Evidencias electrónicas

Nombre Estudiante: Manuel Turner Vergel

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Nombre Consultor: Enric Hernández Jiménez

Centro: Universitat Oberta de Catalunya/Ancert

Fecha entrega: 20 de junio de 2014

Agradecimientos

En primer lugar, me gustaría agradecer a mi mujer Lorena, su apoyo en todo momento, motivación y su comprensión en los momentos difíciles.

Por último, agradecer a Enric Hernández Jiménez su ayuda para poder sacar adelante este Trabajo Final de Máster, aportando recursos, conocimientos, tiempo y claridad.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Evidencias electrónicas
Nombre del autor:	Manuel Turner Vergel
Nombre del consultor:	Enric Hernández Jiménez
Fecha de entrega (mm/aaaa):	06/2014
Área del Trabajo Final:	
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Resumen del Trabajo (máximo 250 palabras):

El Consejo General del Notariado desea ofrecer a sus colegiados la posibilidad de capturar y generar evidencias electrónicas que acrediten la publicación de determinado contenido en páginas Web

Para satisfacer dicha necesidad se ha desarrollado una aplicación Web que mediante la introducción de una determinada URL, por parte del usuario, se capture, firme y genere evidencia electrónica de la página Web indicada.

El formato utilizado para poder otorgar validez a largo plazo es la firma electrónica avanzada XML XAdES, en su versión XAdES-A.

Abstract (in English, 250 words or less):

The General Council of Notaries wants to offer their members a framework for capturing and generating electronic evidences on the contents of web pages..

In order to meet this functionality, a web application has been developed allowing the introduction of the URL, from whose content the user wants to generate electronic evidence.

The format used to provide long-term validity is the XML Advanced Electronic Signatures (XAdES) in its version XAdES-A.

Palabras clave (entre 4 y 8):

XAdES, firma electrónica, firma, custodia

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El Consejo General del Notariado tiene la necesidad de poder certificar que un contenido electrónico se ha expuesto públicamente en tiempo y, además, éste no ha sido modificado ni alterado a lo largo del paso del tiempo.
Esto puede ocurrir en casos como la publicación de las bases de algún concurso o subasta a partir de una fecha y hora determinada.

1.2 Objetivos del Trabajo

El objetivo del presente trabajo fin de máster, en adelante TFM, es abarcar la realización de una aplicación y proceso que permita al notariado poder satisfacer la necesidad descrita en el punto anterior. De forma que el notariado pueda tener evidencias mediante las que probar que un documento es válido en cuanto a integridad, autenticidad y tiempo en el que se firmó.

1.3 Enfoque y método seguido

Se ha elegido un diseño en cascada tradicional, en el que se realizará un desarrollo del proyecto mediante una secuencia de fases básicas. En este caso se ha determinado la existencia de fases de análisis, diseño, implementación y, por último, de documentación. Estas fases tendrán definidas claramente hitos que darán paso a la siguiente.

· **Análisis:** definición formal de requerimientos.

· **Diseño:** la definición de la arquitectura general del software y la representación de la interfaz gráfica.

· **Implementación:** en esta etapa se desarrollará el software necesario para satisfacer los requerimientos de la fase de análisis.

· **Documentación:** esta etapa será la última fase del proyecto, en la que se ultimará la documentación necesaria para realizar la entrega final.

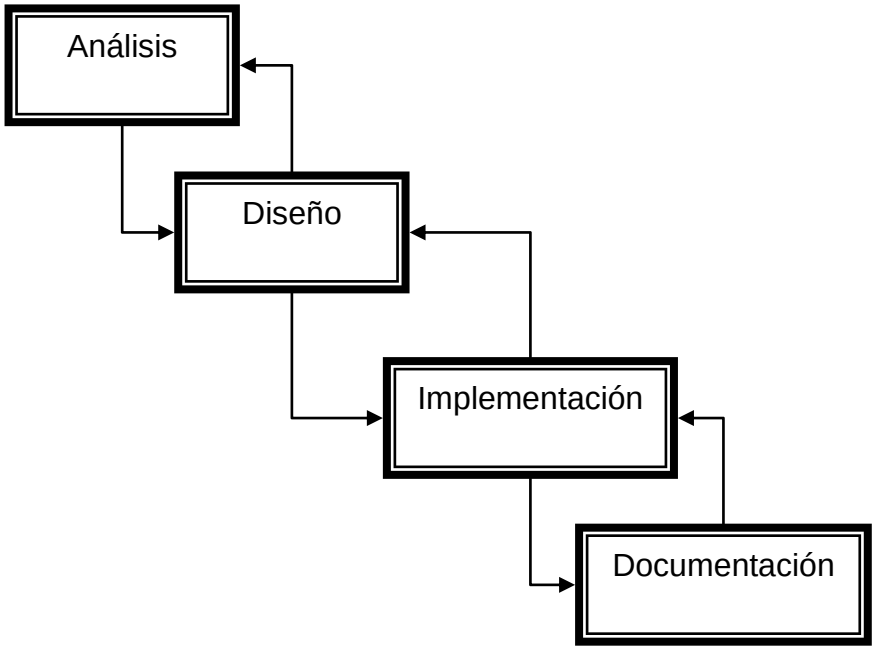

Figura Nº 1.Fases desarrollo del proyecto

1.4 Planificación del Trabajo

Este trabajo final de máster se desarrollará entre el 26 de Febrero de 2014 y el 27 de Junio de 2014.

1.4.1. Tareas

El trabajo final de máster contendrá las siguientes tareas a realizar:

· **Planificación del proyecto:** en esta primera tarea definiremos la planificación, indicando el resto de tareas a realizar y su duración.

· **Análisis de requerimientos:** en esta tarea analizaremos la problemática del proyecto, de forma que podamos obtener todos los requisitos necesarios para el correcto desarrollo del TFM.

· **Casos de uso y diagramas de secuencia:** una vez obtenidos los requisitos necesarios se presentarán los usos y los flujos que contendrán la aplicación y proceso a desarrollar.

· **Diseño - elección de arquitectura e interfaces de usuario:** se decidirá la arquitectura de diseño y se indicarán posibles interfaces de usuario.

· **Implementación de interfaces gráficas:** implementación de interfaces gráficas para poder dar al usuario una presentación amigable.

· **Implementación de algoritmos de custodia:** implementación de los algoritmos diseñados para crear las funcionalidades detalladas.

· **Redacción de la memoria final:** redacción de documentación y memoria para su entrega como final de TFM.

· **Presentación:** elaboración de una presentación gráfica del proceso de custodia en la aplicación desarrollada.

	Nombre	Duracion	Inicio	Terminado	Predecesores
1	**TFM**	88 days?	**26/02/14 8:00**	**27/06/14 17:00**	
2	**PAC1**	14 days?	**26/02/14 8:00**	**17/03/14 17:00**	
3	Planificación proyecto	13 days?	26/02/14 8:00	14/03/14 17:00	
4	Entrega versión	1 day?	17/03/14 8:00	17/03/14 17:00	3
5	**PAC2**	20 days?	**18/03/14 8:00**	**14/04/14 17:00**	
6	Análisis de requirimientos	7 days?	18/03/14 8:00	26/03/14 17:00	4
7	Casos de uso y diagramas de secuencia	6 days?	27/03/14 8:00	3/04/14 17:00	6
8	Diseño: elección arquitectura e Interfaces gráficas	6 days?	4/04/14 8:00	11/04/14 17:00	7
9	Entrega versión	1 day?	14/04/14 8:00	14/04/14 17:00	8
10	**PAC3**	25 days?	**15/04/14 8:00**	**19/05/14 17:00**	
11	Implementación interfaces gráficas	9 days?	15/04/14 8:00	25/04/14 17:00	9
12	Implementación de algoritmos de custodia	15 days?	28/04/14 8:00	16/05/14 17:00	11
13	Entrega versión	1 day?	19/05/14 7:00	19/05/14 17:00	
14	**PAC4**	29 days?	**13/05/14 8:00**	**20/06/14 17:00**	
15	Realización de memoria final	28 days?	13/05/14 8:00	19/06/14 17:00	
16	Entrega versión	1 day?	20/06/14 8:00	20/06/14 17:00	15
17	**PAC5**	5 days?	**23/06/14 8:00**	**27/06/14 17:00**	
18	Realización presentación	4 days?	23/06/14 8:00	26/06/14 17:00	16
19	Entregar versión	1 day?	27/06/14 8:00	27/06/14 17:00	18

Figura Nº 2.Tareas

1.4.2. Diagrama de Gantt

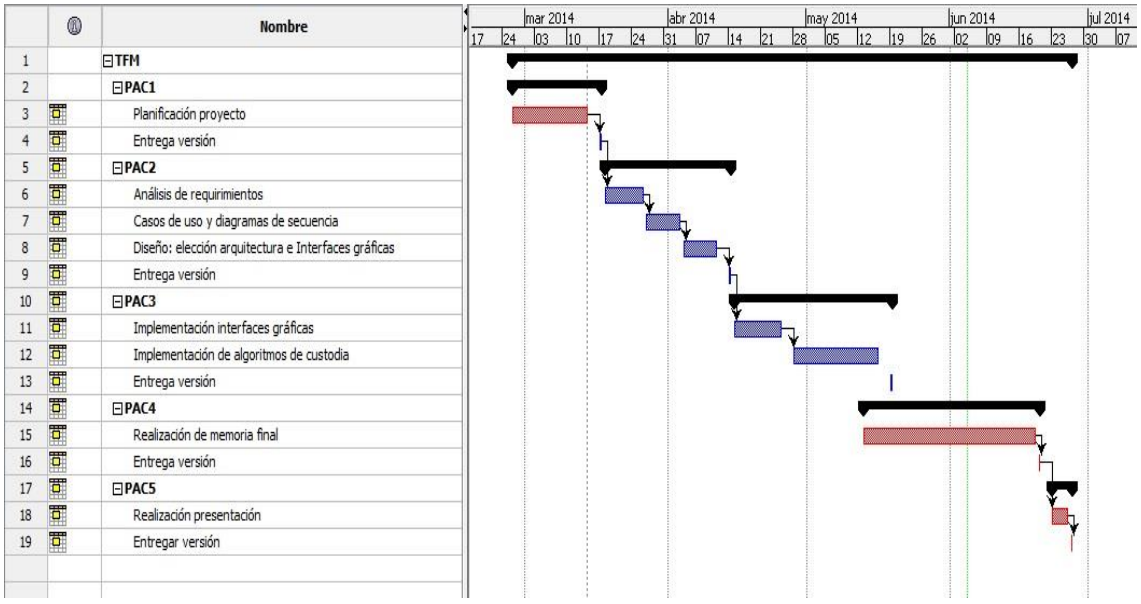

Figura Nº 3.Planificación de tareas

1.5 Breve sumario de productos obtenidos

Se ha obtenido una aplicación Web desarrollada en Java, que puede ser desplegada mediante un fichero .war en un servidor web Tomcat. Esta aplicación permitirá ofrecer un servicio de custodia electrónica de páginas web al colectivo notarial.

1.6 Breve descripción de los otros capítulos de la memoria

A continuación, se indican los capítulos que se desarrollan a lo largo de la presente memoria:

Estado del arte: información teórica de los aspectos necesarios para la realización del presente proyecto.

Análisis: se analizará la problemática del proyecto para poder obtener posteriormente el producto deseado.

Implementación y diseño: detalles de la construcción del producto objetivo.

