Breve introducción a SAML v2.0

Perfiles *Web Browser SSO Profiler* & *Single Logout Pofile*

JUNTA DE ANDALUCIA

Daniel García [@] prise es

Cándido Rodriguez [@] prise es

JUNTA DE ANDALUCIA

Tabla de contenidos

JUNTA DE ANDALUCIA

Antes de comenzar

- Quién sabe qué es un SSO
- … una federación
- … un IdP o proveedor de identidad
- … un SP o proveedor de servicio
- ... un contexto de seguridad
- … diferencia entra autenticación y atribución
- … relación de confianza en este contexto
- … una aserción
- … un agente de usuario (user agent)
- … un principal o sujeto

JUNTA DE ANDALUCIA

1. ¿Qué es SAMLv2.0?

JUNTA DE ANDALUCIA

¿Qué es SAMLv2.0?

- Según la wikipedia

> El Lenguaje de Marcado para Confirmaciones de Seguridad, conocido como SAML, (pronunciado como "sam-el") es un estándar abierto que define un **esquema XML** para el **intercambio de datos de autenticación y autorización**.

- Por lo que básicamente SAML es marco de trabajo basado en XML para intercambiar información sobre
  - Autenticaciones
  - Derechos
  - Información sobre atributos
  - Y otras cosas que queramos

¿Qué es SAMLv2.0?

- Seguramente lo conocéis como un protocolo
- Estandarizado por OASIS en Marzo de 2005
- La especificación completa comprende de 8 documentos
  - Assertions and Protocols [SAMLCore]
  - Bindings [SAMLBind]
  - Profiles [SAMLProf]
  - Metadata [SAMLMeta]
  - Authentication Context
  - Conformance Requirements
  - Security and Privacy Considerations
  - Glossary

¿Qué es SAMLv2.0?

- A parte de la especificación completa existen
- Un resumen ejecutivo (7 pág.)
- Y un resumen técnico (51 pág.)
- Para leer tranquilamente dejo estos enlaces

The original SAML 2.0 OASIS Standard set (PDF format) and XML Schema files are available in this ZIP file.

http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip

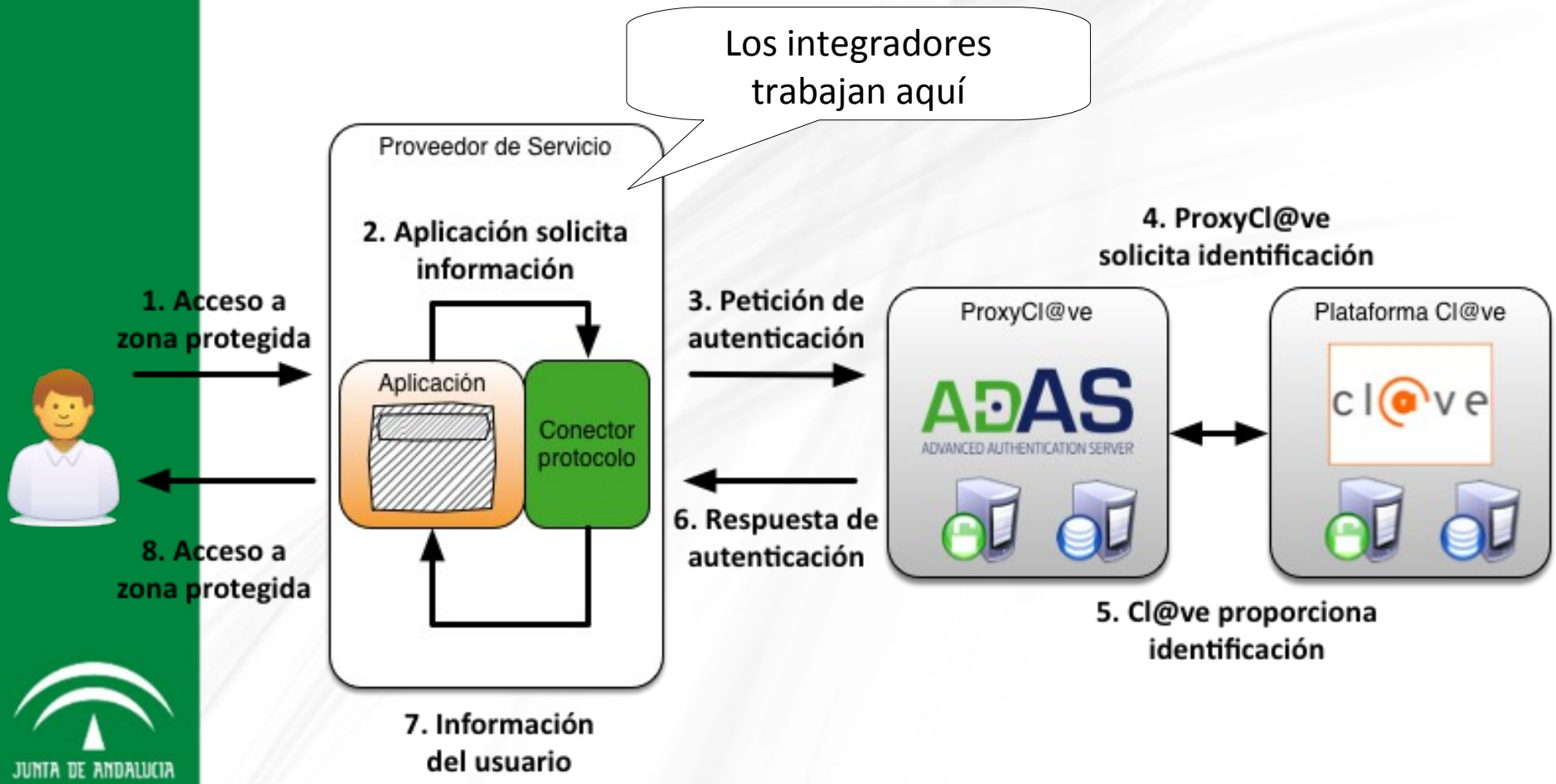
JUNTA DE ANDALUCIA

2. ¿Perfiles?

JUNTA DE ANDALUCIA

¿Perfiles?

