Universitat Oberta de Catalunya

uoc.edu

Firma electrónica en la nube

Nombre Estudiante: David de la Hoz Martínez

Plan de Estudios del Estudiante: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Área del trabajo final: Firma Electrónica

Nombre Consultor/a: Enric Hernández Jiménez

Nombre Profesor/a responsable de la asignatura: Víctor García Font

Fecha Entrega: 4 de Junio de 2018

Licencias alternativas (elegir alguna de las siguientes y sustituir la de la página anterior)

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Firma electrónica en la nube*
Nombre del autor:	*David de la Hoz Martínez*
Nombre del consultor/a:	*Enric Hernández Jiménez*
Nombre del PRA:	*Víctor García Pons*
Fecha de entrega (mm/aaaa):	06/2018
Titulación::	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)*
Área del Trabajo Final:	*M1.830 - TFM-Ad hoc*
Idioma del trabajo:	*Castellano*
Palabras clave	*Firma electrónica, certificado, cifrar, clave privada* *Electronic signature, certificate, encryption, private key*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

El Trabajo Fin de Máster aquí presentado, está orientado a proveer al colectivo de trabajadores del notariado español una alternativa tecnológica para realizar las funcionalidades de autenticación, firma y cifrado, desde cualquier dispositivo sin necesidad de uso de tarjetas físicas ni tener instalado ningún hardware o software adicional, necesarios para la lectura de dichas tarjetas. El trabajo se ha iniciado realizando un estudio del espectro tecnológico actual para conocer las tecnologías necesarias para cubrir las necesidades funcionales anteriormente descritas. A continuación se ha realizado un diseño arquitectónico para el Sistema de Información propuesto a ANCERT en el ámbito de la firma electrónica centralizada y finalmente se ha desarrollado una prueba de concepto para poder verificar la viabilidad de la aproximación teórica propuesta.

El objetivo principal de este trabajo, es el diseño de una solución que, bajo el amparo del marco legal vigente, permita realizar la firma electrónica de documentos mediante certificados digitales personales, que se encuentran custodiados en un sistema centralizado junto con sus claves. El diseño también ha contemplado la provisión de una capa fuerte de autenticación, para garantizar que el propietario del certificado sea el único que pueda hacer uso del mismo para la realización de la firma.

Abstract (in English, 250 words or less):

This final project introduced here is meant to offer the notary collective a technological alternative to log in, signature and encrypt from any device without the need of neither smart cards nor hardware or any extra software needed for the read of the mention cards. It started by the making of a study of the current technological spectrum to first knowing the main lack of functionalities requested. In addition, an arquitechtonical design was made for ANCERT and its "Info system" inside the scope of action of electronic signature. And last but not least, a proof of concept was developed to verify the viability between two worlds, theory and practice.

The main object of this work is, the design of a solution in which, under the protection of the current legal framework, allows to sign in documents through customized digital certificates, guarded in a cloud altogether with their passwords. This design has also taken into account the need of a strong layer of authentication to ensure and guarantee the owners that these certificates are personal and non-transferable, so no one else can make use of the signature.

Índice

1. Introducción 1
1.1. Contexto y justificación del Trabajo 1
1.2. Objetivos del Trabajo 1
1.3. Enfoque y método seguido 2
1.4. Planificación del Trabajo 2
1.4.1. Planificación Temporal 2
1.4.2. Planificación del Proyecto 3
1.4.3. Diseño de la Arquitectura 4
1.4.4. Desarrollo del servicio de Firma 4
1.4.5. Realización de la memoria 5
1.4.6. Realización del vídeo-presentación 5
1.5. Breve descripción de los otros capítulos de la memoria 6
2. Estado del Arte 7
2.1. Gestión de Identidades 7
2.1.1. Contexto 7
2.1.2. Funcionalidades 7
2.1.2.1. Provisión de Usuarios 7
2.1.2.2. Gestión de Roles 7
2.1.2.3. Atestación 8
2.1.2.4. Auditoría 8
2.2. Modelos de Autenticación N-Factor 8
2.2.1. Contexto 8
2.2.2. Factores adicionales de Autenticación 9
2.2.2.1. One Time Password (OTP) 9
2.2.2.2. Mecanismos biométricos 9
2.3. Firma Electrónica 9
2.3.1. Contexto 9
2.3.2. Tipos de firma 9
2.3.3. Formatos de Firma 10
2.3.3.1. CAdES (CMS Advanced Electronic Signatures) 10

2.3.3.2. XAdES (XML Advanced Electronic Signatures) 11
2.3.3.3. PAdES (PDF Advanced Electronic Signatures) 11
2.3.4. Estrategias de correlación con el documento original 11
2.3.5. Firmas múltiples 11
2.3.6. Sello de tiempo 12
2.3.7. Custodia y almacenamiento de certificados 12
3. Arquitectura 13
3.1. Esquema de Autenticación 13
3.1.1. Flujo de autenticación 13
3.1.1.1. Descripción del escenario: 13
3.1.2. Esquema de autenticación delegado en WSO2. 14
3.2. Esquema de Firma Electrónica 16
3.2.1. Flujo de Firma Electrónica 16
3.2.2. Esquema de firma delegado en REALSEC. 17
3.2.2.1. Características del producto: 17
3.2.2.2. El producto incorpora las siguientes funcionalidades: 17
3.3. Arquitectura del Servicio de Firma Electrónica centralizada 19
3.4. Definición de Interfaces 20
3.4.1. Proveedor de Identidad 20
3.4.1.1. Validación de primer nivel de autenticación (user/password) 20
3.4.1.2. Validación del segundo nivel de autenticación (OTP) 20
3.4.2. Servicio de Firma Electrónica 21
3.4.2.1. Obtención de certificados 21
3.4.2.2. Firma Electrónica 21
3.4.3. Servicio de Firma Digital 22
3.4.3.1. Obtención de certificados 22
3.4.3.2. Firma 23
4. Desarrollo de la prueba de Concepto 24
4.1. Introducción: 24
4.2. Entorno 24
4.3. Diseño 25
4.3.1. Adaptación de la Arquitectura a la prueba de concepto. 25
4.3.2. Diagrama de Interfaces proporcionadas. 27
4.4. Test de Funcionamiento del piloto 27
4.4.1. Juego de Ensayo 27

4.4.2. Navegación 28
4.4.2.1. Acceso inicial al portal. Solicitud de Credenciales..... 28
4.4.2.2. Acceso a la sección de firmas con usuario autenticado. 29
4.4.2.3. Acceso a “Firmar Documentos”. Solicitud previa de PIN..... 30
4.4.2.4. Selección de Certificados y documento a firmar 30
4.4.2.5. Resultado de la Firma. 31
4.4.2.6. Flujo alternativo: Usuario sin certificados 32
4.4.2.7. Autorización. Flujo alternativo: Usuario no autorizado 33
4.4.3. Firma generada: 33
5. Conclusiones 35
6. Glosario 36
7. Bibliografía 39
8. Anexos 41
8.1. Prueba de Concepto 41
8.2. Instalación de la aplicación Prueba de Concepto 41
8.2.1. Servidor Tomcat preinstalado. 41
8.2.2. Instalación completa 41
8.3. Manual de Usuario 42
8.3.1. Usuarios de la aplicación 42
8.3.2. Navegación: 42
8.3.2.1. Home. Barra de menú: 42
8.3.2.2. Autenticación 43
8.3.2.3. Acceso a la sección de Firma de Documentos: 43
8.3.2.4. Solicitud de PIN. 44
8.3.2.1. Funcionalidad de Firma. 44

Lista de figuras

Ilustración 1. Planificación Global 3
Ilustración 2. Planificación del Proyecto 3
Ilustración 3. Diseño de la Arquitectura 4
Ilustración 4. Desarrollo del servicio de Firma 4
Ilustración 5. Realización de la memoria 5
Ilustración 6. Realización del vídeo presentación 5
Ilustración 7. Flujo de autenticación 13
Ilustración 8. Flujos de Autenticación con WSO2 15
Ilustración 9. Flujo de Firma Electrónica 16
Ilustración 10.- Flujo de Firma Electrónica con CryptoSign Server 18
Ilustración 11. Arquitectura de la solución global de Firma Electrónica 19
Ilustración 12. Adaptación de la Arquitectura a la prueba de concepto. 25
Ilustración 13. Interfaces Proporcionadas 27
Ilustración 14. Piloto. Solicitud de Credenciales 29
Ilustración 15. Piloto. Sección de Firma de Documentos. 29
Ilustración 16. Piloto. Solicitud OTP 30
Ilustración 17. Piloto. Selección de certificados 31
Ilustración 18. Piloto. Documento firmado 32
Ilustración 19. Piloto. Flujo alternativo. Usuario sin certificados 32
Ilustración 20. Piloto. Flujo alternativo. Usuario no autorizado. 33
Ilustración 21. Piloto. Documento firmado. Partes de la firma 34
Ilustración 22. Manual de Usuario. Usuarios de Prueba 42
Ilustración 23. Manual de Usuario. Barra de menú 42
Ilustración 24. Manual de Usuario. Página de Login. 43
Ilustración 25. Manual de Usuario. Sección de Firma 43
Ilustración 26. Manual de Usuario. Solicitud de PIN. 44
Ilustración 27. Manual de Usuario. Funcionalidad de Firma 45
Ilustración 28. Manual de Usuario. Documento Firmado 45

1. Introducción

1.1. Contexto y justificación del Trabajo

ANCERT es una empresa que provee de servicios informáticos al colectivo del notariado español. Dentro del área de Firma Electrónica se ha desarrollado la solución FEREN (*Firma Electrónica Reconocida Notarial*) que permite a este colectivo la realización de trámites telemáticos con total garantía jurídica. El siguiente paso hacia el que quiere navegar la empresa es evolucionar dicho sistema hacia una solución de Firma electrónica en la nube para hacer más usable su sistema actual.

El sistema FEREN, se basa en el uso de tarjetas que almacenan los certificados del usuario necesarios para autenticare, cifrar y firmar. El uso de estas tarjetas es de alta fiabilidad, depositándose en dicha tarjeta toda la confianza del sistema. Pero dicha confianza está en contrapunto con la usabilidad de los usuarios: a la necesidad de transportar la tarjeta, se suma la tecnología que deben de aportar los dispositivos que usemos, como lectores de tarjetas y software instalado para permitir el uso del certificado. Estas circunstancias limitan el uso de los sistemas de información por los usuarios.

A partir de la aprobación la normativa *eIDAS 910/2014* (equipara la legalidad de la firma remota con la firma realizada con los mecanismos actuales), ANCERT, como proveedor de servicios tecnológicos al colectivo de Notarios, se plantea la necesidad de diseñar un sistema de firma electrónica en la nube, donde gracias a la custodia centralizada de los certificados personales de su personal, permita a éste la realización de firma electrónica de documentos sin la necesidad de portar una tarjeta o contar con un dispositivo cliente con ciertas características mínimas, tal como se mencionaba en el punto anterior.

Partiendo de este punto de partida, el objetivo principal de este Trabajo Fin de Máster (que a partir de ahora denominaremos como TFM) será el de diseñar una solución telemática, para realizar la firma electrónica con los certificados que el propio sistema custodia y la provisión de una capa fuerte de autenticación para garantizar que sólo el propietario del certificado está haciendo uso del mismo para la realización de la firma, con el fin de proveer al colectivo de trabajadores del notariado español una alternativa tecnológica para realizar las funcionalidades de autenticación, firma y cifrado sin necesidad de portar una tarjeta física donde estén albergados los diferentes certificados necesarios para realizar las funcionalidades anteriormente descritas.

1.2. Objetivos del Trabajo

Se han definido 3 grandes objetivos a alcanzar en este proyecto, a los que se han asignado un peso importancia con el fin de priorizar tareas en la evolución del proyecto en caso de necesidad de realizar una replanificación del mismo.

1. **[PRIORIDAD 2]** Documentar el estado del arte tecnológico en el ámbito de la firma electrónica.
2. **[PRIORIDAD 1]** Realizar una propuesta arquitectónica que permita la realización de firma electrónica con la custodia centralizada de los certificados digitales de los usuario y dotando a la solución de mecanismos de autenticación fuerte para no hacer uso fraudulento de los certificados.
3. **[PRIORIDAD 3]** Realización de una prueba de concepto, mediante un desarrollo ad-hoc que permita validar parcialmente alguno de los subsistema descritos en la Arquitectura propuesta.

1.3. Enfoque y método seguido

El enfoque que se ha querido dar a este trabajo ha sido principalmente, ofrecer a ANCERT una arquitectura sólida que de solución a los retos tecnológicos que nos han transmitido, para garantizar la seguridad de la custodia de los certificados, cumpliendo con los principios de confidencialidad, integridad y no repudio, mejorando sustancialmente la experiencia de usuario.

Para ello, se ha realizado un estudio del marco legal que afecta a la firma electrónica, así como una búsqueda de productos disponibles en el mercado, que ofrezcan soluciones robustas que cubran las necesidades de nuestros requisitos, cumpliendo a su vez con el marco jurídico indicado.

