Autenticación @firma v5

Nueva fachada de autenticación

Migración de la autenticación web a la fachada de tickets

Febrero 2009

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 - Fachada de ticket -

- Plataforma @firma
- Autenticación y Tipos
  - WebServices
  - Fachada
- Fachada de autenticación web (extensión)
- Fachada de autenticación por tickets (nativa)
- Adaptación de la aplicación
- Notas
- Ejemplos de integración

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 - Fachada de ticket -

- **Plataforma @firma**
- Autenticación y Tipos
  - WebServices
  - Fachada
- Fachada de autenticación web (extensión)
- Fachada de autenticación por tickets (nativa)
- Adaptación de la aplicación
- Notas
- Ejemplos de integración

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -

¿Qué es @Firma?

- Es una plataforma electrónica que utiliza certificados digitales X.509 v3 según las principales recomendaciones y estándares internacionales (RFC 2360, 3280, ETSI TS 101 733 v1.5.1, etc.) para la generación y validación de firmas digitales en múltiples formatos (CMS, XADES, XMLDSignature…), así como la validación avanzada de certificados digitales para garantizar en todo momento la integridad y validez de los mismos en el momento de la realización de una firma.

- Versiones de @firma
  - V3.x (Fielato, Consejería de Hacienda)
  - V4.x (Junta de Andalucía: C. Justicia, C. Medio Ambiente, etc.)
  - V5.x (Ministerio de Administraciones Públicas – Junta de Andalucía). Actualmente en uso la versión 5.0.1_05 en la Consejería de Justicia y Administración Pública.

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 - Fachada de ticket -

- Plataforma @firma
- **Autenticación y Tipos**
  - **WebServices**
  - **Fachada**
- Fachada de autenticación web (extensión)
- Fachada de autenticación por tickets (nativa)
- Adaptación de la aplicación
- Notas
- Ejemplos de integración

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -

Sistema de Autenticación y Tipos

El módulo de Autenticación es un sistema genérico y centralizado basado en certificados digitales, que permite a cualquier aplicación ya desarrollada o por desarrollar delegar el proceso de autenticación en este sistema.

El módulo de Autenticación contiene las interfaces y componentes web necesarios para la realización de los siguientes procesos:

- *Autenticación mediante WebServices Nativa*
- *Autenticación/Reautenticación Web.*

Autenticación @firma v5 – Fachada de ticket -

Autenticación por WebService (Nativa)

Mediante una comunicación directa mediante WS con el núcleo la aplicación se produce la autenticación, la aplicación será la encargada de extraer los datos del certificado y enviárselos a la aplicación mediante los métodos nativos de la aplicación

Es necesario la ejecución del cliente de firma, por lo que nos garantizamos al inicio de la aplicación el correcto funcionamiento del cliente

En la Migración de @firma 4 a @firma 5, Utilizando el nuevo WSDL, se puede generar la estructura necesaria para la comunicación entre la aplicación y la plataforma de @firma v5

https://<servidor_firma>:<puerto>/axis/servlet/AxisServlet

La modificación fundamental es la información que se envía y que se recibe en esa comunicación.

- *En @firma 4 y la Extensión se utilizaba un conjunto de objetos para la comunicación*
- *En @ Firma v5, la información está contenida en cadenas de texto, formadas por el contenidos de ficheros XML, que hay que procesar tanto para enviar como al recibir.*

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -

Fachada de autenticación web

La obtención de los datos del certificado para la autenticación se apoya en una fachada encargada de realizar la extracción del certificado. En este caso no es necesario el cliente. En aplicaciones que sólo utilice autenticación será menos pesado.

Las aplicaciones Web que empleen tecnología de páginas Web dinámicas en el servidor podrán hacer uso del sistema de autenticación mediante certificados digitales X. 509 basado en tickets. La base de este sistema de autenticación se centra en el protocolo SSL. La versión 3 de este protocolo y las versiones TLS permiten la opción del establecimiento de conexiones seguras usándose certificados reales (no generados por el protocolo) en ambos extremos de la conexión.

Esto junto a un navegador que acepte conexiones SSL v3 o TLS y un servidor correctamente configurado permite llevar a cabo de forma simple el sistema de autenticación por certificados

