Pasarela cl@ve *de SIR2*

Instrucciones de configuración de proveedores de servicio en el entorno de pruebas

Autores	José Manuel Macías, Francisco José Aragó
Última modificación	septiembre 2016
Versiones	1.0 Versión inicial, basada en documento utilizado durante el piloto versión 1.0h

Índice

1. Introducción

El presente documento se utilizará como guía para la configuración de proveedores de servicio que se conecten al entorno de pruebas de la pasarela para la plataforma cl@ve en RedIRIS, la cual es fruto del acuerdo entre CRUE y MINHAP.

Esta pasarela ha sido implementada por la Universitat Jaume I de Castellón, sobre la base del software de código abierto SimpleSAMLphp[1]. La pasarela soporta dos modos de funcionamiento, el primero implica respuestas siguiendo el perfil de WebSSO de SAML 2.0[SAML2WebSSO], mientras que el segundo implica respuestas con extensiones STORK [STORK], tal y cual son emitidas por la pasarela original de cl@ve . Se ha incluido soporte a ambos comportamientos pues pensamos que contribuirá a un despliegue más fácil de SPs por parte de las instituciones. Los estándares y documentos que describen estas dos formas de funcionamiento se describen en el perfil tecnológico cl@ve de SIR2 [SIR2Clave].

Este documento no entra en cuestiones administrativas, y sólo trata de explicar con más detalle varios aspectos que no cambian, o cambian poco en el paso a producción, el cual se recoge en una guía similar a esta.

Para información adicional sobre configuración de su proveedor de servicio, remitimos a la documentación recogida en el apartado 5 de estas instrucciones, proporcionada por el Ministerio de Hacienda y Administraciones Públicas [MINHAPClave], así como a la propia del software de proveedor de servicios usado.

1.1 Casos de uso contemplados

Proveedores de servicio de cara a posibles usuarios externos a la organización.

Se trata de la posibilidad de que determinadas aplicaciones de la organización, como pueden ser un portal de proveedores, o un portafirmas, puedan tener autenticación desde cl@ve, con el fin de dar servicios a entes externos de la propia organización.

Proveedor de identidad propio que delega autenticación al sistema cl@ve.

Tras consultar con MINHAP, este caso de uso, que implica utilizar la pasarela para la autenticación ordinaria de usuarios propios, es preferible retrasarlo de momento. Se avisará cuando esta posibilidad sea posible, pero en principio debería ser posible en el futuro también.

1 **SimpleSAMLphp:** http://simplesamlphp.org/

1.2 Firma de aserciones desde la pasarela

La respuesta original desde cl@ve firma tanto las aserciones como la propia respuesta de autenticación, pero al pasar por la pasarela, sólo se mantendrán de la firma original las aserciones internas de la respuesta desde la plataforma cl@ve, es decir:

- la respuesta emitida por la propia pasarela en RedIRIS va firmada con una clave propia (usada para establecer la confianza con los SPs conectados a la misma)

- las aserciones contenidas en la respuesta emitida por la pasarela, conservarán la firma de aserciones original de la plataforma cl@ve, pudiéndose verificar por separado.

La pasarela actualmente firma las respuestas con SHA256.

1.3 Selección de un subconjunto de IdPs para realizar la autenticación

La pasarela soporta la elección de un subconjunto de los posibles IdPs soportados por clave, mediante el uso del parámetro `idpList` en el POST de la petición inicial, donde se consignará, separados por puntos y coma (carácter **`;`**), el subconjunto de los IdPs posibles a los que queremos limitar la autenticación. Por ejemplo: `aFirma;Stork;AEAT`. También se puede definir la lista de IdPs a excluir del total mediante el parámetro **`idpExcludedList`**, siguiendo la misma sintaxis descrita anteriormente.

Si se desea forzar un IdP concreto para evitar mostrar la pantalla de selección, se puede emplear el parámetro **`forcedIdP`** (anteriormente se empleaba **`forzar`**, y se sigue soportando por compatibilidad). Este deberá contener el nombre de un sólo IdP.

La lista de proveedores de identidad tras la pasarela cl@ve de MINHAP, en el momento de escribir esta documentación, es la siguiente:

Proveedor	Descripción
`aFirma`	@firma es una plataforma de validación y firma electrónica multi-PKI
`Stork`	STORK (ciudadanos extranjeros)
`SS`	Seguridad Social
`AEAT`	Agencia Tributaria

Para los SP que empleen la pasarela WebSSO estándar, estas opciones de configuración están disponibles en los metadatos de la propia pasarela, pudiendo establecerse por cada SP, pero no dinámicamente por cada petición como puede hacer un SP Clave.