Conclusiones: se indicará si se han alcanzado los objetivos definidos inicialmente y la posible evolución futura del proyecto.

2. Estado del arte

2.1. Firma digital

La firma digital es un método criptográfico para poder proporcionar integridad, autenticación y no repudio a un documento [10][11]. Para ello, el emisor crea una función resumen (hash) del mensaje a firmar. A continuación, dicho resumen es cifrado con la clave privada del firmante para de esta forma generar la firma digital.

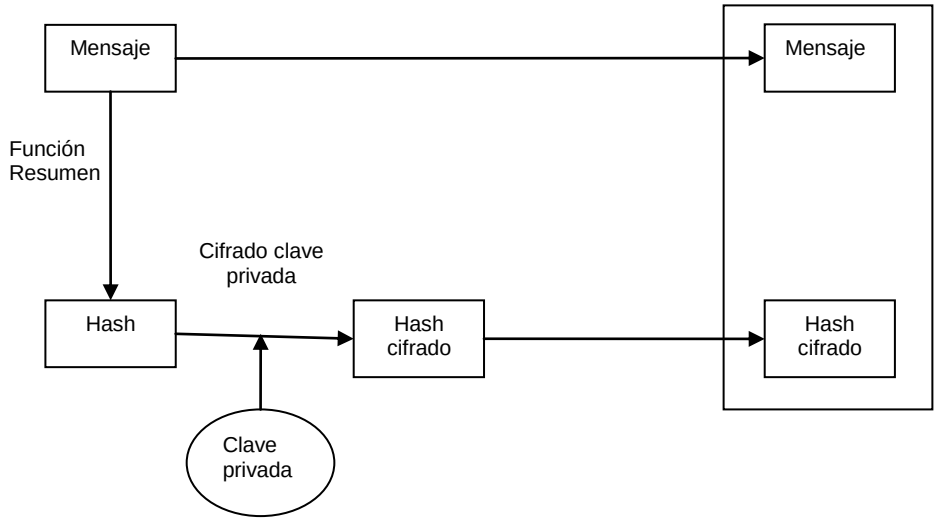

Figura Nº 4.Generación de firma digital

Para poder validar, por parte del receptor, que el mensaje recibido no ha sido modificado y la firma es correcta, éste deberá generar el resumen del mensaje. Posteriormente, el resumen recibido es descifrado mediante la clave pública del emisor. Si el resumen recibido descifrado coincide con el resumen realizado por parte del receptor del mensaje recibido puede decirse que la firma digital es válida.

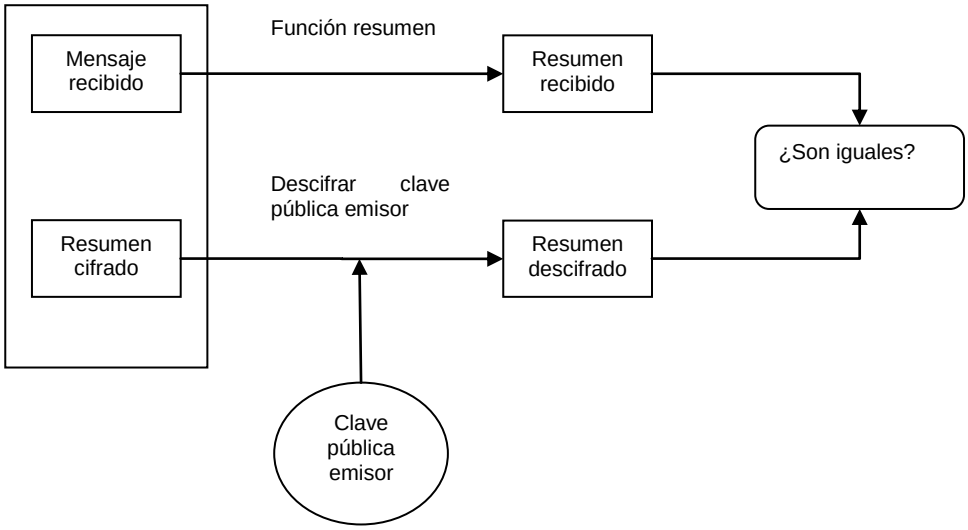

Figura Nº 5.Verificación de firma digital

2.2. Firma electrónica

La firma electrónica es un concepto más amplio que la firma digital, ya que está regulada en la Directiva 1999/93/CE de la Unión Europea y la transposición de dicha Directiva en España que corresponde a la Ley 59/2003 de Firma electrónica. Este marco regulatorio otorga validez jurídica. [11][12][13]
La ley 59/2003 de Firma electrónica define tres tipos de firma:

· **Simple:** permite identificar al firmante.

· **Avanzada:** permite identificar al firmante y puede garantizar si hay cambios realizados en el documento firmado.

· **Avanzada reconocida:** firma electrónica avanzada generada mediante un certificado reconocido y un dispositivo seguro.

La firma electrónica reconocida es equivalente a la firma manuscrita.

2.3. Custodia electrónica

La custodia electrónica pretende que documentos almacenados a largo plazo sean válidos. Los objetivos que debe garantizar son: integridad, autenticidad, control de acceso, trazabilidad, localización y preservación a largo plazo. [8][9]

· **Integridad y autenticidad:** se garantiza mediante la firma electrónica, aunque también se incluyen controles para poder detectar cambios.

· **Control de acceso:** se garantiza mediante el cifrado con clave pública, ya que la firma electrónica no puede asegurar que la información no pueda ser consultada por terceros que no tienen autorización.

· **Trazabilidad:** en este caso la firma electrónica junto con sellado de tiempo proporciona quien y cuando se realizó el acceso. Sin embargo, se necesita de algún control más para saber de posteriores accesos.

· **Localización:** una posible tecnología para realizar esta función es Content Address Storage (CAS) [16][17]. Para ello se almacenará el documento en la plataforma CAS añadiendo un identificador único que especifica la localización donde está almacenado. Este identificador será distinto en el caso que haya cualquier modificación, por lo que se considerará como un documento distinto.

· **Preservación:** se puede garantizar mediante el estándar XAdES y definiendo políticas de preservación como, por ejemplo, replicación.

2.4. XML-Dsig

Sintaxis XML para la creación de firma electrónica que puede ser aplicada a cualquier tipo de documento. [1][2]

Dicha firma electrónica XML tiene la siguiente estructura:

```
<Signature ID?>
   <SignedInfo>
     <CanonicalizationMethod/>
     <SignatureMethod/>
     (<Reference URI? >
       (<Transforms>)?
       <DigestMethod>
       <DigestValue>
     </Reference>)+
   </SignedInfo>
   <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
 </Signature>
```

Para cada documento u objeto que se quiera firmar debe realizarse el siguiente proceso:

- Generación de los elementos de referencia:
  · Aplicar las transformaciones indicadas al documento.

  · Calcular el valor Digest sobre el objeto que se ha obtenido de las transformaciones aplicadas.

  · Crear un elemento <Reference> incluyendo la identificación del objeto, elementos <Transform> y el algoritmo <Digest> del elemento <DigestValue>.

- Generación de la firma:

  · Crear un elemento <SignedInfo> mediante elementos <SignatureMethod>, <CanonicalizationMethod> y <Reference>.

· Canonicalización y cálculo de elementos <SignatureValue> sobre un elemento <SignedInfo> basados en algoritmos de dicho elemento <SignedInfo>.

· Construir el elemento <Signature> que incluye <SignedInfo>, <Object>, <KeyInfo> y <SignatureValue>.

2.5. XAdES

Se toma como base la sintaxis y reglas de proceso de generación de firmas XML indicadas para XML-Dsig, siendo ésta la estructura a la que después se irán añadiendo propiedades y elementos para evolucionar a un formato de firma XAdES. [3][4][5]

```
<Signature Id="MyFirstSignature"
xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-
      xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-
sha1"/>
    <Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
      </Transforms>
      <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue> … </DigestValue>
    </Reference>
  </SignedInfo>

  <SignatureValue> … </SignatureValue>

  <KeyInfo>
    <KeyValue>
    </KeyValue>
  </KeyInfo>
</Signature>
```

A continuación, se indican los elementos necesarios para cumplir los estándares en función del formato deseado de firma XAdES.

2.5.1. XAdES-BES

Se incorpora al proceso de firma XML-Dsig una serie de propiedades, que se incluirán en un objeto <ds:Object>. Estas propiedades se dividen en propiedades cubiertas por la firma (SignedProperties) y propiedades no firmadas (UnSignedProperties).

Para poder proteger el certificado firmante, se deberá proceder a realizar al menos una de las siguientes indicaciones:

- Incluir elemento <SigningCertificate>: que deberá hacer referencia al valor del digest del certificado firmante.

- Si no se indica <SigningCertificate> se deberán realizar modificaciones a <ds:KeyInfo>. Incluyendo el certificado con el que se va a firmar <ds:X509Data>, el elemento <ds:SignedInfo> debe contener referencia a <ds:KeyInfo>

Además, para evitar una sustitución del certificado firmante se incluirán: <SigningTime>, <DataObjectFormat>,<CommitmentTypeIndication>, <SignerRole>, <SignatureProductionPlace>,<IndividualDataObjectsTimeStamp>, <AllDataObjectTimeStamp> y <CounterSignature> en las propiedades no firmadas.

El formato XAdES-BES por sí solo no permite la verificación de la firma a lo largo del tiempo, ya que el certificado utilizado para firmar debe ser válido en el momento actual de la verificación.

```
<ds:Signature ID?>
      <ds:SignedInfo>
            <ds:CanonicalizationMethod/>
            <ds:SignatureMethod/>
            (<ds:Reference URI? >
                  (<ds:Transforms>)?
                  <ds:DigestMethod/>
                  <ds:DigestValue/>
            </ds:Reference>)+
      </ds:SignedInfo>
      <ds:SignatureValue/>
      (<ds:KeyInfo>)?

      <ds:Object>

            <QualifyingProperties>

                  <SignedProperties>

                        <SignedSignatureProperties>
                              (SigningTime)?
                              (SigningCertificate)?
                              (SignatureProductionPlace)?
```

```
                    (SignerRole)?
                </SignedSignatureProperties>

                <SignedDataObjectProperties>
                    (DataObjectFormat)*
                    (CommitmentTypeIndication)*
                    (AllDataObjectsTimeStamp)*
                    (IndividualDataObjectsTimeStamp)*
                </SignedDataObjectProperties>

            </SignedProperties>

            <UnsignedProperties>

                <UnsignedSignatureProperties>
                    (CounterSignature)*
                </UnsignedSignatureProperties>

            </UnsignedProperties>

        </QualifyingProperties>

    </ds:Object>

</ds:Signature>
```

2.5.2. XAdES-EPES

Este formato de firma XAdES se construye a partir de la firma electrónica XAdES-BES. Para ello, se introduce un elemento firmado <SignaturePolicyIdentifier>, esta propiedad indica la política a utilizar para realizar la validación.

```
<ds:Signature ID?>
      <ds:SignedInfo>
            <ds:CanonicalizationMethod/>
            <ds:SignatureMethod/>
            (<ds:Reference URI? >
                  (<ds:Transforms>)?
                  <ds:DigestMethod/>
                  <ds:DigestValue/>
            </ds:Reference>)+
      </ds:SignedInfo>
      <ds:SignatureValue/>
      (<ds:KeyInfo>)?

      <ds:Object>

            <QualifyingProperties>

                  <SignedProperties>

                        <SignedSignatureProperties>
                              (SigningTime)?
                              (SigningCertificate)?
                              (SignaturePolicyIdentifier)
                              (SignatureProductionPlace)?
                              (SignerRole)?
                        </SignedSignatureProperties>

                        <SignedDataObjectProperties>
                              (DataObjectFormat)*
                              (CommitmentTypeIndication)*
                              (AllDataObjectsTimeStamp)*
                              (IndividualDataObjectsTimeStamp)*
                        </SignedDataObjectProperties>

                  </SignedProperties>

                  <UnsignedProperties>

                        <UnsignedSignatureProperties>
                              (CounterSignature)*
                        </UnsignedSignatureProperties>

                  </UnsignedProperties>

            </QualifyingProperties>

      </ds:Object>

</ds:Signature>
```

2.5.3. XAdES-T

Se deberá construir en base al formato XAdES-BES o XAdES-EPES. XAdES-T proporciona un sello de tiempo mediante el elemento <SignatureTimeStamp>. Este elemento se encontrará entre las propiedades no firmadas (UnsignedProperties).