REQUERIMIENTOS: Identificación – Autenticación – Confidencialidad

FASES: Autenticación – Autorización

BASES: Certificado - SSL

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

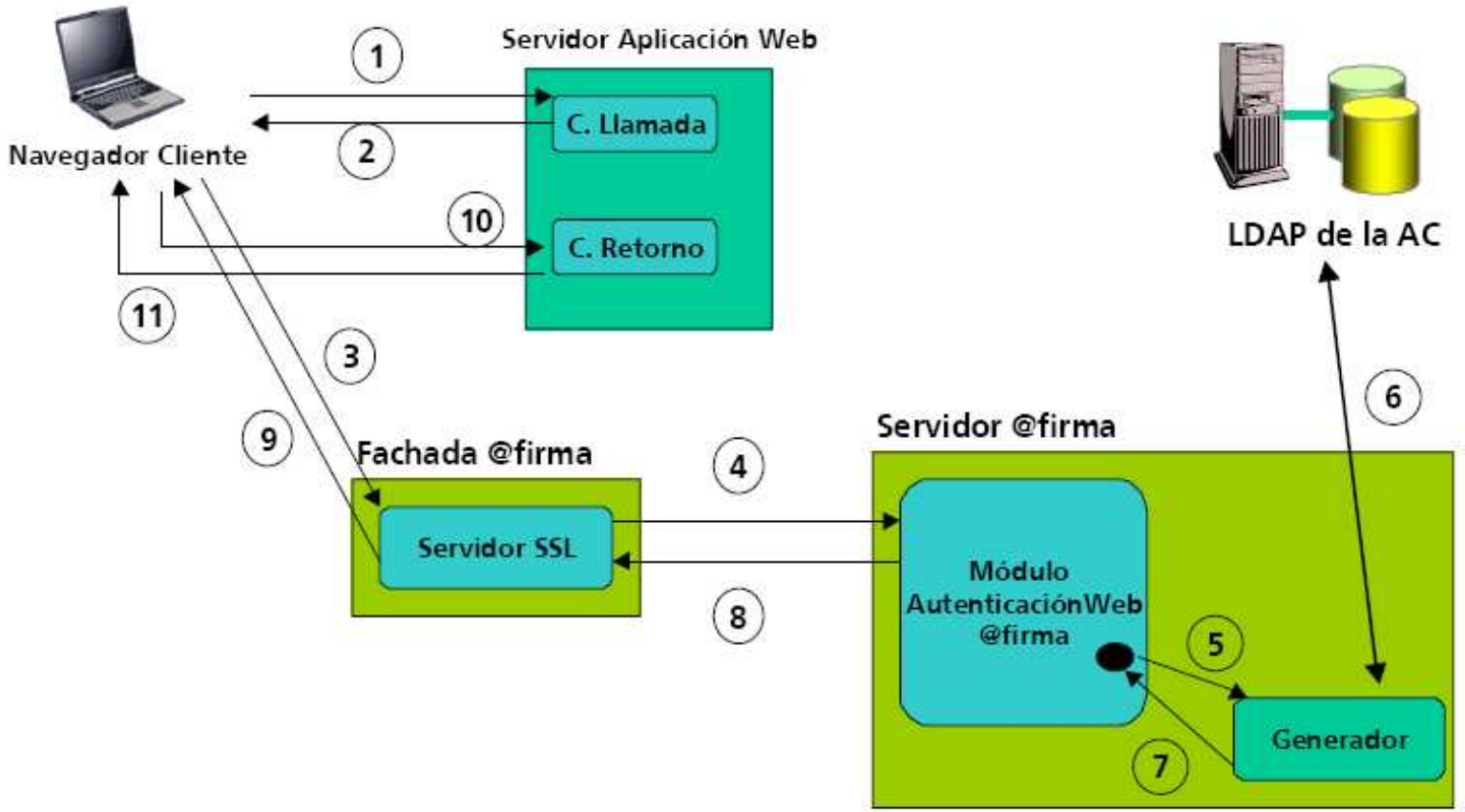
Autenticación @firma v5 - Fachada de ticket -

- Plataforma @firma
- Autenticación y Tipos
  - WebServices
  - Fachada
- **Fachada de autenticación web (extensión)**
- Fachada de autenticación por tickets (nativa)
- Adaptación de la aplicación
- Notas
- Ejemplos de integración

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -

Fachada de autenticación web



JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -

1. El Navegador Cliente accede al Componente de Llamada.
2. El Componente de Llamada redirecciona al cliente web hacia el ServidorSSL.
3. El navegador establece la conexión https y le pide al usuario que seleccione el certificado que se enviará al ServidorSSL (SSL v 3.0).
4. El ServidorSSL obtiene el certificado y los parámetros (nombre aplicación y valor aleatorio) de la llamada con los que realiza una petición RMI-IIOP al ModuloAutenticacionWeb, securizada mediante SSL y JAAS.
5. El ModuloAutenticacionWeb crea el generador asociado a la aplicación.
6. El generador verifica la validez del certificado y comprueba su estado de revocación.
7. El generador saca la información del certificado y genera con ella un objeto Subject.
8. El ModuloAutenticacionWeb encripta con la clave 3DES el resultado del proceso, lo codifica en Base64 y lo devuelve al ServidorSSL.
9. El ServidorSSL genera la llamada al Componente de Retorno pasando como parámetro los datos encriptados.
10. EL navegador realiza la llamada al Componente de Retorno el cuál decodifica los datos en Base 64 y los desencripta con la clave 3DES. Con los datos del certificado devueltos se procede a realizar la fase de autorización.
11. En base a las comprobaciones anteriores el Componente de Retorno devuelve el control a la aplicación para que proceda a la fase de autorización, o redirecciona a una página de error indicando el error producido.

Autenticación @firma v5 – Fachada de ticket -

JSP **response.sendRedirect(url_servidor+"?**

ap="+idaplicacion+"&sesion="+sessionID);

Retorno Certificado

1) **Recogemos los datos de la request**
2) **Con la clave 3DES descodificamos**
3) **Extraemos los campos en un objeto tipo**

CertificateUserVO

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 - Fachada de ticket -

- Plataforma @firma
- Autenticación y Tipos
  - WebServices
  - Fachada
- Fachada de autenticación web (extensión)
- **Fachada de autenticación por tickets (nativa)**
- Adaptación de la aplicación
- Notas
- Ejemplos de integración