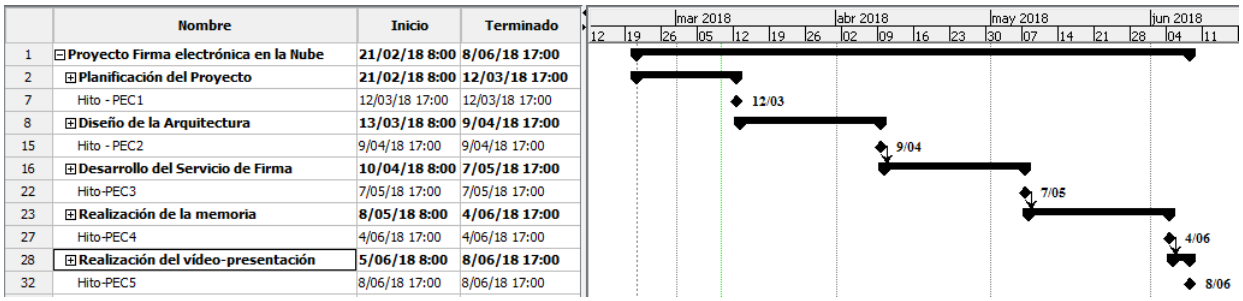
Una vez realizado todo este estudio, el trabajo se ha centrado en la definición de una arquitectura que orqueste el desarrollo *ad-hoc* con la integración de otros elementos software, middleware y appliance de otros fabricantes. El resultado del mismo ha sido validado mediante una Prueba de Concepto, que se ha centrado en el desarrollo ad-hoc a realizar, simulando el comportamiento de las piezas de integración que se han decidido delegar a productos de terceros.

1.4. Planificación del Trabajo

El TFM consiste en un estudio tecnológico y propuesta arquitectónica para cubrir las necesidades expuestas anteriormente para proveer a colectivo de notariado español de una plataforma de firma electrónica en la nube.

1.4.1. Planificación Temporal

Se propone la siguiente planificación inicial de trabajos para alcanzar el objetivo principal del Trabajo:



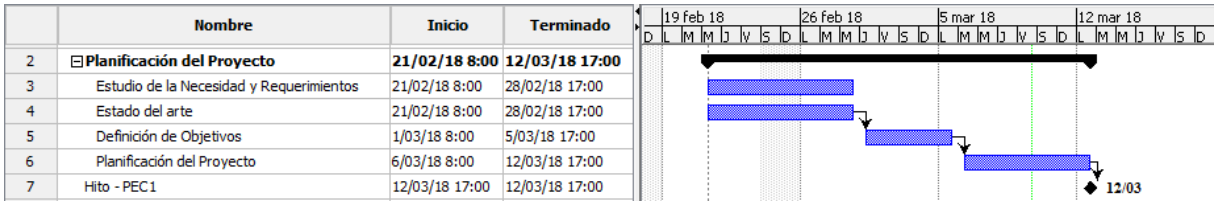
	Nombre	Inicio	Terminado
1	Proyecto Firma electrónica en la Nube	21/02/18 8:00	8/06/18 17:00
2	Planificación del Proyecto	21/02/18 8:00	12/03/18 17:00
7	Hito - PEC1	12/03/18 17:00	12/03/18 17:00
8	Diseño de la Arquitectura	13/03/18 8:00	9/04/18 17:00
15	Hito - PEC2	9/04/18 17:00	9/04/18 17:00
16	Desarrollo del Servicio de Firma	10/04/18 8:00	7/05/18 17:00
22	Hito-PEC3	7/05/18 17:00	7/05/18 17:00
23	Realización de la memoria	8/05/18 8:00	4/06/18 17:00
27	Hito-PEC4	4/06/18 17:00	4/06/18 17:00
28	Realización del vídeo-presentación	5/06/18 8:00	8/06/18 17:00
32	Hito-PEC5	8/06/18 17:00	8/06/18 17:00

Ilustración 1. Planificación Global

La planificación de trabajos está orientada a la entrega parcial de trabajos, que permitan valorar el avance del proyecto y la consecución del mismo permitiendo realizar retrospectivas temporales permitiendo al equipo de trabajo recibir feedback de la consecución de los objetivos iniciales planteados.

El calendario se ha configurado considerando los fines de semana y festivos como laborables. Todas las tareas están asignado al único recurso existente que tiene una disponibilidad de 20 horas/semanales.

1.4.2. Planificación del Proyecto



	Nombre	Inicio	Terminado
2	Planificación del Proyecto	21/02/18 8:00	12/03/18 17:00
3	Estudio de la Necesidad y Requerimientos	21/02/18 8:00	28/02/18 17:00
4	Estado del arte	21/02/18 8:00	28/02/18 17:00
5	Definición de Objetivos	1/03/18 8:00	5/03/18 17:00
6	Planificación del Proyecto	6/03/18 8:00	12/03/18 17:00
7	Hito - PEC1	12/03/18 17:00	12/03/18 17:00

Ilustración 2. Planificación del Proyecto

- **Estudio de la Necesidad y Requerimientos:** Preparación y celebración de la reunión de Kick-Off para obtener información de ANCERT, la necesidad y los requerimientos de la empresa dentro del contexto de Firma Electrónica así como los objetivos deseables a alcanzar en el ámbito del proyecto
- **Estado del Arte:** En paralelo a la anterior tarea se realiza un estudio de la tecnología y soluciones comerciales en el ámbito de la firma electrónica de cara a contextualizar la problemática a resolver.
- **Definición de Objetivos:** Definición del alcance del proyecto.
- **Planificación del Proyecto:** Desglose de tareas y planificación temporal de las mismas de cara a cubrir los objetivos del proyecto teniendo en cuenta los recursos disponibles, periodos de entrega y el esfuerzo total admisible.
- **Hito – PEC1:** Cumpliendo con la planificación propuesta, se entrega la documentación con los trabajos descritos en esta fase.

1.4.3. Diseño de la Arquitectura

	Nombre	Inicio	Terminado
8	**Diseño de la Arquitectura**	**13/03/18 8:00**	**9/04/18 17:00**
9	**Valoración de la tecnología existente**	**13/03/18 8:00**	**27/03/18 17:00**
10	Gestión de Identidades	13/03/18 8:00	15/03/18 17:00
11	Modelos de Autenticación N-Factor	16/03/18 8:00	19/03/18 17:00
12	Firma electrónica	20/03/18 8:00	22/03/18 17:00
13	Custodia y almacenamiento de certificados	23/03/18 8:00	27/03/18 17:00
14	Definición arquitectónica de la solución	28/03/18 8:00	9/04/18 17:00
15	Hito - PEC2	9/04/18 17:00	9/04/18 17:00

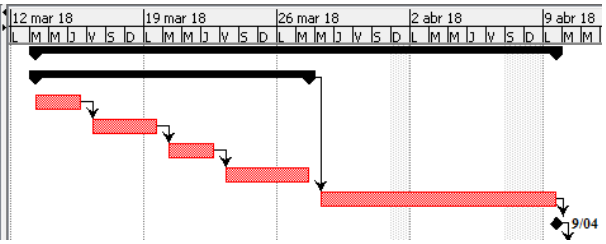


Ilustración 3. Diseño de la Arquitectura

- **Valoración de la tecnología existente:** Estudio del arte tecnológico que de cobertura a la solución planteada. Realizaremos estudio en las siguientes áreas:
- Gestión de Identidades
- Modelos de Autenticación N-Factor
- Firma electrónica
- Custodia y almacenamiento de certificados
- **Definición arquitectónica de la solución:** En base al estudio tecnológico anterior, se elaborará una propuesta arquitectónica que de solución a la necesidad expuesta.
- **Hito – PEC2:** Cumpliendo con la planificación propuesta, se entrega la documentación con los trabajos descritos en esta fase

1.4.4. Desarrollo del servicio de Firma

	Nombre	Inicio	Terminado
16	**Desarrollo del Servicio de Firma**	**10/04/18 8:00**	**7/05/18 17:00**
17	Instalación de la infraestructura base	10/04/18 8:00	12/04/18 17:00
18	Diseño Técnico de la Solución	10/04/18 8:00	12/04/18 17:00
19	Desarrollo de la Solución	13/04/18 8:00	2/05/18 17:00
20	Pruebas del desarrollo	16/04/18 8:00	3/05/18 17:00
21	Documentación	4/05/18 8:00	7/05/18 17:00
22	Hito-PEC3	7/05/18 17:00	7/05/18 17:00

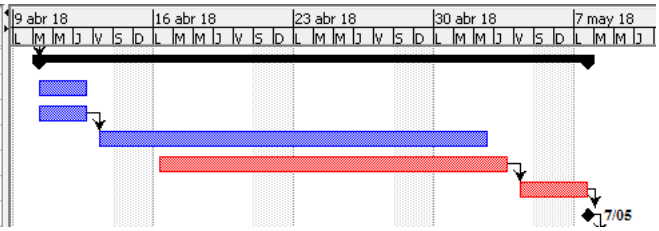


Ilustración 4. Desarrollo del servicio de Firma

En base a la propuesta arquitectónica realizada en la fase anterior se realizará un desarrollo concebido como prueba de concepto de demostración de la arquitectura propuesta.

- **Instalación de la Infraestructura base:** instalación del software base para la realización y despliegue del desarrollo.
- **Diseño Técnico de la Solución:** Diseño técnico de detalle del desarrollo a realizar
- **Desarrollo de la Solución:** codificación del servicio de Firma.
- **Pruebas del desarrollo:** ciclo de pruebas del desarrollo realizado para certificar que se cubren los requisitos y objetivos deseados. Esta tarea se realizará en paralelo con la tarea de desarrollo, retroalimentando dicha fase con nuevas mejoras a realizar.

- **Documentación:** realización de la documentación asociada al desarrollo realizado.
- **Hito – PEC3:** Cumpliendo con la planificación propuesta, se entrega la documentación con los trabajos descritos en esta fase.

1.4.5. Realización de la memoria

	Nombre	Inicio	Terminado
23	**Realización de la memoria**	**8/05/18 8:00**	**4/06/18 17:00**
24	Recopilación de toda la información	8/05/18 8:00	10/05/18 17:00
25	Retrospectiva de los trabajos realizados	11/05/18 8:00	17/05/18 17:00
26	Realización de la Memoria	18/05/18 8:00	4/06/18 17:00
27	Hito-PEC4	4/06/18 17:00	4/06/18 17:00

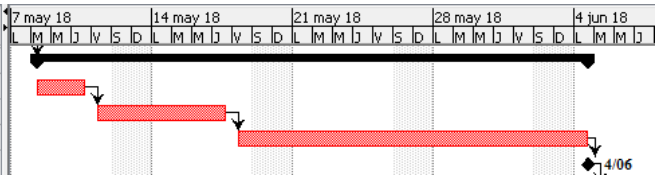


Ilustración 5. Realización de la memoria

- **Recopilación de toda la información:** se recabará toda la información acumulada a lo largo del proyecto. Se agrupará y clasificará para su utilidad como inputs de la realización de la memoria.
- **Retrospectiva de los trabajos realizados:** se repasarán todos los entregables parciales de cara a obtener lecciones aprendidas para enriquecer la memoria final.
- **Realización de la memoria:** escritura de la memoria final del proyecto.
- **Hito – PEC4:** Cumpliendo con la planificación propuesta, se entrega la documentación con los trabajos descritos en esta fase.

1.4.6. Realización del vídeo-presentación

	Nombre	Inicio	Terminado
28	**Realización del vídeo-presentación**	**5/06/18 8:00**	**8/06/18 17:00**
29	Realización del guión	5/06/18 8:00	6/06/18 17:00
30	Grabación	7/06/18 8:00	7/06/18 17:00
31	Postproducción	8/06/18 8:00	8/06/18 17:00
32	Hito-PEC5	8/06/18 17:00	8/06/18 17:00

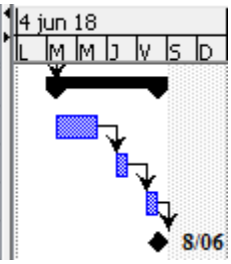


Ilustración 6. Realización del vídeo presentación

- **Realización del guión:** componer el guión y los materiales audiovisuales para la realización del vídeo-presentación del TFM.
- **Grabación:** grabación del vídeo.
- **Postproducción: tareas** de montaje de vídeo y audio.
- **Hito – PEC5:** Cumpliendo con la planificación propuesta, se entrega la documentación con los trabajos descritos en esta fase.

1.5. Breve descripción de los otros capítulos de la memoria

La memoria está dividida en 3 grandes bloques, que se corresponden a los siguientes capítulos que a continuación describimos:

- ***Capítulo 2: Estado del Arte****.* En este bloque se describe todo el entorno tecnológico, metodológico y jurídico que están involucrados en el proceso de la firma electrónica de documentos.
- ***Capítulo 3: Arquitectura.*** Este capítulo recoge el bloque principal del trabajo, con diferentes aproximaciones arquitectónicas que cubren las necesidades funcionales fundamentales, que son objetivo de este trabajo.
- ***Capítulo 4: Desarrollo de la prueba de Concepto.*** En este capítulo, se describen las acciones realizadas en la implementación de una prueba de concepto para poner en práctica, el enfoque arquitectónico descrito en el capítulo anterior. Los trabajos realizados en este ámbito han sido usado como lecciones aprendidas que han servido para retroalimentar y ajustar el diseño de la arquitectura global.

2. Estado del Arte

De cara a plantear la Arquitectura global de la solución, vamos a realizar un estudio del arte tecnológico, para investigar sobre productos, patrones, buenas prácticas, librerías, tendencias, en diversas áreas que están afectadas en nuestra solución, como son la gestión de identidades con diferentes modelos de autenticación N-Factor, Firma Electrónica y la custodia y almacenamiento seguro de certificados digitales.

2.1. Gestión de Identidades

2.1.1. Contexto

El contexto del escenario en el que estamos trabajando es abandonar la confianza que nos aporta las tarjetas físicas de los usuarios que contienen los certificados que son necesarios para autenticarse, cifrar y firmar. Dado que el Sistema va a realizar la firma de los usuarios con certificados digitales que tiene almacenados en custodia, un frente que tenemos que garantizar es asegurar que la identidad del usuario que nos solicita realizar la firma, se corresponde realmente con el propietario real del certificado digital.

Por ello la capa de autenticación es una parte muy importante para asegurar el éxito de la solución.