Además, para que sea válida la marca de tiempo y, por tanto, un formato XAdES-T válido, deberá incorporarse dicha marca de tiempo antes de la revocación o caducidad del certificado.

XAdES-T vincula una firma electrónica a un tiempo confiable.

```
<ds:Signature ID?>
      <ds:SignedInfo>
            <ds:CanonicalizationMethod/>
            <ds:SignatureMethod/>
            (<ds:Reference URI? >
                  (<ds:Transforms>)?
                  <ds:DigestMethod/>
                  <ds:DigestValue/>
            </ds:Reference>)+
      </ds:SignedInfo>
      <ds:SignatureValue/>
      (<ds:KeyInfo>)?

      <ds:Object>

            <QualifyingProperties>

                  <SignedProperties>

                        <SignedSignatureProperties>
                              (SigningTime)?
                              (SigningCertificate)?
                              (SignaturePolicyIdentifier)
                              (SignatureProductionPlace)?
                              (SignerRole)?
                        </SignedSignatureProperties>

                        <SignedDataObjectProperties>
                              (DataObjectFormat)*
                              (CommitmentTypeIndication)*
                              (AllDataObjectsTimeStamp)*
                              (IndividualDataObjectsTimeStamp)*
                        </SignedDataObjectProperties>

                  </SignedProperties>

                  <UnsignedProperties>

                        <UnsignedSignatureProperties>
                              (CounterSignature)*
                              (SignatureTimeStamp)+
                        </UnsignedSignatureProperties>

                  </UnsignedProperties>
```

```
            </QualifyingProperties>
      </ds:Object>
</ds:Signature>
```

2.5.4. XAdES-C

Se construirá añadiendo al formato XAdES-T elementos que permitan almacenar valores de la ruta de certificación e información de revocación. Y, por tanto, referencias de datos para la validación de la firma electrónica.

Los elementos a añadir son <CompleteCertificateRefs>, <CompleteRevocationRefs>, si además, los atributos de certificado aparecieran en la firma se indicarán: <AttributeCertificateRef>s y <AttributeRevocationRefs>.

<CompleteCertificateRefs> contiene referencias a los certificados de autoridades certificadoras para poder validar desde la firma electrónica hasta el certificado.

<CompleteRevocationRefs> contiene referencias a los datos de revocación usados para la validación del certificado del firmante y de las autoridades de certificación.

```
<ds:Signature ID?>
      <ds:SignedInfo>
            <ds:CanonicalizationMethod/>
            <ds:SignatureMethod/>
            (<ds:Reference URI? >
                  (<ds:Transforms>)?
                  <ds:DigestMethod/>
                  <ds:DigestValue/>
            </ds:Reference>)+
      </ds:SignedInfo>
      <ds:SignatureValue/>
      (<ds:KeyInfo>)?

      <ds:Object>

            <QualifyingProperties>

                  <SignedProperties>

                        <SignedSignatureProperties>
                              (SigningTime)?
                              (SigningCertificate)?
                              (SignaturePolicyIdentifier)
                              (SignatureProductionPlace)?
                              (SignerRole)?
                        </SignedSignatureProperties>

                        <SignedDataObjectProperties>
                              (DataObjectFormat)*
                              (CommitmentTypeIndication)*
                              (AllDataObjectsTimeStamp)*
                              (IndividualDataObjectsTimeStamp)*
                        </SignedDataObjectProperties>

                  </SignedProperties>

                  <UnsignedProperties>
```

```
                        <UnsignedSignatureProperties>
                              (CounterSignature)*
                              (SignatureTimeStamp)+
                              (CompleteCertificateRefs)
                              (CompleteRevocationRefs)
                              (AttributeCertificateRefs)?
                              (AttributeRevocationRefs)?
                        </UnsignedSignatureProperties>

                  </UnsignedProperties>

            </QualifyingProperties>

      </ds:Object>

</ds:Signature>
```

2.5.5 XAdES-X

Este formato se construirá añadiendo marcas de tiempo al tipo de firma que tenga las propiedades <CompleteCertificateRefs> y <CompleteRevocationRefs> (XAdES-C). Estas marcas de tiempo protegen los certificados referenciados, lista de certificados revocados (CRL) e información del estado de los certificados (OCSP), proporcionando integridad e información de tiempo confiable.

Para ello, hay dos tipos en función del elemento añadido:

- <SigAndRefsTimeStamp>: marcas de tiempo calculadas mediante los elementos <SignatureValue>, <SignatureTimeStamp>, <CompleteCertificateRefs> y <CompleteRevocationRefs>.
- <RefsOnlyTimeStamp>: marcas de tiempo calculadas mediante las propiedades <CompleteCertificateRefs> y <CompleteRevocationRefs>.

```
<ds:Signature ID?>
      <ds:SignedInfo>
            <ds:CanonicalizationMethod/>
            <ds:SignatureMethod/>
            (<ds:Reference URI? >
                  (<ds:Transforms>)?
                  <ds:DigestMethod/>
                  <ds:DigestValue/>
            </ds:Reference>)+
      </ds:SignedInfo>
      <ds:SignatureValue/>
      (<ds:KeyInfo>)?

      <ds:Object>

            <QualifyingProperties>

                  <SignedProperties>

                        <SignedSignatureProperties>
                              (SigningTime)?
                              (SigningCertificate)?
                              (SignaturePolicyIdentifier)
                              (SignatureProductionPlace)?
                              (SignerRole)?
                        </SignedSignatureProperties>

                        <SignedDataObjectProperties>
                              (DataObjectFormat)*
                              (CommitmentTypeIndication)*
                              (AllDataObjectsTimeStamp)*
                              (IndividualDataObjectsTimeStamp)*
                        </SignedDataObjectProperties>

                  </SignedProperties>

                  <UnsignedProperties>
```

```
                        <UnsignedSignatureProperties>
                              (CounterSignature)*
                              (SignatureTimeStamp)+
                              (CompleteCertificateRefs)
                              (CompleteRevocationRefs)
                              (AttributeCertificateRefs)?
                              (AttributeRevocationRefs)?
                              ((SigAndRefsTimeStamp)*|
                              (RefsOnlyTimeStamp)*)
                        </UnsignedSignatureProperties>

                  </UnsignedProperties>

            </QualifyingProperties>

      </ds:Object>

</ds:Signature>
```

2.5.6. XAdES-X-L

Para poder formar este formato se deberán añadir los elementos <CertificateValues> y <RevocationValues>. Estos valores contendrán los certificados usados para la validación de la firma electrónica (incluido el certificado del firmante) y la información de revocación utilizada para la validación. Esta información es necesaria que sea archivada en este formato de firma XML para proporcionar firma electrónica a largo plazo.

Incluir esta información sobre el certificado y su estado de revocación permite la verificación de la firma incluso en casos en los que no es posible acceder a dicha información de revocación en línea.

```
<ds:Signature ID?>
      <ds:SignedInfo>
            <ds:CanonicalizationMethod/>
            <ds:SignatureMethod/>
            (<ds:Reference URI? >
                  (<ds:Transforms>)?
                  <ds:DigestMethod/>
                  <ds:DigestValue/>
            </ds:Reference>)+
      </ds:SignedInfo>
      <ds:SignatureValue/>
      (<ds:KeyInfo>)?

      <ds:Object>

            <QualifyingProperties>

                  <SignedProperties>

                        <SignedSignatureProperties>
                              (SigningTime)?
                              (SigningCertificate)?
                              (SignaturePolicyIdentifier)
                              (SignatureProductionPlace)?
                              (SignerRole)?
                        </SignedSignatureProperties>

                        <SignedDataObjectProperties>
                              (DataObjectFormat)*
                              (CommitmentTypeIndication)*
                              (AllDataObjectsTimeStamp)*
                              (IndividualDataObjectsTimeStamp)*
                        </SignedDataObjectProperties>

                  </SignedProperties>

                  <UnsignedProperties>

                        <UnsignedSignatureProperties>
                              (CounterSignature)*
                              (SignatureTimeStamp)+
                              (CompleteCertificateRefs)
                              (CompleteRevocationRefs)
                              (AttributeCertificateRefs)?
```

```
                                    (AttributeRevocationRefs)?
                                    ((SigAndRefsTimeStamp)*|
                                    (RefsOnlyTimeStamp)*)
                                    (CertificatesValues)
                                    (RevocationValues)
                                    (AttrAuthoritiesCertValues)?
                                    (AttributeRevocationValues)?
                                </UnsignedSignatureProperties>

                            </UnsignedProperties>

                        </QualifyingProperties>

                    </ds:Object>

                </ds:Signature>
```

2.5.7. XAdES-A

Se deberán incluir marcas de tiempo al formato XAdES-X-L. Esto debe realizarse antes de que los algoritmos y claves utilizadas para la construcción del formato XAdES-C sean vulnerables. Estas marcas de tiempo deberán incluirse en la propiedad sin firma <ArchiveTimeStamp> calculadas en base a XAdES-X-L.