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

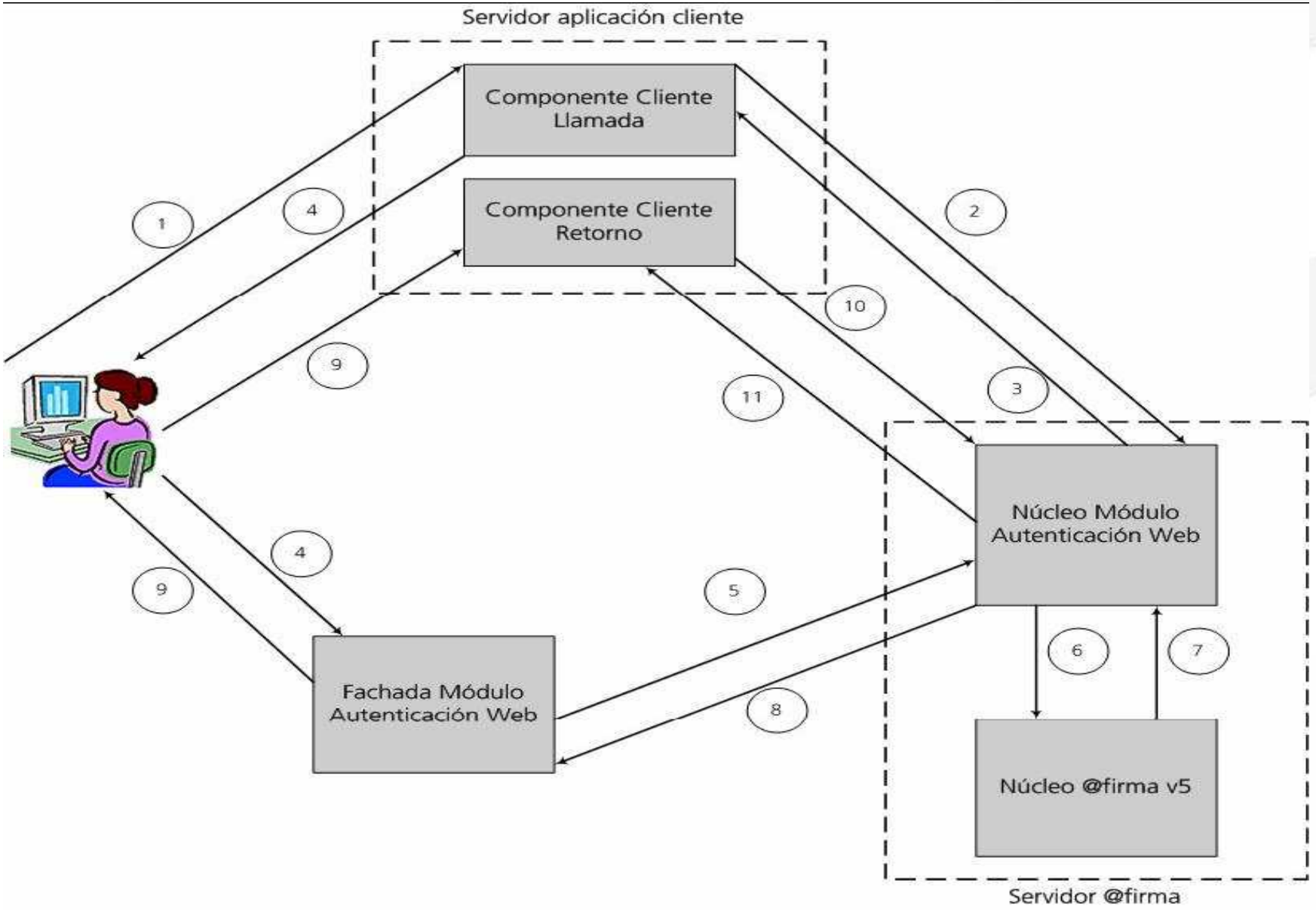
Autenticación @firma v5 – Fachada de ticket -

Fachada Autenticación VS Fachada Ticket

- Independencia de la extensión
- La respuesta con los datos del certificado ya no pasa por el navegador, la comunicación es directa entre la aplicación y @firma
- Generalización de las distintas entradas, en la extensión se guardaba la dirección de retorno, por lo que era necesario tener una alta (distinto identificador) para cada una de las URL desde las que se pudiese acceder. En la nueva fachada, la dirección de retorno la envía en la propia comunicación.
- Seguridad, Utiliza no sólo la comunicación SSL, que garantiza la autenticidad del servidor web y negociado de una clave DES que será utilizada para cifrar los siguientes mensajes a ser intercambiados. Sino que además utiliza la negociación en modo cifrado, con la utilización de un sistema de clave pública (RSA o similar), a partir del certificado digital del servidor Web. Este mecanismo garantiza que ningún intruso tome conocimiento de la clave simétrica a ser utilizada en el transcurso de la sesión. Cada mensaje intercambiado durante esa sesión está protegido, además de la criptografía, por un número de secuencia y por un código de autenticación de mensaje, que refuerza la garantía de integridad y es generado utilizando una función de resumen aplicada sobre el cómputo del mensaje, número de secuencia, la clave utilizada y algunas constantes.

Autenticación @firma v5 – Fachada de ticket -

Autenticación por Fachada de Ticket



Autenticación @firma v5 – Fachada de ticket -

1) El navegador cliente accede al Componente Cliente de Llamada de la aplicación en la que desea autenticarse.

2) El Componente de Llamada realiza una llamada Web Service al núcleo del módulo de Autenticación Web pasándole como parámetros: Identificador de aplicación Y Identificador de sesión Web.

3) El núcleo del módulo de Autenticación Web inicia una transacción de autenticación y genera un ticket o identificador de transacción.

4) Dicho ticket será empleado en el componente de llamada, que junto con el identificador de aplicación, identificador de sesión Web y URL del componente de retorno será lo único que circule entre Aplicación <-> Usuario <-> Fachada del módulo de Autenticación Web.

5) Se almacena el ticket unto con el identificador de aplicación en la sesión Web y posteriormente se envía al usuario el ticket generado, junto con el identificador de aplicación y sesión Web, que lo redirige al componente Fachada del módulo de Autenticación Web para obtener su certificado.

6) El componente fachada obtiene el certificado, el ticket de la llamada, el identificador de aplicación y de sesión y realiza una petición de validación de certificado asociado a ticket al núcleo del módulo de Autenticación Web.

Autenticación @firma v5 – Fachada de ticket -

7) El núcleo del módulo de Autenticación verifica que el ticket generado es válido y procede a realizar la validación del certificado mediante el núcleo de la plataforma.

8) La respuesta obtenida es asociada al ticket, indicado en la solicitud de validación, por el núcleo del módulo de Autenticación Web.

9) El componente fachada recibe el resultado de la validación y redirige el flujo de comunicación, a través del usuario, al componente de retorno. A la URL indicada le serán concatenados un código de finalización, el identificador de ticket y sesión Web.