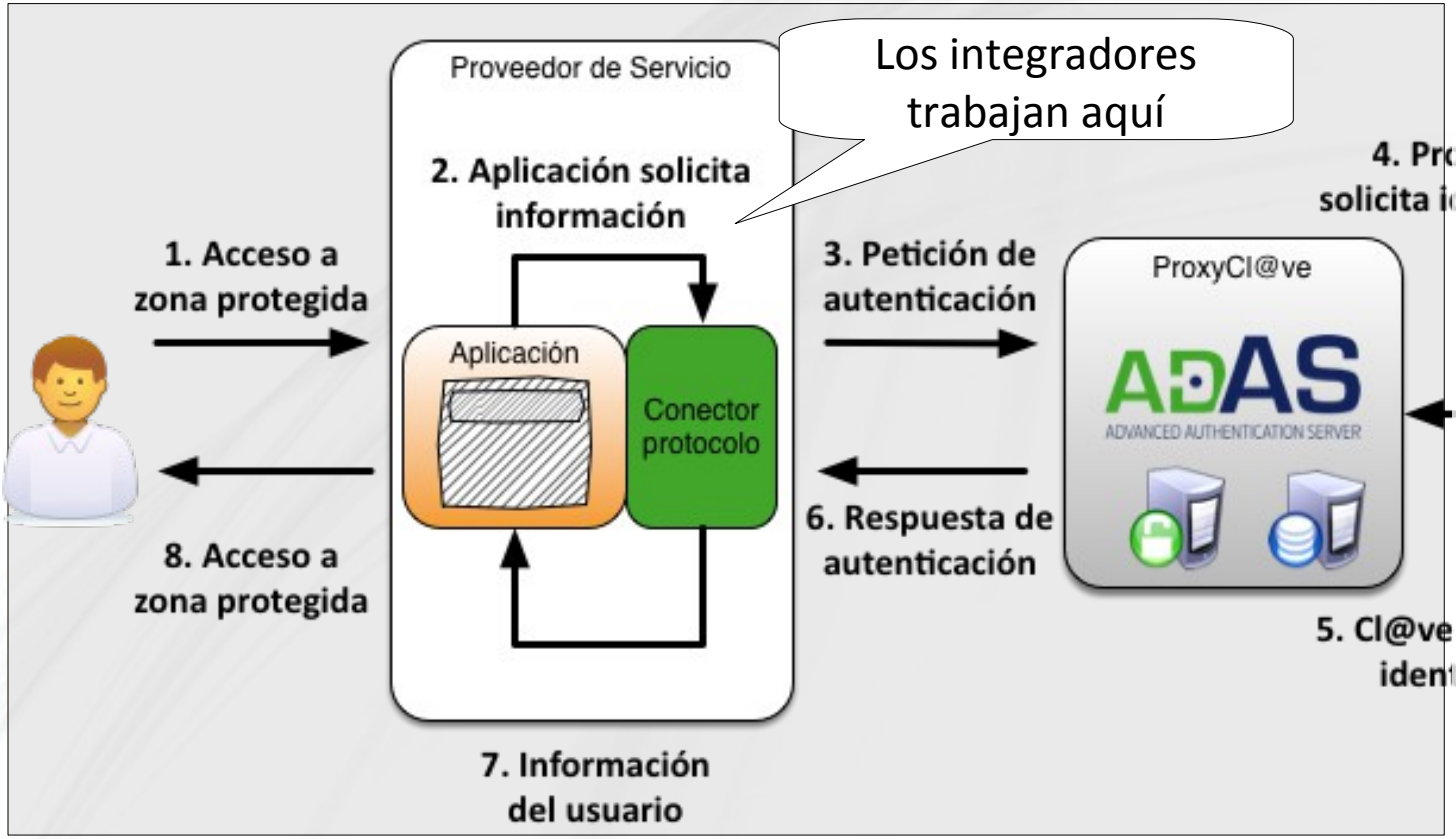
- Veamos antes el escenario que nos ha traído aquí ¿no?



JUNTA DE ANDALUCIA

¿Perfiles?

- Los perfiles SSO Web Browser y Single Logout son los que definen el comportamiento de la zona sombreada



JUNTA DE ANDALUCIA

¿Perfiles?

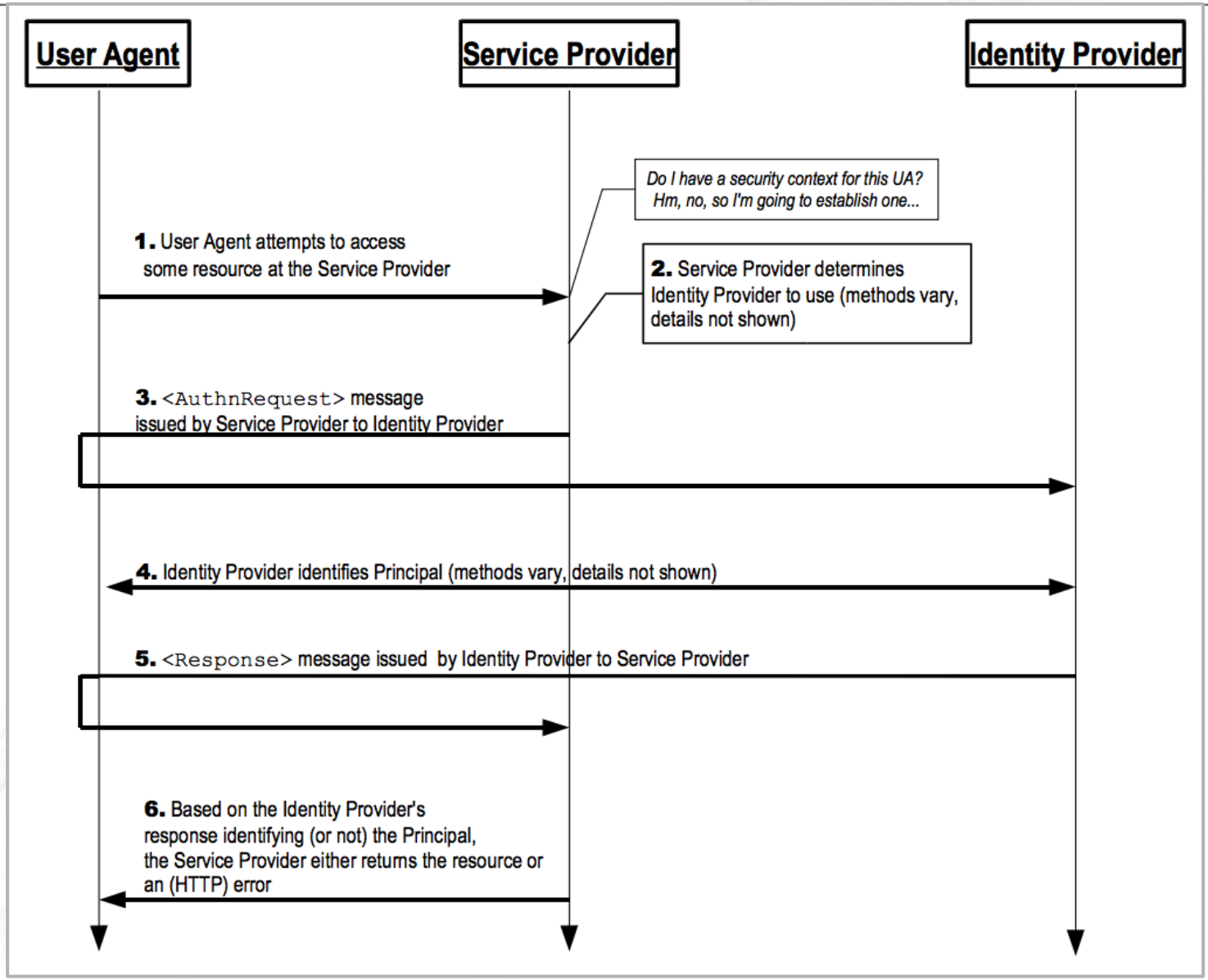
- Concepto de perfil SAMLv2
  - Un perfil esquematiza un conjunto de reglas definiendo como “añadir” y “extraer” **aserciones** SAML en y de un **protocolo**

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

¿Perfiles?