De esta forma el formato XAdES-A permite almacenar firma electrónica a lo largo del tiempo, sin depender de si son vulnerables los algoritmos de cifrado o están revocados los certificados, en cuyo caso se resellaría temporalmente el archivo con claves y algoritmos seguros en el momento actual.

```
<ds:Signature ID?>
      <ds:SignedInfo>
            <ds:CanonicalizationMethod/>
            <ds:SignatureMethod/>
            (<ds:Reference URI? >
                  (<ds:Transforms>)?
                  <ds:DigestMethod/>
                  <ds:DigestValue/>
            </ds:Reference>)+
      </ds:SignedInfo>
      <ds:SignatureValue/>
      (<ds:KeyInfo>)?

      <ds:Object>

            <QualifyingProperties>

                  <SignedProperties>

                        <SignedSignatureProperties>
                              (SigningTime)?
                              (SigningCertificate)?
                              (SignaturePolicyIdentifier)
                              (SignatureProductionPlace)?
                              (SignerRole)?
                        </SignedSignatureProperties>

                        <SignedDataObjectProperties>
                              (DataObjectFormat)*
                              (CommitmentTypeIndication)*
                              (AllDataObjectsTimeStamp)*
                              (IndividualDataObjectsTimeStamp)*
                        </SignedDataObjectProperties>

                  </SignedProperties>

                  <UnsignedProperties>

                        <UnsignedSignatureProperties>
                              (CounterSignature)*
                              (SignatureTimeStamp)+
                              (CompleteCertificateRefs)
                              (CompleteRevocationRefs)
                              (AttributeCertificateRefs)?
```

```
                                    (AttributeRevocationRefs)?
                                    ((SigAndRefsTimeStamp)*|
                                    (RefsOnlyTimeStamp)*)
                                    (CertificatesValues)
                                    (RevocationValues)
                                    (AttrAuthoritiesCertValues)?
                                    (AttributeRevocationValues)?
                                    (ArchiveTimeStamp)+
                                </UnsignedSignatureProperties>

                            </UnsignedProperties>

                        </QualifyingProperties>

                    </ds:Object>

                </ds:Signature>
```

2.5.8. Proceso XAdES-BES a XAdES-A

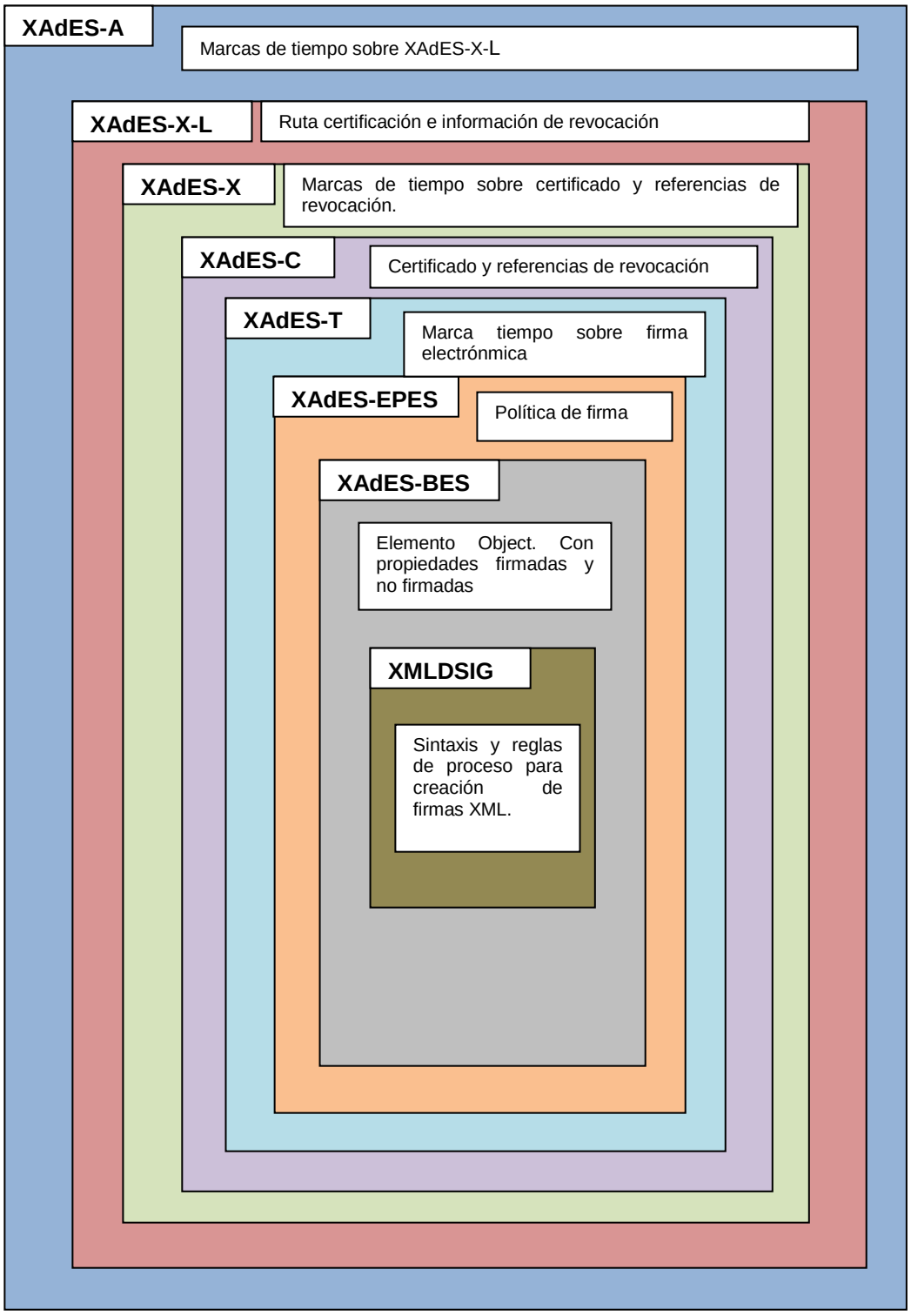

Figura Nº 6.Proceso XAdES-BES a XAdES-A

2.6. Sellado de tiempo

Este mecanismo definido en el RFC 3161 permite que una autoridad de sellado de tiempo (TSA) genere una marca de tiempo para un determinado documento. De esta forma se establece la evidencia de que una información existe en el momento especificado. [6][7]

Una petición de sellado de tiempo tiene la siguiente estructura:

```
TimeStampReq ::= SEQUENCE  {
   version                      INTEGER  { v1(1) },
   messageImprint               MessageImprint,
   reqPolicy             TSAPolicyId              OPTIONAL,
   nonce                 INTEGER                  OPTIONAL,
   certReq               BOOLEAN                  DEFAULT FALSE,
   extensions            [0] IMPLICIT Extensions  OPTIONAL  }
```

Y una respuesta de sellado de tiempo tiene la siguiente estructura:

```
TimeStampResp ::= SEQUENCE  {
      status                  PKIStatusInfo,
      timeStampToken          TimeStampToken     OPTIONAL  }
```

3. Análisis

3.1. Análisis de requerimientos

El Consejo General del Notariado desea ofrecer a sus colegiados la posibilidad de capturar y generar evidencias electrónicas que acrediten la publicación de determinado contenido en páginas Web. Para ello se pretende desarrollar una aplicación Web que capture el código de una página indicada por el usuario, firme su contenido y genere evidencia electrónica longeva en formato XAdES.

La forma de indicar el usuario la página WEB será añadiendo la URL de dicho sitio WEB.

Tras realizarse la firma por parte del sistema, se enviará al usuario un documento de confirmación de dicha firma.

De forma que el usuario pueda acceder a la aplicación Web, se desarrollará un acceso de autenticación básico.

3.2. Casos de uso

En esta sección se especifica los casos de uso a contemplar:

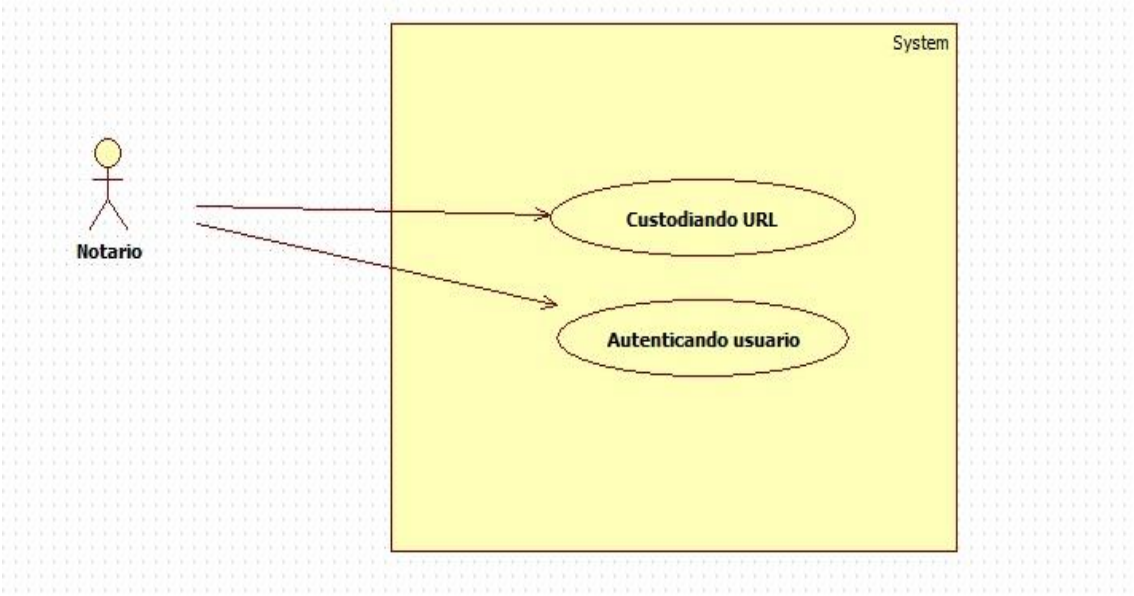

Figura Nº 7.Casos de uso

Caso de uso: Custodiando URL	
Actor: Notario	
Curso Normal	Alternativas
1) El usuario se comunica con el sistema de firma.	
2) Usuario introduce URL que desea firmar.	2.1) Si no existe URL se indicará al usuario.
3) Se confirma al usuario la realización de la firma.	

Caso de uso: Autenticando usuario	
Actor: Notario	
Curso Normal	Alternativas
1) El usuario se comunica con el sistema de firma.	
2) Usuario introduce usuario y contraseña.	2.1) Si usuario y/o contraseña son incorrectas se indicará al usuario.
3) Se accede a la pantalla principal de la aplicación Web.	

3.3. Diagrama de secuencia

A continuación se muestra el diagrama de secuencia de la aplicación WEB, en la que solicita la custodia y el contenido de una determinada URL.

