio
Fase de identificación
Fase de validación de la aserción y login

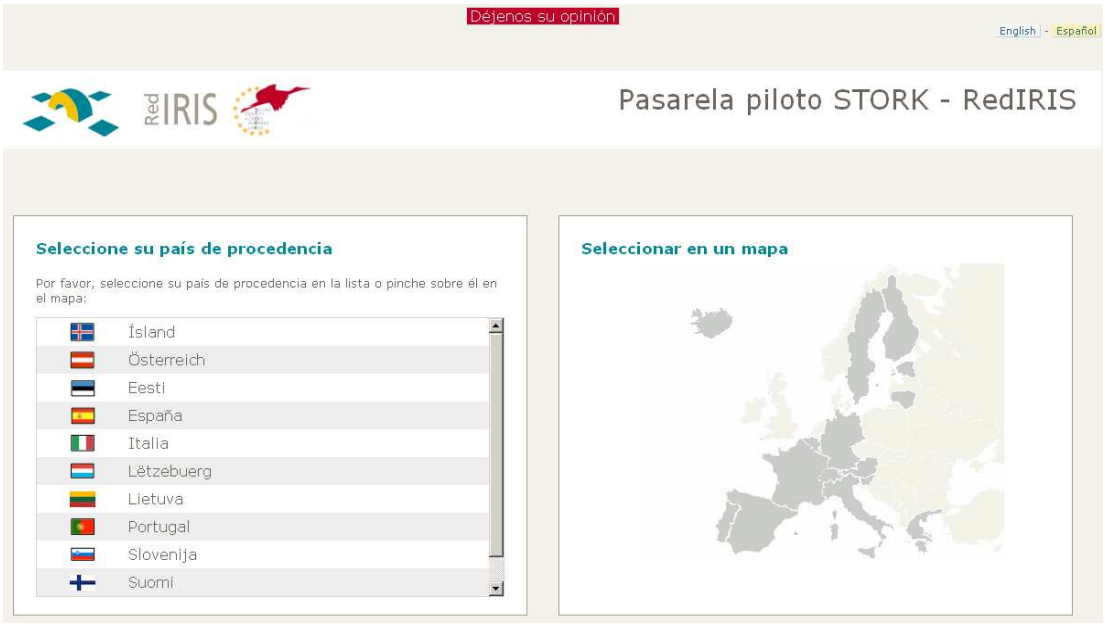
Para ilustrar este flujo de proceso abstracto, presentamos unas capturas de pantallas de cómo un usuario portugués podría acceder al servicio de la Universidad Jaume I.



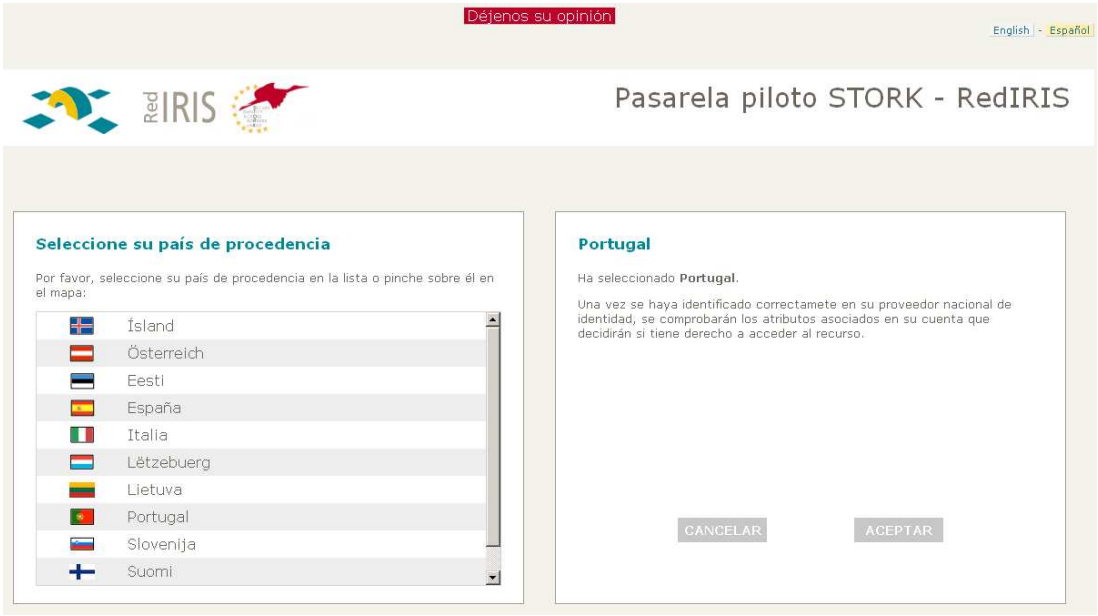
La página principal de la UJI, www.uji.es, es presentada en valenciano, y tiene la opción de cambiar el idioma arriba a la derecha. Justo debajo de esta facilidad está la posibilidad de identificación. Al pulsar este enlace aparece la siguiente página, que pregunta al usuario como se quiere autenticar.