- Bien, podríamos decir que los casos de uso que resuelve la especificación SAML son los **perfiles**
  - Perfil SSO Web Browser
  - Caso de uso:
    - Autenticación de un sujeto por medio de un proveedor de identidad a petición de una aplicación
    - Todo ello en modo “user centric”, es decir, centrado en el usuario
      - Todos los menajes pasan por el agente web (navegador) del usuario

Perfil: SSO Web Browser



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

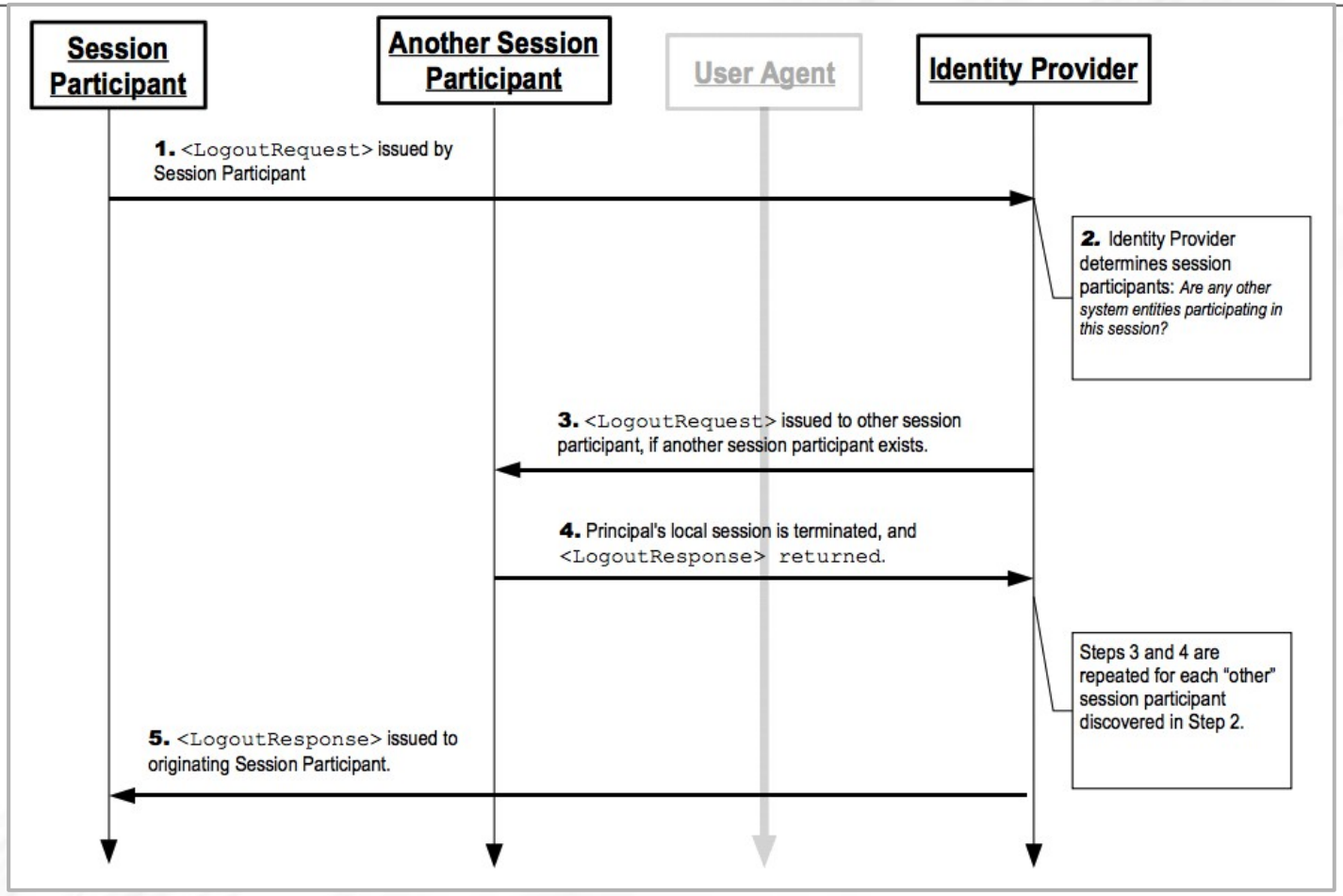
JUNTA DE ANDALUCIA

Perfil: SSO Web Browser

- 2 Mensajes usados (protocolo Authentication Request Protocol)
  - **<AuthRequest>** emitido desde el SP hacia el IdP
    - `ForceAuthn = [true|false]`
    - `<RequestedAuthnContext>` requiere un tipo de identificación
  - **<Response>** ó Artefacto devuelto desde el IdP hacia el SP
    - El SP procesa el mensaje y las `<Assertion>`(s) que pueda contener

JUNTA DE ANDALUCIA

Perfil: Single Logout



Fuente: Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.
Epígrafe 4.4.2 Profile Overview
Pág. 33

JUNTA DE ANDALUCIA

Perfil: Sigle Logout

- 2 Mensajes usados (protocolo Authentication Request Protocol)
  - **<LogoutRequest>** emitido desde un SP hacia el IdP
    - o (3) desde el IdP hacia un SP
    - Síncrono (SOAP Binding) o asíncrono (HTTP Redirect, POST, or Artifact bindings)
  - **<LogoutResponse>** emitido desde el IdP hacia un SP
    - O (4) desde un SP hacia un IdP
    - Síncrono o asíncrono

JUNTA DE ANDALUCIA

¿Perfiles?

- Hemos visto que los perfiles usan
  - Protocolos
    - Mensajes a intercambiar
  - Bindings
    - Métodos de transporte de mensajes
  - Aserciones
    - Información o datos sobre autenticación y autorización intercambiada entre SPs e IdP

3. Entidades, roles y relaciones

JUNTA DE ANDALUCIA

Entidades, roles y relaciones

Entidades SAML

Subject

Entidad que puede ser autenticada

Relying Party

Entidad que actúa en base a la información de otra

Asserting Party

Entidad que emite aserciones SAML

Roles en SSO Web Browser Profile

Service Provider

Usan las aserciones para controlar el acceso a los servicios que proporcionan a los usuarios

Identity Provider

Emite aserciones sobre los usuarios para los proveedores de servicios

Relaciones de confianza

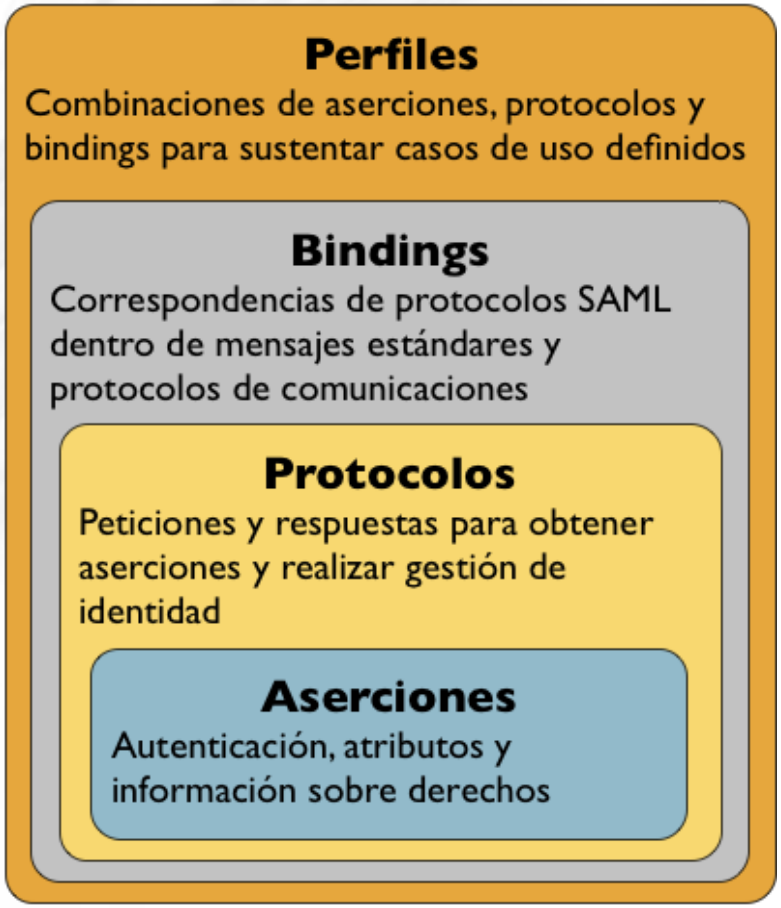
Metadatos

Información y datos de configuración para los proveedores de identidad (IdP) y para los proveedores de servicios (SP)