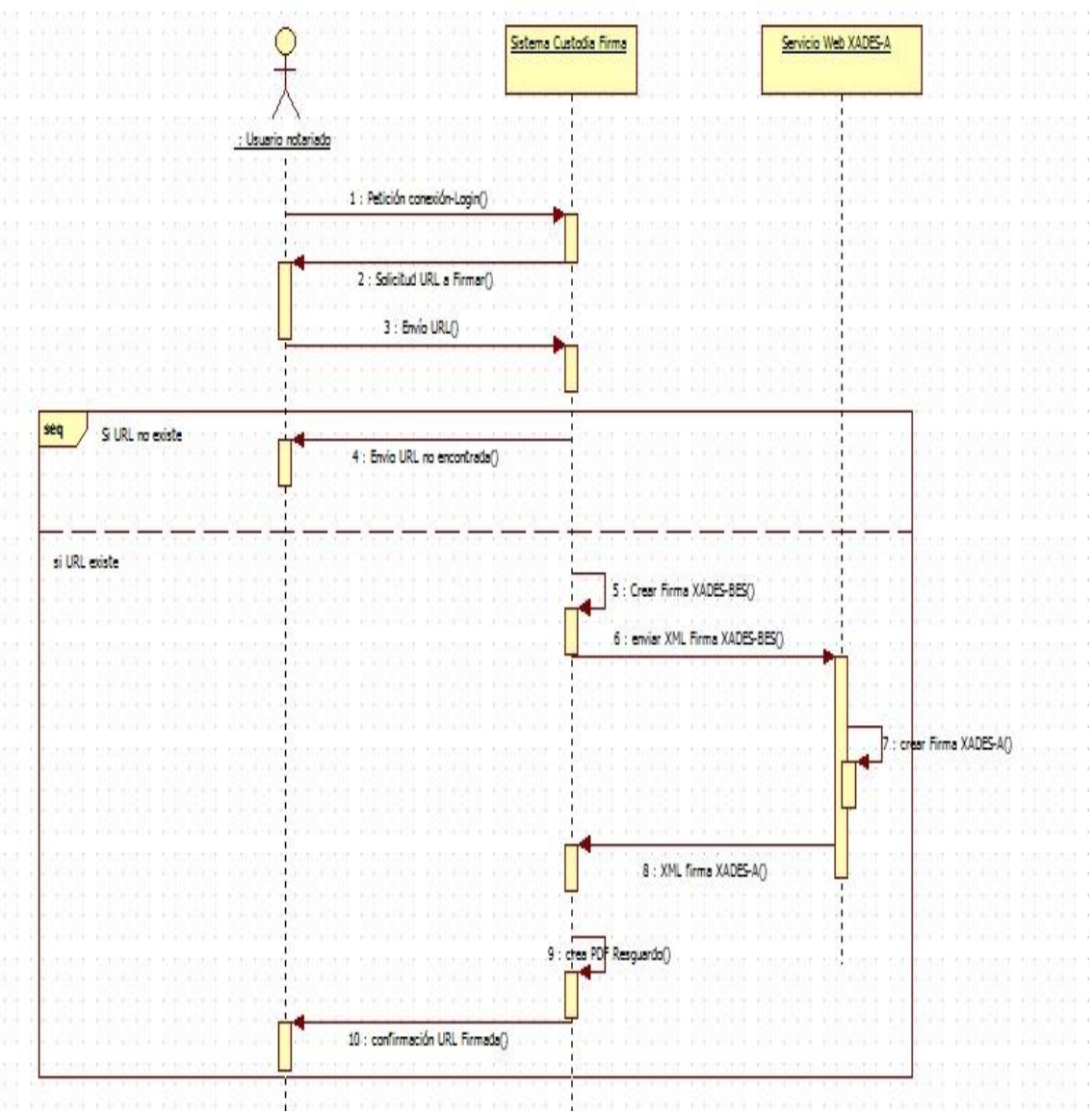

Figura Nº 8.Diagrama de Secuencia

4. Implementación y Diseño

4.1. Patrón MVC

Se va a utilizar un patrón de arquitectura Modelo-Vista-Controlador (MVC) para construir el software deseado. De esta forma separaremos la interfaz de usuario, la lógica de control y la lógica de negocio.[14][15]

· **Modelo:** representará la creación de la firma electrónica sobre los documentos obtenidos desde la interfaz de usuario.
· **Vista:** interfaz de usuario, desde la que se proporcionará la información de URL a firmar por parte del usuario.

· **Controlador:** responde a los eventos lanzados desde la interfaz de usuario para invocar al modelo.

Entre otros beneficios de este patrón de arquitectura podemos obtener las siguientes ventajas:

· Evolución y mantenimiento por separado tanto de la interfaz de usuario como de la lógica de negocio.

· Reutilización y escalabilidad de los desarrollos.

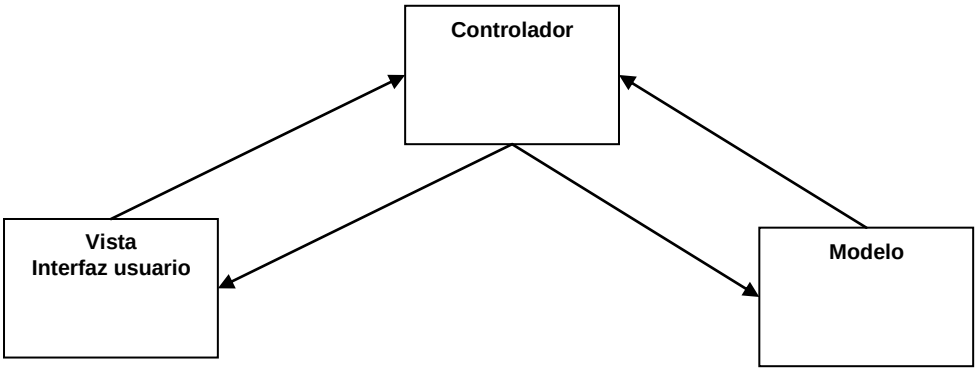

Figura Nº 9.Patrón MVC

4.2. Interfaz de usuario

A continuación, se muestra la interfaz de usuario mediante la que los usuarios podrán interactuar con la aplicación de custodia.