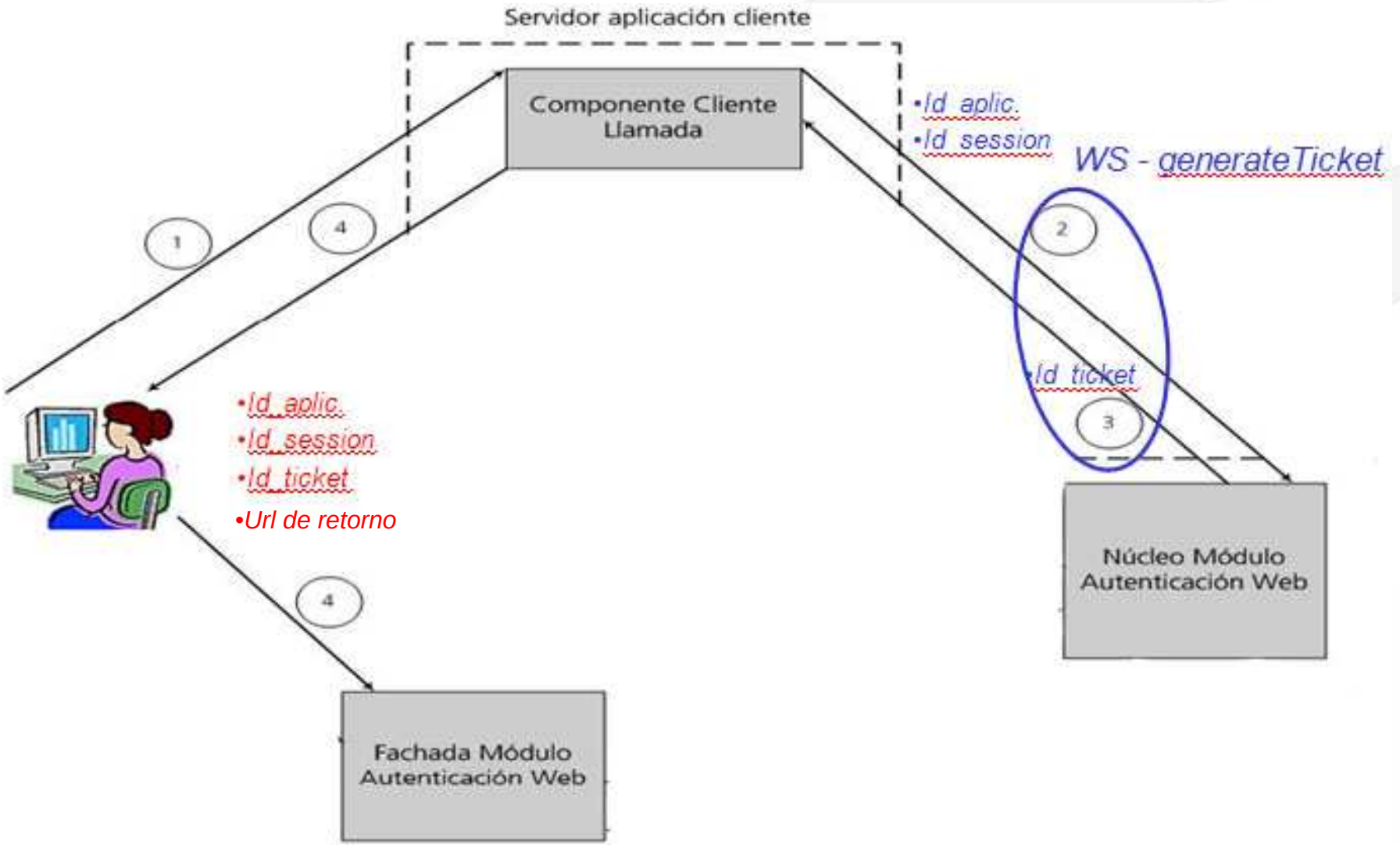
10) El componente de retorno de la aplicación recibe el código de finalización, comprueba que es correcto, valida los parámetros presentados en la URL con los almacenados en sesión y, si todo es correcto, procederá a consultar al núcleo del módulo de Autenticación Web los datos del usuario asociados al ticket presentado mediante una llamada Web Service.

11) El núcleo del módulo de autenticación verifica si existe información disponible para el ticket solicitado y se la devuelve a la aplicación. La información devuelta será el resultado de la autenticación y mediante la cual la aplicación podrá iniciar la fase de autorización.

Autenticación @firma v5 – Fachada de ticket -

Componente Cliente - Solicitar Ticket

Solicitamos un id_ticket al núcleo y se inicia una autenticación



Autenticación @firma v5 – Fachada de ticket -

Autenticación Fachada de ticket

SolicitarTicket

1) **Llamada WS al modulo de autenticación para obtener un nuevo ticket**

   Datos Necesarios : Id Aplicación e ID session → Estructura XML (input) → Llamada al servicio → Estructura XML (output) → Objeto Map

2) **Extraemos el código de ticket, lo guardamos en la request**

3) **Codificamos los campos de la URL y Redirigimos el flujo de comunicación hacia el interfaz web del módulo de autenticación para realizar la validación del certificado**

   https://"+authServerIP+":"+authServerSecurePort+"/authenticationFacade?