JUNTA DE ANDALUCIA

Entidades, roles y relaciones

- Perfiles
- Bindings
- Protocolos
- Aserciones



Entidades, roles y relaciones

- Componentes principales de un **Proveedor de Identidad**
  - **Servicio de SSO**: implementa el protocolo Authentication Request
    - Endpoint indicado metadatos `<md:SingleSignOnService>`
  - **Servicio de SLO**: implementa el protocolo Single LogOut
    - Endpoint indicado metadatos `<md:SingleLogoutService>`
  - **Servicio de resolución de artefactos**: implementa el protocolo Artifact Resolution
    - No se usa en proxyCl@ve

Entidades, roles y relaciones

- Componentes principales de un **Proveedor de Servicio**
  - **Servicio de Consumo de Aserciones**: implementa del protocolo Authentication Request
    - Endpoint indicado metadatos `<md:AssertionConsumerService>`
  - **Servicio de SLO**: implementa el protocolo Single LogOut
    - Endpoint indicado metadatos `<md:SingleLogoutService>`
  - **Servicio de resolución de artefactos**: implementa el protocolo Artifact Resolution
    - No se usa en proxyCl@ve

JUNTA DE ANDALUCIA

4. Aserciones en SAML v2.0

JUNTA DE ANDALUCIA

Aserciones

- Una aserción es una **afirmación** hecha por alguien (asserting party) a cerca de alguien (*subejct*)
  - Aunque el uso de un sujeto es opcional (no está definido en el estándar)
- Los **SPs** usan **aserciones** sobre **sujetos** para **controlar acceso** y proveer servicios personalizados.
- Esto es así dado que los **SPs** son *relying party* de una *asserting party*, esto es de un **IdP**

Aserciones

- SAML define 3 tipos diferentes de declaración de aserciones
  - Todas están asociadas con un sujeto
- Los tres tipos son:
  - **Autenticación**: El sujeto fue autenticado por un método concreto a una hora concreta
  - **Atributo**: El sujeto está asociado con los atributos suministrados
  - **Decisión de Autorización**: Una petición para permitir al sujeto acceder al recurso especificado a sido concedida o denegada

Aserciones

- Ejemplo: elemento <saml:Assertion>

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

JUNTA DE ANDALUCIA

Aserciones

- Ejemplo: elemento `<saml:Issuer>` y `<ds:Signature>`

```
<saml:Issuer>
  https://ws050.juntadeandalucia.es/proxyclavepru/
  metadata/federation/validation/ClaveSEQAA3
</saml:Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  …
</ds:Signature>
```

JUNTA DE ANDALUCIA

Aserciones

- Ejemplo: elemento <saml:Subject>

```
<saml:Subject>
 <saml:NameID
  SPNameQualifier="vea:unificado:cancanaprun"
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
  _8869961fb62b4b4f0d1fbbac266309925519eb80
 </saml:NameID>
 <saml:SubjectConfirmation
  Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
  <saml:SubjectConfirmationData
   NotOnOrAfter="2018-06-18T09:52:09Z"
   Recipient="https://cancanaprun1.chap.junta-
    andalucia.es/haciendayadministracionpublica/
    veauni_vea-webpru/DatosTicket"
  InResponseTo="afa289j1j2216205b6beh32h7de5bb"/>
 </saml:SubjectConfirmation>
</saml:Subject>
```

JUNTA DE ANDALUCIA

Aserciones

- Ejemplo: elemento `<saml:Conditions>`

```
<saml:Conditions
 NotBefore="2018-06-18T08:52:07Z"
 NotOnOrAfter="2018-06-18T09:52:09Z">
 <saml:AudienceRestriction>
  <saml:Audience>
   vea:unificado:cancanaprun
  </saml:Audience>
 </saml:AudienceRestriction>
</saml:Conditions>
```

JUNTA DE ANDALUCIA

Aserciones

- Ejemplo: elemento `<saml:AuthnStatement>`

```
<saml:AuthnStatement
 AuthnInstant="2018-06-18T08:52:07Z"
 SessionIndex="_e15361b0-72d4-11e8-8011-616263646566">
 <saml:AuthnContext>
  <saml:AuthnContextClassRef>
   urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
  </saml:AuthnContextClassRef>
  <saml:AuthenticatingAuthority>
   https://ws050.juntadeandalucia.es/proxyclavepru
   /metadata/federation/validation/ClaveSEQAA3
  </saml:AuthenticatingAuthority>
 </saml:AuthnContext>
</saml:AuthnStatement>
```

JUNTA DE ANDALUCIA

Aserciones

- Ejemplo: elemento `<saml:AttributeStatement>`

```
<saml:AttributeStatement
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <saml:Attribute
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  Name="citizenQAALevel"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xsi:type="xs:string">3
</saml:AttributeValue>
 </saml:Attribute>
 ...
```

JUNTA DE ANDALUCIA

Aserciones

- Ejemplo: elemento `<saml:Attribute>`

```
<saml:Attribute
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 Name="afirmaResponse"
 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
 <saml:AttributeValue
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xsi:type="xs:string">
   PD94gdmVy … c2lvbj0iMS4wlbmNv=
 </saml:AttributeValue>
</saml:Attribute>
...
```

JUNTA DE ANDALUCIA

Aserciones

- Ejemplo: elemento `<saml:Attribute>` Resto

```
<saml:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Name="eIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xsi:type="xs:string">ES/ES/00000002</saml:AttributeValue>
</saml:Attribute>

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

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

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

<saml:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Name="registerType"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xsi:type="xs:string">0</saml:AttributeValue>
</saml:Attribute>

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

JUNTA DE ANDALUCIA

5. Protocolos

JUNTA DE ANDALUCIA

Protocolos

- Del estándar... [SAMLCore]
- Los mensajes de los protocolos SAML pueden ser generados e intercambiados usando diferentes protocolos

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

- Si os fijáis habla de protocolos SAML y protocolos de transporte

Protocolos

- Importante
  - No confundir protocolos SAML con protocolos de transporte como pueden ser HTTP, SOAP, etc.
  - El uso o aplicación de los protocolos así como sus reglas de procesado, restricciones y requisitos se definen en [SAMLProf]
  - Los mensajes y las reglas básicas se definen en [SAMLCore]

Protocolos

- Los protocolos definidos por SAML “hacen” las siguientes acciones
  - Devuelven una o más aserciones solicitadas
  - “Disparan” la autenticación tras una petición y devuelven la aserción correspondiente
  - Registran un “name identifier” o eliminan su registro
  - Obtienen un mensaje de un protocolo que ha sido solicitado por medio de un artefacto
  - “Disparan” un cierre de sesión
  - Etc...

Protocolos: Authenticaction Request

- Usado por un “principal” o un **agente** en representación de este
- Para **obtener una aserción** con una declaración de **autenticación**
- Que permita **establecer un contexto de seguridad** en uno o más SPs
- Envía un mensaje `<AuthnRequest>` a un IdP requiriendo que devielva unmensaje `<Response>`

JUNTA DE ANDALUCIA

Protocolos: **Authenticaction Request**

- Mensaje de petición de autenticación.

  Elemento `<AuthnRequest>`

  - Debe (SHOULD) ser firmado, en otro caso la privacidad e integridad debe ser proporcionada por el Binding usado (HTTP sobre TLS, en el caso del binding HTTP-GET)
- Mensaje de respuesta de autenticación.

  Elemento `<Response>`

  - Dependiente del perfil y el binding utilizado...

JUNTA DE ANDALUCIA

Protocolos: **Single Logout**

- Proporciona mensajes para que todos los SPs con sesión de un mismo IdP la cierren casi simultáneamente
- Para ello el sujeto desea cerrar la sesión bien en un SP, o bien en el IdP
- Permite identificar el motivo por el que se desea el cierre de la sesión
- Cuando el sujeto solicita un cierre de sesión a un SP éste debe (MUST) enviar un mensaje `<LogoutRequest>` al IdP
- Se debe (MUST) responder con un mensaje `<LogoutResponse>`

Protocolos: **Single Logout**

- **¡IMPORTANTE!**
- Esto no es SAML, sino de uso de biblioteca SAML
- Al recibir una petición de cierre de sesión en vuestra aplicación, invocad a vuestra biblioteca SAML para que emita la petición de LOGOUT a ProxyCl@ve antes de cerrar la sesión.
- Cerrad la sesión cuando vuestra biblioteca os informe de
  - A) Una petición de LOGOUT
  - B) Una respuesta de LOGOUT
- Al final con un diagrama

6. Bindings

Bindings

- Del estándar... [SAMLBind]
- La correspondencia entre el intercambio de mensajes de petición y respuesta SAML en mensajes estándares o protocolos de comunicación se conoce en SAML como *SAML protocol bindings* o sólo *bindings*
- Por ejemplo el Binding SOAP describe como se intercambian peticiones y respuestas SAML dentro de mensajes SOAP
- Por tanto... **definen la capa de transporte SAML**

Bindings

- Los perfiles SSO Web Browser y Single Logout usan los bindings
  - HTTP Redirect, HTTP POST y HTTP Artifact bindings
  - SOAP, HTTP Redirect, HTTP POST y HTTP Artifact bindings
- Nos centraremos en los disponibles en ProxyCl@ve:
  - HTTP Redirect y HTTP POST

JUNTA DE ANDALUCIA

Bindings: HTTP Redirect

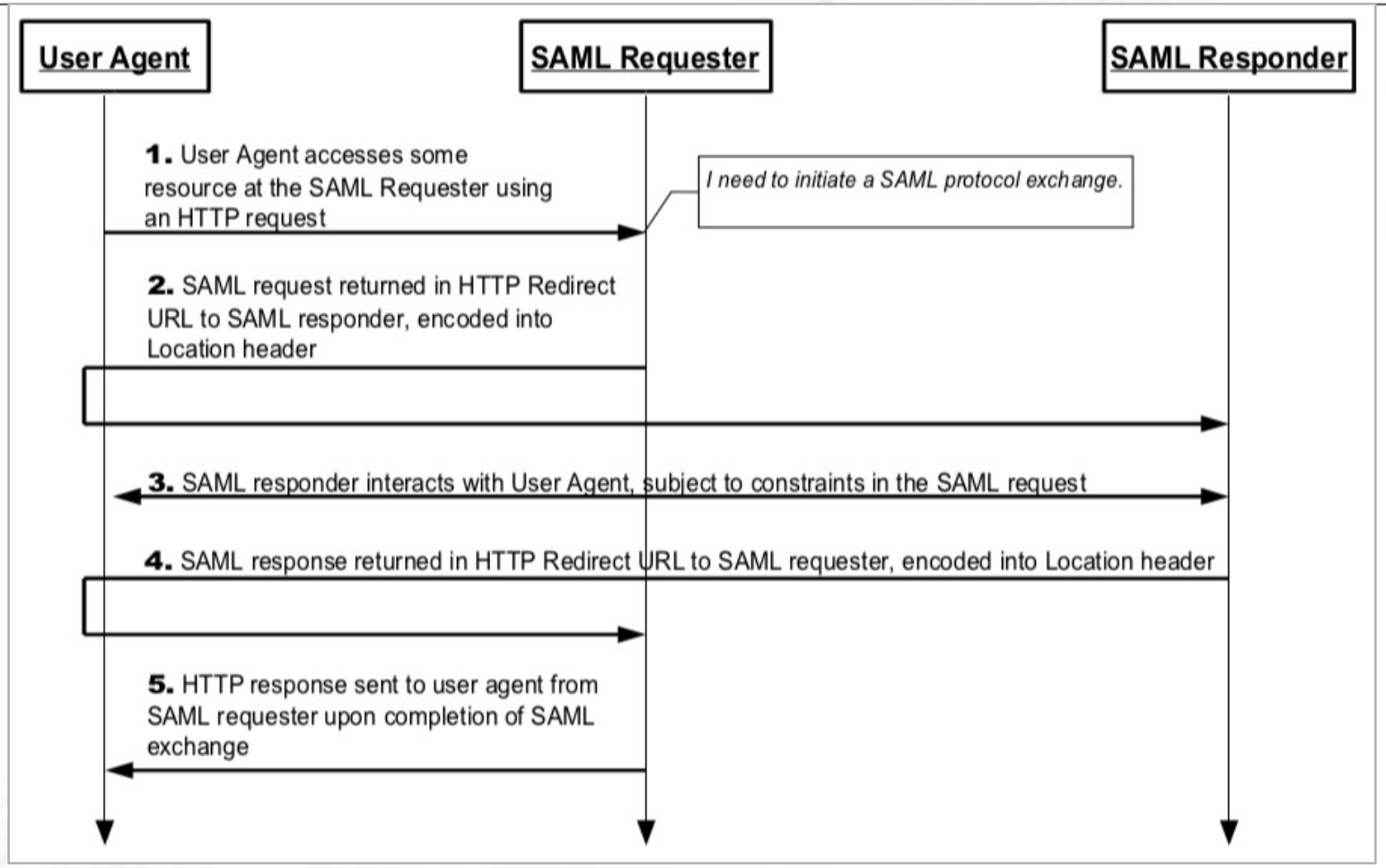
- Consiste en enviar los mensajes como parámetros de peticiones HTTP GET y hacer uso de respuestas HTTP con código de estado 302
  - Esto es, redirecciones
- El tamaño de una petición GET no está restringido... pero en la práctica esto no es real
- Se ha de codificar los mensajes XML para transportarlos en una URL
- Por lo que lo mensajes de mayor tamaño o más complejos se suelen dejar para bindings como HTTP-POST o HTTP Artifact.

Bindings: HTTP Redirect

- En el perfil SSO Web Browser se suele utilizar para enviar los mensajes de petición de autenticación

JUNTA DE ANDALUCIA

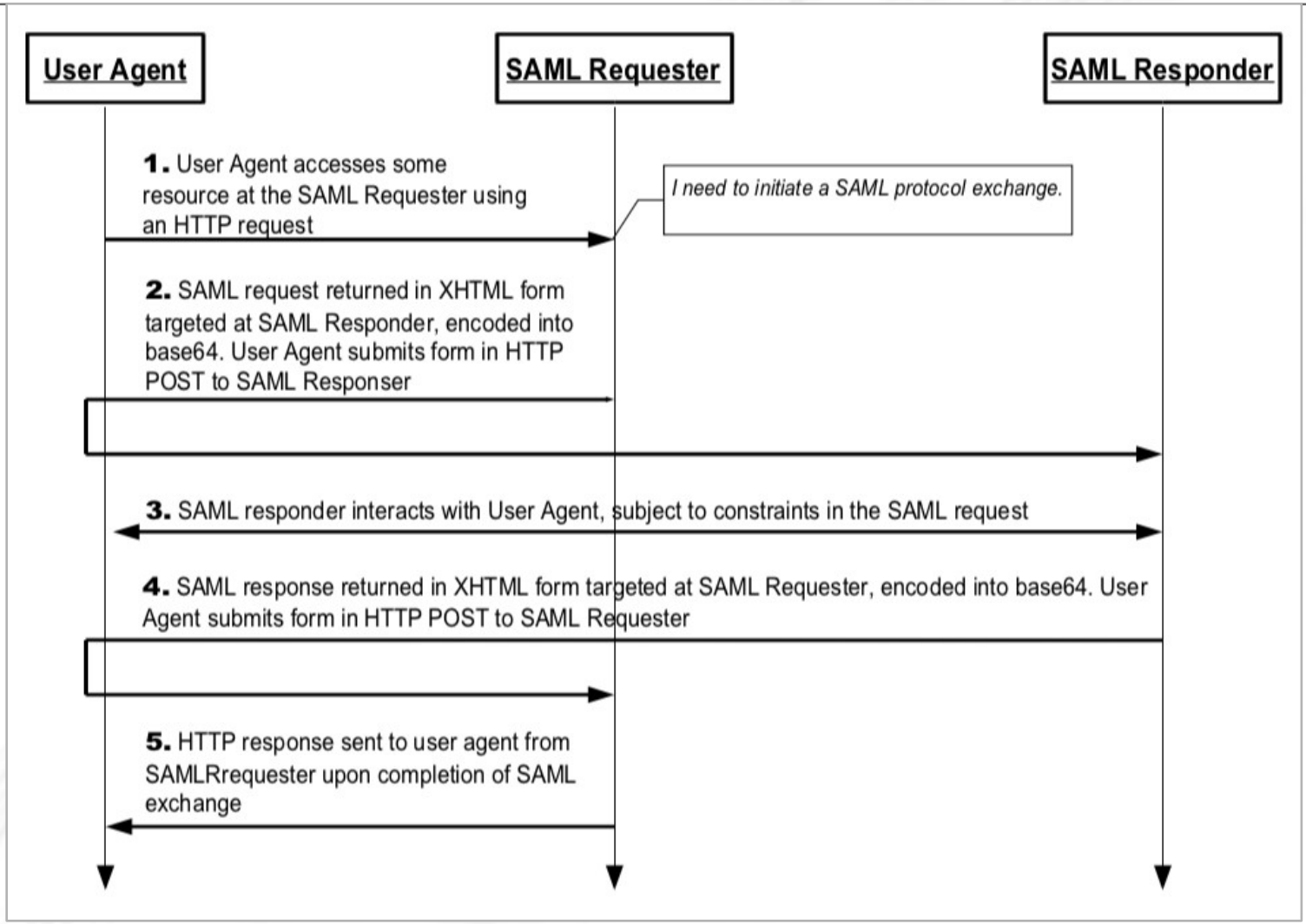
Bindings: HTTP Redirect



Bindings: HTTP POST

- Consiste en enviar los mensajes dentro del contenido de un formulario HTML, codificados en base64.
- Se usa cuando nos encontramos en un escenario “user centric”, es decir, todo el contenido de los mensajes pasa por el agente web del usuario.

Bindings: HTTP POST



JUNTA DE ANDALUCIA

7. Metadatos

JUNTA DE ANDALUCIA

Metadatos

- Del estándar … [SAMLMeta]
- Los perfiles SAML requieren “acuerdos” sobre identificadores, bindings soportados, “endpoints”, certificados y claves, etc, entre las entidades del sistema
- Qué significa esto...
- Que las entidades que forman el sistema deben saber:
- Dónde preguntar y dónde responder
- Cómo preguntar y cómo responder
- Qué preguntar qué responder

Metadatos

- Para esto se usan y se intercambian los metadatos
- En un SSO...
  - El IdP debe saber a qué SPs atender/responder
  - Los SPs deben saber dónde escucha el IdP y que bindings soporta
  - Ambos deben intercambiarse certificados para realizar operaciones de firma y cifrado
  - Unos y otros deben poder identificarse entre ellos

Metadatos

- Los metadatos son un documento XML
- Se recomienda firmadolos por la entidad a la que pertenecen
- Esta firma permite mantener la integridad
- Identificar los metadatos (si se usa AC reconocida)

JUNTA DE ANDALUCIA

Metadatos

- Elementos XML importantes [producción]
- Raíz
  - <EntitiesDescriptor>
  - <EntityDescriptor>
  - <Organización>
  - <ContactPerson>
  - <AdditionalMetadataLocation>

JUNTA DE ANDALUCIA

Metadatos

- Elementos XML importantes [producción]
- Descriptores de rol
  - <IDPSSODescriptor>
  - <SPSSODescriptor>
    - <AttributeConsumingService>