4.2.1. Login Inicial

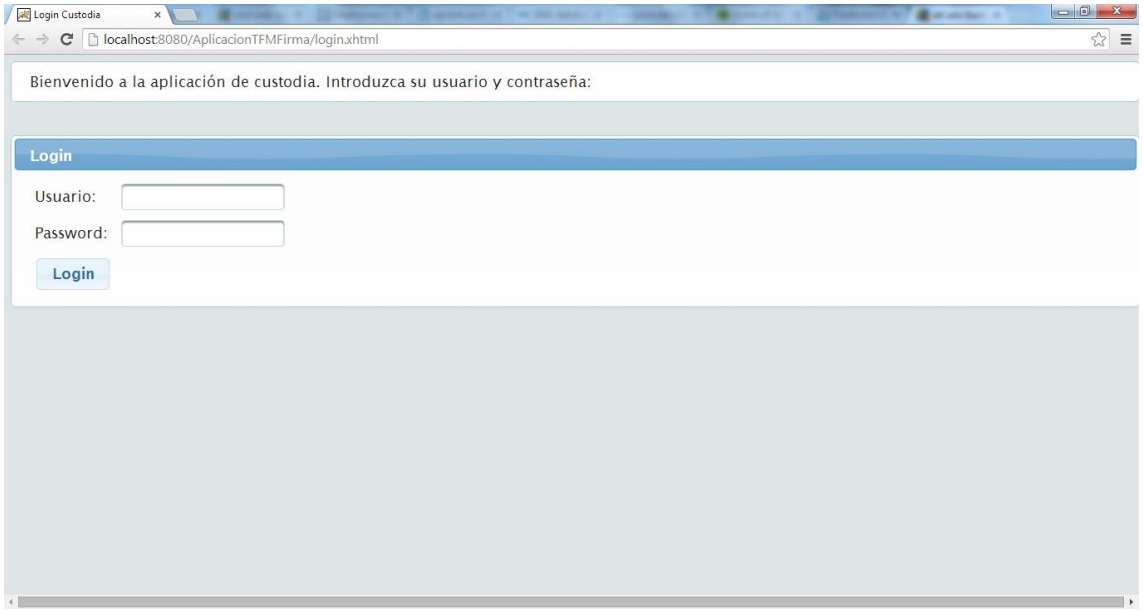

Figura Nº 10.Login inicial

4.2.2. Menú principal

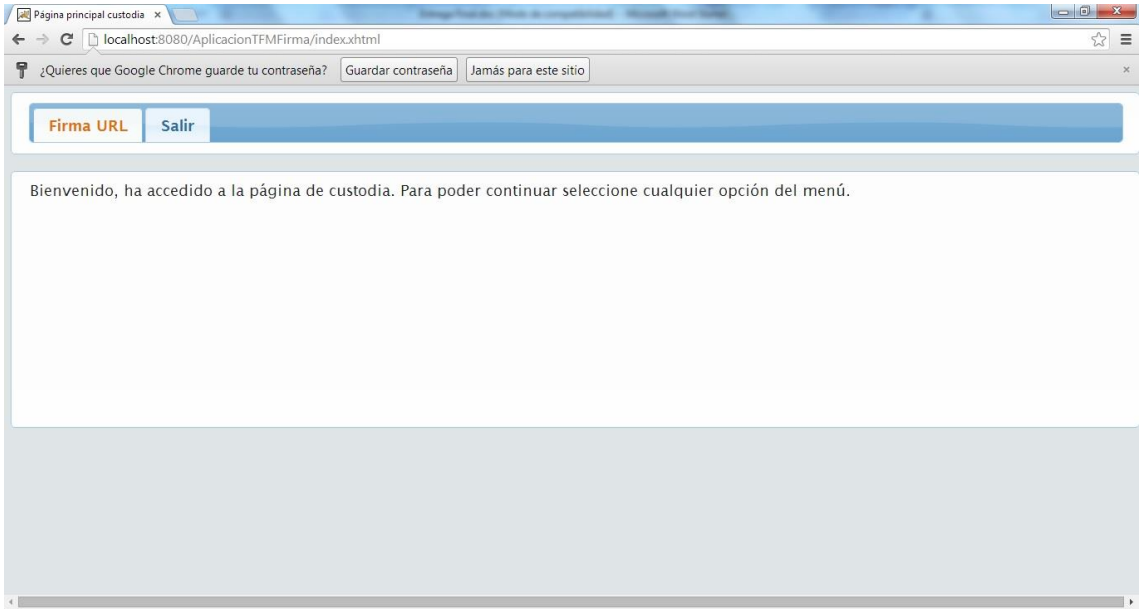

Figura Nº 11.Menú Principal

4.2.3. Firma URL

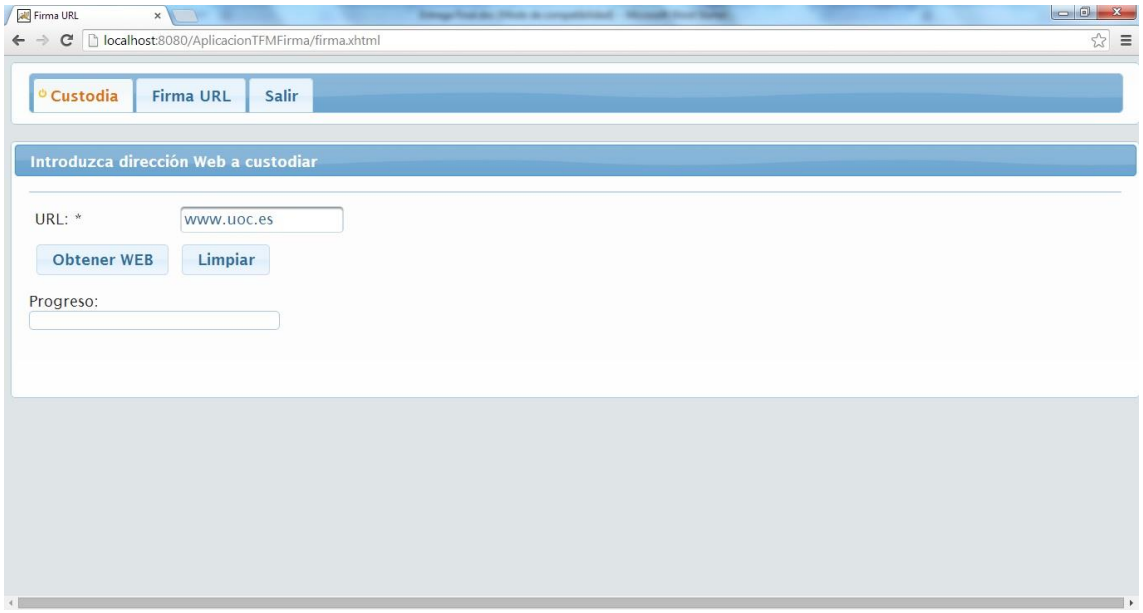

Figura Nº 12.Firma URL

4.2.4. Recibo custodia

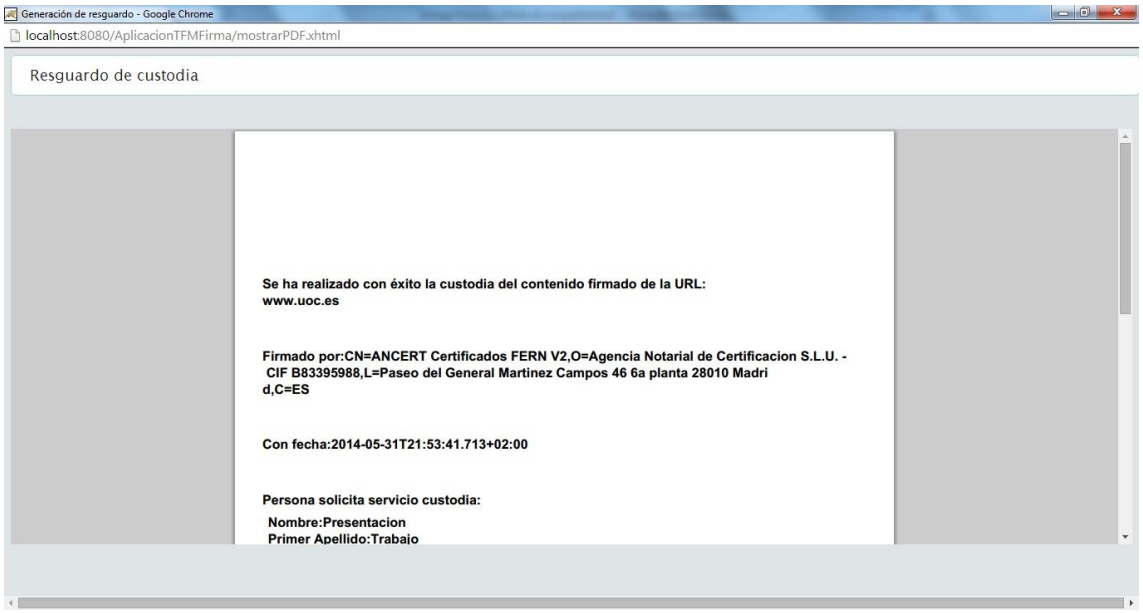

Figura Nº 13.Recibo custodia

4.3. Diagrama de Componentes

En esta sección se describe el diagrama de componentes correspondiente a la aplicación desarrollada:

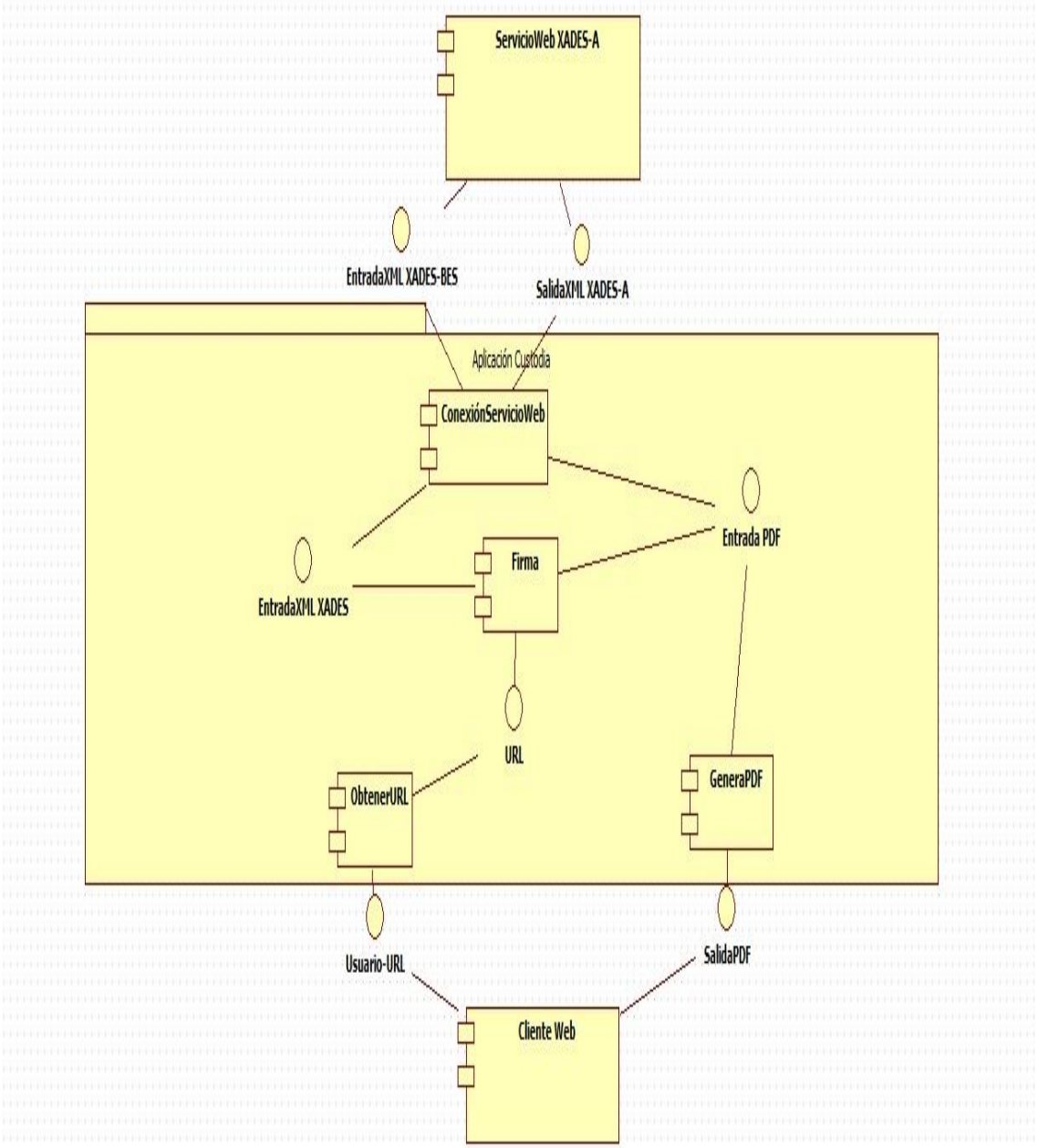

Figura Nº 14.Diagrama de componentes

4.4. Diagrama de despliegue

En esta sección se describe el diagrama de despliegue correspondiente a la aplicación desarrollada:

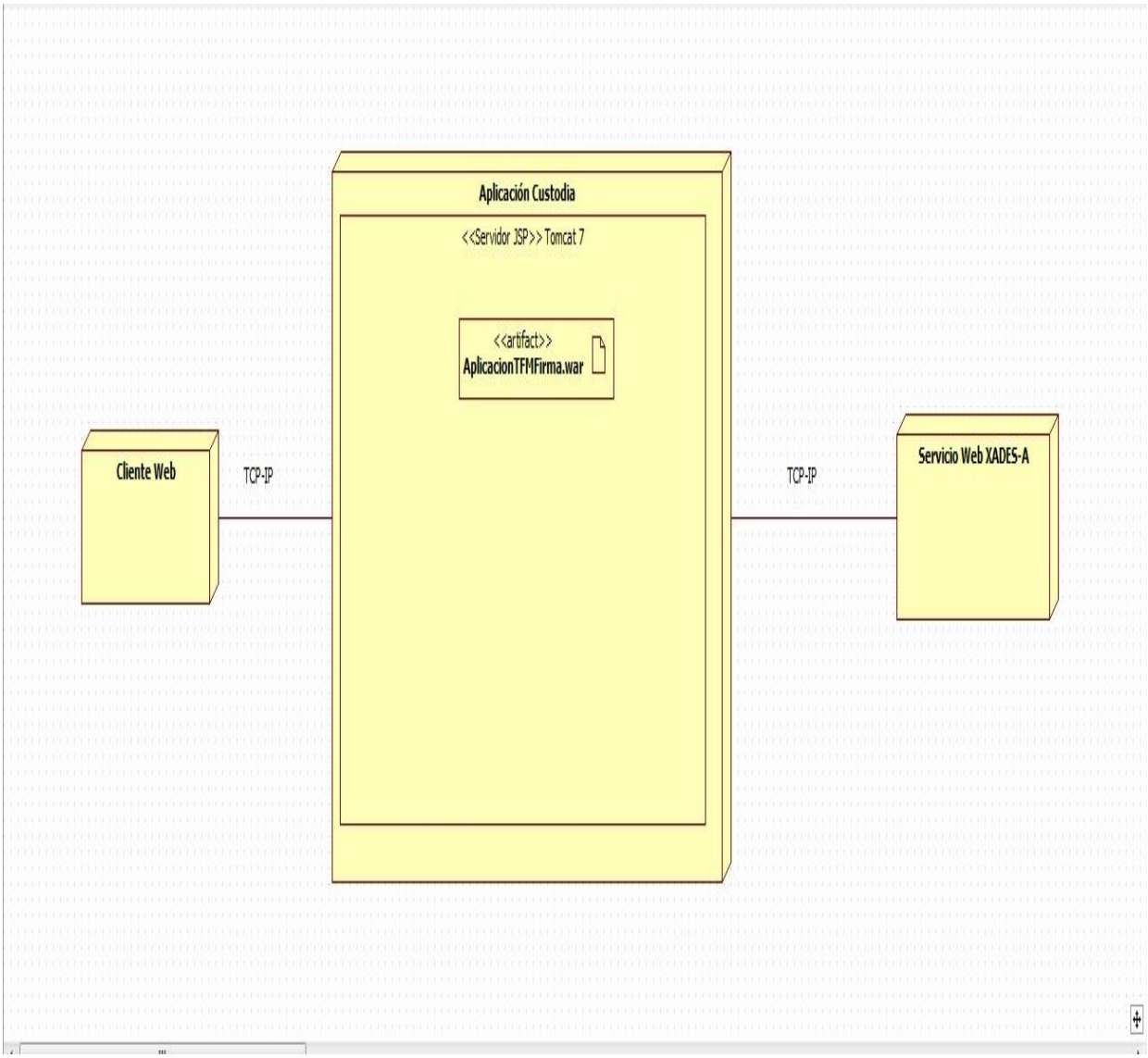

Figura Nº 15.Diagrama de despliegue

4.5. Tecnologías utilizadas

Para la implementación de la aplicación Web de custodia se ha utilizado Java en su versión J2EE. En concreto se ha utilizado el framework JSF y su extensión PrimeFaces. Además, para la creación de la firma XAdES-BES se ha utilizado una librería con licencia GPL llamada XAdES4J.

4.5.1. JSF

Es un framework para entornos Java J2EE basado en el patrón MVC. JSF utiliza Java Server Pages (JSP) para realizar el despliegue de las páginas. Esta tecnología de servidor permite asociar clases Java para recoger la información indicada por parte del usuario y, además, permite asociar métodos para generar eventos ante dicha interacción. [19][20][21]

4.5.2. PrimeFaces

Es una librería de componentes visuales que sirve como extensión a JSF con licencia Apache License V2. Desarrollada y mantenida por PrimeTek Informatics.
Algunas características son:

- Amplio catálogo de componentes (Panel, InputText…).
- Trabaja con Ajax basado en las APIs Ajax del estándar JSF 2.0.
- Variedad de Temas.
- Kit para crear aplicaciones para móviles.

4.5.3. XAdES4j

Es una librería Java con licencia LGPL que implementa la firma electrónica avanzada XAdES en sus versiones 1.3.2 o 1.4.1. Este API comenzó como proyecto en el año 2009 realizado por Luis Goncalves y actualmente está en su versión 1.3.1. [18]
Los formatos de XAdES que permite producir y verificar la librería son: XAdES-BES, XAdES-EPES, XAdES-T y XAdES-C.

4.5.4. Apache PDFBox

Librería Java con licencia Apache License v2.0. que permite crear nuevos nuevos PDF o modificar ficheros PDF existentes.

4.5.5. Apache Tomcat 7

Servidor de web con licencia Apache License v2.0. que soporta servlets y páginas Java Server Pages (JSP).

5. Conclusiones

Tal y como se indicó en los objetivos, el Consejo General del Notariado necesitaba firmar páginas Web para su posterior custodia, de forma que a lo largo del tiempo fuera posible validar. Con este proyecto se ha logrado alcanzar las necesidades descritas y planificadas inicialmente, ya que el Consejo General del Notariado tiene a su disposición una aplicación accesible vía Web que permite, mediante la inclusión de una URL, realizar el firmado a largo plazo de una página Web.

La metodología utilizada ha permitido poder obtener un producto ajustado a las necesidades y recursos destinados.

La aplicación Web desarrollada tiene la posibilidad de evolucionar para ofrecer servicios de custodia para nuevos tipos de contenido: imágenes ISO, correos electrónicos,...

Actualmente, la aplicación Web utiliza para realizar la autenticación un fichero de texto. Esta forma de autenticación podría evolucionar a un Single Sign On con el sistema de autenticación de la empresa.

6. Glosario

XAdES: **X**ML **Ad**vanced **E**lectronic **S**ignatures
XAdES-BES: XAdES Basic Electronic Signature
XAdES-EPES: XAdES Explicit Policy based Electronic Signature
XAdES-C: XAdES Complete validation data
XAdES-T: XAdES with Time-stamp
XAdES-X; XAdES eXtended validation data
XAdES-X-L: Extended long electronic signatures with time
XAdES-A: XML Advanced Electronic Signature
XML: eXtensible Markup Language
XMLDSIG: eXtensible Markup Language Digital SIGnature
URL: Uniform Resource Locator

7. Bibliografía

Además, de los siguientes recursos se han utilizado recursos proporcionados por Ancert.

[1] http://www.w3.org/TR/xmldsig-core/#sec-Editorial
[2] http://es.wikipedia.org/wiki/Firma_XML
[3] http://www.w3.org/TR/XAdES/
[4] http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.01_60/ts_101903v010401p.pdf
[5] http://es.wikipedia.org/wiki/Xades
[6] http://es.wikipedia.org/wiki/Sellado_de_tiempo
[7] https://tools.ietf.org/html/rfc3161
[8] http://es.wikipedia.org/wiki/Custodia_electr%C3%B3nica
[9] http://www.sia.es/img/SICSept07page58a60.pdf
[10] http://es.wikipedia.org/wiki/Firma_digital
[11] http://www.upv.es/contenidos/CD/info/711250normalc.html
[12] http://es.wikipedia.org/wiki/Firma_electr%C3%B3nica
[13] http://noticias.juridicas.com/base_datos/Admin/l59-2003.t1.html#a3
[14] https://www.fdi.ucm.es/profesor/jpavon/poo/2.14.MVC.pdf
[15] http://es.wikipedia.org/wiki/Modelo_Vista_Controlador
[16] http://searchstorage.techtarget.com/definition/content-addressed-storage
[17] http://es.wikipedia.org/wiki/Content_Addressed_Storage
[18] https://code.google.com/p/xades4j/
[19] http://www.oracle.com/technetwork/java/javaee/javaserverfaces-139869.html
[20] http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=IntroduccionJSFJava
[21] http://es.wikipedia.org/wiki/JavaServer_Faces
[22] http://www.primefaces.org/
[23] http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=introduccionPrimefaces
[24] http://es.wikipedia.org/wiki/PrimeFaces

Anexo A. Estructura de ficheros XML

A.1. XML XAdES-BES

```
<?xml version="1.0" encoding="UTF-8"?>
<data id="mensaje1">
    <text>...</text>
     <ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="xmldsig-
2ffb2a95-12c0-49b6-96ed-61f4444dac36">
          <ds:SignedInfo>
          <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
          <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
          <ds:Reference Id="xmldsig-2ffb2a95-12c0-49b6-
96ed-61f4444dac36-ref0" URI="">
          <ds:Transforms>
          <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
          </ds:Transforms>
          <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue></ds:DigestValue>
          </ds:Reference>
          <ds:Reference
Type="http://uri.etsi.org/01903#SignedProperties"
URI="#xmldsig-2ffb2a95-12c0-49b6-96ed-61f4444dac36-
signedprops">
          <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue></ds:DigestValue>
          </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue Id="xmldsig-2ffb2a95-12c0-
49b6-96ed-61f4444dac36-sigvalue">
          </ds:SignatureValue>
          <ds:KeyInfo>
          <ds:X509Data>
          <ds:X509Certificate>
          </ds:X509Certificate>
          </ds:X509Data>
          </ds:KeyInfo>
          <ds:Object>
               <xades:QualifyingProperties
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
```

```
xmlns:xades141="http://uri.etsi.org/01903/v1.4.1#"
Target="#xmldsig-2ffb2a95-12c0-49b6-96ed-61f4444dac36">
                    <xades:SignedProperties Id="xmldsig-
2ffb2a95-12c0-49b6-96ed-61f4444dac36-signedprops">
                         <xades:SignedSignatureProperties>
                              <xades:SigningTime>2014-05-
17T22:17:12.595+02:00</xades:SigningTime>
                              <xades:SigningCertificate>
                                   <xades:Cert>
                                        <xades:CertDigest>

     <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

     <ds:DigestValue></ds:DigestValue>
                                        </xades:CertDigest>

     <xades:IssuerSerial>

     <ds:X509IssuerName></ds:X509IssuerName>

     <ds:X509SerialNumber></ds:X509SerialNumber>

     </xades:IssuerSerial>
                                   </xades:Cert>
                              </xades:SigningCertificate>
                         </xades:SignedSignatureProperties>
                    </xades:SignedProperties>
               </xades:QualifyingProperties>
          </ds:Object>
     </ds:Signature>
</data>
```

A.2. XML XAdES-A

```
<?xml version="1.0" encoding="UTF-8"?>
<data>
     <text>...</text>
     <ds:Signature Id="xmldsig-a5fa1aa0-d7fa-431c-b8fa-
f4f0a5f7ead0"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
               <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
               <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
               <ds:Reference Id="xmldsig-a5fa1aa0-d7fa-
431c-b8fa-f4f0a5f7ead0-ref0" URI="">
                    <ds:Transforms>
```

```
                        <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                    </ds:Transforms>
                    <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

     <ds:DigestValue>WITRazd5HeqjIOMW3wPE90D/6xjYVOXy5sNRIf
z2KEI=</ds:DigestValue>
               </ds:Reference>
               <ds:Reference
Type="http://uri.etsi.org/01903#SignedProperties"
URI="#xmldsig-a5fa1aa0-d7fa-431c-b8fa-f4f0a5f7ead0-
signedprops">
                    <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

     <ds:DigestValue>zrQjQ9wf6arBdWtjIjBJh6t9bUMr8wJEHk5P/U
tB3JM=</ds:DigestValue>
               </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue Id="xmldsig-a5fa1aa0-d7fa-
431c-b8fa-f4f0a5f7ead0-sigvalue">...</ds:SignatureValue>
          <ds:KeyInfo>
               <ds:X509Data>

     <ds:X509Certificate>...</ds:X509Certificate>
               </ds:X509Data>
          </ds:KeyInfo>
          <ds:Object>
               <xades:QualifyingProperties
Target="#xmldsig-a5fa1aa0-d7fa-431c-b8fa-f4f0a5f7ead0"
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
xmlns:xades141="http://uri.etsi.org/01903/v1.4.1#">
                    <xades:SignedProperties Id="xmldsig-
a5fa1aa0-d7fa-431c-b8fa-f4f0a5f7ead0-signedprops">
                         <xades:SignedSignatureProperties>
                              <xades:SigningTime>2014-05-
20T13:07:22.523+02:00</xades:SigningTime>
                              <xades:SigningCertificate>
                                   <xades:Cert>
                                        <xades:CertDigest>

     <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

     <ds:DigestValue>Ikq1K+LlCcgvx6ZNB2eREnMjKdL3ecIQXkt9A7
yhNUs=</ds:DigestValue>
                                        </xades:CertDigest>

     <xades:IssuerSerial>
```

```
     <ds:X509IssuerName>CN=ANCERT Certificados FERN
V2,O=Agencia Notarial de Certificacion S.L.U. - CIF
B83395988,L=Paseo del General Martinez Campos 46 6a planta
28010 Madrid,C=ES</ds:X509IssuerName>

     <ds:X509SerialNumber>390238180066077333863377686984002
88224</ds:X509SerialNumber>

     </xades:IssuerSerial>
                                    </xades:Cert>
                               </xades:SigningCertificate>
                          </xades:SignedSignatureProperties>
                          <xades:SignedDataObjectProperties>

     <xades:CommitmentTypeIndication>
                                    <xades:CommitmentTypeId>

     <xades:Identifier>http://uri.etsi.org/01903/v1.2.2#Pro
ofOfOrigin</xades:Identifier>

     <xades:Description>Indicates that the signer
recognizes to have created, approved and sent the signed
data object</xades:Description>

     </xades:CommitmentTypeId>

     <xades:AllSignedDataObjects/>

     </xades:CommitmentTypeIndication>

     </xades:SignedDataObjectProperties>
                    </xades:SignedProperties>
                    <xades:UnsignedProperties>

     <xades:UnsignedSignatureProperties>
                               <xades:CertificateValues
Id="CertificateValues">

     <xades:EncapsulatedX509Certificate>...</xades:Encapsul
atedX509Certificate>

     <xades:EncapsulatedX509Certificate>...</xades:Encapsul
atedX509Certificate>

     <xades:EncapsulatedX509Certificate>...</xades:Encapsul
atedX509Certificate>
                               </xades:CertificateValues>
                               <xades:RevocationValues
Id="RevocationValues">
                                    <xades:CRLValues>
```

```
     <xades:EncapsulatedCRLValue>...</xades:EncapsulatedCRL
Value>
                                    </xades:CRLValues>
                                    <xades:OCSPValues>

     <xades:EncapsulatedOCSPValue>...</xades:EncapsulatedOC
SPValue>
                                    </xades:OCSPValues>
                               </xades:RevocationValues>
                               <xades:ArchiveTimeStamp
Id="ArchiveTimeStamp_20140520_130725">

     <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>

     <xades:EncapsulatedTimeStamp
Encoding="http://uri.etsi.org/01903/v1.2.2#DER">...</xades:
EncapsulatedTimeStamp>
                               </xades:ArchiveTimeStamp>

     </xades:UnsignedSignatureProperties>
                    </xades:UnsignedProperties>
               </xades:QualifyingProperties>
          </ds:Object>
     </ds:Signature>
</data>
```

A.3. Recibo de custodia

Se ha realizado con éxito la custodia del contenido firmado de la URL:
www.uoc.es

Firmado por:CN=ANCERT Certificados FERN V2,O=Agencia Notarial de Certificacion S.L.U. - CIF B83395988,L=Paseo del General Martinez Campos 46 6a planta 28010 Madrid,C=ES

Con fecha:2014-06-04T20:35:00.839+02:00

Persona solicita servicio custodia:

Nombre:Presentacion
Primer Apellido:Trabajo
Segundo Apellido:Master
DNI/CIF:65900145Y