   action=validateCert

   &ticketId=ticketId

   &appId=appId

   &webSessionId=sessionId

   &comeBackURL=comeBackURLEncoded

Autenticación @firma v5 – Fachada de ticket -

Autenticación Fachada de ticket

SolicitarTicket

Comprobar código fuente de la aplicación de prueba

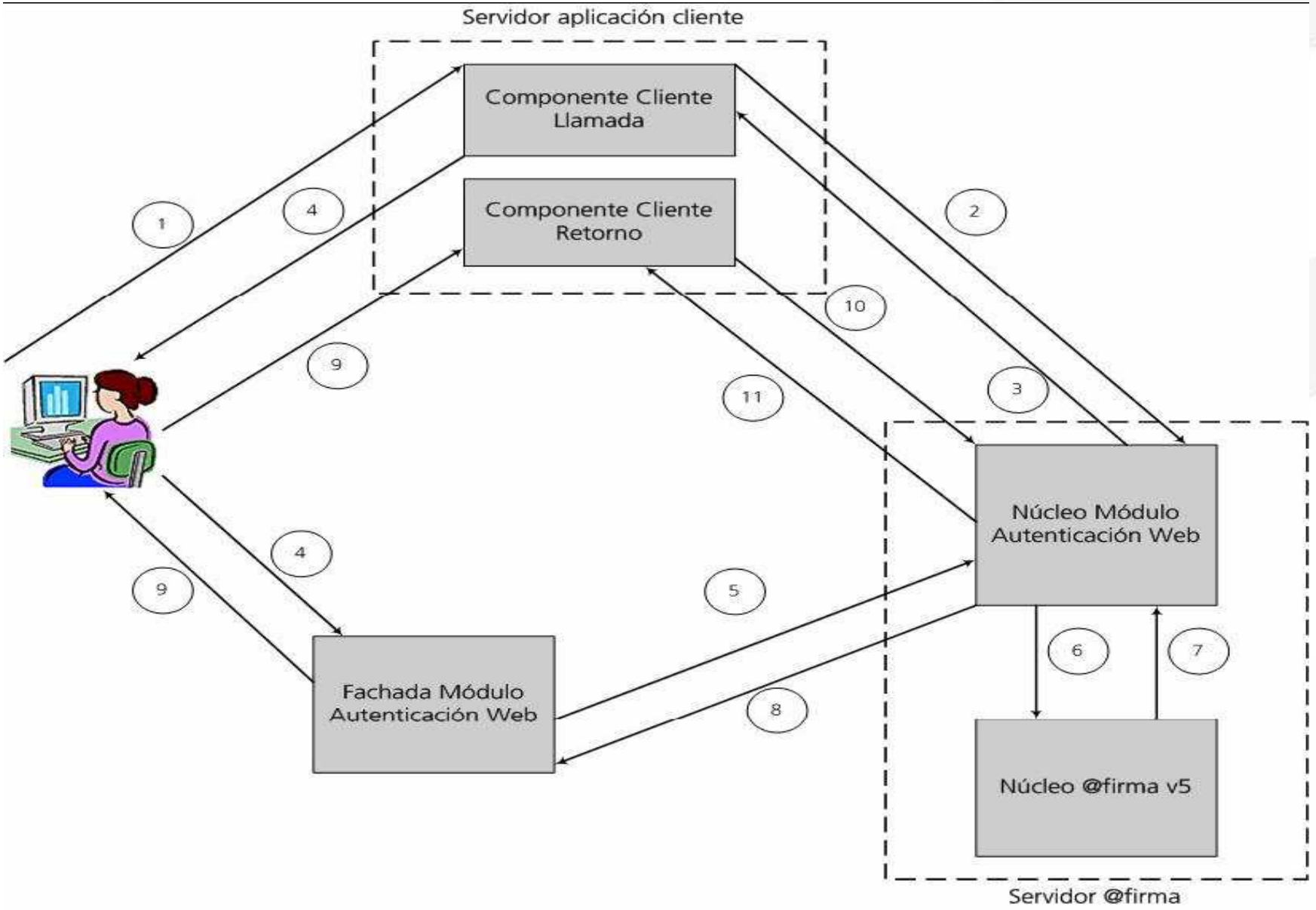
es.andaluciajunta.cjap.autenticacion.SolicitarTicket.java

```
//Efectuamos una llamada web service al modulo de autenticación para obtener un nuevo ticket
UtilidadesAutFachada util = new UtilidadesAutFachada();
Map ticketResp = util.generateTicket(appId,sessionId);
```

En UtilidadesAutFachada podemos ver generateTicket(appIf,sessionId),
Método que crea el XML para realizar la petición del servicio, obtiene un XML de respuesta y lo mapea a un MAP