2.1.2. Funcionalidades

2.1.2.1. Provisión de Usuarios

Es necesario plantear una política de aprovisionamiento de usuarios lo más automática posible, estudiando el ciclo de vida por el que pasan los usuarios en los sistemas de ANCERT. En el caso de existir un punto de entrada en el que se gestionen los procesos de Alta y Baja de los notarios en un sistema externo, este sistema debería estar conectado con nuestro Sistema de aprovisionamiento de Gestión de Identidades para tener ambos sistemas sincronizados sin incorporar nuevos procesos manuales en los procedimientos de Alta y Baja anteriormente mencionados.

2.1.2.2. Gestión de Roles

Una vez los usuarios se encuentren aprovisionados en el Sistema, es responsabilidad de la plataforma de Gestión de Identidades la asignación de roles.

De cara a enriquecer las analíticas de monitorización y la definición de alertas de seguridad, es recomendable asignar a los roles un nivel de riesgo, para mapearlos con la severidad de las alertas de seguridad que ocurran en tiempo de ejecución.

2.1.2.3. Atestación

De cara a facilitar la gobernanza de las identidades de nuestra plataforma, se debe considerar habilitar procedimientos con el fin de revisar y validar el estado de la autorización de los usuarios. Para dicho cometido tenemos 2 líneas de actuación:

- **Revisión de la definición de permisos:** el responsable de la aplicación debe de validar los permisos asignados a cada rol definido en la seguridad declarativa/programática de la aplicación.
- **Revisión de la asignación de servicios:** el responsable de cada unidad organizativa, debe validar los permisos que se deben de otorgar a los usuarios que componen dicha unidad.

2.1.2.4. Auditoría

En el ámbito de la Gestión de Identidades, debemos contemplar la necesidad de incluir funcionalidades de generación de informes orientados a facilitar las labores de Gobierno del Identidad:

- Revisión de usuarios, roles, grupos, privilegios y recursos existentes.
- Identificación de las relaciones entre las distintas definiciones.
- Identificación de no conformidades con respecto a la normativa vigente.
- Revisión de las definiciones de roles existentes y políticas de aprovisionamiento.
- Estadísticas y pautas de comportamiento generales de la plataforma de gestión de credenciales y autorizaciones.

2.2. Modelos de Autenticación N-Factor

2.2.1. Contexto

El Sistema actual de autenticación que proveen los sistemas informáticos de ANCERT, solicita al usuario la presentación de un certificado y su pin asociado. La confianza de este sistema está basada en que dicho certificado se encuentra en una tarjeta que es custodiada por el usuario legítimo del mismo. Dado que es una necesidad la eliminación del uso de dichas tarjetas, se debe plantear el uso de otras credenciales para presentarse ante el Sistema. Como primera aproximación se podría plantear el uso de un mecanismo monofactor de solicitud de usuario y contraseña. Este sistema es sencillo y no costoso, pero en su contra tiene que no aporta un nivel elevado de certeza quién es realmente quien está haciendo uso de las credenciales. Por esta razón se ve necesario añadir al mecanismo de autenticación factores adicionales de autenticación que permitan la verificación de quién está usando la credencial.

2.2.2. Factores adicionales de Autenticación

2.2.2.1. One Time Password (OTP)

One Time Passwords, son contraseñas únicas que sólo son válidas para realizar una única autenticación en un periodo limitado de tiempo desde que son solicitadas y enviadas. Debido a estas características, no son vulnerables a *"replay attacks".*

2.2.2.2. Mecanismos biométricos

Dichos mecanismo consisten en vincular una característica física única (huellas dactilares, reconocimiento facial, iris, voz,...)

La ventaja de estos sistemas es que no pueden perderse ni pueden ser robadas. La experiencia de usuario es muy buena y aceptada, puesto que eliminan la necesidad de recordar contraseñas u olvidos de tarjetas. Aunque los rasgos biométricos se pueden falsificar, estos mecanismos son más seguros que las tarjetas inteligentes.

La desventaja, es su elevado coste, necesidad de disponer en los equipo dispositivos para leer los rasgos biométricos, así como el riesgo de tener falsos rechazos, que provoca descontento de los usuarios y los falsos positivos, que provoca una brecha de seguridad. Debido a este tipo de desventajas, consideramos los mecanismos biométricos no son adecuados para incorporarlos como factores adicionales de autenticación en nuestro contexto de proyecto.

2.3. Firma Electrónica

2.3.1. Contexto

El mecanismo de firma electrónica se encuentra en una fase muy madura tanto desde el punto de vista tecnológico como legislativo (*véase la Ley 59/2003 de 19 de diciembre de firma electrónica*). El siguiente avance necesario es la facilidad de uso, limitando la inteligencia de los dispositivos utilizados y llevando dicha capacidad a los dispositivos móviles, aumentando la opción de movilidad de los usuarios. Por ello la evolución tecnológica en este campo está orientada a proveer Sistemas de firma remota, donde los certificados digitales de los usuarios se encuentren custodiados de forma seguro en un repositorio centralizado. El amparo jurídico para dar garantía a esta solución la tenemos en La normativa eIDAS 910/2014 que establece *"que las firmas electrónicas remotas deben tener el mismo reconocimiento legal que las efectuadas por los dispositivos criptográficos tradicionales"*.

2.3.2. Tipos de firma

La ley 59/2003, de firma electrónica, regula y marca las condiciones para la firma electrónica:

- **Firma electrónica simple:** “los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.”
- **Firma electrónica avanzada:** “la firma electrónica que cumple los requisitos contemplados en el artículo 26”:
- estar vinculada al firmante de manera única
- permitir la identificación del firman
- haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y
- estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
- **Firma electrónica cualificada:** “una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.”

2.3.3. Formatos de Firma

Los formatos de firma son la forma como se genera y firma y el modo en que se guarda la información de firma en el documento generado. Existen diferentes formatos y a continuación pasamos a describir brevemente los más utilizados para firma electrónica avanzada:

2.3.3.1. CAdES (CMS Advanced Electronic Signatures)

Es el formato adecuado para ficheros grandes. La información se guarda en binario, que lo que impide visualizar la información firmada. Tiene diferentes perfiles, en función del grado de protección que se quiera dar al documento:

- **CAdES:** Forma básica que cumple con el Reglamento Europeo.
- **CAdES-T (Timestamp):** Se incorpora un sello de tiempo para evitar repudio
- **CAdES-C (Complete):** CAdES-T al que se le añaden referencias de certificados y listas de revocación utilizadas, para posibilitar la validación de la firma de forma off-line
- **CAdES-X (Extended):** CAdES-C en el que se incorpora la fecha y hora de los datos de la extensión C
- **CAdES-X-L (Extended Long Term):** CAdES-X al que se anade la clave pública de los certificados y listas de validación utilizadas, para permitir la validación de la firma, aunque las referencias no estuvieran disponibles.
- **CAdES-A (Archivado):** Incluye todo lo anterior más toda la información de política de refirmado. Usado para aquellos documentos de tiempo de validez elevada.

2.3.3.2. XAdES (XML Advanced Electronic Signatures)

Familia de firmas avanzadas, basadas en formatos XML. Genera información de firma muy grande, así que no son recomendables para ficheros grandes. Es el formato ideal para comunicación de la información de firma entre máquinas.

Contiene las mismas extensiones descritas en el formato CAdES-XX

2.3.3.3. PAdES (PDF Advanced Electronic Signatures)

Este es el formato más adecuado cuando el documento original es un pdf. El destinatario de la firma puede comprobar fácilmente la firma y el documento firmado. Los documentos firmados electrónicamente con este formato permanecerán válidos durante un largo periodo de tiempo, aunque los algoritmos utilizados pasad el tiempo, hayan sido rotos.

Tiene los siguientes perfiles:

- **PAdES Basic:** cumple con los requisitos de la norma ISO 32000-1
- **PAdES-BES Profile (Enhece):** incorpora añadir un sello de tiempo
- **PAdES-EPES Profile (Enhace):** añade un identificador de política de firma.
- **PAdES-LTV Profile (Long Term):** Permite prorrogar por tiempo indefinido la validez de las firmas en el documento PDF.

2.3.4. Estrategias de correlación con el documento original

Existen 2 estrategias:

- La firma incluye el documento: ofrece una gestión más cómoda por que se tiene todo en un único fichero, pero en caso de archivos grandes, el consumo de espacio es elevado.
- El documento no se incluye en la firma: la firma incluye una referencia a la ubicación donde se encuentra el documento. Al contrario que en el caso anterior, la firma ocupa mucho menos espacio aunque la gestión y control de la correlación entre documento y firma es más complicada.

2.3.5. Firmas múltiples

Cubren los casos, en los que el documento necesita ser firmado por más de un usuario. Bajo este criterio contemplamos 3 tipos de firma:

- **Firmas Simples:** un único firmante.
- **Co-Firma:** varios firmantes pero no importa el orden en el que se realizan las firmas
- **Contra-Firma:** varios firmantes en el orden importa, pues cada firma debe certificar la firma anterior.

2.3.6. Sello de tiempo

El sellado de tiempo es un método para garantizar que la información existía antes de un momento dado y que dicha información no ha sido alterada posteriormente.

El Sello de Tiempo es una firma de un TSA (Autoridad de Sellado de Tiempo) que actúa como tercera parte de confianza.

Hay que tener en cuenta que el sello de tiempo se realiza con un certificado de la TSA y cuando éste caduca el sello y la firma dejan de ser validas, por lo que para evitar esta circunstancia, es necesario aplicar de nuevo el sello: a este proceso se le conoce como Resellado.

2.3.7. Custodia y almacenamiento de certificados

El almacenamiento de las claves privadas de los certificados es un punto crítico desde el punto de vista de la seguridad y se deben de utilizar los mecanismos adecuados para garantizar la protección de las claves y del uso de las mismas, únicamente por el propietario legítimo.

En el panorama tecnológico, los sistemas HSM son los más utilizados para este propósito, en los sistemas de firma centralizada.

Un HSM (Hardware Security Module) es un módulo de seguridad de hardware que genera, almacena y protege las claves criptográficas en su dispositivo hardware, cumpliendo las funciones de protección y custodia de las claves para el cifrado, descifrado, firma electrónica (firma digital) y autenticación digital. Se trata de un dispositivo altamente securizado, que imposibilita la extracción de las claves privadas del certificado, teniendo la posibilidad incluso de generar dichas claves en el propio HSM.

La configuración propuesta, consiste en tener el HSM conectado al servidor de firma con protección física punto a punto.

3. Arquitectura

3.1. Esquema de Autenticación

3.1.1. Flujo de autenticación

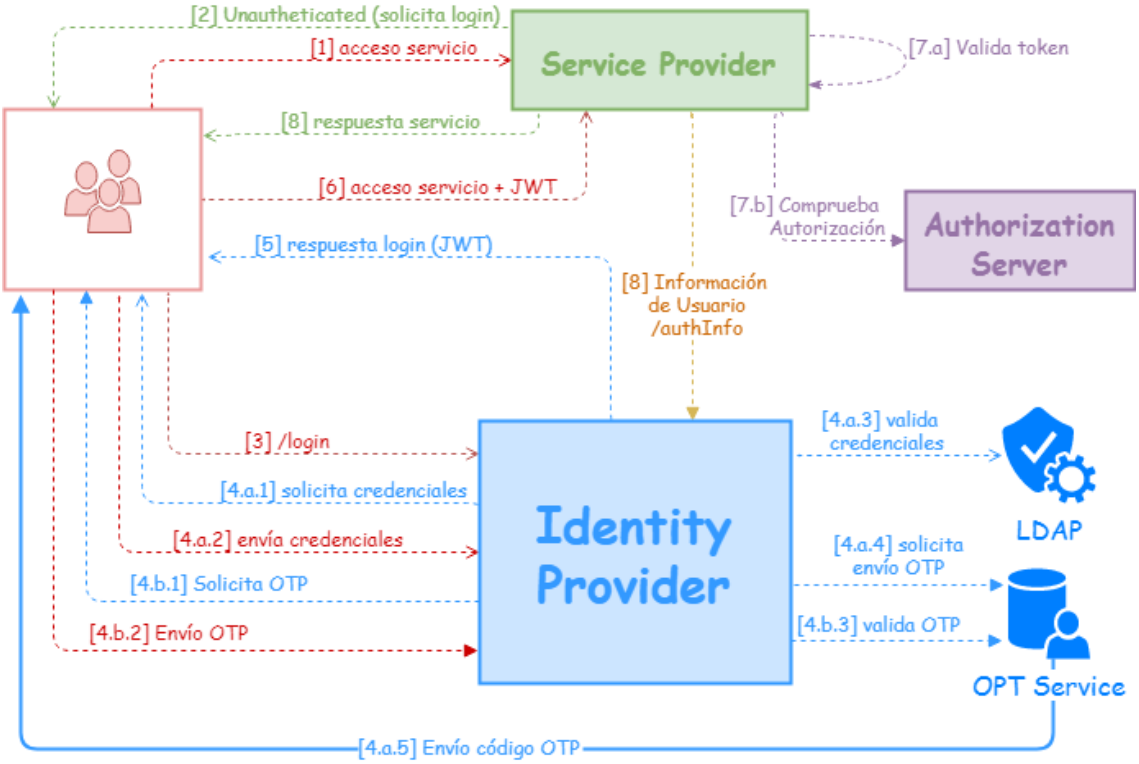


Ilustración 7. Flujo de autenticación

3.1.1.1. Descripción del escenario:

[1] La aplicación cliente invoca a un servicio seguro y protegido.

[2] El servicio contesta al cliente es necesario que el usuario que intenta consumir el servicio se autentique.

[3] La aplicación cliente negocia con el Identity Provider una apertura de sesión autenticada en el sistema.