Figura Nº 16.Datos de recibo de custodia

A.4. Guía de instalación rápida

A.4.1. Instalación Apache Tomcat 7

Para poder realizar el despliegue de la aplicación utilizaremos el servidor Web Apache Tomcat 7. Por lo que, descargaremos la última versión de dicho servidor Web de su página oficial http://tomcat.apache.org/

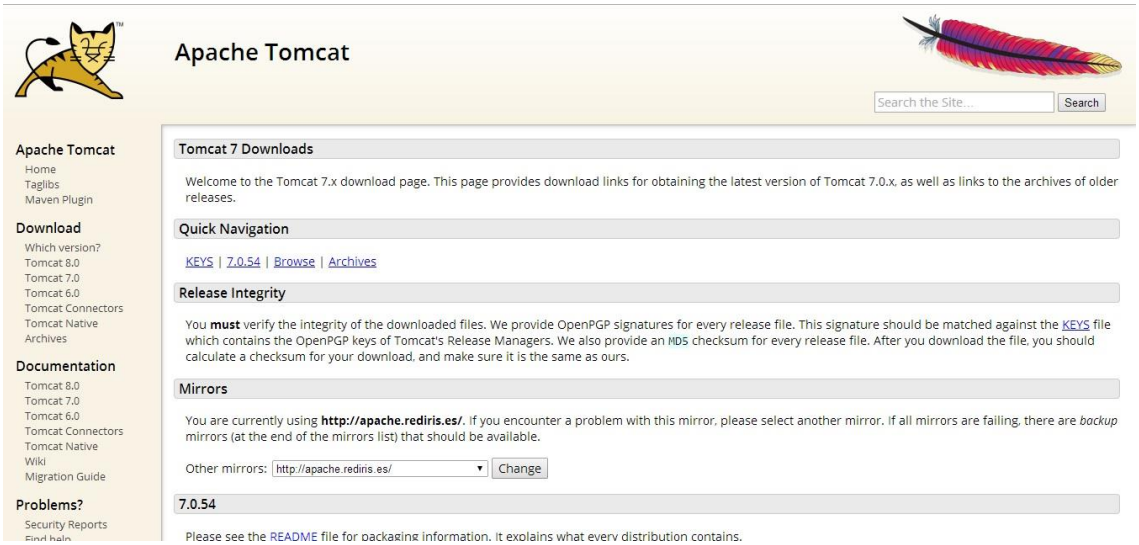

Figura Nº 17. Página Apache Tomcat 7

Una vez descargada la última versión procederemos a instalar el servidor Web. Esta instalación se realizará en función del sistema operativo y la descarga seleccionada.

A.4.2. Despliegue de aplicación de custodia

En el momento que se ha realizado la instalación de Apache Tomcat 7 y que funciona perfectamente procederemos al despliegue de la aplicación Web de custodia desarrollada. Para ello, utilizaremos el fichero .war, en principio denominado “AplicacionCustodia.war”, y lo incluiremos en la ruta de aplicaciones de Apache Tomcat 7 (/webapps).

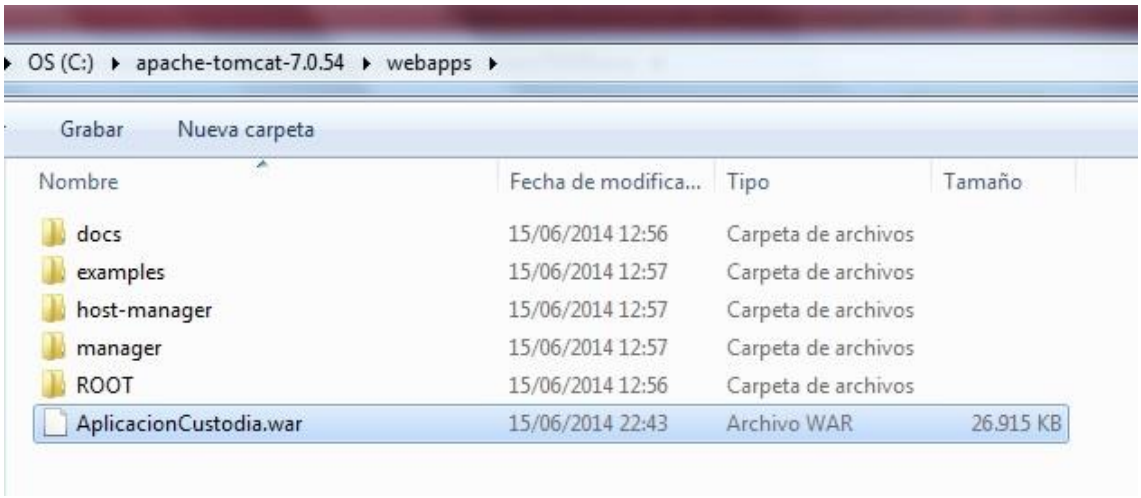

Figura Nº 18. Ruta webapps Apache Tomcat 7

Después de esto, arrancaremos el servidor Web mediante el fichero “startup” que se encuentra en la ruta /bin del servidor.

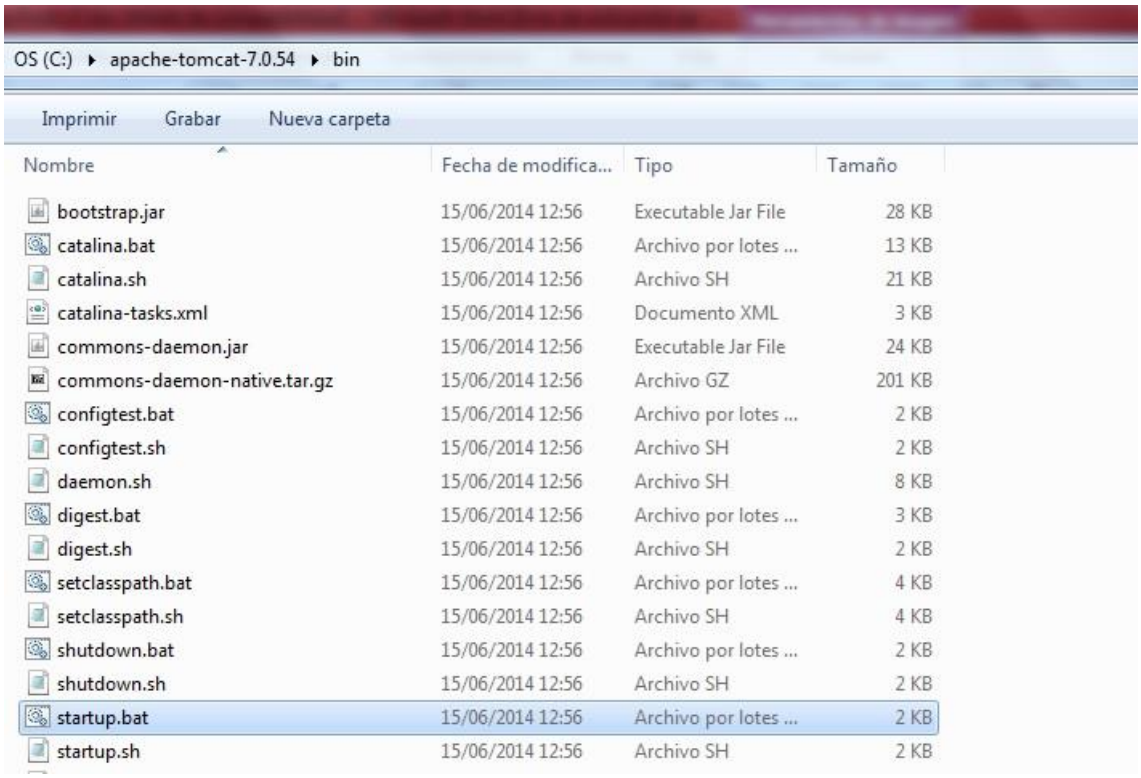

Figura Nº 19. Ruta bin Apache Tomcat 7

A su vez automáticamente desplegará la aplicación de custodia y podremos acceder vía navegador Web a la aplicación mediante la URL http:// localhost:8080/AplicacionCustodia

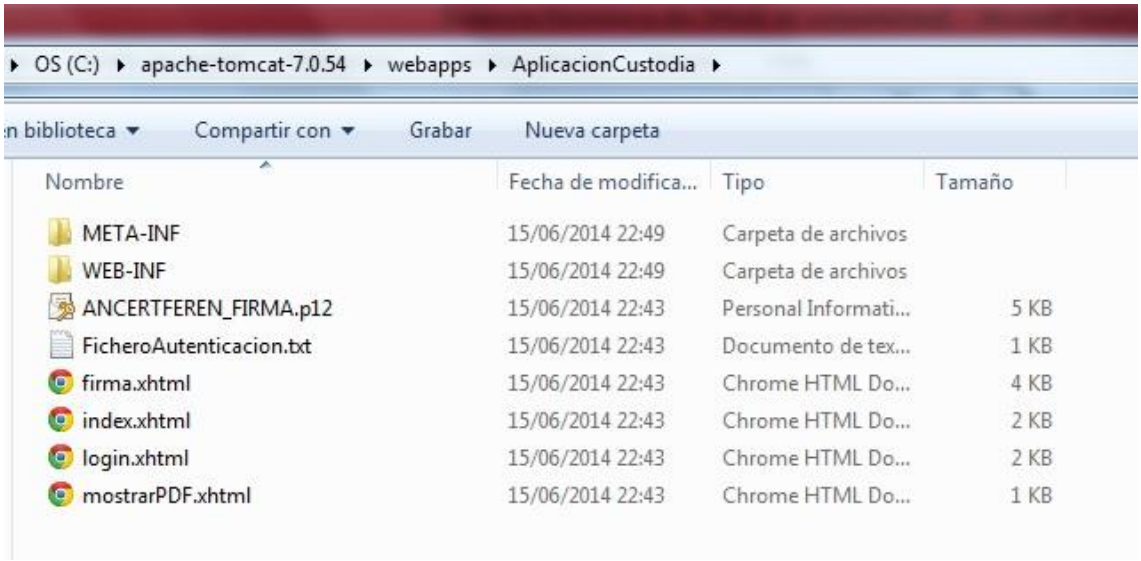

Figura Nº 20. Aplicación desplegada

A.4.3. Preguntas frecuentes

P- Cuando un usuario va a realizar la custodia de una web mediante el botón "Obtener Web", devuelve el siguiente error: "Error.sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target". ¿Qué puedo hacer?

R- La aplicación de custodia conecta con un servicio Web de Ancert para realizar la firma XAdES-A. Este servicio Web necesita de un certificado de Ancert v2 Pre. Por tanto, para poder acceder se deberá incluir en el Keystore de Java definido para la utilización de Apache Tomcat 7.

Para ello, cogeremos el certificado ancert_v2_pre.cer que se distribuye junto con el fichero .war de la aplicación Web y lo instalaremos en nuestro equipo.

Por último, añadiremos el certificado exportado a la Keystore de Java. Desde el directorio /bin de Java y como administrador indicaremos el siguiente comando:

keytool -import -alias <aliascertificado> -keystore ..\lib\security\cacerts -file <ruta> ancert_v2_pre.cer

P- No conozco los usuarios y contraseñas definidas de inicio en el fichero de autenticación.

R- Inicialmente se han definido tres usuarios dentro del fichero de autenticación: Manuel-passManuel; Enric-passEnric; Presentacion-passPresentacion.