Autenticación @firma v5 – Fachada de ticket -

Autenticación por Fachada de Ticket

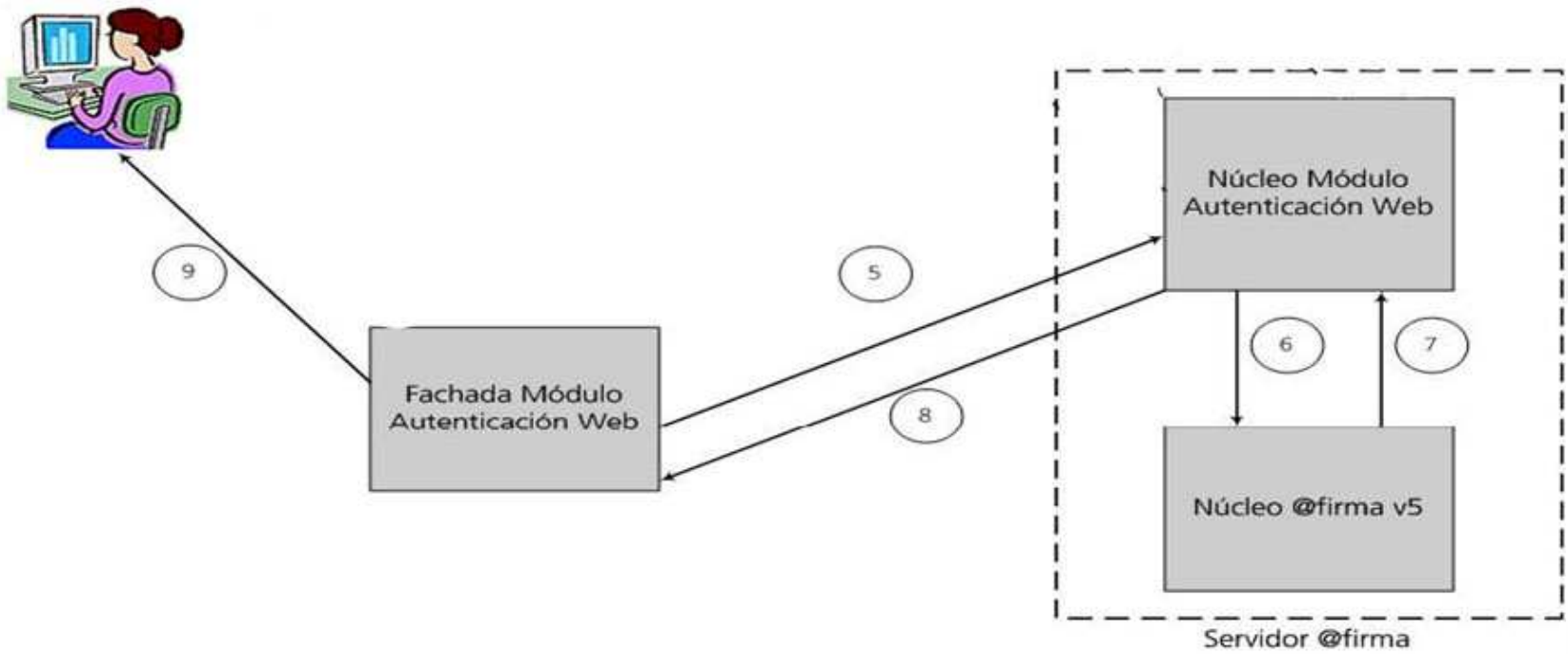


Autenticación @firma v5 – Fachada de ticket -

Fachada Modulo Autenticación Web ticket

Envía el certificado

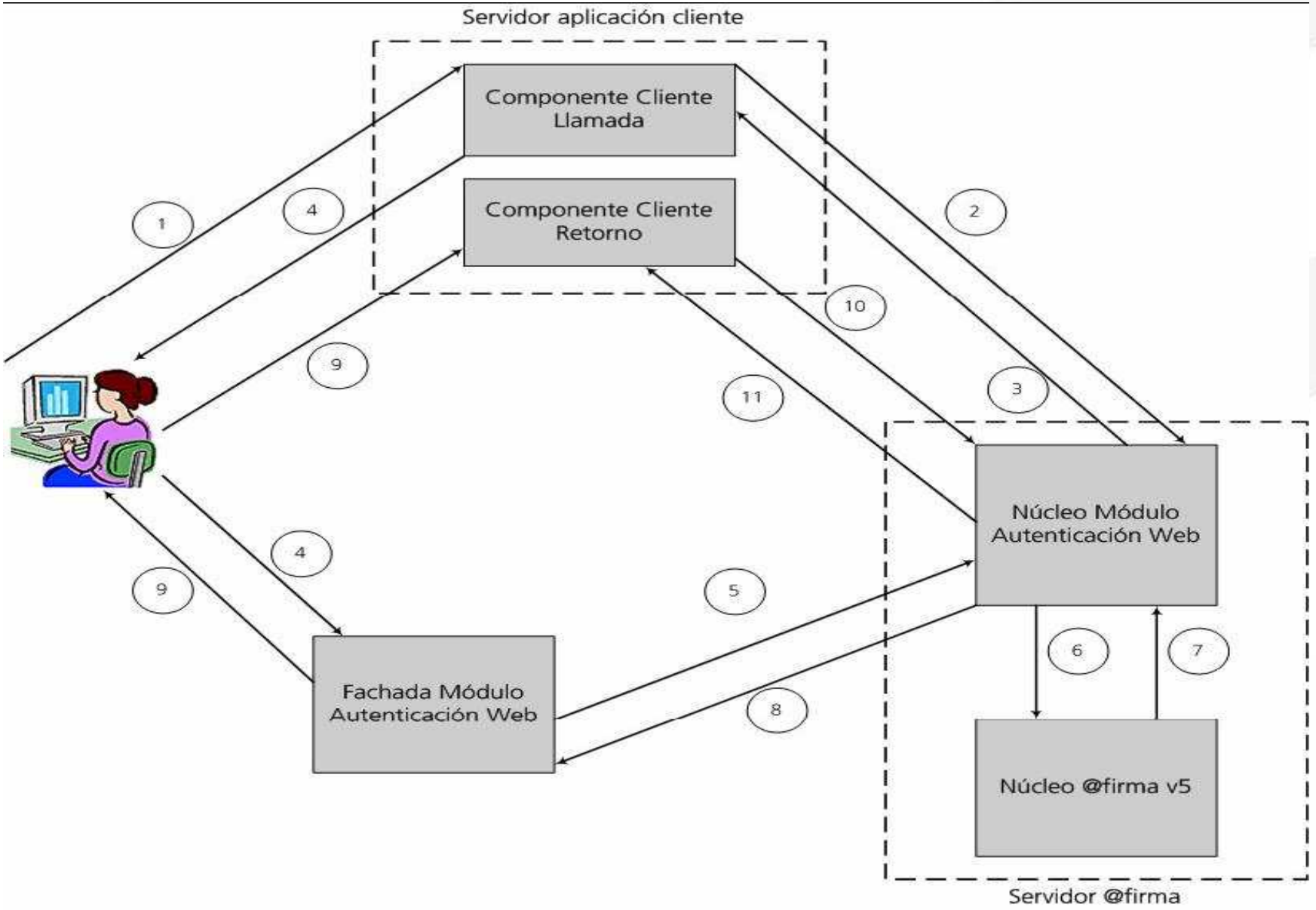
Devuelve código de confirmación



JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -

Autenticación por Fachada de Ticket



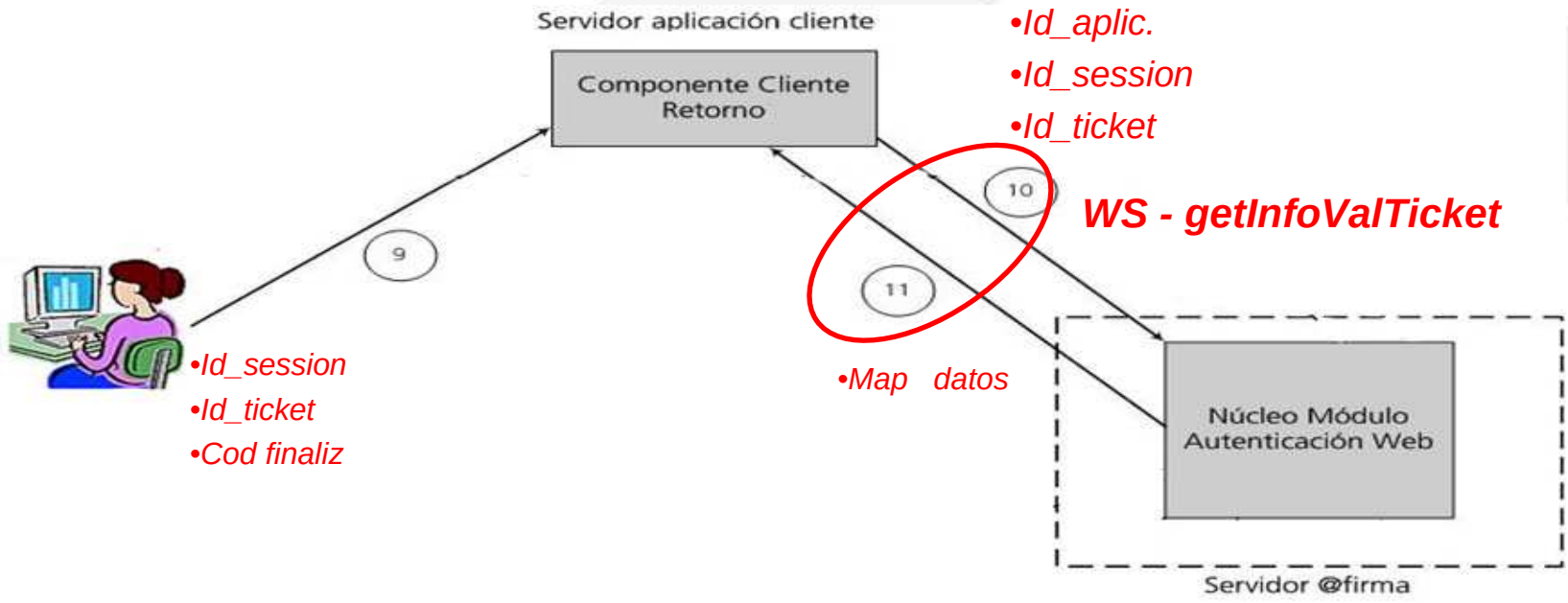
Autenticación @firma v5 – Fachada de ticket -

Componente Retorno - Datos Ticket

1)Recogemos los datos de la request

2)Acudimos al nucleo y extraemos los datos

3)Mapeamos al objeto que deseemos



Autenticación @firma v5 – Fachada de ticket -

Autenticación Fachada de ticket

DatosTicket

1) **Establecimiento de variables extraídas de la petición por la request**

   rErrorCode *(error devuelto por módulo)*, rTicketId, rAppId y rSessionId

2) **Establecimiento de variables extraídas de la sesión (sTicketId y sAppId) y borradas después de la sesión**

3) **Comprobación de los campos (rErrorCode, rTicketId, rAppId y rSessionId)**

4) **Si todo OK, Llamada WS al modulo de autenticación para obtener la información de validación de certificado asociada al ticket de la petición**

   Datos Necesarios : rTicketId, rAppId y rSessionId → Estructura XML (input) → Llamada al servicio → Estructura XML (output) → Objeto Map

5) **Tratar el objeto Map para obtener los datos del certificado**

Autenticación @firma v5 – Fachada de ticket -

Autenticación Fachada de ticket

```
//Efectuamos una llamada web service al módulo de autenticación para obtener la
      información de validación de certificado asociada al ticket de la petición

      UtilidadesAutFachada util = new UtilidadesAutFachada();

      ticketValInfoResp = util.getInfoValTicket(rTicketId,rAppId,rSessionId);

-------------------------------------------------------------------------------------

Map resValInfo =
      TransformersFacade.getInstance().parseResponse(valInfo,"ValidarCertificad
      o",TransformersConstants.version10);

-------------------------------------------------------------------------------------

 validacion = UtilidadesAutFachada.mapeoValInfoResultadoVal(resValInfo);

      if ((validacion == null)||(! "0".equals(validacion.getResultado()))){