El enlace “Acceso para estudiantes extranjeros (STORK)” nos lleva a la selección del país del estudiante:



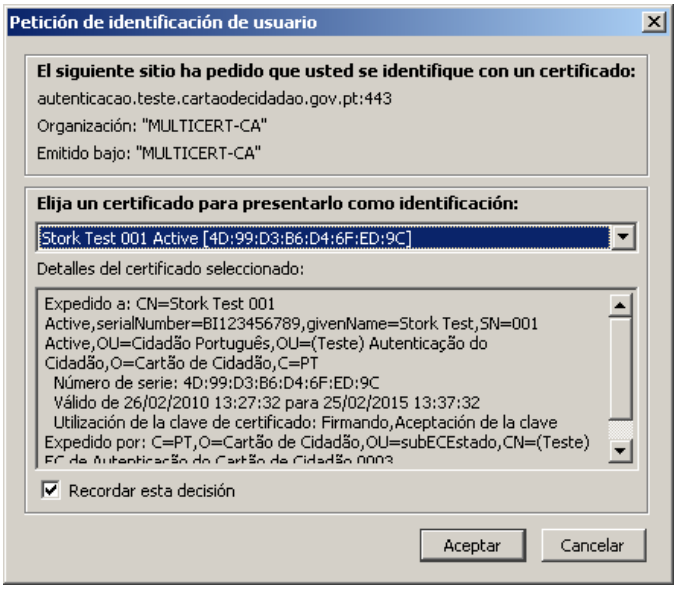
Al pulsar sobre Portugal en el mapa o en la lista pide confirmación:



El botón aceptar redirige el usuario al PEPS español que sólo le redirige al usuario, sin presentar ninguna pantalla, al PEPS portugués, que pide el usuario que autorice enviar los datos pedidos al extranjero.



Al autorizar este envío, el PEPS portugués pide el certificado, que Firefox presenta así:



Después de esta selección aparecerá la siguiente pantalla.



Al cabo de unos segundos esta pantalla es sustituida por la siguiente en la que se pide consentimiento para el envío de los datos del usuario.



Al autorizar este envío, estos datos son enviados a la UJI. Si es un usuario desconocido, pedirá completar sus datos personales. En este caso se trata de un usuario conocido por lo que le lleva a la misma página principal, pero con el enlace “identifícate” cambiado por “desconéctate”



En consecuencia, permitirá pulsar cualquier opción que requiera estar identificado.

1.4 QAA

Entre tantas credenciales diferentes, está claro que no todas son igual de seguras: el DNIe por ejemplo es mucho más fuerte que una identificación mediante nombre de usuario y contraseña. Para poder compararlas, se ha definido un parámetro de calidad de la credencial: QAA (*Quality of Authentication Assurance*, Aseguramiento de la Calidad de la Autenticación). Este parámetro especifica las exigencias para cada uno de los 7 factores que determinan esta calidad, que tiene en cuenta por un lado el procedimiento de registro y emisión, y por otro lado las características del uso de la credencial.

Podemos resumir su definición mediante la siguiente tabla:

QAA	Descripción	Mecanismos	Ejemplos de comprobación identidad
1	Mínima	Usuario / contraseña	Ninguna
2	Baja	Usuario / contraseña fuerte Certificado no reconocido	Los datos son enviados por la combinación de correo electrónico y tradicional
3	Sustancial	Usuario / contraseña fuerte, reforzado con otros mecanismos Certificado reconocido en software	Por correo, después de la validación de varios de los datos del titular de la misma

4	Alta	Certificado reconocido en dispositivo criptográfico	Después de haberse presentado físicamente en una oficina de registro.

Antes de conectar a la plataforma STORK, los proveedores de servicio tienen que considerar el nivel de QAA que van a exigir para el acceso a su aplicación, teniendo en cuenta que un mayor nivel de QAA aportará mayor seguridad, pero también excluye a un mayor grupo de ciudadanos europeos que no disponen de credenciales de esa calidad. Para las aplicaciones españolas, los niveles de aseguramiento 3 y 4 facilitan la identificación de ciudadanos de otros países europeos con certificados electrónicos supervisados y homologados a los que se utilizan en España.