[4] Proceso de autenticación:

[4.a] Flujo de validación User/password

[4.a.1] El Identity Provider muestra al usuario un formulario para que ingrese sus credenciales (usuario y password)

[4.a.2] El usuario ingresa el usuario y password de acceso y se lo envía al Identity Provider

[4.a.3] El Identity Provider valida las credenciales aportadas por el usuario, consultando LDAP

[4.a.4] Si las credenciales son correctas el Identity Provider inicia el segundo factor de autenticación, solicitando al OPT Service que envíe un mensaje al teléfono del usuario con un código (OTP).

[4.a.5] El OTP Service envía el código generado al usuario

[4.b] Flujo de validación OTP:

[4.b.1] El Identity Provider, solicita al usuario el segundo factor de autenticación (OTP).

[4.b.2] El usuario manda al Identity Provider el código que ha recibido en su teléfono.

[4.b.3] El Identity Provider envía el código al OTP Service para validarlo.

[5] Si el proceso de autenticación ha sido correcto, el Identity Provider envía al usuario un token de acceso.

[6] La aplicación cliente vuelve a intentar consumir el servicio, inyectando el token de acceso en la llamada.

[7] Control de Acceso.

[7.a.1] El Service Provider, comprueba que el token de acceso es válido.

[7.a.2] Una vez comprobado que el token de acceso es válido, va a consultar al Servidor de Autorización si el usuario asociado al token, tiene los permisos adecuados para consumir el servicio.

[8] Se ejecuta el Servicio, devolviendo la respuesta del mismo, al usuario que originó la petición de la llamada al servicio.

3.1.2. Esquema de autenticación delegado en WSO2.

WSO2 es una familia de productos opensource de middleware enfocadas a facilitar las integraciones de arquitecturas orientadas a servicios.

WSO2 Identity Server es el producto específico que se encarga de la Gestión de Identidades en las aplicaciones, servicios y API's empresariales. Presenta las siguientes capacidades, que hace de dicho producto el candidato ideal para delegarle la responsabilidad de la autenticación de nuestro sistema:

- **Single Sign On y federación de identidades**, utilizando los protocolos abiertos que son los mejores estándares del mercado: OpenID Connect, SAML 2.0 y WS-Federation.
- **Autenticación fuerte,** cumpliendo con nuestro requisito de autenticación multifactor, con contraseña de un solo uso de SMS / correo electrónico (OTP)
- **Administración de Identidades,** permitiendo gestionar usuarios y grupos de usuarios.

- **Control de Acceso,** basado en roles y basado en atributos basado en XACML.
- **Monitorización, reporting y auditoria,** que permite obtener analíticas para comprender los patrones de autenticación utilizados, detectar flujos de autenticación no permitidos y auditar las operaciones más comprometidas.
- **Facilidad de integración** con el resto de sistemas de la compañía gracias a la incorporación de múltiples conectores.
- **Cumplimiento con GDPR,** ayudando a abordar los nuevos requisitos de GDPR, como la privacidad de los datos del cliente, un portal para habilitar los derechos del cliente definidos en el GDPR y la administración del ciclo de vida de consentimiento. La solución es compatible con el aprovisionamiento de identidad segura en todos los sistemas de forma compatible con GDPR.

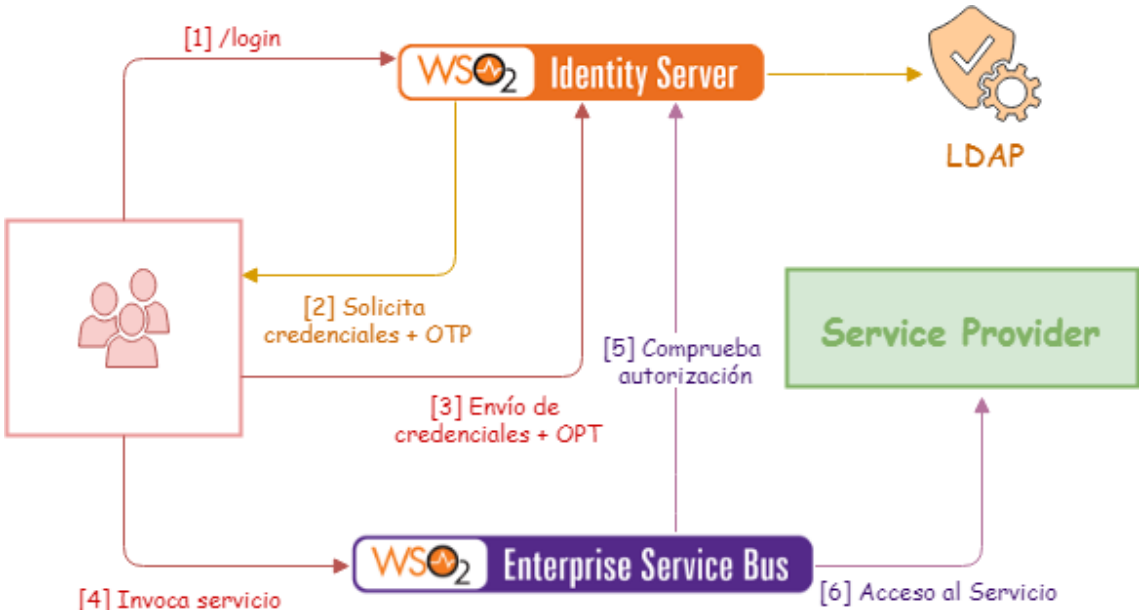


Ilustración 8. Flujos de Autenticación con WSO2

[1] La aplicación cliente solicita al Identity Provider (implementado por Identity Server de WSO2) un inicio de sesión.

[2] El IS inicia un flujo de comunicación con la aplicación cliente, solicitando las credenciales al usuario así como el envío de OTP como segundo factor de autenticación.

[3] El usuario envía las credenciales y el OTP al IS que lo valida y le entrega a la aplicación cliente un token de acceso.

[4] La aplicación solicita consumir un servicio.

[5] La petición es interceptada por el bus de Integración (implementado por Enterprise Service Bus de WSO2) y comprueba que la petición http viene con un token de acceso correcto y

comprueba que el usuario está autorizado a consumir el servicio requerido, mediante una petición a IS.

[6] El ESB, una vez validado que la petición es autorizada, propaga la petición del usuario hacia el Servicio requerido.

3.2. Esquema de Firma Electrónica

3.2.1. Flujo de Firma Electrónica

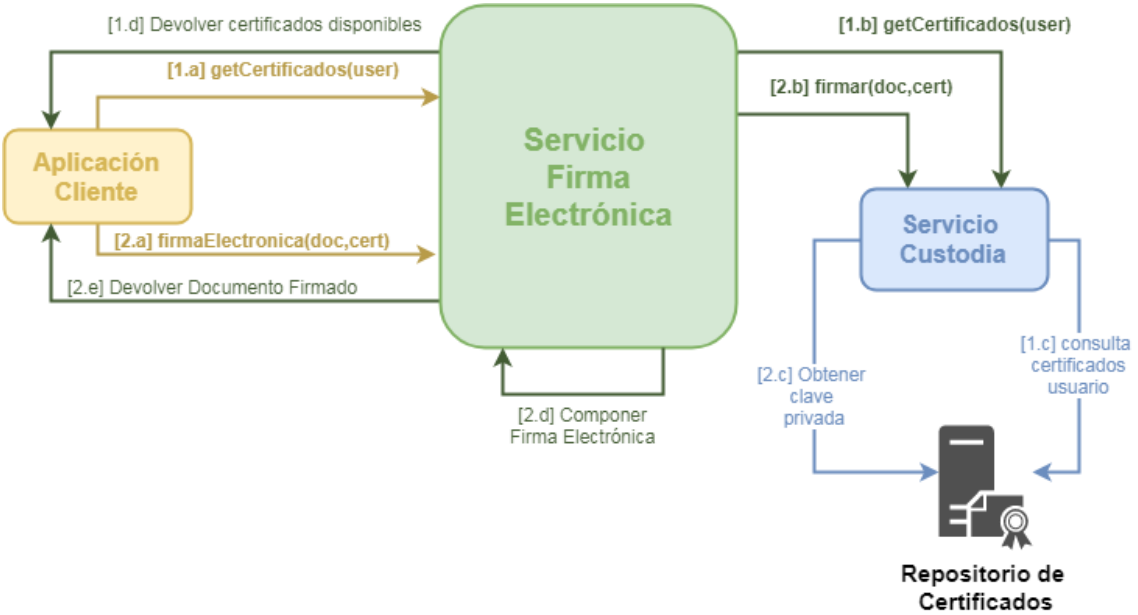


Ilustración 9. Flujo de Firma Electrónica

[1] Flujo de obtención de certificados.

[1.a] **getCertificados(user):** La aplicación solicita al Servicio central de Firma Electrónica los certificados que tiene disponibles el usuario con el que tiene una sesión abierta.

[1.b] **getCertificados(user):** El Servicio central de Firma Electrónica delega la consulta al Servicio de Custodia de Certificados.

[1.c] El Servicio de Custodia, consulta en el repositorio privado de certificados digitales los certificados que tiene del usuario consultado

[1.d] La aplicación Cliente recibe los certificados digitales que tiene disponible el usuario, para que seleccione el certificado con el que quiere realizar la firma

[2] Flujo de Firma

[2.a] **firmaElectronica(doc,cert):** La aplicación cliente realiza una petición al Servicio Central de Firma Electrónica la firma de un documento con el certificado seleccionado por el usuario.

[2.b] El Servicio central de Firma Electrónica realiza la composición de los datos a firmar para proceder a solicitar la firma digital de los mismos, al Servicio de Custodia.

[2.c] El Servicio de Custodia, obtiene las claves privadas del certificado y procede a realizar la firma digital de los datos recibidos.

[2.d] Una vez realizada la firma digital del documento, el Servicio central de Firma Electrónica, realiza la composición de la Firma Electrónica.

[2.e] La aplicación cliente recibe el documento firmado.

3.2.2. Esquema de firma delegado en REALSEC.

Realsec es una empresa tecnológica que desarrolla soluciones de cifrado y firma digital para entidades financieras, Gobierno y sector empresarial. Entre su gama de productos se encuentra *CriptoSign Server*, que se trata de un servidor criptográfico integrado para servicios de Firma Digital o Firma Electrónica Certificada de documentos.

3.2.2.1. Características del producto:

- Servidor en formato *appliance* de alta seguridad (hardware, software y HSM)
- Cliente compatible con cualquier lenguaje de programación o Sistema Operativo, que permite ser invocado desde las aplicaciones web o de gestión.
- Soporte para múltiples formatos de firma: Adobe PDF, CAdES, PAdESy XAdES y PKCS#7
- Firma de cualquier archivo electrónico.
- Firmas múltiples sobre el mismo documento PDF.
- Firma gráfica de varios firmantes sobre un mismo documento.
- Compatibilidad de firma con OCSP y CRLs.
- Autenticación segura de usuarios vía SSL.
- Firma compatible con sellado de tiempo.
- Máximas prestaciones y rendimiento en procesos de firma y verificación.
- Seguridad de claves y certificados, protegidos mediante hardware criptográfico certificado.

3.2.2.2. El producto incorpora las siguientes funcionalidades:

- Gestión centralizada y segura de claves y certificados.
- Control de caducidad de certificados.
- Generación automática de claves y solicitudes de certificación.

- Importación segura de certificados.
- API para integración con aplicaciones, procesos, sistemas, etc.
- Firma y/o Verificación de firma de cualquier documento, con elección de formato y certificado a emplear.

Impacto en el Flujo de Firma:

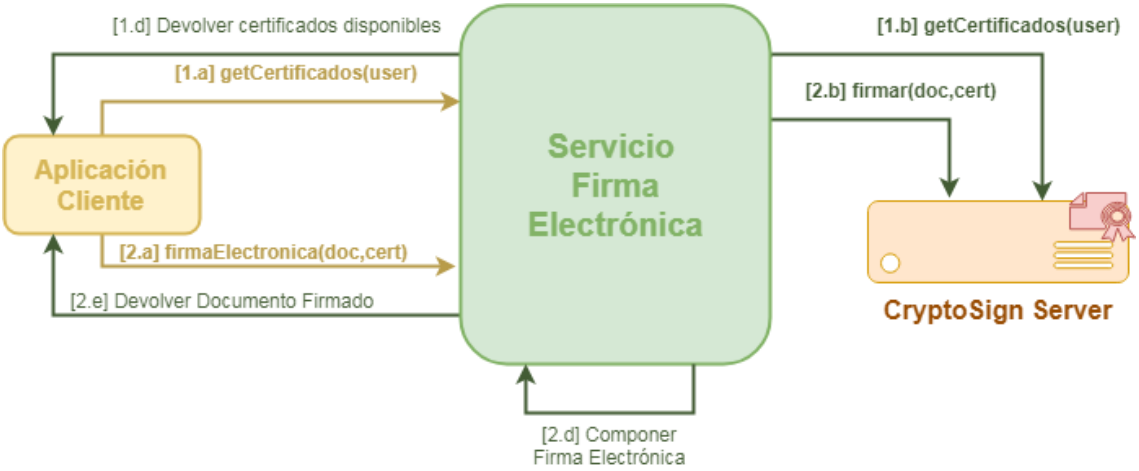


Ilustración 10.- Flujo de Firma Electrónica con CryptoSign Server

3.3. Arquitectura del Servicio de Firma Electrónica centralizada

Se ha decidido incorporar la solución de gestión de identidades de WSO2, a través de sus productos *Identity Server (IS)* y Enterprise *Service Bus (ESB)*. Aunque el producto *CryptoSign Server* de *Realsec*, cubre las necesidades de nuestro proyecto, se decide por razones económicas no incorporarlo en la arquitectura y realizar un desarrollo *adhoc* para cubrir la funcionalidad de firma digital de documentos con certificados digitales de usuarios gestionados y custodiados por la plataforma.