1.4 Autenticación de personas jurídicas

Algunos IdP de la plataforma Clave permiten que el usuario se autentique con este tipo de certificados (de persona jurídica). Para ello debe enviar en un parámetro POST junto a su petición, **`allowLegalPerson`** con el valor '**`true`**'. Puede enviar '**`false`**', pero es el comportamiento por defecto.

En la vuelta, el SP debe esperar los parámetros POST siguientes (Para la pasarela WebSSO estándar, ya que no se pueden enviar parámetros POST adicionales y con la idea de que en el futuro estas opciones se estandarizarán como atributos, el SP debe esperar dichos valores como atributos en la aserción y no en el POST):

- **`isLegalPerson:`** `true` si el usuario se ha autenticado con un certificado de persona jurídica

- **`oid`**: el OID de la CA emisora del certificado empleado.

Para los SP que empleen la pasarela WebSSO estándar, esta opción de configuración está disponible en los metadatos de la propia pasarela, pudiendo establecerse por cada SP, pero no dinámicamente por cada petición como puede hacer un SP Clave.

1.5 Solicitud de un nivel de QAA mínimo

La plataforma cl@ve soporta que los SPs requieran autenticación con un nivel de calidad QAA mínimo, ello se modela utilizando en la petición de autenticación una extensión propia de Stork, de la cual consignamos un ejemplo:

```
<stork:QualityAuthenticationAssuranceLevel>3</stork:QualityAuthenticat
ionAssuranceLevel>
```

Para la pasarela WebSSO estándar, esta opción se puede configurar como metadato por cada SP, pero no especificarla dinámicamente en cada petición.

1.6 Single-Log-Out de la pasarela cl@ve

La pasarela cl@ve en RedIRIS no almacena ni cachea sesiones de autenticaciones previas, volviendo a generar una nueva petición de autenticación hacia la pasarela de cl@ve original por cada petición de un SP conectada a esta.

Por otro lado, cl@ve permite realizar autenticaciones únicas (estableciendo el parámetro `forceAuthn` de la petición) o en su defecto mantiene una sesión autenticada. Por este motivo, en principio no sería necesario cerrar la sesión en la propia pasarela de RedIRIS, sin embargo, la sesión en la pasarela cl@ve de MINHAP sí que queda abierta durante un tiempo, y podría llegar a utilizarse desde otros SPs que no se conecten a través de la pasarela en RedIRIS.

Clave soporta el uso de peticiones de Logout, pero no cumple el estándar SAML por completo (se trata de la versión de Stork). Enunciaremos las diferencias a continuación:

- Sólo soporta el binding HTTP-POST, y las peticiones deben ir firmadas.

- El nodo `NameID`, debe ser de formato 'unspecified' (por defecto) y debe contener el EntityID del SP (para que se pueda relacionar con sus metadatos). En cl@ve contendría el `providerName` empleado en las peticiones de autenticación.

- El nodo `Issuer`, no debe contener el EntityID, sino el *endpoint* del SP donde deberá ser entregada la respuesta.

- El parámetro POST a emplear en la redirección no es el estándar `SAMLRequest`, sino `SAMLRequestLogout`.

- El parámetro POST a esperar cuando llegue la respuesta no es el estándar `SAMLResponse`, sino `SAMLResponseLogout`.

Para poder gestionar las sesiones abiertas en cl@ve, la pasarela dispone de un *endpoint* para el *logout* distinto para cada pasarela. Un primer *endpoint* soporta el logout estándar SAML y el otro acepta peticiones de logout del perfil SAML de STORK, imitando el comportamiento del *endpoint* de cl@ve. Al igual que las peticiones de autenticación, sólo retransmitirá aquellas peticiones firmadas por SP autorizados.

Podemos cerrar dicha sesión si lo deseamos, enviando una petición de `Single-Log-Out` SAML al *endpoint*.

El punto de la pasarela estándar se publica en los metadatos, el de la pasarela para el perfil SAML STORK, es:

`https://clave-pre.sir2.rediris.es/clave/module.php/clave/idp/clave-logout.php`

Estas peticiones de Log-Out se extenderán en ambos casos al *endpoint* correspondiente en la pasarela de MINHAP: `https://se-pasarela.clave.gob.es/Proxy/LogoutAction`.

2. Pasarela para perfil WebSSO sin extensiones Stork

La siguiente tabla recoge los parámetros que habrán de ser configurados por un proveedor de servicios que no soporte extensiones STORK, tanto en la petición de autenticación como en la respuesta recibida de la pasarela.