            errorComp = UtilidadesAutFachada.resultadoVal(validacion);

      }else{  user = UtilidadesAutFachada.mapeoValInfoUser(resValInfo);

            request.getSession().setAttribute("usuario",user);   }
```

Autenticación @firma v5 – Fachada de ticket - Comunicación Segura

- **Por usuario/ password**
  - Además de llamar al servicio hay que incluir los parámetros de usuario/password, para que ningún otro servicio pueda utilizar el identificador,
  - **authorizationMethod = UsernameToken**
  - Clear/digest – Por defecto debe siempre enviarse digest
  - Pueden existir distintos usuarios/password
- **Por certificado**
  - Sería necesario enviar a la administración de la aplicación la parte pública del certificado, para identificar la petición.
  - **authorizationMethod = BinarySecurityToken**
- **Ambas comunicaciones con el núcleo deben tener el mismo sistema de seguridad ya que sólo existe una configuración, si podrían utilizar user/pass o certificados distintos**

Autenticación @firma v5 - Fachada de ticket -

- Plataforma @firma
- Autenticación y Tipos
  - WebServices
  - Fachada
- Fachada de autenticación web (extensión)
- Fachada de autenticación por tickets (nativa)
- **Adaptación de la aplicación**
- Notas
- Ejemplos de integración

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -

Adaptación de la aplicación

1) **Incluir en nuestra aplicación las librerías que no tengamos previamente en nuestro proyecto**
2) **Incluir la carpeta xml_parameter,**
3) **Incluir y modificar los siguientes .properties**
   a) **afirma5ServiceInvoker.properties**

      Modificar → com.trustedstore y com.trustedstorepassword

   b) **transformers.properties**

      Modificar → xmlTemplateFilesPath

   c) **.properties de la aplicación**

      Incluir → authServer = https://ws116.juntadeandalucia.es/

      Incluir → comeBackURL = http://aaa.xxxxxxxxxxxxxxx.zzz/

      Incluir → appId = BBB.ccccc

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket - Adaptación de la aplicación (I)

Ahora podríamos nosotros desarrollar nuestro código partiendo del ejemplo o utilizar el código que tenemos incluyéndolo en nuestra aplicación.

IMPORTANTE, es un código de ejemplo, puede ser revisado y adaptado a las necesidades y tecnologías utilizadas en nuestra aplicación.