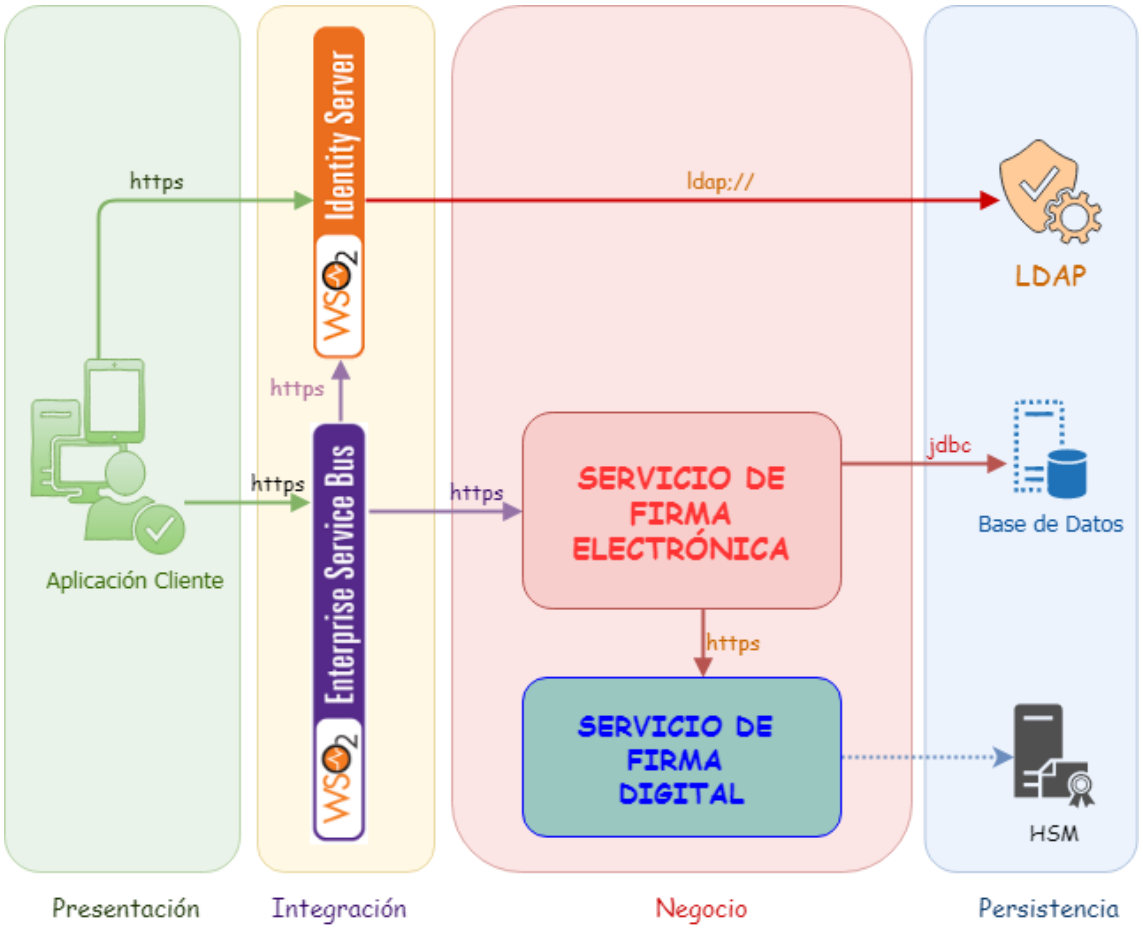


Ilustración 11. Arquitectura de la solución global de Firma Electrónica

La arquitectura presentada tiene un enfoque de 4 capas (Presentación, Integración-Orquestación, Negocio y Persistencia).

La capa de **Presentación,** tiene la responsabilidad de generar las vistas e interfaces de usuarios y será el lugar desde donde se generen las peticiones securizadas hacia el backend.

La responsabilidad de la capa de **Integración** se delegará en la familia de productos de ***WSO2: Identity Server y Enterprise Service Bus,*** que junto con el directorio de usuarios (LDAP) cubrirá el requisito de autenticación fuerte que requiere el servicio de firma centralizada, objeto de este proyecto.

En la capa de **Negocio**, se ubica el servicio de firma electrónica (composición de datos para firmar, proceso de firma con clave privada del certificado digital seleccionado y composición del formato de firma electrónica).

En la capa de persistencia, se ubican el Directorio de Usuarios (LDAP), la Base de Datos para persistir la auditoría del uso del servicio de Firma Electrónica y el repositorio centralizado de custodia de certificados digitales (HSM).

3.4. Definición de Interfaces

3.4.1. Proveedor de Identidad

3.4.1.1. Validación de primer nivel de autenticación (user/password)

```
public abstract boolean isValidPassword(String userId, String
password);
```

- **Parámetros**
  - **userId:** identificador de usuario
  - **password:** contraseña del usuario
- **Retorno:**
  - Indicador booleano credenciales introducidas válidas.

3.4.1.2. Validación del segundo nivel de autenticación (OTP)

```
public abstract boolean isValidPIN(String userId, String pin);
```

- **Parámetros**
  - **userId:** identificador de usuario
  - **pin:** pin del usuario
- **Retorno:**
  - Indicador booleano credenciales introducidas válidas.

3.4.2. Servicio de Firma Electrónica

3.4.2.1. Obtención de certificados

```
public abstract java.util.List<java.security.cert.X509Certificate>
getCertificados(
String userId)
throws
edu.uoc.errores.firmaelectronica.CertificadoException,
edu.uoc.errrore.seguridad.SeguridadException
```

- **Parámetros**
  - **userId:** identificador de usuario registrado en el sistema y titular de los certificados solicitados
- **Retorno:**
  - Lista de certificados cuyo titular es el identificador de usuario recibido.
- **Excepciones:**
  - `CertificadoException:` errores en la extracción y/o lectura del certificado.
  - `SeguridadException:` el usuario no tiene los permisos suficientes para realizar la operación solicitada.

3.4.2.2. Firma Electrónica

```
public byte[] firmaElectronica(
String userId,
byte[] documento,
java.security.cert.X509Certificate certificado,
String algoritmo,
String formato)
throws
edu.uoc.errores.firmaelectronica.CertificadoException,
edu.uoc.errrore.seguridad.SeguridadException
```

- **Parámetros**
  - **userId:** identificador de usuario registrado en el sistema y titular del certificado con el que se va a realizar la firma
  - **documento:** array de bytes del contenido del documento que se solicia firmar

- **certificado:** certificado digital con el que se solicita realizar la firma
- **algoritmo:** algoritmo de firma que se desea realizar. rsa-sha1, rsa-sha256, rsa-sha384, rsa-sha512
- **formato:** formato de firma electrónica: CaDES, XaDES, PaDES

- **Retorno:**
  - Firma electrónica realizada.

- **Excepciones:**
  - `edu.uoc.firmaelectronica.FirmaElectronicaException:` el certificado no es válido o no pertenece al usuario que solicita la firma electrónica.
  - `edu.uoc.seguridad.SecurityException:` el usuario no tiene los permisos suficientes para realizar la operación solicitada.

3.4.3. Servicio de Firma Digital

3.4.3.1. Obtención de certificados

```
public java.util.List<java.security.cert.X509Certificate>
getCertificados(

String userId)

throws

java.io.FileNotFoundException,
java.io.IOException,
java.security.KeyStoreException,
java.security.CertificateException
```

- **Parámetros**
  - **userId:** identificador de usuario registrado en el sistema y titular de los certificados solicitados

- **Retorno:**
  - Lista de certificados cuyo titular es el identificador de usuario recibido.

- **Excepciones:**
  - `FileNotFoundException:` errores de I/O: certificado no encontrado.
  - `IOException:` errores de I/O generales
  - `KeyStoreException:` Errores al cargar el KeyStore.

- `CertificateException:` errores en la extracción y/o lectura del certificado.

3.4.3.2. Firma

```
public byte[] firmar(
String userId,
byte[] datos,
java.security.cert.X509Certificate certificado
XMLSignature signature)

throws
java.security.KeyStoreException,
java.security.UnrecoverableKeyException,
java.security.cert.CertificateException,
java.security.NoSuchAlgorithmException
java.io.IOException
```

- **Parámetros**
  - **userId**: Identificador de usuario.
  - **datos:** array de bytes que deben ser firmados.
  - **certificado:** certificado digital con el que se solicita realizar la firma.
  - **signature:** firma electrónica generada para el documento
- **Retorno:**
  - Firma realizada.
- **Excepciones:**
  - `KeyStoreException:` errores al cargar el keystore del certificado.
  - `UnrecoverableKeyException:` errores al obtener la clave privada: error de encoding, tamaño,....
  - `CertificateException:` errores del certificado: problemas de encoding, certificado inválido, certificado revocado, certificado expirado.
  - `NoSuchAlgorithmException:` Algoritmo no soportado.
  - `IOException:` errores de Entrada/Salida

4. Desarrollo de la prueba de Concepto

4.1. Introducción:

Se ha elaborado una pequeña aplicación para poner en valor práctico el enfoque arquitectónico de la solución.

El lenguaje de programación elegido para el desarrollo del software ha sido JAVA y el desarrollo se ha desplegado en el servidor de aplicaciones Apache TOMCAT.

El diseño de esta aplicación, se ha centrado en poner en valor la custodia centralizada de los certificados y el esfuerzo de la separación funcional de la composición de la firma electrónica y de la firma digital con el uso del certificado, para permitir aislar esta última pieza de forma física para garantizar la seguridad de la custodia de los certificados de los usuarios.

Por ello y entendiendo que no forma parte de la prioridad de este trabajo el ámbito de la autenticación y autorización para el acceso a los servicios de firma electrónica, se ha prescindido de los elementos middleware, sustituyéndose por piezas software y repositorios localizados en el fileSystem local para la realización del piloto.

El enfoque distribuido del enfoque arquitectónico propuesto, se ha decidido realizarse en un monolito para facilitar el seguimiento de los flujos del proceso de negocio y hacer más comprensible el desarrollo realizado, ejecutando todo el contexto en una única máquina virtual, abstrayendo el trabajo de la problemática de la ejecución distribuida propuesta para un entorno de explotación.

Los certificados utilizados en la aplicación han sido autogenerados con la herramienta keytool incorporada en la distribución de Java y se ha utilizado el fyleSystem local del servidor como mecanismo de persistencia y custodia de los mismos.

El piloto realizado se ha limitado a la firma XaDES de documentos con formato XML.

4.2. Entorno

La prueba de concepto se ha desarrollado y desplegado en el siguiente entorno de trabajo:

- **Hardware**: Portátil *Samsung (Core i5-2450M a 2.5 GHz, 6144 MB RAM)*
- **Sistema Operativo**: *Microsoft Windows 7 Home Premium 6.1.7601 SP1*
- **IDE**: *Eclipse Mars Release (4.5.0)*
- **Java:** *1.7.0_79*
- **Servidor de aplicaciones**: *Apache Tomcat 8.0.52*

4.3. Diseño

4.3.1. Adaptación de la Arquitectura a la prueba de concepto.

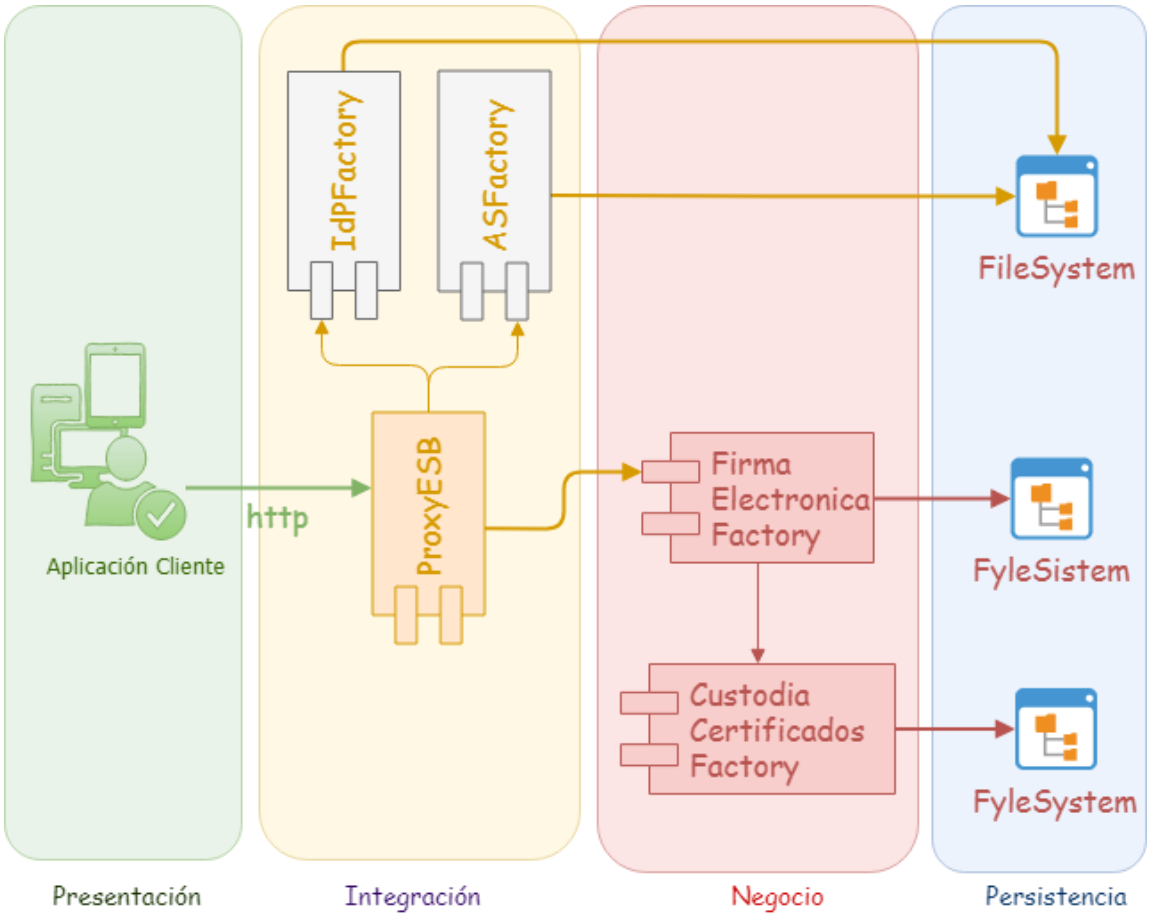


Ilustración 12. Adaptación de la Arquitectura a la prueba de concepto.