Parámetro	Valor
Nombre del Proveedor	`https://clave-pre.sir2.rediris.es/clave`
End-point remoto (IdP)	`https://clave-pre.sir2.rediris.es/clave/saml2/idp/SSOService.php`
Dirección de metadatos (opcional)	`https://clave-pre.sir2.rediris.es/clave/saml2/idp/metadata.php`

Certificado de la pasarela	`-----BEGIN CERTIFICATE-----`
	`MIIDODCCAqGgAwIBAgIJAMqU+wr6z/l5MA0GCSqGSIb3DQEBCwUAMIG0MRUwEwYK`
	`CZImiZPyLGQBGRYFY2xhdmUxFDASBgoJkiaJk/IsZAEZFgRzaXIyMRcwFQYKCZIm`
	`iZPyLGQBGRYHcmVkaXJpczESMBAGCgmSJomT8ixkARkWAmVzMR4wHAYDVQQKDBVj`
	`bGF2ZS5zaXIyLnJlZGlyaXMuZXMxGDAWBgNVBAsMD0NlcnRpZmljYWRvIFNQVDEe`
	`MBwGA1UEAwwVY2xhdmUuc2lyMi5yZWRpcmlzLmVzMB4XDTE1MDkwMjExNTI0MVoX`
	`DTI1MDkwMTExNTI0MVowgbQxFTATBgoJkiaJk/IsZAEZFgVjbGF2ZTEUMBIGCgmS`
	`JomT8ixkARkWBHNpcjIxFzAVBgoJkiaJk/IsZAEZFgdyZWRpcmlzMRIwEAYKCZIm`
	`iZPyLGQBGRYCZXMxHjAcBgNVBAoMFWNsYXZlLnNpcjIucmVkaXJpcy5lczEYMBYG`
	`A1UECwwPQ2VydGlmaWNhZG8gU1BUMR4wHAYDVQQDDBVjbGF2ZS5zaXIyLnJlZGly`
	`aXMuZXMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOtBus8tyx2JFH4ILKRf`
	`vnJ+Eyb0UG1wOZm0hMutS0MvNQuvBZVytR8lVMFqlRX7U1+FP6O10c2GDniuom3v`
	`01uq2guHlu8omR3Tj54ySJf4y7m4b42i8iU+uy3ZK7voPHcyB/zKEDnDxVc5Kmti`
	`oLuk/3M9Ofz+Xsed3yCCfMb1AgMBAAGjUDBOMB0GA1UdDgQWBBSSe7SJPTtSLi+O`
	`bAQD/8QhvORUPzAfBgNVHSMEGDAWgBSSe7SJPTtSLi+ObAQD/8QhvORUPzAMBgNV`
	`HRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4GBAF7Md4GMmPl92hUBq1LOOM4Jl6J/`
	`nHSYLkb3SYvQUyiHOcsU2NaXCg6QlrJf9T+kG3XdAv550cNhLtkbiF2stnQByX1O`
	`HPY9kIudyQ3/c7DHFRfi3kkBzL4T1AGdn9PvzpQGtDL3owLsI3H5smfhA8ApogJk`
	`B5C7gzj6U9m1ZAYz`
	`-----END CERTIFICATE-----`

Por su parte el responsable del proveedor de servicio deberá proporcionar los siguientes parámetros para su configuración en la pasarela, o su URL de metadatos si dispone de esta y es accesible:

- **Identificador del Proveedor de Servicio.** Deberá corresponderse con el `Issuer` de la petición de autenticación originada desde el SP (P. ej.: https://clave-sp-x.uyy.es/).
- **Dirección del AssertionConsumerService.** Se corresponderá con el punto al que enviar la respuesta desde la pasarela.
- **Certificado.** El certificado configurado en el Proveedor de Servicio para firmar peticiones de autenticación, en formato PEM.

- **(Opcional) Lista de atributos autorizados**. Si se desea limitar qué atributos se quieren recibir de aquellos ofrecidos por Clave (consultar documentación de Clave para obtener esta lista)
- **(Opcional) Lista de fuentes de autenticación a mostrar, ocultar, o forzar**. De las ofrecidas por Clave: aFirma, SS, AEAT, Stork.
- (Opcional) **Si acepta que el usuario pueda autenticarse como persona jurídica**.
- (Opcional) **Un valor para el issuer distinto de su EntityID**. En el futuro, este campo podría ser sobreescrito siempre con un valor de la pasarela. Aún no existe consenso en su uso.
- (Opcional)

3. Pasarela para perfil WebSSO con extensiones STORK

La siguiente tabla recoge los parámetros que habrán de ser configurados por un proveedor de servicios que soporte extensiones STORK, tanto en la petición de autenticación como en la respuesta recibida de la pasarela.