1.5 Países conectados a STORK

Originalmente los países conectados a STORK fueron Alemania, Austria, Bélgica, Eslovenia, España, Estonia, Islandia, Italia, Luxemburgo, Portugal y Suecia. Recientemente también Finlandia y Lituania se han conectado, y en breve esperamos dar la bienvenida a Francia, Grecia y el Reino Unido. En el futuro otros países pueden conectar a la plataforma. El siguiente mapa muestra la situación a 31/12/2011. En azul están los países que próximamente se unirán.



Se puede prever que, con el tiempo, todos los países de la UE estén conectados. De sus más de 500 millones de ciudadanos serán más de 400 millones de ciudadanos que tienen identidades electrónicas que, a través de la plataforma STORK, pueden usar los servicios electrónicos conectados a esta plataforma.

1.6 Control por el Usuario

Como dicho en el primer párrafo, la plataforma permite a los usuarios recibir nuevos eServicios de gobiernos extranjeros. La transferencia de sus datos de identidad requiere que el usuario tome la iniciativa de conectarse a este servicio, y cuando le pida su identidad necesite introducir su credencial y dar su consentimiento a la transferencia de datos. Así el usuario siempre tiene el control sobre sus datos, y la plataforma cumple la ley de protección de datos de carácter personal de cada país, la LOPD (15/1999) en España.

Nota: todos los países participantes son de la Unión Europea o del Espacio Económico Europeo, por lo que tienen una legislación para la protección de datos de carácter personal similar, en todos los casos inspirado por la Directiva europea 95/46/EC.

La plataforma STORK no almacena datos de carácter personal.

1.7 Servicios disponibles

La plataforma STORK del Ministerio de Hacienda y Administraciones Públicas puede ser usada para 3 servicios:

1) Registro de usuarios.

   El registro de usuarios en un portal se produce cuando un usuario accede por primera vez al servicio de administración pública electrónica. La administración enviará una petición al PEPS español, pidiendo varios datos; por lo menos el identificador (DNI), nombre y apellidos; muchas administraciones adicionalmente piden fecha de nacimiento y género. En el apartado "2.2 Datos disponibles que maneja la plataforma" se detallan todos los datos que se pueden pedir, con una breve descripción de los mismos. De algunos datos hay una descripción ampliada en los subapartados siguientes al 2.2.

   Cuando el usuario termina de autenticarse, el PEPS español le enviará la respuesta a la aplicación. Podría ser que su aplicación necesite datos que no pueden ser suministrados por STORK, o no son devueltos por la plataforma. En este caso la aplicación debería pedir estos datos al usuario. En este formulario la aplicación debería pre-rellenar los datos recibidos de la plataforma. Los datos suministrados por STORK son fiables, los datos tecleados por el usuario podrían no ser ciertos.

2) Autenticación de usuarios registrados.

   Para la autenticación de usuarios registrados la petición al PEPS español será más breve: habitualmente sólo se requiere el identificador del usuario (DNI) para esta función, y no se necesita otros datos como su nombre, apellidos, etc., puesto que ya figuran en el registro de usuarios del portal.

   En el apartado "2.2.1 eIdentifier" se detallan varios temas acerca del identificador, especialmente limitaciones en cuanto a su persistencia en algunos países.

3) Validación de certificados.

   En primer lugar se diseñó la plataforma para la autenticación y registro de ciudadanos.

   No obstante, también ofrece una funcionalidad para apoyar la firma transfronteriza: la validación de certificados. Como existen muchos formatos de firma, el proveedor de servicio que elija un formato debería realizar las comprobaciones de validez del formato de una firma recibida. Así mismo debe ser capaz de validar la propia firma en sentido matemático, de fechas de validez del certificado usado, la parte criptográfica etc. Lo que no siempre puede verificar es si el certificado es válido, es decir si no está revocado ni

suspendido, puesto que servicios de validación no siempre están disponibles de forma gratuita y accesible para cualquiera en Internet.