En la adaptación arquitectónica realizada para adaptarse al alcance de la prueba de concepto, se han realizado las siguientes adaptaciones:

- **Bus de Integración**: se ha adaptado al uso de un ***Web Filter*** de la especificación de Servlet. La clase que implementa dicho comportamiento es `edu.uoc.esbmock.controller.ProxyESB`
- **Identity Server:** El middleware encargado de implementar la gestión de identidades han sido simuladas con 2 piezas software desacopladas del contexto de la aplicación mediante la separación de la implementación y de la interfaz, desacoplando la implementación utilizada por la aplicación mediante el uso del patrón Factory. El LDAP se ha simulado con el uso del FileSystem, a través de 2 ficheros que contienen las credenciales y las autorizaciones.
    - usuarios.properties: contiene las credenciales de los usuarios, el formato del mismo es: `<CódigoUsuario>=<Password>#<PIN>`

- `roles.properties:` contiene los grupos de autorizaciones a las funcionalidades del sistema, el formato del mismo es: `<Funcionalidad>=<CódigoUsuario_1>|<CódigoUsuario_2>|…|<CódigoUsuario_N>`

Las clases que implementan este comportamiento son:

- **Identity Provider:**
  - **Paquete Base:** `edu.uoc.auth`
    - **Factoría:** `IdPFactory`
    - **Interfaz:** `IProveedorIdentidad`
    - **Implementación:** `Authenticate`
- **Servidor de Autorización:**
  - **Paquete Base:** `edu.uoc.auth`
  - **Factoría:** `ASFactory`
  - **Interfaz:** `IServidorAutorizacion`
  - **Implementación:** `Authorization`

- **Servicios de Firma:** Los servicios distribuidos de Firma se han implementado con clases java locales. Se ha desacoplado la implementación utilizada por el contexto de la aplicación mediante la segregación de interfaz e implementación y el uso del patrón Factory. El mecanismo de persistencia se ha simulado con el uso del FileSystem: los certificados de los usuarios se guardan en disco y las contraseñas de los mismos son almacenadas en ficheros properties asociados a los usuarios.
  Las clases que implementan los servicios de firma son
  - **Firma Electrónica:**
    - **Paquete Base:** `edu.uoc.servicios.firmaelectronica`
      - **Factoría:** `FirmaElectronicaFactory`
      - **Interfaz:** `IFirmaElectronicaService`
      - **Implementación:** `FirmaElectronicaService`
  - **Custodia de Certificados:**
    - **Paquete Base:** `edu.uoc.servicios.custodia`
      - **Factoría:** `CustodiaCertificadosFactory`
      - **Interfaz:** `ICustodiaCertificadosService`
      - **Implementación:** `CustodiaCertificadosService`
  - **Firma XAdES:** Para la realización de la firma XAdES nos hemos ayudado de las clases java autogeneradas a partir de la definición xsd de XAdES mediante el plugin maven XMLBeans.

Definición esquema XAdES:
(http://uri.etsi.org/01903/v1.3.2/XAdES.xsd)

4.3.2. Diagrama de Interfaces proporcionadas.

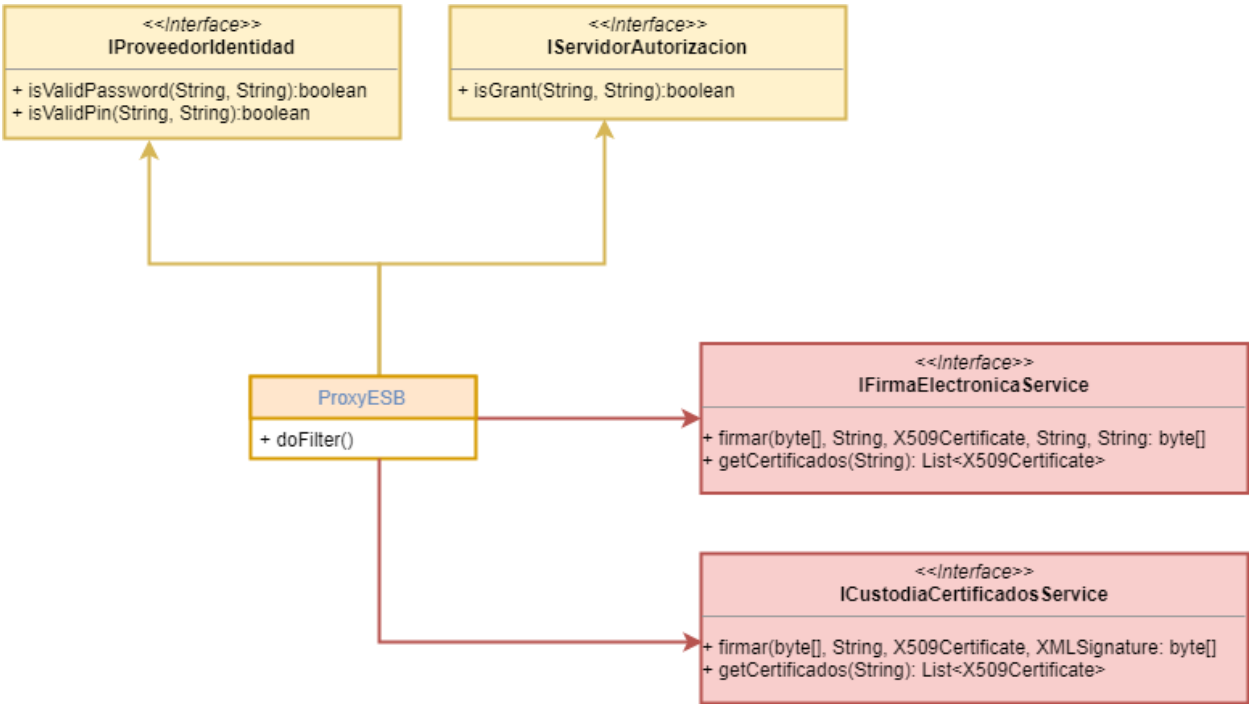


Ilustración 13. Interfaces Proporcionadas

4.4. Test de Funcionamiento del piloto

4.4.1. Juego de Ensayo

En la aplicación se han definido los siguientes usuarios con las siguientes credenciales:

Código Usuario	Password	PIN simulado enviado por SMS	¿Autorizado a Firmar?
99999990S	1000	0000	SI
99999991S	1001	1111	SI
99999992S	2002	2222	SI
99999993S	3003	3333	NO

En el sistema se encuentran custodiados los siguientes certificados:

Código Usuario	Certificado	DN
99999990S	99999990S-Fresno.pfx	CN=Usuario 99999990S, O=UOC,C=EDU, L=Fresno,S=Palencia,C=ES
99999990S	99999990S-Oliva.pfx	CN=Usuario 99999990S, O=UOC,C=EDU, L=Oliva,S=Valencia,C=ES
99999990S	99999990S-Badajoz.pfx	CN=Usuario 99999990S, O=UOC, C=EDU, L=Fregenal,S=Badajoz,C=ES
99999991S	99999991S-CapRoig.pfx	CN=Usuario 99999991S, O=UOC, C=EDU, L=Cap Roig,S=Alacant,C=ES

4.4.2. Navegación

4.4.2.1. Acceso inicial al portal. Solicitud de Credenciales

http://localhost:8088/FirmaElectronica/inicio.jsp

Accedemos al recurso web inicial del portal simulado UC-ANCERT destinado al notariado español. Para el acceso al portal es necesario ser un usuario registrado en la comunidad de notarios, así que el sistema presenta la página de login, para el usuario introduzca sus credenciales.

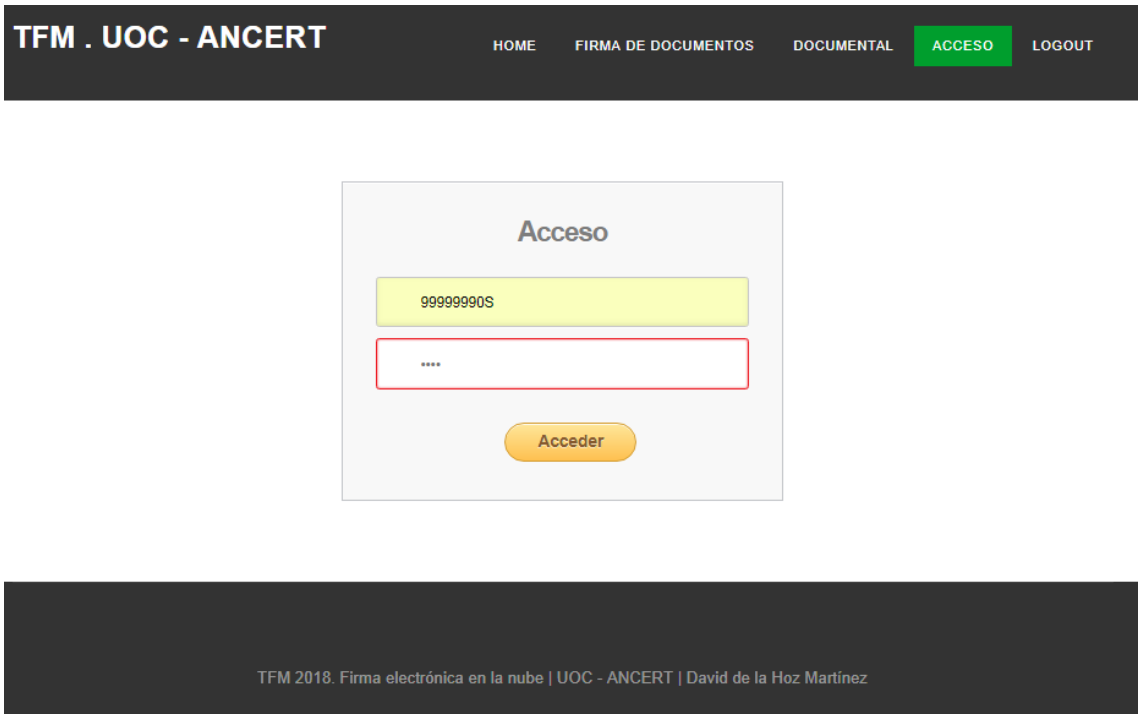


Ilustración 14. Piloto. Solicitud de Credenciales

4.4.2.2. Acceso a la sección de firmas con usuario autenticado.

http://localhost:8088/FirmaElectronica/inicio.jsp

Una vez autenticado, el Sistema nos presenta la Home del portal y el usuario accede a la sección de “Firma de Documentos”.

Ilustración 15. Piloto. Sección de Firma de Documentos.

4.4.2.3. Acceso a “Firmar Documentos”. Solicitud previa de PIN

http://localhost:8088/FirmaElectronica/firmar.jsp

Por medidas de seguridad, para acceder a la sección de Firmas de documentos, el sistema solicita un segundo factor de autenticación, basado en la introducción del PIN que el usuario ha recibido vía SMS.

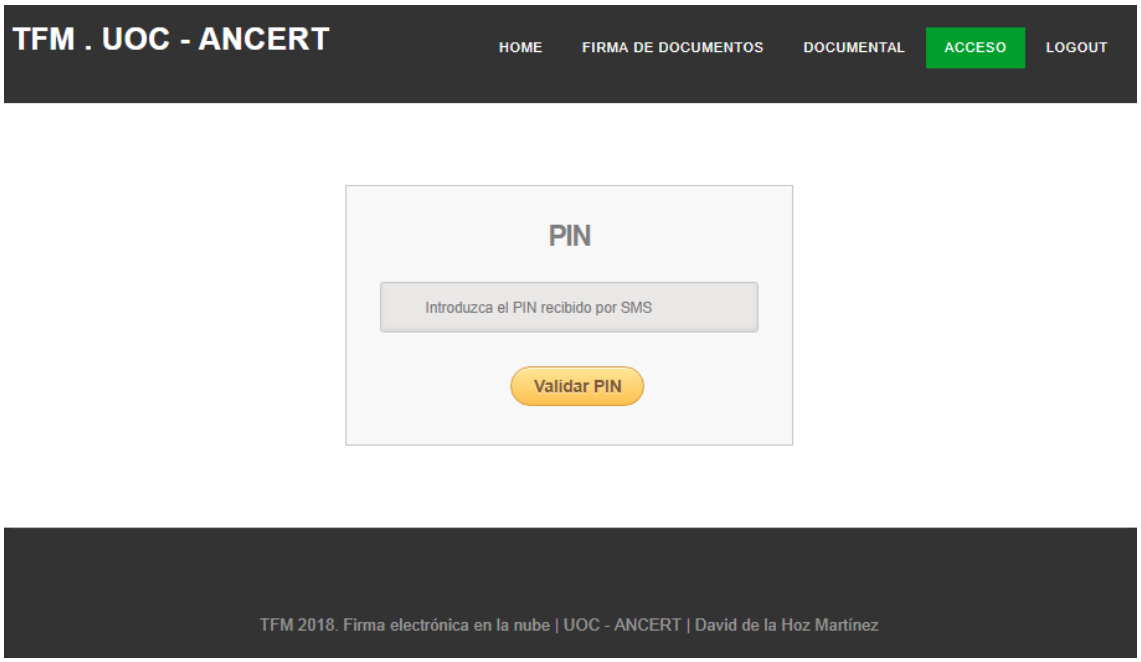


Ilustración 16. Piloto. Solicitud OTP

4.4.2.4. Selección de Certificados y documento a firmar

http://localhost:8088/FirmaElectronica/firmar.jsp

Una vez validado el segundo factor de autenticación, el sistema presenta al usuario todos los certificados que están custodiados en el sistema y que le pertenecen al usuario que se ha autenticado contra el sistema.