Parámetro	Valor
Nombre del Proveedor	`https://clave-pre.sir2.rediris.es/clave`
End-point remoto (IdP)	`https://clave-pre.sir2.rediris.es/clave/module.php/clave/idp/clave-bridge.php`

Certificado de la pasarela	`-----BEGIN CERTIFICATE-----`
	`MIIDODCCAqGgAwIBAgIJAMqU+wr6z/l5MA0GCSqGSIb3DQEBCwUAMIG0MRUwEwYK`
	`CZImiZPyLGQBGRYFY2xhdmUxFDASBgoJkiaJk/IsZAEZFgRzaXIyMRcwFQYKCZIm`
	`iZPyLGQBGRYHcmVkaXJpczESMBAGCgmSJomT8ixkARkWAmVzMR4wHAYDVQQKDBVj`
	`bGF2ZS5zaXIyLnJlZGlyaXMuZXMxGDAWBgNVBAsMD0NlcnRpZmljYWRvIFNQVDEe`
	`MBwGA1UEAwwVY2xhdmUuc2lyMi5yZWRpcmlzLmVzMB4XDTE1MDkwMjExNTI0MVoX`
	`DTI1MDkwMTExNTI0MVowgbQxFTATBgoJkiaJk/IsZAEZFgVjbGF2ZTEUMBIGCgmS`
	`JomT8ixkARkWBHNpcjIxFzAVBgoJkiaJk/IsZAEZFgdyZWRpcmlzMRIwEAYKCZIm`
	`iZPyLGQBGRYCZXMxHjAcBgNVBAoMFWNsYXZlLnNpcjIucmVkaXJpcy5lczEYMBYG`
	`A1UECwwPQ2VydGlmaWNhZG8gU1BUMR4wHAYDVQQDDBVjbGF2ZS5zaXIyLnJlZGly`
	`aXMuZXMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOtBus8tyx2JFH4ILKRf`
	`vnJ+Eyb0UG1wOZm0hMutS0MvNQuvBZVytR8lVMFqlRX7U1+FP6O10c2GDniuom3v`
	`01uq2guHlu8omR3Tj54ySJf4y7m4b42i8iU+uy3ZK7voPHcyB/zKEDnDxVc5Kmti`
	`oLuk/3M9Ofz+Xsed3yCCfMb1AgMBAAGjUDBOMB0GA1UdDgQWBBSSe7SJPTtSLi+O`
	`bAQD/8QhvORUPzAfBgNVHSMEGDAWgBSSe7SJPTtSLi+ObAQD/8QhvORUPzAMBgNV`
	`HRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4GBAF7Md4GMmPl92hUBq1LOOM4Jl6J/`
	`nHSYLkb3SYvQUyiHOcsU2NaXCg6QlrJf9T+kG3XdAv550cNhLtkbiF2stnQByX1O`
	`HPY9kIudyQ3/c7DHFRfi3kkBzL4T1AGdn9PvzpQGtDL3owLsI3H5smfhA8ApogJk`
	`B5C7gzj6U9m1ZAYz`
	`-----END CERTIFICATE-----`

Por su parte el responsable del proveedor de servicio deberá proporcionar los siguientes parámetros para su configuración en la pasarela:

- **Identificador del Proveedor de Servicio.** Deberá corresponderse con el `Issuer` de la petición de autenticación originada desde el SP (P. ej.: https://clave-sp-x.uyy.es/).

- **Dirección del AssertionConsumerService (Opcional).** Se corresponderá con el punto al que enviar la respuesta desde la pasarela. El comportamiento actual se basa en el de Clave, que lee el ACS de la propia petición.

- **Certificado.** La clave pública del certificado configurado en el Proveedor de Servicio, en formato PEM.

4. Atributos devueltos por la pasarela

Dependiendo del método elegido por el usuario para autenticarse en la pasarela, esta emitirá unos atributos u otros de vuelta. En cualquier caso la pasarela soporta, y puede transmitir en la respuesta los siguientes atributos soportados en cl@ve:

Atributo Personal	Tipo	Valores / Comentario
eIdentifier	String	CP/12345678X (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	
citizenQAAlevel	Number	[2,3,4] No se contempla el nivel 1 definido en STORK.
AfirmaResponse	String	
isdnie	Number	
RegisterType	String	

5. Documentación adicional

El portal de administración electrónica (PAe) reúne la información más actual de la plataforma cl@ve. Para su referencia incluimos también el perfil base de Web single-Sign-On del estándar SAML 2.0, y toda la documentación del proyecto STORK en el que está basada la plataforma cl@ve.

- **Cl@ve: Identidad electrónica para las Administraciones.**
  http://administracionelectronica.gob.es/ctt/clave

- **[MINHAPClave] Área de descargas del PAe (necesaria autenticación y acceso desde red SARA).**
  http://administracionelectronica.gob.es/ctt/clave/descargas

- **[SAML2WebSSO] Perfil WebSSO de SAML 2.0.**
  https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

- **[SIR2Clave] Perfil tecnológico cl@ve de SIR2.**
  https://www.rediris.es/sir2/politica/#perfiles-tecnológicos

- **[STORK] Área de documentación del proyecto STORK.**
  https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&id=312&Itemid=60