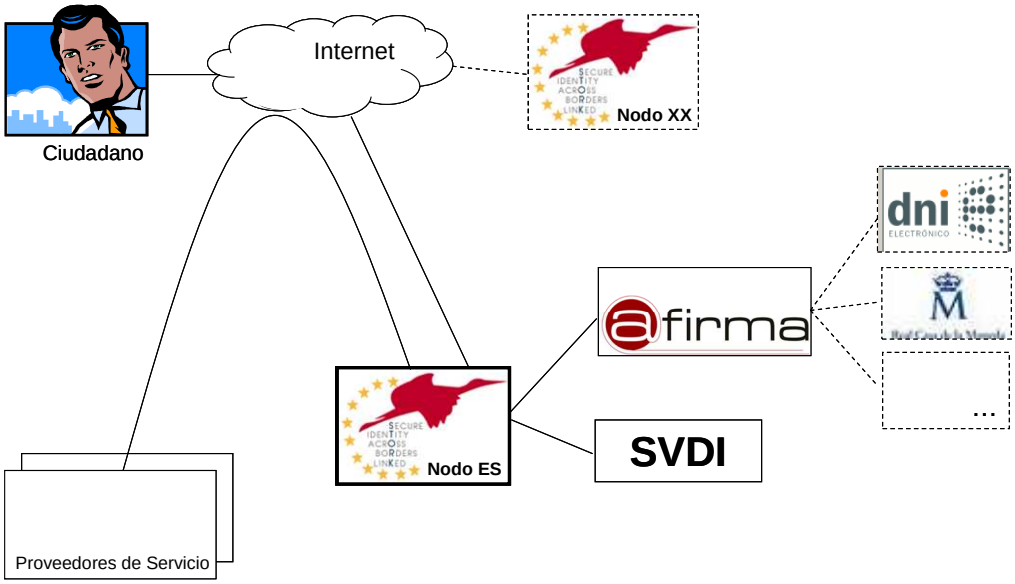
La implementación de los servicios 1 y 2 se ha realizado mediante peticiones y respuestas SAML conforme a su protocolo de autenticación. En estas peticiones y respuestas puede viajar cualquier conjunto de los datos especificados en el apartado "2.2 Datos disponibles que maneja la plataforma". En STORK no se diferencian entre las peticiones para registro y las de autenticación; también las respuestas son iguales en ambos casos.

La implementación del servicio 3) de validación de certificados se ha realizado mediante una pasarela OCSP en España, que conecta con los servidores OCSP en el extranjero, que a su vez validan el certificado contra los mecanismos establecidos por el emisor del mismo, habitualmente OCSP o CRL. Nota que no todos los países disponen de este servicio.

1.8 El nodo de STORK en su entorno

Todos los nodos que tienen interfaz con los proveedores de servicios son simples pasarelas.

Cada nodo de STORK que obtiene las credenciales de sus ciudadanos tiene su propia arquitectura. El nodo español por ejemplo sigue la arquitectura que se muestra a continuación. Si el portal de la administración pública electrónica permite credenciales españolas en su portal, podría ser interesante conocer este servicio.



Las entidades dibujadas en este esquema son las siguientes:

- Nodo ES: Es el PEPS Español, que conecta su portal de administración electrónica a la plataforma STORK y así permitirá admitir que sus usuarios se identifiquen con sus credenciales nacionales. Así mismo atiende peticiones de portales extranjeros, a través de los nodos extranjeros homólogos, para que puedan obtener datos de identidad de los ciudadanos españoles.
- Ciudadano: los usuarios de los portales de los proveedores de servicio son los actores principales del esquema

- Proveedores de servicio españoles: son administraciones públicas electrónicas cuyos portales están habilitadas para STORK, es decir que admiten que sus usuarios extranjeros utilicen sus credenciales nacionales.
- Nodo XX: simboliza los PEPSes de todos los demás países conectados a STORK. Actualmente son los enumerados en "1.5 Países conectados a STORK", pero en el futuro se ampliará a más países.
- @firma: es la plataforma de la Dirección General de Modernización Administrativa, Procedimientos y para el Impulso de la administración electrónica que facilita la validación de todos los certificados reconocidos en España. Esta plataforma en primer lugar verifica el estado del certificado contra su emisor, mediante el mecanismo que haya establecido (CRL u OCSP). A continuación extrae del certificado los datos de su titular y los devuelve a la aplicación que solicitó la validación.
- SVDI es el Sistema de Validación y Consulta de Datos de Identidad de la misma Dirección General. Este sistema consulta la BD de la policía nacional para devolver los datos de una persona. Mediante este sistema el PEPS es capaz de completar los datos pedidos por el proveedor del servicio, que no estaban en el certificado. Antes de acudir a este sistema, el PEPS pide autorización al usuario.

1.9 SAML2.0

SAML quiere decir *Security Assertion Markup Language*. Es un estándar que permite intercambiar datos de identidad entre un proveedor de identidades y un proveedor de servicios. STORK utiliza este estándar para este intercambio de datos personales. Fue definido por el grupo OASIS, basándose en estándares anteriores para la federación. SAML2.0 es muy flexible y permisivo; STORK ha hecho una implementación más estricta según las especificaciones acordadas entre todos los países conectados. Estas especificaciones necesitan usar las extensiones contempladas en SAML para cubrir las necesidades legales y organizativas de todos los países conectados a STORK.

Para los interesados en este estándar seguimos con una breve introducción del mismo. Según el estándar, tanto las peticiones como las respuestas son enviadas por el proveedor de servicio (Relying Party en términos de SAML) y proveedor de identidad (Id Provider) a través del navegador del usuario. El método usado para este intercambio se llama en términos de SAML el *binding*. El binding determina tanto la petición como la respuesta; en el caso de STORK soportamos redirect/POST. Este binding quiere decir que la petición es enviada mediante un http redirect y la respuesta es enviada mediante un http POST.

Dentro del mensaje viaja una petición conforme a un protocolo; hay 3 protocolos: para la autenticación, para la transferencia de atributos o para la autorización. La respuesta correspondiente será del tipo pedido. Como no hay limitación de atributos que viajan, sólo hemos implementado el protocolo de autenticación, que se puede usar tanto para el registro del ciudadano, con varios atributos, como para posteriores accesos pidiendo sólo su identificador.

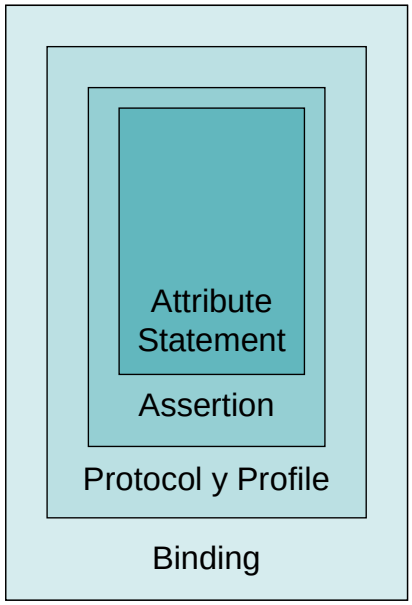
Los mensajes tienen una estructura conforme a su perfil. De los 5 perfiles básicos el de Single Sign On (SSO) tiene además 5 sub-perfiles. En STORK se usa el perfil más utilizado en SAML: Web browser SSO.

En los pilotos de STORK no había necesidad de la transferencia de atributos como proceso de negocio diferenciado del registro.

Dentro de la respuesta pueden haber varias aserciones. Una aserción es una afirmación de un proveedor de datos de identidad acerca de una persona. Si hay datos de varios proveedores, deben haber varias aserciones. En el caso de STORK sólo hay una aserción por mensaje.

Y dentro de una aserción pueden viajar varias sentencias de atributos; estas sentencias siempre especifican una combinación de nombre del atributo y su valor.

Todos estos términos se relacionan según el siguiente esquema.



El grupo OASIS recomienda que las respuestas sean firmadas, garantizando la integridad del mensaje STORK no solo exige que se firme la respuesta, sino también la petición.

Además de utilizar la firma para comprobar la integridad del mensaje intercambiado, también sirve para validar la confianza en el emisor. Así que el nodo español de STORK sólo aceptará peticiones de proveedores de servicio registrados. Esto implica que la parte pública del certificado de firma usado por el proveedor de servicio tiene que estar registrado a su nombre. Este nombre tiene que coincidir con el nombre del proveedor tal y como está incluido en la petición SAML de autenticación.

En cuanto a la confidencialidad, todas las comunicaciones discurren por canales protegidos mediante TLS o SSL.

2 Conectarse a STORK

2.1 Diseño de la integración

Antes de conectarse a STORK en sentido tecnológico, se debe hacer unas consideraciones.

En primer lugar se debe determinar en mínimo nivel de confianza en la identificación presentada por el usuario. En esta cuestión se debe tener en cuenta que un mayor nivel de QAA aportará mayor seguridad para su aplicación, pero también excluye a un mayor grupo de ciudadanos europeos que no disponen de credenciales de esa calidad. Para las aplicaciones españolas, los niveles de aseguramiento 3 y 4 facilitan la identificación de ciudadanos de otros países europeos con certificados electrónicos supervisados y homologados a los que se utilizan en España.

En segundo lugar debe determinar el conjunto mínimo de datos necesarios para poder aceptar una persona en el proceso del registro, y cuales de estos datos deben ser validados por la autoridad de su país. En el apartado siguiente se detallan los datos disponibles, y en este punto se aplica lo mismo que en el anterior: cuantos más datos se exijan, más ciudadanos se excluyen.

En tercer lugar debe determinar cuales de estos datos validados por autoridades extranjeras podrán ser modificados por el propio usuario, cuando después de recibirlos el portal se los presenta al usuario para que los complete.

2.2 Datos disponibles que maneja la plataforma

El consorcio ha definido los datos de identidad que pueden ser intercambiados entre los países conectados a STORK; esta es la definición de conjunto máximo. Ningún país dispone de todos los datos; algunos solo disponen de identificador, nombre, apellidos, y fecha de nacimiento, y otros tienen más de 10 atributos. En capítulo 5 de este documento podrá conocer qué país dispone de qué atributos.

Datos necesarios que no son soportados por STORK pueden ser pedidos al usuario. La única diferencia es que datos tecleados por el usuario no son garantizados por el gobierno.

Ese conjunto máximo de datos es:

eIdentifier	Identificador nacional del ciudadano, con un prefijo del país emisor de la credencial)
givenName	Nombre
surname	Apellidos
inheritedFamilyName	Apellidos heredados
adoptedFamilyName	Apellidos adoptados (por ejemplo por matrimonio)
gender	Género. [M] Masculino ó [F] femenino
nationality	Nacionalidad
maritalStatus	Estado civil. [S] Soltero / [M] Casado / [P] Separado /

	[D] Divorciado / [W] Viudo
dateOfBirth	Fecha de nacimiento
countryOfBirth	País de nacimiento (En formato ISO 3166-1 alpha-2)
age	Edad
isAgeOver	"Es Mayor De". Este campo permite preguntar si el ciudadano autenticado tiene una edad superior a la solicitada.
residenceAddress	Dirección de residencia. En formato texto de hasta 5 líneas
canonicalResidenceAddress	Dirección de residencia. En formato *canónico*: countryCodeAddress, State, MunicipalityCode, Town, PostalCode, StreetName, StreetNumber, ApartmentNumber
residencePermit	Permiso de residencia
email	
title	Título
pseudonym	Seudónimo
fiscalNumber	Número fiscal
citizenQAALevel	Nivel de QAA de la credencial con la que se autenticó [1..4]

La definición de los mismos está en capítulo 2 de este documento. Los siguientes párrafos detallan algunos comentarios acerca de algunos de estos datos.

2.2.1 eIdentifier

En algunos países como Portugal, España, Estonia y Suecia los ciudadanos están muy acostumbrados a que se les pida el número de su documento de identidad (como el DNI); tanto en gobiernos como en empresas privadas. Normalmente estas personas darán su identificador también a administraciones extranjeras, por lo que el identificador enviado será del estilo PT/ES/12345678Z.

En otros países esto no es tan normal; la gente no da su DNI a cualquiera, solo si hay una razón especial. En estos países se aplican un algoritmo matemático sobre el identificador, que resulta en diferentes números para diferentes servicios. Con este método se evita que un fichero de sanidad sea comparado con un fichero de multas de tráfico. En estos países el identificador tendrá una forma como BE/ES/fDt01567jlNm.[1]

[1] Este identificador puede tener hasta 92 caracteres.

En casi todos los países el eIdentifier es persistente, lo que quiere decir que el valor que tiene este atributo la primera vez que el usuario accede al servicio es el mismo que todas las veces posteriores. No obstante, en algunos países el ciudadano no tiene un identificador, sino su tarjeta de ciudadano tiene un número. Al ser renovado, la nueva tarjeta tiene otro número.

Este es el caso de ciudadanos alemanes y griegos.

2.2.2 Surname y givenName

En algunos países, en caso de matrimonio la mujer adopta el apellido del marido. La legislación moderna amplió esta adopción al caso inverso y a otros tipos de relaciones que el matrimonio heterosexual. Así que en algunos países el apellido puede cambiar.[2]

En algunos países se utilizan alfabetos diferentes, con letras "raras" como en el griego, cirílico y ruso. En STORK se ha acordado utilizar siempre las letras latinas (a-z), aunque algunas letras pueden ser un poco curiosas, como la ñ, ç, ð, etc. Así se permite que la persona que lo lea lo pueda pronunciar.

2.2.3 Países

La nacionalidad y otros indicadores de países siguen el estándar ISO3166-1, que da una abreviatura de 2 letras para cada país, ES de España y PT de Portugal. En país de nacimiento, countryOfBirth, pueden haber países que han dejado de existir, como la República Democrática de Alemania (o Alemania oriental), de antes de octubre del 1989. En tales casos se usa el estándar ISO3166-3, que utiliza 4 letras para indicar el país.

2.2.4 isAgeOver

Este dato es derivado de la edad, que a su vez es derivado de la fecha de nacimiento. Se puede pedir múltiples veces, por ejemplo isAgeOver(15) y isAgeOver(18). Si la respuesta es isAgeOver(15) y isAgeOver(<vacío>), el proveedor de servicio sabe que el usuario tiene 15 o más, pero menos de 18 años.

2.2.5 ResidenceAddress

La dirección de residencia es donde el ciudadano vive oficialmente. Existen 2 formatos del dato: el primero es en formato texto de 5 líneas, entendible por Correos en el país destino, y en el formato canónico, que es una estructura XML que subdivide la dirección en:

- countryCodeAddress
- state
- municipalityCode
- town
- postalCode
- streetName
- streetNumber
- apartmentNumber

[2] En la mayoría de países los ciudadanos tienen solo un apellido.

2.3 Datos obligatorios y opcionales

Antes de conectar la función "Alta en el servicio" de la aplicación a STORK, su administrador debe determinar los datos necesarios para el alta de un usuario, dependiendo de su rol. Y dentro de estos datos, cuales necesitan ser verificados, y cuales podrían ser opcionales o pedidos al usuario. Los datos pedidos como obligatorios siempre serán devueltos en caso de una exitosa identificación del usuario, pero si los datos obligatorios no están disponibles o no son conocidos, ningún dato es devuelto, y falla el proceso de identificación. Los datos opcionales son devueltos siempre que estén disponibles.

2.4 Protección de Datos de Carácter Personal y Seguridad

La directiva europea 95/46/EC y la ley LOPD en España marcan que toda petición y recogida de datos tiene que ser proporcional al propósito del servicio. En este marco reiteramos que es importante pedir el mínimo necesario de datos personales del usuario.

Adicionalmente es buena práctica publicar su política de privacidad en su sitio en Internet, tal y como lo muestra el ejemplo en el fondo de la página. Si su sitio en Internet también se dirige a extranjeros, esta política debe estar disponible en otros idiomas, por lo menos en inglés.



Aunque la ley no exige, es buena práctica realizar el intercambio de datos personales por canales protegidos por SSL o TLS. De hecho, todas las comunicaciones de la plataforma STORK se producen con esta protección.

Esta y otras recomendaciones de seguridad realizadas por el grupo de expertos de seguridad en el proyecto han sido implementadas por cada uno de los países conectados. Así mismo en cada país se cumple los requisitos de seguridad vigentes. En España estos requisitos están enumerados en Esquema Nacional de Seguridad; el PEPS español cumple las medidas de nivel medio. En otros países se cumplen requisitos equivalentes, conforme a las normativas nacionales, por ejemplo la BS7799 en el Reino Unido.

2.5 Procedimiento

El procedimiento de conexión a STORK al entorno de preproducción implica que tiene que rellenar un formulario y enviarlo a stork@indra.es. Este formulario en blanco se encuentra el anexo de este documento.

Cualquier problema también puede ser reportado a la misma dirección de correo.

Para conectar al entorno definitivo (entorno de producción) se utiliza el mismo formulario, y su certificado de producción, preferiblemente uno emitido por una autoridad de certificación reconocida por el Ministerio de Industria, Energía y Turismo. Por favor, asegúrese que la persona de contacto es la persona responsable del sistema en producción.

3 Paquete de Integración de STORK para Proveedores de Servicios

Este documento forma parte del paquete de integración de STORK para proveedores de servicios. Este paquete puede ser descargado del PAE en http://administracionelectronica.gob.es/es/ctt/stork, y del sitio de Joinup, el sustituto de OSOR, y existe en diferentes versiones para Java bajo Tomcat, Glassfish, JBoss o Weblogic, php y .NET.

Todos los paquetes españoles incluyen este documento; paquetes para otros países tienen un documento similar en otro idioma.

A continuación se explica el resto del contenido del paquete.

3.1 Un paquete software

Este software incluye en primer lugar las librerías de STORK, que facilitan la generación de peticiones y la recepción y descodificación de sus respuestas. En segundo lugar dos ejemplos de integración de STORK en dos aplicaciones: una sencilla que le permitirá desplegar una aplicación habilitada con STORK en muy poco tiempo; la otra aplicación es completamente flexible. Esta última aplicación permite generar cualquier petición STORK, con QAA a elegir por el usuario, con atributos a elegir por el usuario. Suponemos que sus necesidades se aproximen más a la primera aplicación.

Por favor, asegúrese de descargar este paquete para la tecnología (java, php o .NET) que desee utilizar en su aplicación.

Este paquete software está configurado para conectar con su nodo nacional STORK de pruebas.

3.2 Un documento de instalación, configuración e integración

El otro documento en el paquete, que se llama algo similar a ManualInstalaciónProveedoresServicoxxxx_xx.doc es el manual de instalación, configuración e integración describe como desplegar el paquete software e integrarlo en su aplicación.

3.3 Kit de herramientas

El kit de herramientas incluye credenciales de pruebas, tanto nacionales como extranjeras.

4 Preguntas frecuentes

¿Cómo puedo usar este servicio en mi portal?

La plataforma STORK facilita la aceptación de credenciales extranjeros en su portal. Es decir, mediante STORK puede aceptar ciudadanos de otros países como usuarios de su portal. El paquete de integración le ofrece todo lo necesario, además de la presente introducción: librerías de integración, ejemplos con código fuente, un manual de instalación, configuración e integración.

¿Está basado en algún estándar?

Sí, los mensajes intercambiados entre los nodos de STORK utilizan el estándar SAML 2.0 de OASIS. Este estándar es flexible y abierto, por lo que podemos suponer que será soportado durante mucho tiempo. De este estándar hemos hecho una implementación conforme a unas especificaciones más estrictas.

¿Son seguros los mensajes?

Los mensajes intercambiados son firmados, tanto las peticiones como las respuestas. En consecuencia no pueden ser manipulados sin que esa manipulación es detectada. Además el certificado de firma del proveedor de servicio tiene que ser conocido por el nodo de STORK en España. Además, el intercambio del los mismos discurre por canales seguros (SSL o TLS).

¿Puedo reenviar el mensaje a otro proveedor?

Los mensajes no están diseñados para ser reenviados, por eso tienen una validez muy breve.

¿Es segura la plataforma?

Todos los nodos nacionales de STORK cumplen las normativas de seguridad nacionales; en España el ENS, por ejemplo en el Reino Unido la BS7799. Todos los países han realizado una autoevaluación de los temas de seguridad más relevantes.

¿Necesito estar conectado a la Red SARA?

Todas las redirecciones se producen a través del navegador, por lo que en un principio todas las peticiones procederán de Internet.

¿Necesito dar de alta mi aplicación en algún sitio?

Sí. En el anexo de este documento se encuentra un formulario de solicitud que hay que enviar al buzón de soporte: stork@indra.es

¿Hay exigencias a estos certificados de firma?

Los certificados tienen que ser válidos para firmar y ser válidos, es decir no estar revocados ni suspendidos. Se recomienda usar certificados emitidos por las autoridades de certificación reconocidas en España, con una longitud de la clave de 2048 bits.

¿Tanta redirección no provoca lentitud?

No mucha. Tanta redirección sirve para la escalabilidad: así un proveedor de servicio sólo necesita conocer un único punto en España, para poder aceptar credenciales de muchos proveedores de identidades de varios países.

¿Dónde puedo obtener más información acerca del proyecto?

Su sitio web es www.eid-stork.eu. Allí puedes conseguir toda la información relevante que el proyecto ha producido.

¿Dónde puedo obtener ayuda o soporte?

En stork@indra.es se hará todo lo posible para solucionar sus dudas, preguntas y problemas.

¿Qué pasa si un nuevo país entra en producción?

El selector de países de su instalación se modificará automáticamente, si un nuevo país se conecta a la plataforma STORK, si cumple con sus requisitos de atributos necesarios y calidad de la autenticación.

¿Y si no quiero aceptar credenciales de algún país?

Si un país sí cumple con los requisitos de calidad y de atributos disponibles, pero por cualquier otra razón no quiere aceptar sus credenciales, puede excluirlas. Una razón para no aceptar credenciales españolas a través de STORK podría ser que Vd ya tiene implantada la aceptación de credenciales españolas en modo nativo. O se puede excluir las credenciales de DE y GR pues su número de identificación no es persistente.

¿Puedo usar este software sin pagar?

Si, el software es licenciado LGPL. Eso implica que puede usar este software de forma gratuita para los fines que quiera, sin necesidad de hacer público cualquier otro software relacionado *(copyleft)*. Los códigos fuentes de los ejemplos son libres de uso.

¿Puedo conectar el portal de mi empresa?

No, por el momento se ha establecido el servicio de STORK para servicios de Administración electrónica. Pueden existir servicios afines a los servicios públicos, por ejemplo universidades, y por lo tanto podrían conseguir la conexión.

5 ANEXO: Petición de Alta como Proveedor de Servicios con acceso a la Plataforma STORK

Fecha_Petición	*Fecha actual*
Nombre	*Nombre del Proveedor de Servicio*
Descripción	
Entorno	*PRE o PRO*
Persona_Contacto	*Persona de Contacto del Proveedor de Servicio (nombre, apellidos, teléfono y email)*
Cerificado_SP	*Parte pública del certificado usado por el Proveedor de Servicio en la firma SAML*
-----BEGIN CERTIFICATE----- -----END CERTIFICATE-----	
Fecha_ prevista	*Fecha de Inicio prevista para pruebas en el entorno indicado*

Nota que nombre del proveedor de servicio y el certificado de firma tienen que coincidir con los valores configurados.

.