Ilustración 17. Piloto. Selección de certificados

4.4.2.5. Resultado de la Firma.

http://localhost:8088/FirmaElectronica/FirmaServlet

El usuario previamente ha seleccionado un certificado con el que realizar la firma del documento que también debe de seleccionar. El Sistema firma el documento con el certificado seleccionado y muestra el documento seleccionado con la firma electrónica realizada.

(Visualización del documento xml con la firma. Ver el análisis del resultado en el punto 4.3.3)

ustración 18. Piloto. Documento firmado

4.4.2.6. Flujo alternativo: Usuario sin certificados

El Usuario 99999992S se autentica correctamente, accede a la sección de Firmas y el sistema le solicita el PIN enviado por SMS. Se valida correctamente, pero el usuario no dispone de certificados en el sistema

Ilustración 19. Piloto. Flujo alternativo. Usuario sin certificados

4.4.2.7. Autorización. Flujo alternativo: Usuario no autorizado

El Usuario 99999993S se autentica correctamente, accede a la sección de Firmas y el Sistema comprueba que el usuario no tiene los privilegio para acceder a dicha sección.

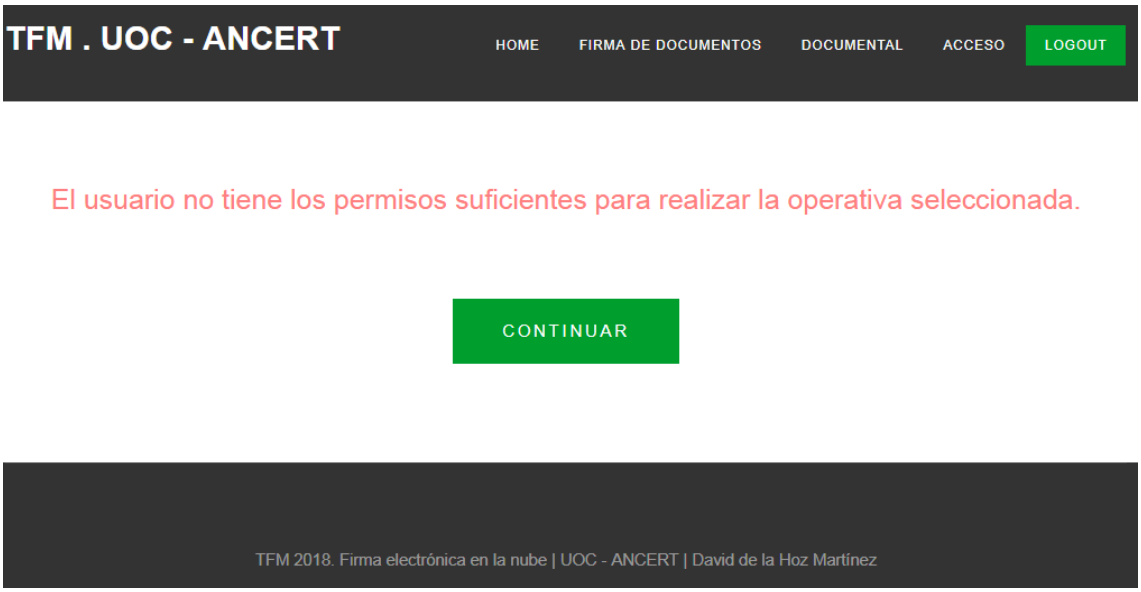


Ilustración 20. Piloto. Flujo alternativo. Usuario no autorizado.

4.4.3. Firma generada:

En los documentos adjuntos que se entregan junto a esta memoria se dispone del documento original (/test/documento.xml) y del documento firmado (/test/documentoFIRMADO.xml)

La firma generada es una firma XAdES enveloped y a continuación vamos a mostrar las partes más importantes del la firma generada:

- La firma se inserta dentro del documento XML, antes del últmo tag
- Se inicia el bloque de Firma (`ID='FirmaID'`) con la parte de la definición XMLDSIG (bloque de color rojo)
- Se añaden las propiedades marcadas en l definición de firma XAdES (Bloque de color verde)

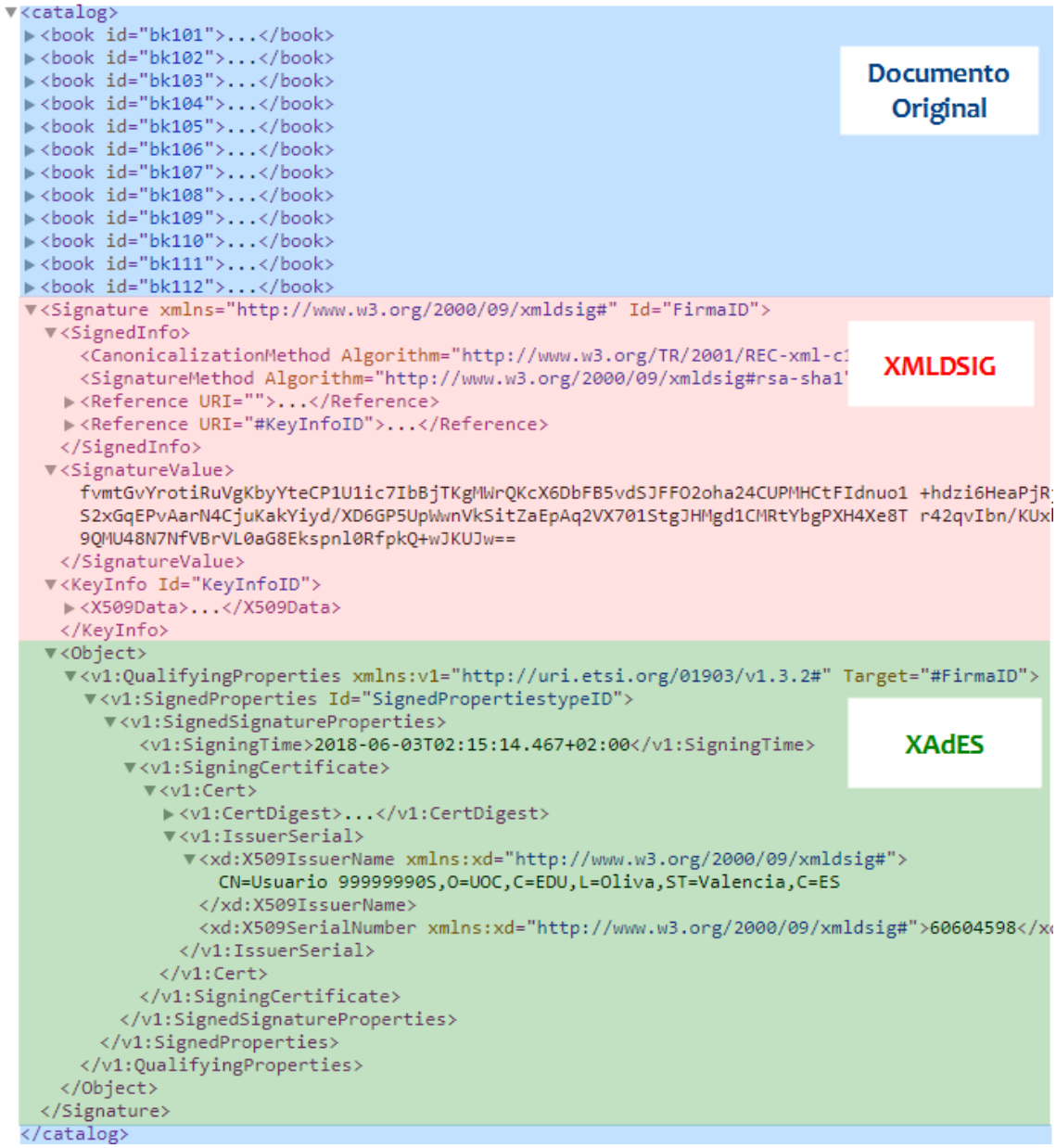


Ilustración 21. Piloto. Documento firmado. Partes de la firma

5. Conclusiones

El trabajo realizado cumple con las expectativas personales que había puesto en la concepción del proyecto. El diseño arquitectónico propuesto se adapta a las necesidades de mejora requeridas por ANCERT y aporta un valor añadido en el ámbito de la gestión de Identidades para garantizar el uso lícito del sistema. La modularización planteada de esta arquitectura distribuida, permite intercambiar productos sin afectar al *core* de la aplicación, por lo que los productos de terceros recomendados, pueden ser sustituidos por aquellos que se adapten mejor a la decisión estratégica de la compañía.

Mi conocimiento en el área de la Firma Electrónica, se limitaba al mundo académico, así que el proceso de aprendizaje ha sido muy fructífero y las lecciones aprendidas han sido un caldo de cultivo muy valioso para mi desarrollo profesional, desde ámbitos jurídicos hasta los más puros tecnológicos.

Los 3 grandes objetivos planteados al inicio del proyecto han sido satisfechos en la medida de lo exigible, aunque también es cierto que el alcance logrado en el tercer objetivo: "*Prueba de Concepto"*, no ha cubierto del todo mis expectativas, pues muchas funcionalidades de tipos de firma no se han podido implementar.

La planificación original, se ha cumplido escrupulosamente en los 2 primeros hitos, pero de cara al cumplimiento del Hito 3, la estimación de esfuerzo de las actividades de dicho Hito, fue inferior al tiempo real necesario y del tiempo de dedicación disponible. Esta circunstancia se ha resuelto reduciendo el alcance del desarrollo de la Prueba de Concepto y aumentando el tiempo de dedicación al proyecto planificado durante la iteración 4 del mismo, para realizar tareas que habían sido planificadas para ser entregadas en el Hito 3.

Tomando como inicio la finalización de este trabajo, existen muchas líneas de trabajo futuro a seguir explorando. Destaco las 3 más interesantes:

- Una clara línea de trabajo es continuar con los desarrollos iniciados en la prueba de concepto, para que el sistema contemple todos los tipos de firma electrónica en todos sus perfiles.
- Otra línea de trabajo es la dedicación exclusiva al estudio del appliance de Firma propuesto: *Crypto Sign Server* o cualquier otro disponible en el mercado como *TrustedX*. Esta línea de trabajo tiene entidad por sí sola para un TFM y estaba fuera del alcance del trabajo, pero personalmente, me hubiera gustado investigar con más dedicación a alguno de estos productos.
- Implementación de la Gestión de Identidades propuesta en este trabajo. En la prueba de Concepto está totalmente simulada, pues estaba fuera del ámbito del área de trabajo, pero es fundamental para la consistencia del sistema concebido.

6. Glosario

A

ANCERT: Agencia Notarial de Certificación.

API: Interfaz de Programación de Aplicaciones.

AS: Servicio de autorización

Appliance: dispositivo con un software (firmaware) específico, diseñad para proveer un recurso computacional.

B

Backend: Capa software que se encuentra en el servidor.

C

CAdES: CMS Advanced Electronic Signatures.

Co-Firma: Proceso de firma en el que intervienen varios firmantes pero no importa el orden en el que se realizan las firmas.

contra-Firma: Proceso de firma en el que intervienen varios firmantes en el orden importa, pues cada firma debe certificar la firma anterior.

CRL: Lista de Revocación de Certificados.

E

eIDAS: Reglamento de la Unión Europea Nº 910/2014

ESB: Entreprise Service Bus. Middleware que implementa el patrón BUS es utilizado como mecanismo de integración entre diferentes sistemas de información empresariales.

F

FileSystem: Sistema de Ficheros.

G

GDPR: Reglamento General de Protección de Datos de la Unión Europea.

H

HSM: Hardware Security Module. Dispositivo criptográfico que genera, almacena y protege claves criptográficas

I

IS: Servidor de Identidad

IdP: Proveedor de Identidad.

L

LDAP: Protocolo Ligero/Simplificado de Acceso a Directorios. Protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

M

Monofactor: Sistema de autenticación que hace uso de un solo mecanismo de identificación del usuario.

Middleware: Software que se sitúa entre un sistema operativo y las aplicaciones que se ejecutan en él. Funciona como una capa de traducción oculta para permitir la comunicación y la administración de datos en aplicaciones distribuidas

N

N-Factor: Sistema de autenticación que hace uso de varios mecanismos para la identificación del usuario.

O

OTP: One Time Password. Password que sólo es válida para autenticarse una sóla vez en us sistema.

Opensource: Modelo de desarrollo de software basado en la colaboración abierta

OIDC. Open ID Connect. Protocolo de autenticación implementada utilizando el framework de autorización OAuth 2.0.

OCSP: Protocolo de comprobación del Estado de un Certificado.

P

PAdES: PDF Advanced Electronic Signatures

S

SP: Service Provider. Figura genérica que representa al provvedor de un servicio.

SSO: Single Sign On. Procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con un único proceso de autenticación.

SAML: Lenguaje de Marcado para Confirmaciones de Seguridad. Estándar abierto, que define un esquema XML para el intercambio de datos de autenticación y autorización.

SSL: Secure Sockets Layer. Protocolo criptográfico que proporcionan comunicaciones seguras.

T

TSA: Autoridad de Sellado de Tiempo. Prestador de servicios de certificación que proporciona certeza sobre la preexistencia de determinados documentos electrónicos a un momento dado.

Tomcat: Servidor de aplicaciones *opensource*, distribuido por Apache

X

XAdES: XML Advanced Electronic Signatures.

XACML: EXtensible Access Control Markup Language. Estándar que define un lenguaje declarativo de políticas de control de acceso implementado en XML y un modelo de procesamiento que describe cómo evaluar peticiones de acceso según las reglas definidas en las políticas.

XMLDSIG: Firma XML. Es una recomendación del W3C que define una sintaxis XML para la firma digital.

W

WSO2: Compañía que desarrolla middleware de código abierto enfocadas en proveer una arquitectura orientada a servicios.

7. Bibliografía

1. ***ANCERT. Información de empresa (Marzo 2018)***
   http://www.ancert.com/liferay/web/ancert/sobre-nosotros
2. ***ANCERT. Estructura Organizativa (Marzo 2018)***
   http://www.ancert.com/liferay/web/ancert/estructura-organizativa
3. ***ANCERT. Portfolio de servicios (Marzo 2018)***
   http://www.ancert.com/liferay/web/ancert/nuestros-productos-y-servicios
4. ***CarmerFirma. Gestión centralizada de claves (Mayo 2018)***
   http://www.camerfirma.com/es/soluciones/gestion-de-claves-centralizada/
5. ***DocuSign. Appliance de Firma (Mayo 2018)***
   https://www.docusign.com/products/signature-appliance
6. ***MINHAFP. Esquemas XML (Marzo 2018)***
   http://www.sefp.minhafp.gob.es/dam/es/web/publicaciones/centro_de_publicaciones_de_la_sgt/Monografias0/parrafo/Manual_XML/text_es_files/Manual_esquemas-XML-intercambio-doc-exp-elec-INTERNET.pdf
7. ***PAe. Conceptos generales de Firma centralizada (Marzo 2018)***
   http://clave.gob.es/clave_Home/dnin/queEs.html
8. ***PAe. Sistema Cl@veFirma (Marzo 2018)***
   https://administracionelectronica.gob.es/ctt/clavefirma/infoadicional#.WqWnJGrOXIU
9. ***PAe. Sistema FIRe de firma electrónica (Marzo 2018)***
   https://administracionelectronica.gob.es/ctt/fire#.WqUSSmrOXIU
10. ***Planeta Tandem. Autenticación doble factor (Abril 2018)***
    https://www.ttandem.com/blog/autenticacion-por-doble-factor-en-servicios-online/
11. ***Realsec. CryptoSign Server (Abril 2018)***
    http://realsec.com/productos-y-soluciones/soluciones-seguridad-transformacion-digital/cifrado-y-firma-digital/cryptosign-server/
12. ***Redtrust. Gestión centralizada de certificados digitales (Mayo 2018)***
    http://www.evolium.com/gestion-certificados-digitales

13. ***Realsec. HSM (Mayo 2018)***

http://realsec.com/productos-y-soluciones/hsms-proposito-general/hsm-hardware-security-module/

14. ***REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 (Abril 2018)***

http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=EN

15. ***Thales. HSM. (Mayo 2018)***

https://es.thalesesecurity.com/products/general-purpose-hsms

16. ***Verisec. HSM. (Mayo 2018)***

https://www.verisec.com/es/cifrado/general-purpose-hsm/

17. ***ViaFirma. Formatos de firma electrónica. (Abril 2018)***

https://www.viafirma.com/es/formatos-de-firma-electronica

18. ***W3C. Formatos de Firma electrónica.XAdES (Mayo 2018)***

https://www.w3.org/TR/XAdES/#Syntax_overview_The_QualifyingProperties_SignedDataObjectProperties

19. ***WSO2. Identity Server (Abril 2018)***

https://wso2.com/identity-and-access-management

20. ***WSO2. Identity Server (Abril 2018)***

https://wso2.com/library/articles/2016/09/article-use-case-building-a-secure-identity-framework-with-wso2-identity-server/

21. ***XMLBeans (Mayo 2018)***

https://www.adictosaltrabajo.com/tutoriales/xml-beans/

8. Anexos

8.1. Prueba de Concepto

Se anexa junto con la memoria el fichero comprimido FirmaElectronica_PruebaConcepto.zip que tiene el siguiente contenido:

- **/bin:** directorio donde se encuentran el fichero con los binarios de los fuentes desarrollados y empaquetados en un único fichero (FirmaElectronica.war) preparado para ser desplegado en el servidor de aplicaciones.
- **/sources:** directorio que contiene el proyecto con todos los fuentes desarrollados para la prueba de concepto.
- **/servidor:** Directorio que contiene un único fichero comprimido con la instantánea de la instalación del servidor Tomcat con el que se han realizado los despliegues y las pruebas de los desarrollos realizados.
- **/test:** Directorio que contiene documentos para probar el proceso de firma.
- **/configuración:** Directorio que contiene todos los certificados autogenerados con los que se han realizado las pruebas, así como los ficheros de definición de usuarios y autorizaciones de los mismos.

8.2. Instalación de la aplicación Prueba de Concepto

8.2.1. Servidor Tomcat preinstalado.

Si se desea desplegar la aplicación en un servidor Tomcat previamente instalado:

[1] Descomprimir el fichero que se ha distribuido junto con esta memoria: `FirmaElectronica_PruebaConcepto.zip`

[2] Acceder al directorio /bin y obtener el fichero `FirmaElectronica.war`

[3] Desplegar el fichero /war en el servidor Tomcat preinstalado.

[4] Acceder al directorio /configuración y copiar todos los ficheros en la ruta del servidor Tomcat `/[Directorio_Instalación_Tomcat]/bin/configuracion/`

[5] Arrancar el servidor Tomcat y acceder a la página de inicio de la aplicación: `http://[host]:[puerto]/ FirmaElectronica/inicio.jsp`

8.2.2. Instalación completa

Si se desea realizar una instalación completa (servidor + aplicación), se deben seguir los siguientes pasos:

[1] Descomprimir el fichero que se ha distribuido junto con esta memoria: `FirmaElectronica_PruebaConcepto.zip`

[2] Acceder al directorio /servidor y obtener el fichero `instalacionCompleta.zip`

[3] Descomprimir el archivo `instalacionCompleta.zip` en la máquina destino.

[4] Arrancar el servidor Tomcat embebido:
`/[Directorio_Descompresion]/apache-tomcat-8.0.52/bin/startup.bat`

[5] Acceder a la página de inicio de la aplicación:
`http://localhost:8088/FirmaElectronica/inicio.jsp`

8.3. Manual de Usuario.

8.3.1. Usuarios de la aplicación

Por defecto se encuentran dados de alta los siguientes usuarios, con los que se podrá probar la aplicación

Código Usuario	Password	PIN simulado enviado por SMS	¿Autorizado a Firmar?
99999990S	1000	0000	SI
99999991S	1001	1111	SI
99999992S	2002	2222	SI
99999993S	3003	3333	NO

Ilustración 22. Manual de Usuario. Usuarios de Prueba

8.3.2. Navegación:

8.3.2.1. Acceso a la aplicación

http://localhost:8088/FirmaElectronica/inicio.jsp

8.3.2.2. Home. Barra de menú:

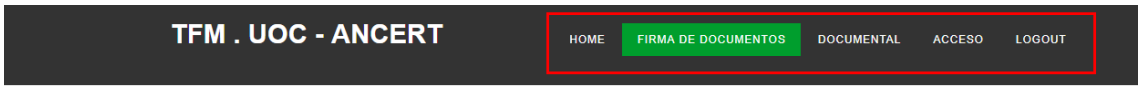


Ilustración 23. Manual de Usuario. Barra de menú

La aplicación tiene en la parte superior una barra de menú con las siguientes opciones:

- HOME: enlace a la página inicio del portal

- FIRMA DE DOCUMENTOS: enlace a la sección de Firma de Documentos
- DOCUMENTAL: Enlace No activo
- ACCESO: Enlace a la funcionalidad de autenticarse en el sistema
- LOGOUT: Enlace a la funcionalidad de finalizar sesión en el sistema.

8.3.2.3. Autenticación

Para acceder al portal es necesario estar autenticado en el sistema. Se puede utilizar cualquier usuario/password indicados en el punto inicial.

Ilustración 24. Manual de Usuario. Página de Login.

8.3.2.4. Acceso a la sección de Firma de Documentos:

Pulsamos en la opción de menú “FIRMA DE DOCUMENTOS”. Para acceder a la funcionalidad de Firma, pulsamos el botón “FIRMAR DOCUMENTOS”

Ilustración 25. Manual de Usuario. Sección de Firma

8.3.2.5. Solicitud de PIN.

Para acceder a la funcionalidad de Firma, el Sistema solicita un segundo factor de autenticación. Para ello envía al usuario un SMS con el PIN que debe de introducir en la siguiente pantalla. Se puede utilizar el PIN asociado al usuario autenticado indicado en el punto inicial.

Ilustración 26. Manual de Usuario. Solicitud de PIN.

8.3.2.1. Funcionalidad de Firma.

En la funcionalidad de Firma, el Sistema nos presenta los certificados que nuestro usuario tiene dados de alta.

[1] Seleccionamos de la lista de certificados, el certificado con el que deseamos firmar

[2] Pulsamos el botón “Seleccionar el fichero que desea firmar” y el Sistema nos muestra un popoup con acceso a nuestro sistema de ficheros, para poder seleccionar el fichero que se desea firmar (Nota: esta versión de la aplicación sólo acepta ficheros XML)

[3] Pulsamos el botón “FIRMAR”.

[4] El sistema nos muestra por pantalla el contenido del fichero y su firma electrónica.

Ilustración 27. Manual de Usuario. Funcionalidad de Firma

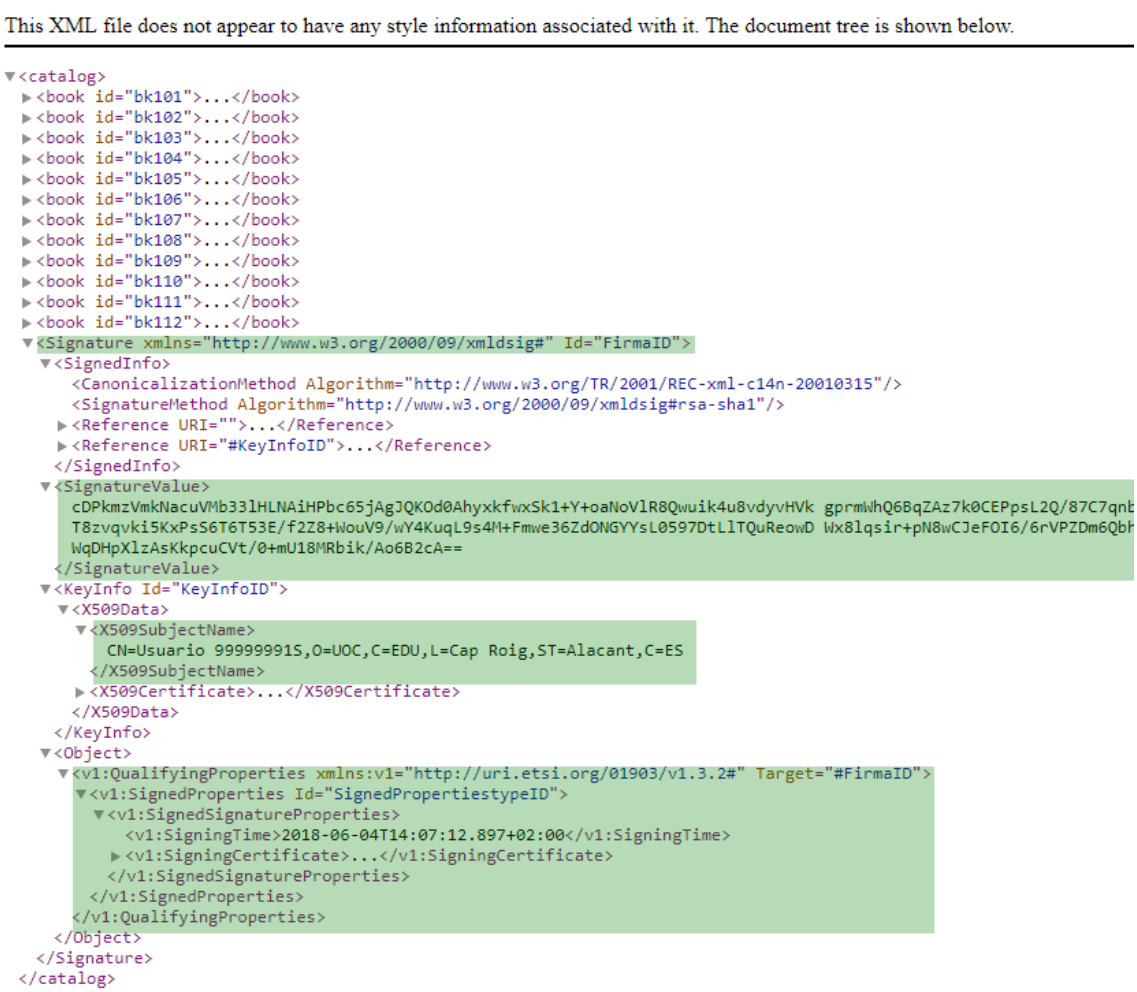


Ilustración 28. Manual de Usuario. Documento Firmado