    - <RequestedAttribute>
  - <AuthnAutorityDescriptor>
  - <PDPDescriptor>
  - <AttibuteAuthorityDescriptor>

JUNTA DE ANDALUCIA

Metadatos: **ProxyCl@ve**

- URL de producción

https://ws050.juntadeandalucia.es/proxyclaveexp/metadata/federation/production

- Actualmente (ayer) hay
  - 3 IdPs
  - 13 SPs
- Veamos algunos

JUNTA DE ANDALUCIA

Metadatos: ProxyCl@ve IdPs

- IdP ClaveSEQAA2
  - <md:EntityDescriptor **EntityID**="...**ClaveSEQAA2**">
  - <md:KeyDescriptor ... use="**signing**">
  - <md:KeyDescriptor ... use="**encryption**">
  - <md:**SingleLogoutService**
    Binding="...:HTTP-Redirect"
    Location=".../ClaveSEQAA2/SAML2/SLOService.php">
  - <md:**SingleSignOnService**
    Binding="...:HTTP-Redirect"
    Location=".../ClaveSEQAA2/SAML2/SSOService.php"/>
  - <md:**SingleSignOnService**
    Binding="...:HTTP-POST"
    Location=".../ClaveSEQAA2/SAML2/SSOService.php"/>

JUNTA DE ANDALUCIA

Metadatos: ProxyCl@ve SPs

- SP pruebaProxyClave
  - <md:EntityDescriptor **EntityID**="**pruebaProxyClave**">
  - <ds:Signature>...</ds:Signature>
  - <md:**SPSSODescriptor** AuthnRequestsSigned="true" WantAssertionsSigned="true" ...>
  - <md:KeyDescriptor … use="**signing**">
  - <md:KeyDescriptor … use="**encryption**">
  - <md:**SingleLogoutService** Binding="...:HTTP-Redirect" ...>
  - <md:**SingleLogoutService** Binding="...:HTTP-POST" ...>
  - <md:**AssertionConsumerService** Binding="...:HTTP-POST" Location="..."/>

JUNTA DE ANDALUCIA

Metadatos

- Fallos comunes tras enviar metadatos
  - No firmarlos
  - Modificar el entityID
  - AssertionConsumerServiceURL

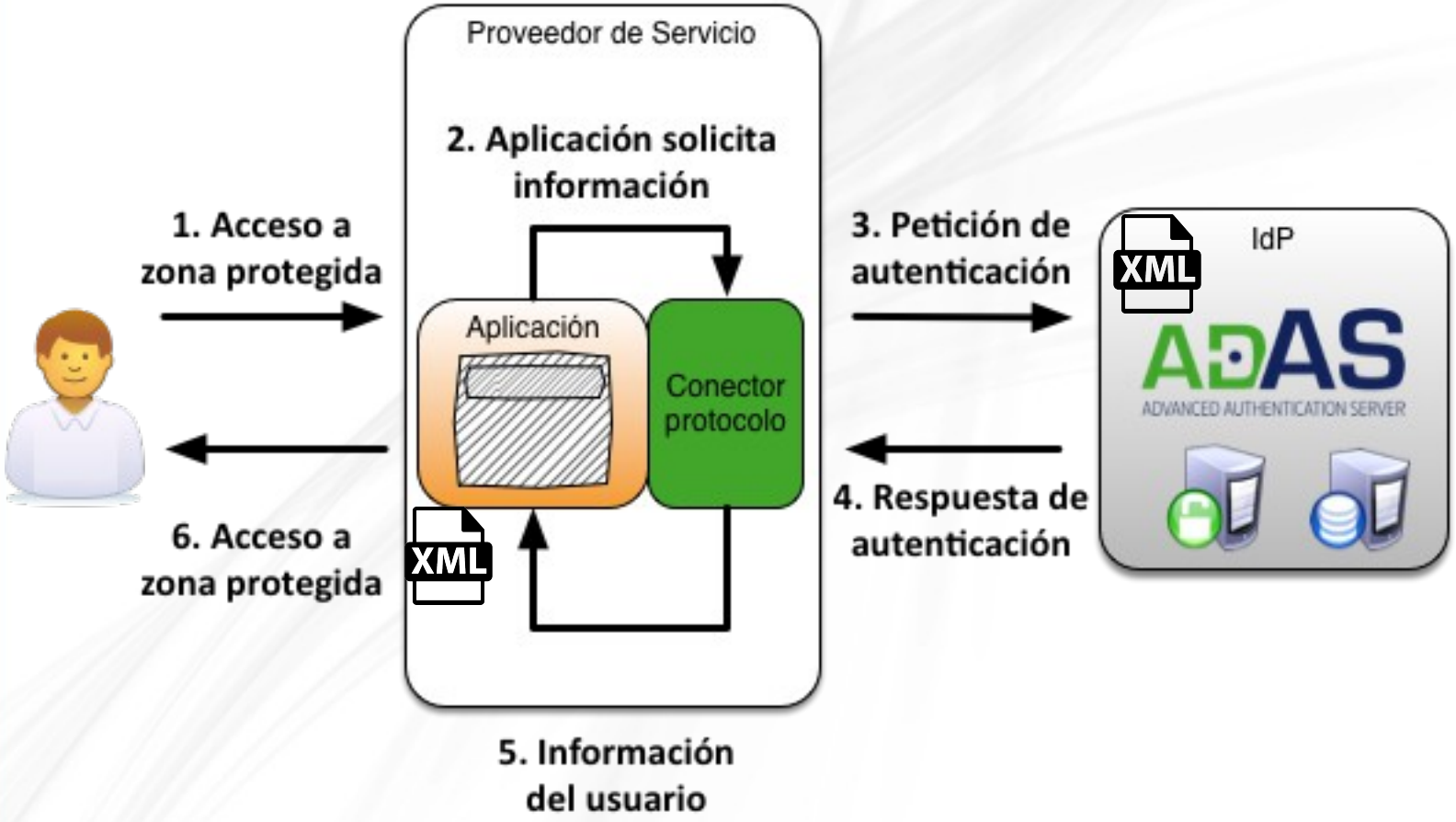
JUNTA DE ANDALUCIA

8. Escenario completo

JUNTA DE ANDALUCIA

Escenario completo

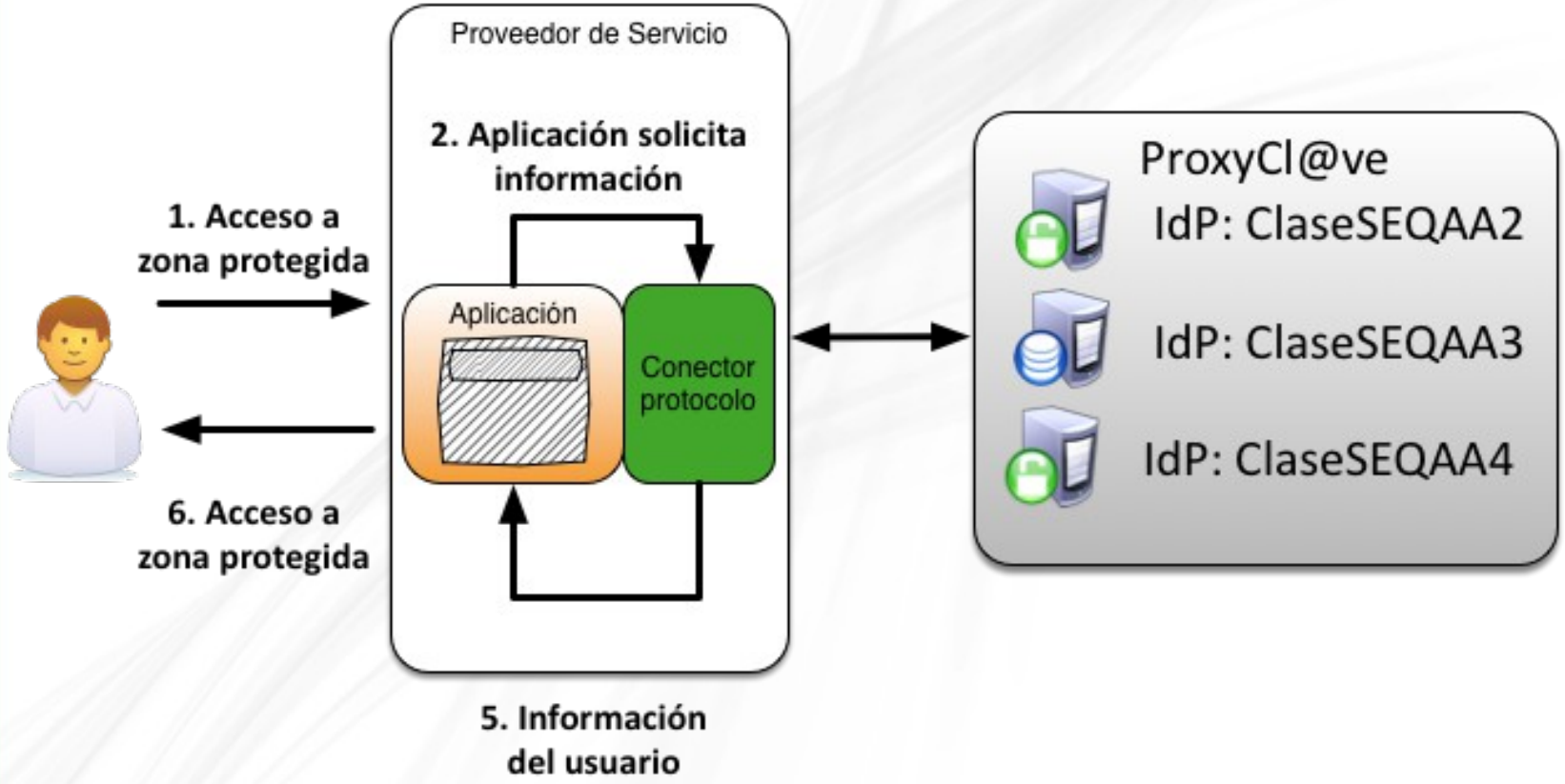
- Escenario de un SSO



JUNTA DE ANDALUCIA

Escenario completo

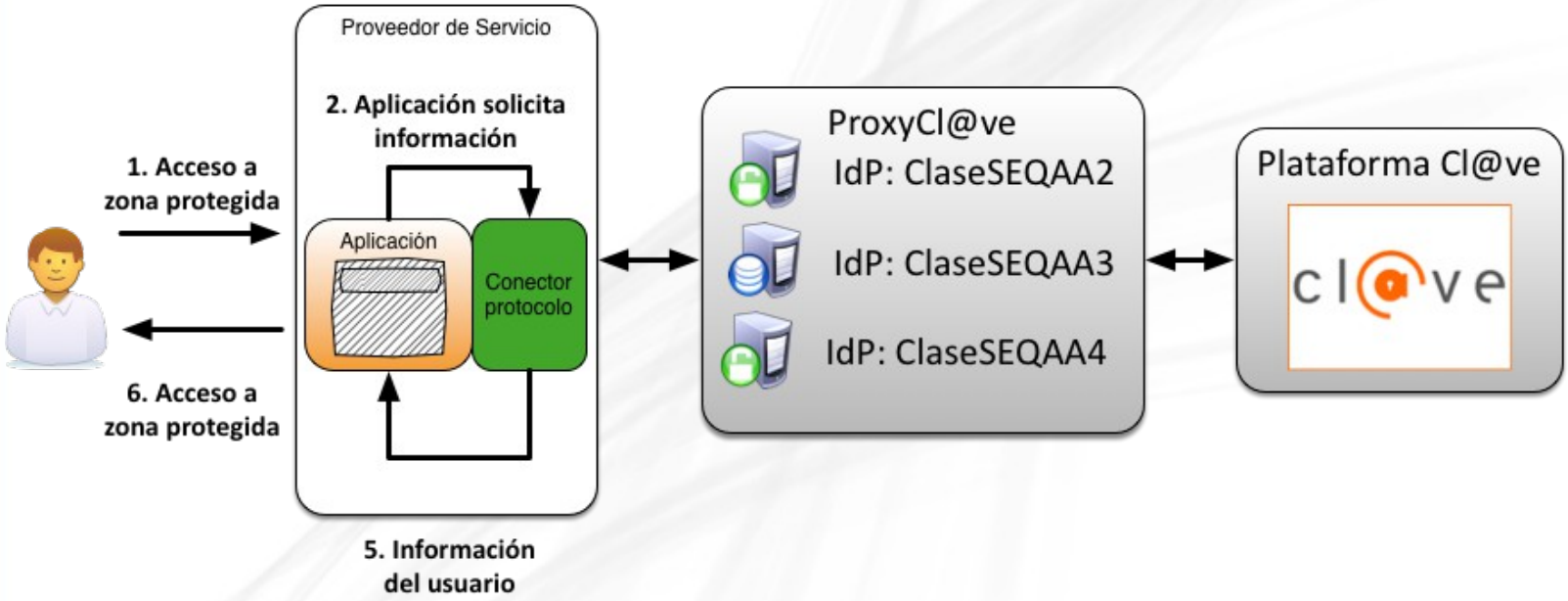
- Escenario ProxyCl@ve sólo SAML



JUNTA DE ANDALUCIA

Escenario completo

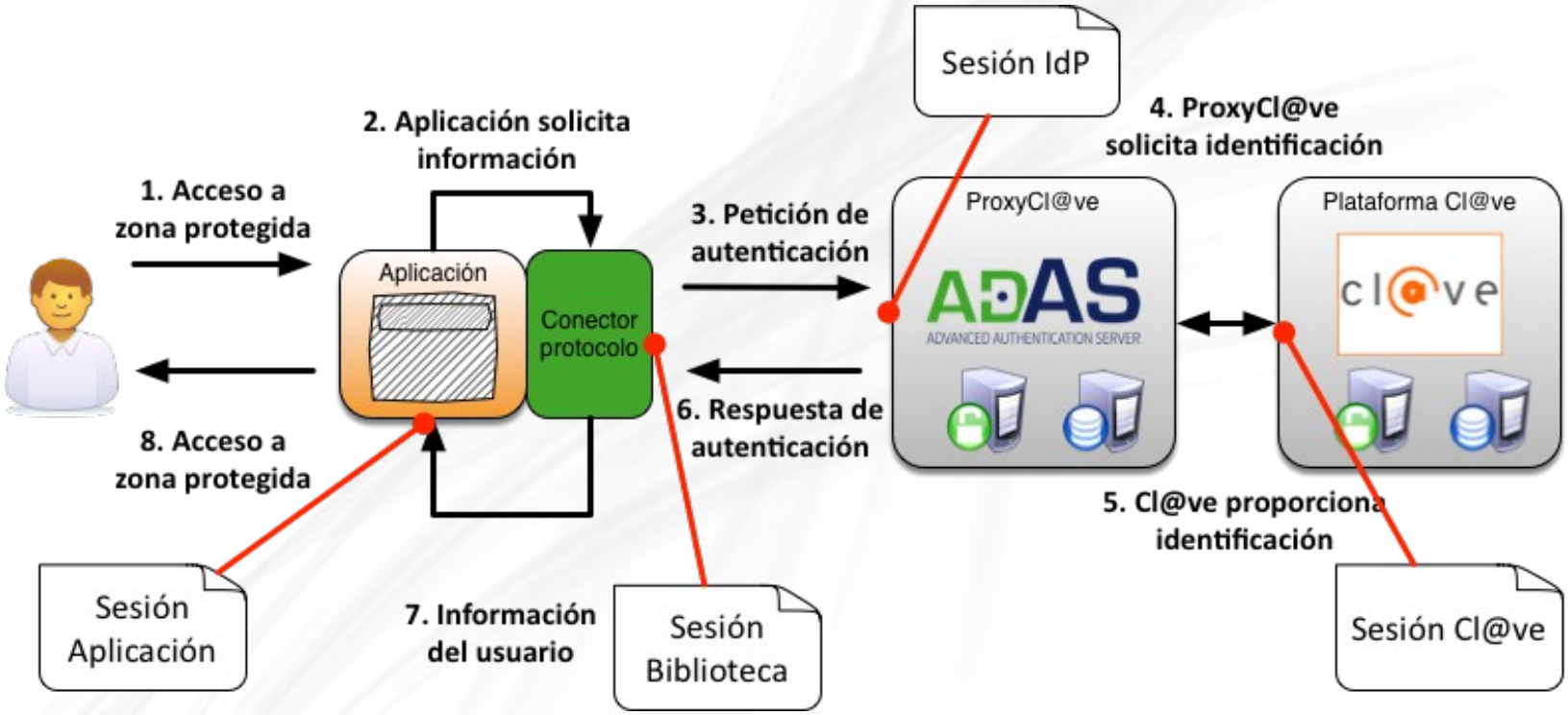
- Escenario ProxyCl@ve completo



JUNTA DE ANDALUCIA

Escenario completo

- Sesiones en los componentes (cookies)



Preguntas

JUNTA DE ANDALUCIA

Gracias por su atención

JUNTA DE ANDALUCIA