4) Copiar el paquete es.andaluciajunta.cjap.autenticacion;

- **SolicitarTicketServlet.java,**
  - **Modificar → archivo de propiedades de la aplicación**

```
static ResourceBundle bun =ResourceBundle.getBundle(“xxxxxxxxxx");
```

  - **Modificar → dirección de retorno.**

```
private static final String comeBackURL =
bun.getString("comeBackURL")+"/autFachadaTicket/DatosTicket";
```

  - **Modificar → página de error de autenticación**

```
response.sendRedirect("callClientComponent.jsp");
```

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket - Adaptación de la aplicación (III)

- **Incluir en el web.xml el servlet de SolicitarDatos**
- **UtilidadesAutFachada.java,**
  - **Modificar → el procedimiento,**

public static CertificateUser mapeoValInfoUser(Map valInfo)

realiza la conversión del objeto map obtenido al objeto que nosotros utilicemos en nuestra aplicación, por lo que será necesario adaptarlo a los datos que necesitamos del certificado, y el tipo del objeto, además será necesario incluir los cambios en las clases desde las que se llame.

- **ResultadoValidacion.java**
- **ValidacionSimple.java**

Autenticación @firma v5 – Fachada de ticket - Adaptación de la aplicación (IV)

- **DatosTicketServlet.java,**
  - **Puede ser el sustituto natural del RetornoCertificado (aplicaciones de ejemplo anteriores), si se utiliza struts, puede convertirse en un Action. Si continua como serlvet ponerlo en el web.xml sino en el strusts-config.xml**
  - **A esta clase una vez realizada las comprobaciones básicas se le puede añadir las comprobaciones de nuestra propia aplicación**

Autenticación @firma v5 - Fachada de ticket -

- Plataforma @firma
- Autenticación y Tipos
  - WebServices
  - Fachada
- Fachada de autenticación web (extensión)
- Fachada de autenticación por tickets (nativa)
- Adaptación de la aplicación
- **Notas**
- Ejemplos de integración

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -

Entregable desarrollo para Fachada de Ticket

Se podrá solicitar la descarga del siguiente contenido:

- Aplicación de ejemplo de Autenticación por fachada de Ticket
- Manuales de desarrollador:
  - Desarrollo con fachada de ticket
  - Migración de fachada de autenticación a fachada de ticket
  - Transparencias del curso
  - Documento de configuración de aplic. seguras
- Recursos
  - XSD
  - WSDL
  - Librerías

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket - Solicitud de alta y cambios

La migración exige la solicitud de nueva alta por entorno (Des, Prod),

Procedimiento de alta

correo a soporte.admonelectronica@juntadeandalucia.es **datos:**

- Entidad a la que pertenece
- Datos del responsable
- Identificador de la aplicación
- Servicios solicitados: “Autenticación Fachada de Tickets”
- Tipo de Autorización elegido (none-UserNameToken-BinarySecutiryToken)
- En caso de BinarySecurityToken, parte pública del certificado

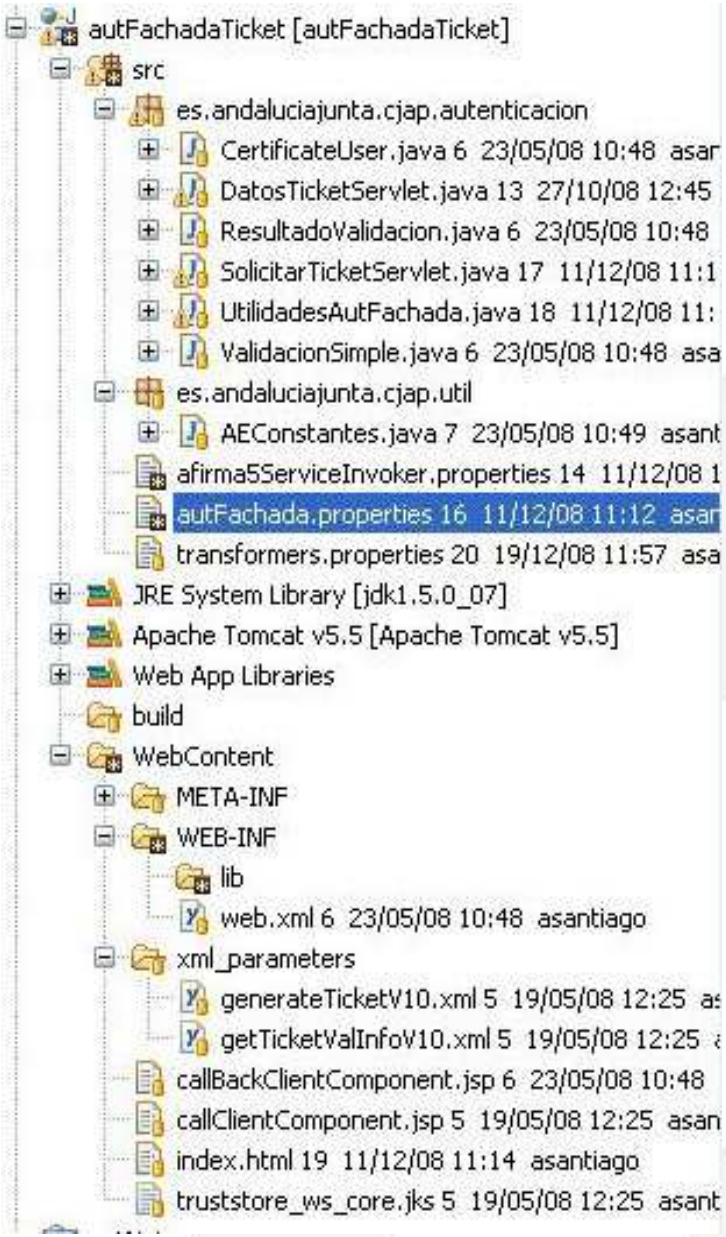
JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 - Fachada de ticket -

- Plataforma @firma
- Autenticación y Tipos
  - WebServices
  - Fachada
- Fachada de autenticación web (extensión)
- Fachada de autenticación por tickets (nativa)
- Adaptación de la aplicación
- Notas
- **Ejemplos de integración**

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -



JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Autenticación @firma v5 – Fachada de ticket -

- **Ruegos y preguntas**
- **Email más información:**
  - Info.admonelectronica@juntadeandalucia.es
  - Soporte.admonelectronica@juntadeandalucia.es
- **Antonio Luis Santiago R. de Adana**

Muchas Gracias

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA