Firma Electrónica para Dispositivos Móviles, en la nube

Nombre Estudiante: Erika Liliana Villamizar Torres

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

Nombre Consultor: Enric Hernández Jiménez

Centro: Agencia Notarial de Certificación –ANCERT (España)

Fecha entrega: 24 de junio de 2015

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 para Dispositivos Móviles - Ancert**
Nombre del autor:	Erika Liliana Villamizar Torres
Nombre del consultor:	**Enric Hernández Jiménez**
Fecha de entrega (mm/aaaa):	Junio/2015
Área del Trabajo Final:	AD –HOC Seguridad Informática
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Resumen del Trabajo (máximo 250 palabras):

La implementación de la firma electrónica en la nube beneficia a los usuarios de Ancert para que puedan firmar digitalmente documentos desde su móvil, sin que siempre sea necesario tener una firma digital instalada localmente en sus dispositivos, sin embargo esta implantación de firma debe inspirar confianza a los usuarios de Ancert garantizando la seguridad de los servicios de firma digital en la nube donde se encuentra alojada.

Para garantizar la confidencialidad, la integridad, la disponibilidad y el no repudio que son algunos aspectos principales de seguridad es necesario recurrir a soluciones de certificación digital que excedan en la confianza de las transacciones de cara al remitente (consumidor) como al destinatario (empresa).

Es por esto que el desarrollo de este trabajo se basa en el análisis de los diferentes tipos de certificados digitales para la tecnología en la Nube y adicionalmente se realiza una recomendación para que se implemente en Ancert una herramienta comercial de firma electrónica.

ELVT

Abstract (in English, 250 words or less):

The implementation of electronic signatures in the cloud benefits Ancert users, because they can digitally sign documents from theme mobile device, without necessary to have a digital signature installed locally on their devices, however this sign implementation must inspire confidence to Ancert users. Ensuring the security of digital signature services in the cloud where it is hosted.

To ensure confidentiality, integrity, availability and non-repudiation that are some of the major safety issues it is necessary to use digital certification solutions that exceed the confidence of transactions for the sender (consumer) and the addressee (business).

That is why the development of this work is based on the analysis of different types of digital certificates for cloud technology and additionally make a recommendation about a commercial tool for electronic signature to implement in Ancert.

Palabras clave (entre 4 y 8):

Firma, certificado, protocolo, cifrado, clave pública.

Signature, certificate, protocol, encryption, public key.

ÍNDICE

1. LISTA DE FIGURAS

2. AGRADECIMIENTOS

En primer lugar agradezco al ingeniero Enric Hernández Jiménez, la oportunidad que me ha brindado para aprender de él y brindarme su ayuda y compartir conocimiento e información para poder sacar adelante mi práctica y trabajo final de Máster, y a ANCERT por haberme permitido realizar este trabajo para tan prestigiosa entidad.

A mi madre que siempre me ha apoyado y ha estado a mi cuando más la he necesitado y a mi esposo por motivarme y orientarme pero sobre todo a los dos por la confianza depositada en mí.

Y por último quiero agradecer a mi compañero y Amigo Freddy Alexander Orozco Forero por su tiempo y ayuda para la consecución de este proyecto, por sus explicaciones cuando me sentía enredada en algunos temas.

3. INTRODUCCIÓN

Las transacciones online son un fenómeno cada vez más utilizado por la población mundial. La adopción de la firma electrónica se está acelerando debido a la rápida evolución de la tecnología y la necesidad de reducir los costos de transacción y de tiempo a la hora de cerrar negocios o realizar trámites.

Para garantizar la confidencialidad, la integridad, la disponibilidad y el no repudio que son algunos aspectos principales de seguridad, es necesario recurrir a soluciones de certificación digital que excedan en la confianza de las transacciones de cara al remitente (consumidor) como al destinatario (empresa).

En el desarrollo de este trabajo se tratarán aspectos como la firma electrónica, el estado del arte de la firma electrónica en la nube documentando los tipos de posibilidades o soluciones para la implementación y posteriormente se analizará los diferentes productos comerciales con el objetivo recomendar a Ancert una solución de implantación de firma electrónica en la nube para el notariado español realizando un análisis comparativo de las herramientas.

4. JUSTIFICACIÓN

Una solución de firma electrónica es un archivo digital que identifica a cada usuario al realizar trámites por internet es única para cada usuario, es un método seguro y en la mayoría de casos cifrado.

La implementación de la firma electrónica en la nube beneficia a los usuarios de Ancert para que puedan firmar digitalmente documentos desde su móvil, sin que siempre sea necesario tener una firma digital instalada localmente en sus dispositivos, sin embargo esta implantación de firma debe inspirar confianza a los usuarios de Ancert garantizando la seguridad de los servicios de firma digital en la nube donde se encuentra alojada.

Aunque actualmente la Firma Electrónica Reconocida Notarial (FEREN) permite al notario seguir ejerciendo su profesión en el marco de las comunicaciones telemáticas y el comercio electrónico, se hace necesario en Ancert brindarle a los usuarios de sus diferentes servicios la posibilidad de poder firmar desde cualquier lugar a través de cualquier dispositivo como: portátil, móvil y Tablet.

Los usuarios de Ancert se beneficiarán con la implantación de esta solución de firma electrónica para dispositivos móviles en aspectos como: ahorro de costos pues ya no necesitan enviar correos certificados, en ahorro de tiempo debido a que no necesitarán desplazarse y realizar un trámite que demoraba horas ahora lo podrán efectuar en minutos, en ahorro de papel debido a que ya no se hará necesario la impresión de documentos que de hecho afectan el espacio del archivo, ayuda al medio ambiente evitando la tala de árboles, y esta tecnología le brindará a los usuarios un alto nivel de seguridad debido a que la firma electrónica es mucho más segura, y sobre todo permite a Ancert mejorar el nivel de servicio permitiendo que firmen documentos online lo que evitará a los a clientes desplazamiento para firmar y un valioso tiempo de espera, mejorando su nivel de satisfacción.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Formular una propuesta para la aplicación de firma digital de documentos en la nube con dispositivos móviles, del cual puedan hacer uso los ciudadanos y el colectivo Notarial, en cumplimiento de la Ley 59/2003, de 19 de diciembre, de firma electrónica y REAL DECRETO 1553/2005, de 23 de diciembre.

5.2 OBJETIVOS ESPECÍFICOS

- Documentar el estado de arte de la implantación de firma electrónica en la nube para dispositivos móviles.

- Analizar los diferentes productos comerciales presentes en el mercado actual para la implementación de firmas digitales.

- Evaluar y recomendar una herramienta comercial para la implantación de firma electrónica para dispositivos móviles aplicable al colectivo notarial Ancert.

6. METODOLOGÍA

6.1 FASE 1: ALINEACIÓN Y PREPARACIÓN

Iniciación: Realizar reunión de conocimiento acerca de Ancert y de la contextualización acerca del tema del proyecto.

Definición de los objetivos: Definir los objetivos, alineados con las expectativas de Ancert y los resultados esperados.

Conocimiento de los servicios de ANCERT: Conocer los servicios de Ancert

Definición del alcance: Determinar lo que se va a realizar dentro de la cobertura del proyecto.
Establecimiento del mandato: Elaboración y aceptación del acta del proyecto y su planificación.

Pequeño estado de arte: Realizar una breve investigación y análisis del estado de arte de firma electrónica para dispositivos móviles.

Conocimiento de la Infraestructura Tecnológica: Profundizar y analizar la información suministrada por el consultor, e investigar en la web de Ancert sobre la infraestructura tecnológica.

Entrega PEC1: Entregar la PEC1 que debe contener como mínimo:
La enumeración de los objetivos que se quieren alcanzar con la realización del TFM.

La descripción de la metodología que se seguirá durante el desarrollo del TFM.

Una pequeña revisión del estado del arte.

6.2 FASE 2: ESTRUCTURACIÓN

Identificación de necesidades funcionales: Conocer las capacidades de firma electrónica de Ancert, identificar los diferentes conceptos relacionados con el tema de investigación.

Documentar el Estado del Arte: Profundizar el análisis y documentación del estado de Arte investigado en la fase I.

Entrega PEC2: Detalle y documentación de las actividades descritas en la Fase II de estructuración.

6.3 FASE 3: ANÁLISIS

Estado de arte final: Aprobación del estado de arte final de Firma electrónica para dispositivos móviles en la nube (Final de la Práctica).

Análisis y documentación de herramientas comerciales de firma electrónica: Analizar y documentar las diferentes herramientas de implementación de firma electrónica para dispositivos móviles.

Recopilación de diferentes arquitecturas de implementación de firma digital en dispositivos móviles.

Propuesta de Implementación de una solución comercial: Realizar la propuesta de implementación de una solución comercial que se ajuste a Ancert para firma electrónica en dispositivos móviles.

Entrega PEC3: Descripción y documentación de las actividades realizadas hasta la fecha, este documento debe ser la primera versión de la memoria.

6.4 FASE 4: PRESENTACIÓN DEL TRABAJO FINAL

Entrega de la PEC4 - Memoria final: Entrega de la memoria del Trabajo Final de Máster.

6.5 FASE 5: EVALUACIÓN

Entrega de la PEC5 - Presentación/Vídeo: Presentar un vídeo en el que se presente una síntesis del trabajo realizado sobre una presentación o guion.

Defensa del TFM: Defensa del TFM ante un tribunal formado por 3 miembros. La defensa se hará de forma virtual en el foro del aula. El tribunal realizará preguntas a los estudiantes, que tendrán un margen de 24 horas para contestar.

7. MARCO REFERENCIAL

7.1 MARCO CONCEPTUAL

7.1.1 Firma simple, digital avanzada y electrónica

Hacia el año 1988, en la norma ISO/IEC 7498-2 *Security Architecture* se hablaba del mecanismo de firma digital, dicho mecanismo define dos procesos:

A. Firmado de una pieza digital de información por parte del firmante.
B. Validación de una pieza de información firmada.

Por lo que a partir del documento original m, mediante un proceso de firma se genera la firma, como se puede apreciar en la figura 1, donde el mensaje m es firmado con una función Asig y da como resultado el documento firmado.

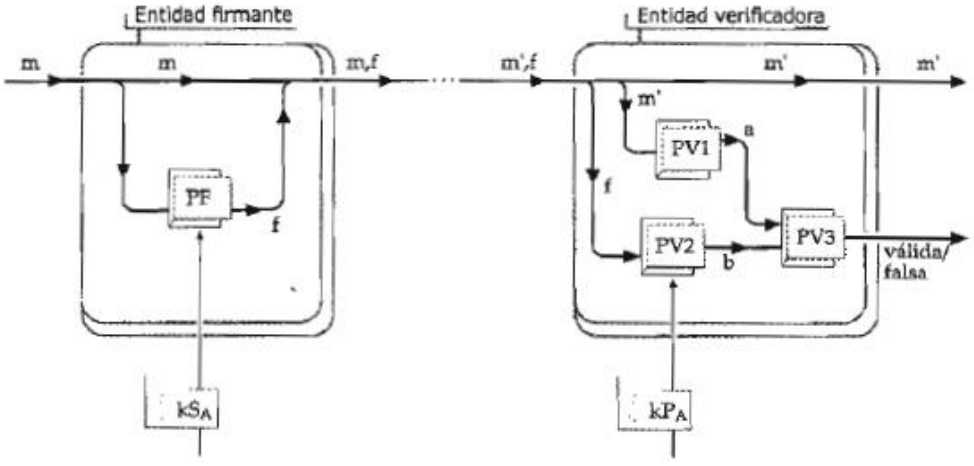
Figura 1. Formula de la obtención de la firma a partir del mensaje

$$f = \mathrm{A}_{\mathrm{sig}}(m).$$

fuente: (Carracedo Gallardo, 2004)

Por tanto el documento firmado es la unión de m y f. Participan además el concepto de entidad firmante y entidad verificadora dentro del proceso de firma, dicho proceso se puede ver de mejor manera en la figura 2.

Figura 2. Mecanismo general de firma digital



Fuente: (Carracedo Gallardo, 2004)

Acorde con lo anterior y según (Carracedo Gallardo, 2004) se imponen dos condiciones al modelo planteado las cuales son:

A. La firma f debe ser de longitud reducida e independiente del tamaño de m.
B. la generación de la firma se realiza a partir del resumen (*hash*) del mensaje m mediante un proceso de cifrado en el que se utiliza la clave privada del firmante.

Para un proceso de firmado sin tener en cuenta las dos condiciones anteriores para (Carracedo Gallardo, 2004) es denominada **firma simple**, pero este proceso no resulta viable por el tamaño que puede tener la firma y la duración del proceso de firmado.

Para un proceso de firmado que cumple con las dos condiciones se dice que es una **firma digital avanza**, puesto que se realiza a partir del resumen (hash) del mensaje m, mediante un proceso de cifrado en el que se utilizan las claves del firmante que son la clave pública y la clave privada, donde la clave pública la otorga la autoridad de certificación que es la entidad en la que todos confían, y genera el certificado digital al validar la solicitud de firma con la clave privada.

La **firma electrónica** consiste en una firma digital con informaciones añadidas para potenciar su validez.

7.2 ALGORITMOS DE FIRMA DIGITAL RSA Y DSA

Aunque hay muchos algoritmos, los más aceptados y sobre los que más pruebas de seguridad se han realizado son: RSA y DSA.

Se puede obtener lo que antes se ha llamado firma simple mediante el cifrado, con RSA, de todo el mensaje con la clave privada del firmante, que será algo totalmente distinto a la firma digital con resumen (*hash*).

Una definición formal del algoritmo de firma digital RSA se puede ver en la figura 3.

Figura 3 Pasos en proceso de cifrado con el algoritmo de firma digital RSA

1. Realiza $h = H(m)$.
2. Cifra $H(m)$ con su clave privada.

$$f = A_S[H(m)] = A_S[h] = h^d \bmod n$$

Fuente: (Carracedo Gallardo, 2004)

La función Hash (H), es parte fundamental en la estructura de los algoritmos de firma digital al utilizar funciones unidireccionales en la autenticación de los mensajes, lo que garantiza que una vez ha sido cifrado el mensaje no se puede descifrar. Es decir que el proceso (1) logra identificar la longitud del mensaje original (m) y obtiene la función hash, posteriormente el siguiente paso (2) corresponde a que la función hash se cifra junto con la clave privada del remitente y se envía con el mensaje al receptor, esto garantiza la autenticación del mensaje, y se genera la firma digital.

Algoritmo de firma digital DSA

Dicho algoritmo es algo más elaborado con relación a algoritmo de firma digital RSA y tiene la propiedad de que es específico para firma, no pudiendo ser usado para otras tareas de cifrado.

El estándar SHS que define el algoritmo de hash SHA-1 y el DSS (Estándar de Firma Digital (DSS), y fueron concebidos por el NIST para ser usados de forma conjunta en apoyo al DSA dado que es un algoritmo que sirve para firmar y no para cifrar información lo que también significa desventaja de este algoritmo ya que requiere mucho más tiempo de cómputo que RSA.

El algoritmo DSA comprende dos grandes números que se calculan de acuerdo con el algoritmo especificado y son: 1 numero entero con dígitos binarios múltiplos de 64 y comprendidos entre 512 y 1024, un número primo de 160 bits divisor del numero entero, esto parámetros permiten la autenticación del firmante, y, como consecuencia, la integridad de los datos del mensaje. La firma se genera en conjunto con el uso de una clave privada; la verificación se lleva a cabo en referencia a una correspondiente clave pública. Cada firmante tiene su propio par de claves la pública y la privada. La clave pública puede ser usada por cualquier persona para verificar la firma.
Usa la función hash en conjunción con el algoritmo DSA para crear la firma digital que se envía con el mensaje. La verificación de firmas implica el uso de la misma función hash.

7.3 VENTAJAS DEL USO DE LA FIRMA ELECTRÓNICA

El autor (Carracedo Gallardo, 2004) específica las ventajas de la implantación y el uso de firmas electrónicas entre las más destacadas documenta:

A. Susceptible de ser reconocida por el receptor:
El receptor del mensaje firmado debe ser capaz de reconocer, de manera fiable, la validez de la firma, ya sea por sí mismo o con la ayuda de terceros que actúen como validadores.

B. Difícil de falsificar:
Aunque es cierto que la seguridad de los algoritmos no es absoluta, al comparar el esfuerzo tecnológico y económico que hay que realizar para romper un criptosistema que maneje una clave de por ejemplo, 2000 bits, con el que sería necesario realizar para encontrar a un falsificador virtuoso, llegaremos a la conclusión de que es muchísimo más segura una firma electrónica que una firma caligráfica.

C. Identifica al firmante.
Autentica al signatario, y detectar cualquier cambio futuro de los datos firmados.

D. Va unida al mensaje formando un todo
Una firma que aparece en un documento no puede ser trasladada a otro. Esto se da porque la firma depende tanto de la clave privada del firmante como del documento firmando.

E. El autor de la firma no puede repudiar su autoría
Quien accede al documento firmado adquiere una prueba, demostrable ante terceros, de que el mensaje ha sido firmado por quien dice ser el signatario, junto con la autenticidad del origen de los datos y la integridad del mensaje, de lo contrario no podría ver su contenido.

F. Permiten incluir información adicional al texto
Puede ser complementada con sellos de tiempo, información sobre la identidad de los destinatarios, etc.

G. Afecta a todo el mensaje
La firma electrónica sirve para garantizar la integridad del mensaje, el cambio de un solo bit produciría una firma totalmente distinta.

7.4 ESQUEMAS DE FIRMA ELECTRÓNICA

La ISO/IEC 7498-2 contemplaba la utilidad de que existieran terceras partes en el escenario donde se llevasen a cabo los procesos de firma y verificación. Acorde con lo anterior se conciben dos tipos de esquemas:

7.4.1 Esquema de firma directa:

En el que la tercera parte es simplemente un juez (definido en sentido genérico, puede ser simplemente alguien aceptado por ambas partes). El juez se mantiene al margen de la comunicación y solamente verifica la firma cuando aparece un conflicto entre los participantes, ya que alguno de ellos puede no decir la verdad.

7.4.2 Esquema de firma arbitrada:

La tercera parte participa activa en el proceso de comunicación entre la entidad firmante y la entidad receptora que autentica la fuente de los datos y puede establecer registros de la operación realizada para utilizarlos en caso de litigio.

7.5 ESTRUCTURA DE LA FIRMA ELECTRÓNICA

Acorde con las definiciones del ETSI (Instituto Europeo de Normas de Telecomunicaciones), además de las especificaciones de la RFC 3369 (sintaxis de mensajes criptográficos), indican que dado un mensaje m, se puede definir un mensaje firmado como un conjunto de datos que incluye:

- El mensaje m que es firmado
- Información sobre algoritmos utilizados
- Información sobre certificados
- Información sobre revocación de certificados
- Información por y de cada uno de los firmantes:
  - Certificado del firmante.
  - Identificación de los algoritmos utilizados.
  - Atributos que son firmados (incluida la identificación de la política de firma).
  - Otros atributos no firmados.
  - Firma digital (Signature value) de m y de los atributos.

7.6 FORMATOS DE FIRMA EN FUNCIÓN DE LA INFORMACIÓN

En función de la información complementaria que contenga la firma, según la especificación del ETSI define varios formatos para la firma electrónica y son:

7.6.1 Formato básico

Simplemente denominada ES (Electronic Signature) considerada con los siguientes parámetros:

- Identificador de la política de firma
- Otros atributos que son firmados
- Firma digital (del mensaje y de los atributos)

Entre los atributos que son firmados deben estar los siguientes:

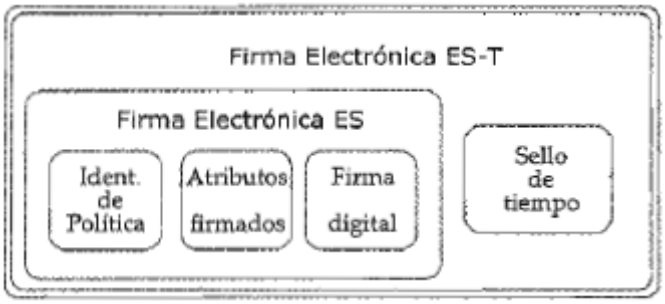
- Identificador preciso de la política del certificado de la clave pública del firmante.
- Tipo de información contenida en el mensaje m firmado.
- Resumen o valor hash del mensaje m.
- Identificador del algoritmo de firma digital utilizado.
- Hora y fecha de la firma.

7.6.2 Firma con sello de tiempo

Está claro que uno de los campos en el formato básico contiene información de tiempo en relación con el momento en el que el firmante declaro que firmó el documento, en un principio esta información no está respaldada por ninguna autoridad de Sellado de Tiempo (TSA), por lo que no cumpliría con el requisito imprescindible de garantizar, a través de una prueba demostrable ante terceros, que la firma ha sido realizada en una fecha y hora específica. Para este propósito es necesario de requerir el concurso de un TSA externa.

En cumplimiento con el requisito anteriormente expresado define la firma electrónica con sello de tiempo ES-T(*ES Timestamp*), la cual toma la ES y le añade una marca de tiempo, lo que posibilita la validez de la firma durante periodos de tiempo largos; el anterior concepto se puede ver enmarcado en el gráfico de la figura 4.

Figura 4 Esquema de la ES-T



Fuente justo carracedo

En síntesis para que la firma sea válida se requiere la existencia de dos indicadores de tiempo y dos firmas:

- Una fecha y hora de firma indicada por el firmante (que forma parte de los datos que éste firma digitalmente).

- Una fecha y hora de firma indicada por una Autoridad de Sellado de Tiempo, TSA, que es firmado por esa TTP sobre el valor de la firma digital de la ES básica.

Las firmas serán consideradas como válidas acorde con una determinada política que según (Carracedo Gallardo, 2004) indica que ambos indicadores de tiempo sean lo suficientemente próximos entre sí (se habla de minutos, horas o incluso días).

7.7 MÚLTIPLES FIRMAS

Es común que en un documento están presentes múltiples firmas o sellos para (Carracedo Gallardo, 2004) la multiplicidad de firmas se lleva a cabo dentro de dos categorías:

7.7.1 Firmas independientes

Son firmas que se realizan en paralelo en las que el orden de aparición en el documento no es relevante. (Carracedo Gallardo, 2004) especifica que su implantación en la estructura se lleva a cabo añadiendo en el formato del mensaje firmado, en el campo <<por cada uno de los firmante>> tanto los atributos que son firmados como los que no lo son, añadiendo la correspondiente firma digital de los datos.

7.7.2 Firmas embebidas (*embedded signatures*)

También llamadas embebidas (Carracedo Gallardo, 2004) indica aquellas que se aplican una a continuación de otra, de forma que cada nueva firma engloba e incluye a la anterior, dicho de otro modo se firman datos ya firmados, por tal motivo el orden de la firma queda reflejado en la firma resultante.

En la vida real puede presentarse que en un mismo documento requiera la firma de distintos agentes, algunas de las cuales puede ser necesario que se realicen en paralelo y otras firmas que se hagan en respuesta a un documento previamente firmado o tengan el carácter de una autorización.

7.8 CERTIFICADO ELECTRÓNICO

El certificado electrónico, es una identificación electrónica que contiene unas claves criptográficas que son los elementos necesarios para firmar. Los certificados electrónicos tienen el objetivo de identificar inequívocamente a su poseedor y son emitidos por Proveedores de Servicios de Certificación.

7.8.1 CERTIFICADO ELECTRÓNICO X.509

La definición del certificado digital se encuentra contenida en la especificación ISO/IEC 9594-8 (o su equivalente Recomendación X.509 de ITU-T)

7.8.2 Versiones 1 y 2 del certificado X.509

La estructura del certificado lo componen 7 campos que según la especificación (IETF, 2008) son definidas así:

A. **Versión.** hace referencia a la versión del certificado conforme a la cual están definidos formalmente sus distintos campos. El valor 0 indica la versión 1 y el valor 1 a la versión 2.

B. **Número de serie**: cada CA debe numerar correlativamente todos los certificados que emita, de forma número de serie sirve de identificador único para este certificado.

C. **Algoritmo de firma del certificado (signature):** especificación del tipo de algoritmo utilizado para cifrar la firma del certificado. Normalmente será RSA o DSA, pero tal y como está concebido el certificado X.509 puede ser cualquier otro algoritmo que sean capaces de manejar las entidades que se fían de los certificados emitidos por esa CA.

D. **Nombre de la CA emisora (issuer):** en la especificación del certificado está previsto que este campo recoja el nombre el nombre X.500 de la CA.

E. **Validez**. Indica el comienzo y el final del período de tiempo durante el cual el certificado es válido.

F. **Nombre del usuario o titular (subject):** es el nombre x.500 de la entidad adscrita a esta CA a la que se le ha expedido el certificado. Puede tratarse de una CA a la que otra CA le haya generado un certificado.

G. **Información sobre la clave del usuario**: es evidentemente, el componente principal del certificado. Consta a su vez de dos elementos:

- Algoritmo con que será usada: identificador del algoritmo con el que se ha previsto que la clave pública sea usada.

- Valor de la clave pública (*subjecgt public key*): es el valor de la clave pública de la que es propietaria la entidad comunicante para la que se ha emitido el certificado.

Para la versión 2 aprobada en 1993 se incluyen los siguientes campos optativos:

Identificador único de CA emisora. Se trata de una cadena de bits, sin formato específico, que de forma opcional sirve para contener información adicional sobre la CA emisora del certificado.

7.9 DIRECTORIO X.500

El servicio de directorio X.500 es un servicio de directorio global. Sus componentes cooperan para manejar información sobre objetos como países, organizaciones, personas, máquinas, etc., en un ámbito mundial. Proporciona la capacidad de buscar información por el nombre (un servicio de páginas blancas) y navegar y buscar información (un servicio de páginas amarillas).

La información está contenida en un "directory information base" (DIB). Las entradas en el DIB se ordenan en una estructura de árbol llamada "directory information tree" (DIT). Cada entrada es un objeto nombrado y consiste en un conjunto de atributos. Cada atributo tiene un tipo de atributo definido y uno o más valores. El esquema de directorio define la obligatoriedad u opcionalidad de los atributos para cada clase de objeto (llamando "clase

objeto"). Cada objeto nombrado podría tener una o más clases objeto asociadas con él.

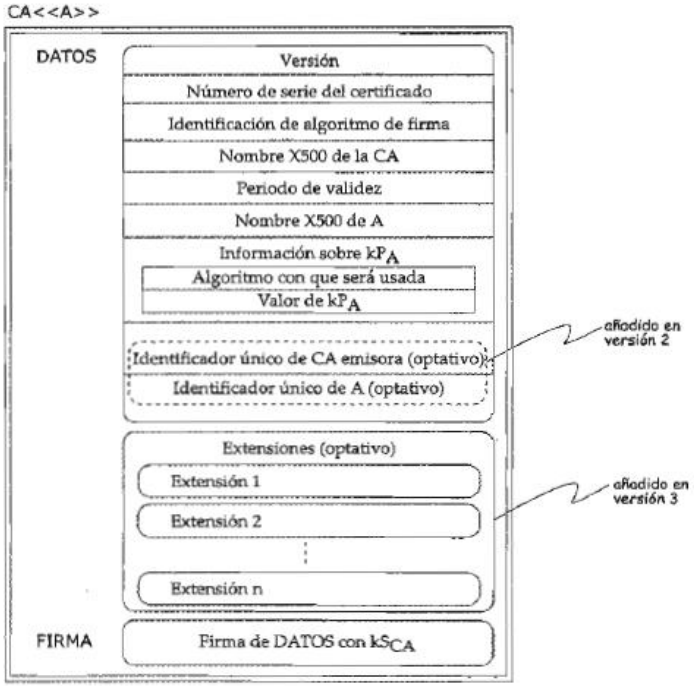
El espacio de nombres X.500 es del tipo árbol. Una entrada es identificada de forma no ambigua mediante un nombre distinguido (DN). Un nombres distinguido es la concatenación de los atributos seleccionados desde cada entrada, llamada nombre relativo distinguido (RDN), en el árbol un path desde la raíz hasta la entrada nombrada.

Lo usuarios del directorio X.500 podrían (sujetos al control de acceso) interrogar y modificar las entradas y los atributos del DIB.

7.9.1 Versión 3 del certificado X.509

La versión 3 del certificado conserva las características de 1 y 2 añadiendo extensiones, más exactamente permite definir un indeterminado número de campos adicionales que recojan los datos de interés para la política de seguridad definida en el dominio para el cual el certificado es generado.

Figura 5. Campos añadidos en versión 3



Fuente: (Carracedo Gallardo, 2004)

7.10 PROTOCOLO DE SEGURIDAD PARA SERVICIOS WEB WS-SECURITY

Protocolo de seguridad para servicios web y aplicaciones distribuidas inicialmente propuesto y desarrollado por IBM, MICROSOFT, VERISIGN. Ahora dicho protocolo es desarrollado por OASIS-OPEN (OASIS-OPEN, 2015). De hecho ha sido aprobado como un estándar de normalización internacional.

Para la IBM el estándar proporciona un conjunto amplio de dispositivos de seguridad para aplicaciones de servicios web, al basarse en estándares establecidos de la industria respecto a criptografía y cifrado y firmado de XML.

Puede especificar los dispositivos a utilizar en una aplicación específica con WS-Policy y WS-SecurityPolicy, lo que permite que los clientes del servicio se configuren automáticamente para acceder al servicio. Con el soporte generalizado de esos estándares en varias plataformas e infraestructuras de servicios web, hay una buena interoperatividad (que mejora a lo largo del tiempo).

Una de las principales desventajas que menciona IBM acerca de la implementación de WS-security es que la configuración puede tornarse compleja y que a veces añade mucho volumen a los mensajes que se intercambian.

Este estándar es empleado plataformas de firma electrónica para determinar el método de autorización de ejecución de los web services. Los métodos empleados son:

Usuario y password: mediante este método es necesario que las peticiones SOAP realizadas contengan el tag de seguridad “UserNameToken” y que el usuario y password alojados en dicho tag estén registrados para la aplicación que intenta ejecutar el servicio Web.

Certificado: mediante este método es necesario que las peticiones SOAP realizadas contengan el tag de seguridad “BinarySecurityToken” y estén firmadas por alguno de los certificados registrados para la aplicación que intenta ejecutar el servicio Web. La parte pública de estos certificados, para poder aplicar esta modalidad, ha de ser facilitada a Soporte para la inclusión de la misma en la Plataforma.

7.11 INFRAESTRUCTURA DE SEGURIDAD

Para (Carracedo Gallardo, 2004) se denomina infraestructura a todo el entorno de comunicación y pertenece a todas y cada una de las entidades que interactúan, pero es de aclarar que no es pertenencia exclusiva de ninguna de ellas en particular, a lo anterior se implanta protocolos de seguridad.

La implantación de los protocolos de seguridad sobre una aplicación telemática concreta requiere determinados componentes telemáticos, que son de uso exclusivo por parte de las entidades que participan en la provisión global del servicio.

La infraestructura de seguridad debe tener las siguientes propiedades o características que permitan dar mayor seguridad y confianza a las operaciones que se realizan a través de los medios electrónicos que intervienen y son:

- Usar una infraestructura para claves, específicamente la de clave pública que permita cifrar los datos, a través de algoritmos Simétricos, cuya finalidad es la de cifrar y descifrar mensajes utilizando una misma clave. Como inconveniente principal encontramos la distribución de las claves entre el emisor y el receptor.

- La firma digital debe cumplir autenticidad, integridad y no repudio; para ello, el mensaje debe cifrarse con la clave privada de cada usuario, y los usuarios que deseen verificarla, descifrarán con la clave pública.

- El cifrado de información, debe cumplir confidencialidad, integridad y no repudio; para ello, se cifra el mensaje con la clave pública del receptor, y el receptor será el único que podrá descifrar con su clave privada (por ejemplo, SSL).

- Las redes (sistemas de aplicaciones y redes de administración), deben permitir la comunicación entre distintas administraciones u organizaciones y de esta forma permitir el intercambio de operaciones.

- El comportamiento de los componentes de la infraestructura es genérico e independiente de la aplicación telemática concreta que le solicite sus servicios.

- Debe existir un tipo de confianza generalizada entre los servicios y las entidades comunicantes que los utilizan.

7.12 Componentes

De acuerdo con la concepción global que aporta acerca de lo que es una infraestructura de seguridad, distingue los siguientes componentes involucrados en la infraestructura de certificación:

- Autoridades de certificación
- Autoridades de registro, RAs (*Registration Authorities)*
- Autoridades de repositorio para el almacenamiento y recuperación de certificados.
- Autoridades para la generación y distribución de CRLs.

Adicionalmente se pueden añadir otras TTPs tales como:

- Autoridades de sellado de tiempo, TSA (*Time-Stamping Authorities*)
- Autoridades de Atributos, AAs (*Atribute Autorities*). Son ttps encargadas de la generación de los Certificados de Atributos, ACs (*Atribute Certificates*), que son unas piezas de información que contienen un conjunto de atributos para una entidad comunicante y alguna información adicional, que están firmadas digitalmente por la AA que las generó.
- TTPs para la provisión del servicio de no-repudio
- TTPs para la provisión del servicio de anonimato.

7.13 SISTEMAS OPERATIVOS PARA DISPOSITIVOS MÓVILES

Cada vez más se confía en los smartphones para almacenar información personal y para acceder a todo tipo de servicios online a través de ellos. En la actualidad, la tecnología en estos dispositivos ha evolucionado, y es posible implementar aplicaciones cada vez más complejas sobre los diferentes sistemas operativos que existen para móviles.
Sin embargo mantener de forma segura los datos en un dispositivo móvil es un reto, no solo por la falta de mecanismos de seguridad por parte de las plataformas, sino en el correcto uso de los dispositivos por parte de los usuarios. Un sistema puede ser muy robusto en cuanto a su seguridad pero si sus usuarios no son conscientes sobre cómo interactuar con este y como mantener de forma segura sus datos, siempre van a existir y surgir amenazas a dicho sistema.

A continuación se describe los principales puntos de seguridad de cada uno de los sistemas operativos mencionados:

7.13.1 ANDROID

La plataforma Android tiene un conjunto de aplicaciones básicas incluyendo un cliente de email, un programa de SMS (Short Message Service: para

enviar y recibir mensajes de texto), calendario, mapas, navegador, contactos, entre otros. Todas las aplicaciones se escriben usando el lenguaje de programación Java aunque también se pueden programar en C++ utilizando el kit de desarrollo Android NDK (Native Development Kit) y permite abstraer al sistema operativo de las aplicaciones a través del middleware basado en la máquina virtual Dalvik que se encargada de realizar una gestión eficiente de las aplicaciones y su memoria. Cada una de las aplicaciones en Android se ejecuta en su propio proceso y tiene su propia instancia de la máquina virtual Dalvik. Dicha máquina está basada en registros y utiliza ficheros Dalvik ejecutables (formato .dex) compilados y optimizados para el ahorro de memoria.

Android es un sistema operativo basado en Linux, diseñado principalmente para dispositivos móviles con pantalla táctil como por ejemplo tablets y smarthphones. Fue desarrollado por Android Inc. con el respaldo económico de Google actual dueño y supervisada por el OHA (Open Handset Alliance).

El sistema operativo Android es completamente libre, es decir que no hay que pagar absolutamente nada ni para programar en él ni para poder instalarlo en un teléfono. Lo que lo hace muy popular entre desarrolladores, que deben pagar muy poco para lanzar una aplicación, y fabricantes de celulares, que ahorran a la hora de elegir el sistema operativo para el teléfono que quieren lanzar al mercado, por tanto Android es el sistema operativo es actualmente tiene una mayor penetración en el mercado lo que lo ha convertido en objetivo principal de ataques de seguridad.

A lo anterior se suma que el código fuente de Android puede descargarse, inspeccionar, modificar y compilar fácilmente, esto hace que el software tenga muchas vulnerabilidades que pueden ser aprovechadas por una aplicación maliciosa, por ejemplo: para robar los contactos del dispositivos, enviar sms sin autorización, utilizar datos del sistema para obtener la geo localización, escalar privilegios y con la instalación de aplicaciones maliciosa se pueden aplicar cambios de funcionalidades no deseados que pueden conllevar a fraudes electrónicos bancarios, suplantaciones de identidad, pérdidas económicas, entre otras.

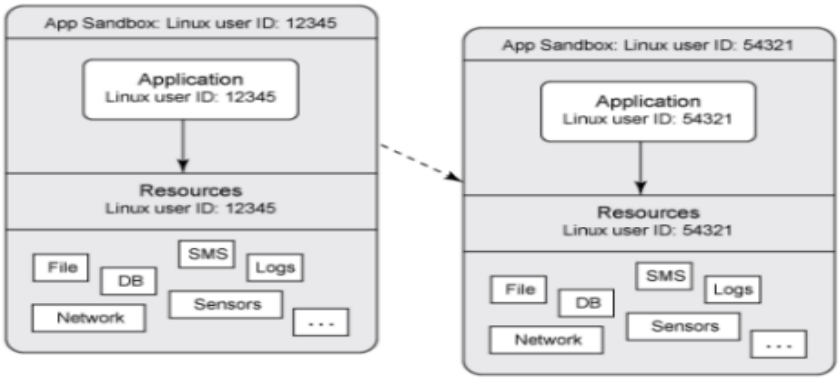
En cuanto a la seguridad de Android:
Android dispone de un sistema de seguridad no centralizado en concordancia con su filosofía de software libre, es decir, no existe un mecanismo central encargado de controlar y verificar la seguridad. La seguridad en Android se basa en tres medidas, la ejecución de las aplicaciones en procesos independientes, la concesión de permisos para la utilización de recursos y la firma de las mismas.

Ejecución en procesos independientes

En primer lugar, Android aprovecha la seguridad que le proporciona su núcleo Linux, gracias al cual puede controlar el acceso de las aplicaciones al hardware y a los recursos de otras aplicaciones. De esta manera, las aplicaciones se ejecutan dentro de procesos independientes que no pueden interactuar con otras excepto cuando se haya declarado explícitamente permiso para ello (Figura 6)

Android mantiene una cuenta de usuario Linux (user ID) por cada aplicación instalada en el sistema. Los datos almacenados por la aplicación son asociados a su usuario Linux de forma que no puedan ser accedidos por otras aplicaciones. Sin embargo, sí que existe la posibilidad de otorgar modos de acceso en la creación de ficheros, permitiendo su lectura o escritura por parte de diferentes aplicaciones, aunque el fichero tendrá un único propietario que será el usuario Linux de la aplicación que lo creó.

Figura 6 Ejemplo de dos aplicaciones de Android con sus propios procesos o recintos de seguridad



Fuente (de Matías García, 2013)

Concesión de permisos

La segunda de las medidas de seguridad se pone de manifiesto en el caso de que una aplicación necesite acceder a datos o componentes del sistema que puedan poner en un compromiso a la seguridad del mismo. Para ello, se deben conceder permisos. Android dispone de un sistema de permisos para el control del acceso a los recursos y características especiales del hardware. Estos permisos son declarados por el desarrollador de la aplicación en el fichero AndroidManifest.xml

Las aplicaciones tienen la obligación de informar sobre los recursos que tienen intención de usar a través de sus paquetes de instalación. Por tanto, el control del comportamiento de las aplicaciones y servicios en Android solo

puede ser llevado a cabo por el usuario en el momento previo a su instalación, a través de la aceptación de las políticas de cada aplicación. Mediante este sistema de concesiones se controla que una aplicación no haga uso de permisos no manifestados, interrumpiéndose y generándose una excepción de permiso en caso de que pretenda acceder a un recurso no declarado en su instalación. Sin embargo, este mecanismo proporciona un control reducido sobre los permisos ya que no es posible conocer cómo se están utilizando por parte de la aplicación tras su aceptación. Además, la decisión sobre la concesión de los permisos es estática, es decir, no existe la posibilidad de que los permisos otorgados puedan ser modificados posteriormente una vez que la aplicación ha quedado instalada. También se debe señalar que Android no permite establecer políticas por las que se conceda a una aplicación el acceso a un recurso un número fijo de veces o solamente bajo ciertas circunstancias.

Firma de una aplicación

Por último y como medida disuasoria de creación de software maligno, toda aplicación debe ser firmada con un certificado digital que identifique a su creador. Igualmente, tras la modificación de una aplicación, ésta debe ser firmada de nuevo de forma que sólo el propietario de la clave privada podrá realizar modificaciones en ella. La firma de las aplicaciones en Android es simple y puede ser realizada de forma autónoma, es decir, no es condición necesaria la firma del certificado digital por parte de una autoridad de certificación, lo que facilita y reduce costes en el proceso de publicación de las mismas.

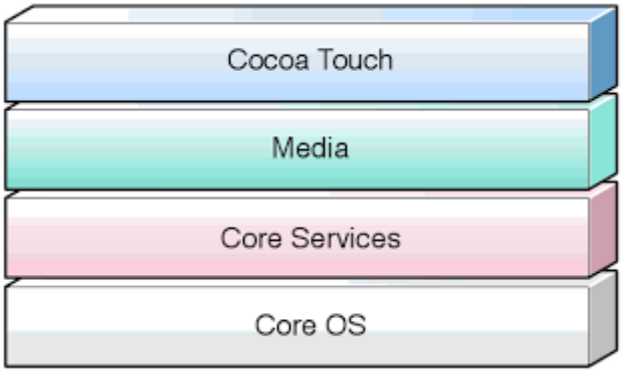
7.13.2 IOS

Es el sistema operativo móvil desarrollado por Apple Inc., inicialmente solo para el teléfono inteligente de la compañía (iPhone), luego fue extendido a otros dispositivos como el iPod Touch, iPad y el Apple TV. Se deriva de Mac OS X basado en lenguaje Darwin SD. No permite la instalación de IOS en hardware de terceros.

Arquitectura IOS

La arquitectura iOS está basada en capas, donde las capas más altas contienen los servicios y tecnologías más importantes para el desarrollo de aplicaciones, y las capas más bajas controlan los servicios básicos.

Figura 7 Arquitectura de capas IOS



Fuente: https://sites.google.com/site/tecnologiaiostm/desarrollo-de-aplicaciones/arquitectura-ios

Cocoa Touch
Es la capa de mayor relevancia para el desarrollo de aplicaciones IOS. Se basa en un conjunto de Frameworks que proporciona el API de Cocoa para desarrollar aplicaciones en donde se destacan: UIKit encargado de contener todas las clases que son necesarias para el desarrollo de una interfaz de usuario y Foundation que define algunos servicios del sistema operativo.

Media
Provee los servicios de gráficos y multimedia a la capa superior. Esta capa se denomina capa de comunicaciones ya que contiene los gráficos, audios y tecnologías de videos que se utilizan en sus aplicaciones.

Core Services
Contiene los servicios fundamentales del sistema que usan todas las aplicaciones.

Core OS
Esta capa contiene características de bajo nivel: ficheros del sistema, manejo de memoria, seguridad, drivers del dispositivo y se utiliza en diferentes marcos que ayudan a la comunicación y seguridad con hardware externo o directamente sobre sus aplicaciones.

Marco Acelerador (Accelerate.framework):
Contiene interfaces para realizar el procesamiento de señal digital (DSP), álgebra lineal, y los cálculos de procesamiento de imágenes.

Marco Core Bluetooth (CoreBluetooth.framework):
Permite a los desarrolladores interactuar específicamente con (LE) accesorios de baja energía Bluetooth. Las interfaces de Objective-C de este marco le permiten hacer lo siguiente:

- Analizar en busca de accesorios Bluetooth y conectar y desconectar.
- Información Broadcast ibeacon desde el dispositivo IOS.
- Preservar el estado de las conexiones Bluetooth y restaurar esas conexiones cuando se inicia posteriormente su aplicación.
- Ser notificado de los cambios a la disponibilidad de periféricos Bluetooth.

Marco accesorio externo (ExternalAccessory.framework):
Proporciona soporte para la comunicación con los accesorios de hardware conectados a un dispositivo. Se puede obtener información sobre cada accesorio disponible y permite iniciar sesiones de comunicaciones.

Marco de servicios de seguridad genéricos (GSS.framework):
Proporciona un conjunto estándar de los servicios relacionados con la seguridad de aplicaciones de iOS. Las interfaces básicas de este marco se especifican en IETF RFC 2743 y RFC 4401 . Además de ofrecer las interfaces estándar, iOS incluye algunas adiciones para la gestión de credenciales que no están especificados por la norma, sino que son requeridos por muchas aplicaciones.

Marco de Seguridad
Además de su base de características de seguridad, iOS también proporciona un marco de seguridad explícita (Security.framework), que se puede utilizar para garantizar la seguridad de los datos de las aplicaciones. Este marco ofrece interfaces para las gestiones de certificados, claves públicas y privadas, y las políticas de confianza. Es compatible con la generación de números pseudoaleatorios criptográficamente seguros. También es compatible con el almacenamiento de certificados y claves criptográficas en el llavero, que es un repositorio seguro para los datos de los usuarios sensibles.

IOS Contiene la biblioteca Común Crypto que ofrece soporte adicional para el cifrado simétrico, códigos de autenticación de mensajes basado en hash (HMAC), y *digiere*. La característica *digiere* proporciona funciones que son esencialmente compatible con los de la biblioteca OpenSSL, que no está disponible en IOS.

Interfaces
IOS proporciona un conjunto de interfaces para acceder a muchas características de bajo nivel del sistema operativo. Su aplicación tiene acceso a estas funciones a través de la LibSystem biblioteca. Las interfaces se basan C y proporcionan apoyo a lo siguiente:

- Concurrencia (hilos POSIX y Grand Central Dispatch).
- Networking (sockets BSD).
- El acceso del sistema de archivos.
- E / S estándar.
- Bonjour y DNS.
- Información Local.
- Asignación de memoria.
- Computaciones matemáticas.

Los Archivos de cabecera para muchas tecnologías Core OS se encuentran en: el *<iOS_SDK>* /usr/include/, donde *<iOS_SDK>* es la ruta de acceso al SDK de destino en el directorio de instalación de Xcode.

MODELO DE SEGURIDAD DE APPLE

Apple tiene un modelo de seguridad de cuatro (4) pilares para disminuir el número de ataques que sufren los dispositivos con el sistema operativo iOS:

A. Control de acceso tradicional
IOS proporciona la seguridad tradicional de todos los dispositivos móviles, como configuración de contraseñas para el bloqueo, y otras más avanzadas para el desbloqueo, la cual ante un determinado número de intentos incorrectos para desbloquear el dispositivo; elimina el contenido automáticamente y la recuperación de la información se puede realizar mediante copias de seguridad; almacenadas en iTunes, a la cual solo tiene acceso el propietario del dispositivo.

B. Cifrado hibrido
Como cualquier persona puede desarrollar aplicaciones para iOS y algunas de estas pueden traer consigo malware, Apple dispone App Store, donde se encuentran centralizadas todas las aplicaciones certificadas para móviles con este sistema operativo. Cifrado, iOS cuenta con un cifrado hibrido, en el cual se usa una aceleración el hardware para compendiar los datos almacenados en la memoria flash.

C. Aislamiento
IOS aísla cada aplicación del resto instaladas en el dispositivo, lo que impide que estas instalen controladores, malware y conozcan que otras aplicaciones existen.

D. Evitar la ejecución del proceso Jailbreak
Para hacer que el sistema de seguridad implementado por IOS funcione, se debe evitar que el dispositivo cuente con Jailbreak, el cual elimina las limitaciones impuestas por Apple en los dispositivos con IOS y permite a los usuarios acceder al sistema operativo y de esta manera descargar aplicaciones y extensiones que no se encuentran disponibles en el App Store, quedando mucho más expuestos al malware y a ataques informáticos.

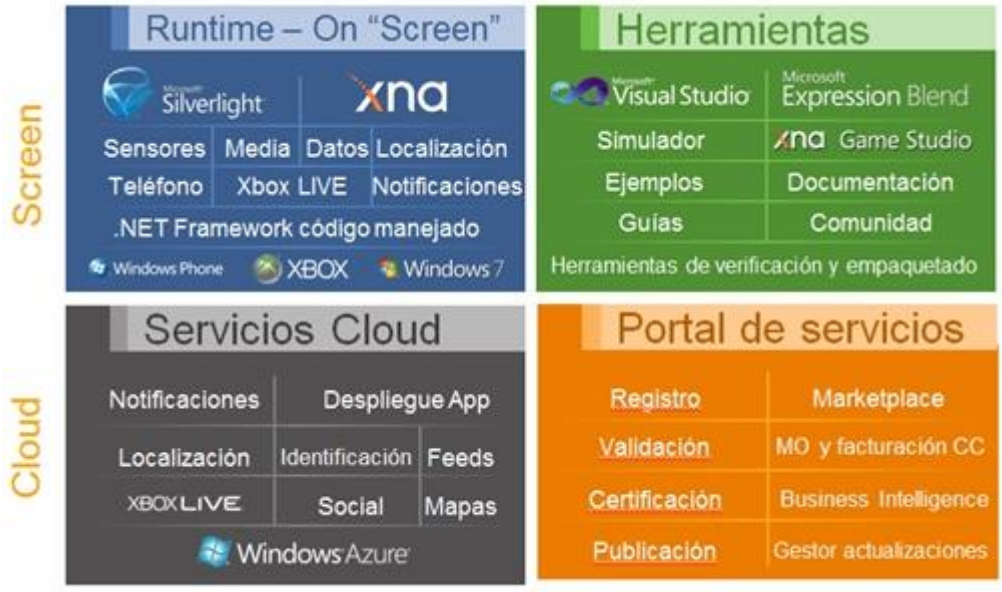
7.13.3 WINDOWS PHONE

Windows Phone es un sistema operativo móvil desarrollado por Microsoft como sucesor de la plataforma Windows Mobile y está diseñado para su uso en teléfonos inteligentes (Smarthphones) y otros dispositivos móviles. Se basa en el núcleo del sistema operativo Windows CE y cuenta con un conjunto de aplicaciones básicas utilizando las API de Microsoft Windows. Está diseñado para ser similar a las versiones de escritorio de Windows estéticamente.

Desarrollo de Aplicaciones
El desarrollo de aplicaciones para Windows phone puede hacerse empleando dos tipos de implementaciones o dos tipos de códigos ambos se ejecutan como procesos separados estos son Silverlight y XNA.

Arquitectura de Windows Phone
La plataforma de Windows Phone, se divide dos grandes bloques, Screen y Cloud:
Screen se refiere al entorno de desarrollo de aplicaciones que se instala en el ordenador, y Cloud es una nueva apuesta de Microsoft que permite realizar diversas tareas o directamente trabajar vía internet.

Figura 8 Arquitectura de desarrollo de Windows Phone



Fuente:
http://sabia.tic.udc.es/gc/Contenidos%20adicionales/trabajos/ProgramacionVideoJuegos/JuegosMoviles/windows.html

Screen
Runtimes-On "Screen": Implementaciones Silverlight, XNA Framework, .NET Compact Framework y sus servicios relacionados, que proveen a la plataforma de un entorno para construir aplicaciones seguras y gráficamente ricas.

Herramientas y soporte: Implementaciones de Visual Studio 2010 y Expression Blend, junto con todas sus utilidades y documentación, que permiten crear un entorno y una experiencia de desarrollo para generar aplicaciones de manera rápida y sencilla.

Cloud
Servicios Cloud: Es un conjunto de servicios en la nube como Windows Azure (plataforma ofrecida como servicio y alojada en los centros de procesamiento de datos de Microsoft, orientada a empresas), XBOX Live Service y otros servicios como los de notificaciones. Acceso a servicios de terceros, como servicios de identificación, almacenamiento, redes sociales, etc.

Portal de Servicios: El Windows Phone Marketplace contiene servicios que permiten a los desarrolladores registrar, certificar y vender sus aplicaciones.

Windows Phone se compone de una arquitectura de doble capa, de las cuales son la capa de núcleo y la capa de usuario: para esta parte el sistema cuenta con una memoria virtual para correr los procesos de una forma separada.

Microsoft Silverlight: este entorno permite desarrollar aplicaciones orientadas a la Web, permite el desarrollo basado en XAML (lenguaje de marcado declarativo).

Microsoft XNA: Es un Framework implementación nativa de .NET Compact Framework, que incluye un conjunto de librerías de clases, especialmente para el desarrollo de juegos, uno de los ejemplos seria para el manejo de dispositivos de entrada, tratamiento de sonidos y video, carga de modelos y texturas, uso de modelos de forma transparente a la plataforma en la que se ejecute desarrollo de juegos online, etc.

Windows Phone realiza sus procesos en forma aislada llamados Sandbox con la finalidad de ejecutar las aplicaciones de una forma segura, de esta forma los procesos no colisionan el uno con el otro lo cual se hace con el fin de evitar que los archivos de aplicación sean dañados por otros. (MICROSOFT , 2015)

7.13.4 BLACKBERRY OS

Es un sistema operativo móvil de código cerrado desarrollado por BlackBerry, antigua *Research In Motion* (RIM); para los dispositivos BlackBerry. El sistema permite multitarea y tiene soporte para diferentes métodos de entrada adoptados por RIM para su uso en computadoras de mano, particularmente la *trackwheel*, *trackball*, touchpad y pantallas táctiles.

Desde la cuarta versión se puede sincronizar el dispositivo con el correo electrónico, el calendario, tareas, notas y contactos de Microsoft Exchange Server además es compatible también con Lotus Notes y Novell GroupWise. BlackBerry Enterprise Server (BES) proporciona el acceso y organización del email a grandes compañías identificando a cada usuario con un único BlackBerry PIN. Los usuarios más pequeños cuentan con el software BlackBerry Internet Service, programa más sencillo que proporciona acceso a Internet y a correo POP3 / IMAP / Outlook Web Access sin tener que usar BES. Al igual que en el SO Symbian desarrolladores independientes también pueden crear programas para BlackBerry pero en el caso de querer tener acceso a ciertas funcionalidades restringidas necesitan ser firmados digitalmente para poder ser asociados a una cuenta de desarrollador de RIM.

Seguridad BlackBerry

A diferencia de otros sistemas operativos, la seguridad en BlackBerry es una de las características más fiables puesto que se lleva a cabo a través de normas, estas se encuentran contenidas dentro de un archivo que se llama las políticas de seguridad (policy.bin). El archivo se carga en la BlackBerry a un nivel muy bajo, lo cual significa que no se puede encontrar navegando por el sistema de archivos y menos aún copiarlo o eliminarlo. El dispositivo lee esta política desde la primera vez en que es puesta en marcha y una vez cargado, nada puede cambiar las reglas allí definidas.

Algunas políticas de seguridad del dispositivo como tal son:

- Desactivar BlackBerry Messenger.
- Desactivar desvío de contactos.
- Control del rango de uso del Bluetooth
- Permitir llamadas salientes en Bluetooth
- Permitir la descarga de aplicaciones a través del navegador
- Permitir navegación por Wi-Fi
- Desactivar Java Script en el navegador
- Establecer tablas HTML en el navegador
- Activar las hojas de estilo
- Desactivar la cámara de fotos
- Desactivar la cámara de vídeo
- Algoritmo de generación de claves públicas y privadas
- Los usuarios deben confirmar antes de enviar SMS, MMS, correo electrónico o mensaje PIN
- Desactivar MMS (Servicios Multimedia)
- Información del Propietario
- Habilitar el PIN de mensajería
- Permitir envío de mensajes SMS
- Elegir browser por defecto
- Dirección de página de inicio del navegador
- Descargar automáticamente archivos adjuntos
- Pantalla del sistema cuando se haga descarga de imágenes
- Desactivar texto enriquecido/HTML en el correo electrónico
- Tiempo de duración para mantener almacenados los mensajes recibidos
- Anteponer descargo de responsabilidad a los mensajes de correo saliente.

Autenticación

Para que las aplicaciones puedan lograr conexión a la Plataforma **IoT BlackBerry** utilizan el protocolo estándar OAuth 2.0 para la autenticación y autorización de usuarios y dispositivos.

El protocolo OAuth 2.0 recepciona la señal de acceso, que se requiere para todas las llamadas a la API de BlackBerry Platform IO. El tiempo de caducidad de un token de acceso es de 365 días. Además, la capa de conexión segura (SSL) se utiliza para todas las comunicaciones entre una aplicación y la Plataforma IoT BlackBerry.

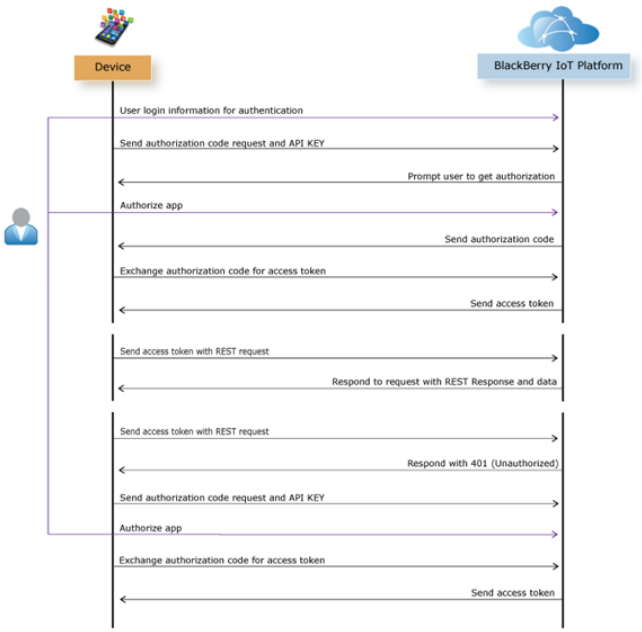
Las aplicaciones que se conecta a la Plataforma de la IO BlackBerry. Puede crear una entidad de aplicación para representar a la aplicación mediante la consola de administración. La Plataforma IoT BlackBerry utiliza la clave y API SECRETOS API de aplicaciones para asegurar y autenticar el software de conexión a la Plataforma IoT BlackBerry.

Cuando las aplicaciones se conectan y se autentica con la Plataforma de la IO BlackBerry introduciendo sus credenciales de inicio de sesión, se asocian con la conexión autenticando al usuario, una entidad de dispositivo se crea la primera vez que usuario inicia sesión en la aplicación. Si un dispositivo integrado se conecta, la entidad dispositivo debe existir, esto habría sido realizado utilizando la consola de administración.

La autenticación gestiona la asociación la autorización y el dispositivo entre una aplicación y la Plataforma IoT BlackBerry. Además, hay un modelo de seguridad que gestiona el acceso de los datos entre los dispositivos de BlackBerry a la Plataforma IoT.

Es importante mencionar que en el dispositivo del usuario, tiene que haber un navegador web disponible para el usuario autorice los permisos a la aplicación. Este escenario utiliza el flujo de código de autorización, como se describe en el OAuth 2.0. En comparación, la autenticación basada en dispositivo no requiere un usuario para participar en el proceso de autenticación. En su lugar, la aplicación utiliza la información almacenada localmente en el dispositivo para identificarse ante la Plataforma IoT BlackBerry. Este escenario de autenticación es útil cuando usted está construyendo aplicaciones que se ejecutan en dispositivos pasivos.

Figura 9 Representación de autenticación basada en el usuario



Fuente: https://docs.iot.blackberry.com/guides/authentication/

7.14 MARCO LEGAL

7.14.1 Ley 59/2003, de 19 de diciembre, de firma electrónica. [1]

La norma regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación. Entre otros aspectos, contiene disposiciones relativas a los prestadores de servicios de certificación sujetos a la ley, firma electrónica, y documentos firmados electrónicamente, empleo de la firma electrónica en el ámbito de las Administraciones públicas, certificados electrónicos, certificados reconocidos, documento nacional de identidad electrónico, dispositivos de firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica.

7.14.2 Directiva 1999/93/CE, por la que se establece un marco comunitario para la firma electrónica [2]

La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica otorga, siempre que se cumplan unos requisitos mínimos en relación con los certificados, los prestadores de servicios de certificación y los dispositivos de creación de firma electrónica, eficacia jurídica equivalente a las firmas electrónica y manuscrita.

Asimismo, la citada Directiva dispone que la Comisión Europea podrá determinar, y publicar en el Diario Oficial de las Comunidades Europeas, los números de referencia de las normas técnicas que gocen de reconocimiento general para productos de firma electrónica, estableciendo una presunción para los productos que se ajusten a dichas normas como conformes con los requisitos de dispositivo seguro de creación de firma electrónica y de producto fiable para un prestador de servicios de certificación.

7.14.3 Reglamento 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014 [3]

Relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Este nuevo Reglamento constituye un paso esencial hacia el Mercado Único Digital. Establece las condiciones para el reconocimiento mutuo de identidades electrónicas entre países de la UE; define reglas para los servicios de confianza, en particular para transacciones electrónicas; y crea un nuevo marco legal para la firma electrónica, los sellos electrónicos, los sellos de tiempo, los documentos electrónicos, los servicios de entrega electrónica certificada, y los servicios de autenticación de sitios web.

7.14.4 Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

Esta Ley, además de modificar algunos preceptos de la Ley 59/2003, incorpora una nueva obligación para determinadas empresas que supone el uso de certificados reconocidos de firma electrónica en las relaciones con sus clientes. (BOE 29-12-2007)

7.14.5 Decisión de ejecución de la Comisión de 17 de marzo de 2014 que modifica la Decisión 2011/130/UE

Por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo, relativa a los servicios en el mercado interior

7.14.6 Ley 24/2001 de Medidas Fiscales, Administrativas y del Orden Social

Incorporación efectiva de las técnicas electrónicas, informáticas y telemáticas a la seguridad jurídica preventiva.

---

[1] GOBIERNO DE ESPAÑA, Agencia Estatal. Normatividad Ley 59/2003, de 19 de diciembre, de firma Electrónica. [En línea] Disponible en: [http://www.boe.es/buscar/act.php?id=BOE-A-2003-23399&p=20140510&tn=2]

[2] MINISTERIO DE INDUSTRIA ENERGÍA Y TURISMO, Telecomunicaciones y Sociedad de la información. Directiva 1999/93/CE, por la que se establece un marco comunitario para la firma electrónica. [En línea] Disponible en: [http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/NormasTecnicas.aspx]

[3]PAE, PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. Disposiciones de la Unión Europea. Firma electrónica. [En línea] Disponible en: [http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_LegUE/pae_NORMATIVA_UE_DISPOSICIONES.html#.VUVigvl_Oko]

8. CONOCIMIENTO GENERAL DE LA ORGANIZACIÓN - ANCERT

La Agencia Notarial de Certificación S.L. Unipersonal (ANCERT), fue constituida en julio de 2002 por el Consejo General del Notariado (C.G.N.) con el objetivo de poner en práctica el ambicioso plan de modernización tecnológica del notariado español (Notarias, Colegios Notariales y C.G.N.).

ANCERT, con sedes en Madrid y Sant Cugat del Vallès (Barcelona), cuenta con más de 190 profesionales, expertos en tecnología y especialistas en el sector financiero y de la Administración Pública, dedicados a la implantación y explotación de los sistemas telemáticos, comunicaciones y firma electrónica para unos 3.000 notarios y 17 Colegios Notariales así como para otros clientes.

ANCERT desarrolla de forma propia y mantiene aplicaciones telemáticas y sistemas basados en el uso de firma electrónica y que están siendo utilizados a diario en las más de 3.000 notarías distribuidas por toda España con una plataforma homogénea de trabajo.

ANCERT dispone de sedes en Sant Cugat (Barcelona) y Madrid.

8.1 MISIÓN

El objetivo de ANCERT es el de modernizar y situar a la vanguardia tecnológica al conjunto de las Notarías de España así como a los diferentes organismos del colectivo notarial.

8.2 ESTRUCTURA ORGANIZACIONAL

Se puede entender a ANCERT desde dos puntos de vista, como institución que hace parte del subsistema del Colectivo Notarial y la otra que explica su organización interna.

8.3 ANCERT DENTRO DEL SISTEMA DEL COLECTIVO NOTARIAL

Ancert dentro de los sistemas del colectivo notarial ayuda a visualizar la extensión de su misión. En la figura 10 se puede apreciar la posición de Ancert dentro del gobierno.

Figura 10 ANCERT como parte la estructura organizativa de la administración pública

Fuente: ANCERT

8.4 ESTRUCTURA ORGANIZACIONAL INTERNA

En cuanto a la estructura interna se puede ver las áreas tecnológicas en las que se desarrolla la actividad de ANCERT.

Figura 1. Estrucura internat de ancert

OPERACIONES	DESARROLLO	EXPLOTACIÓN	SOPORTE Y QA	ADMINISTRAC.
				
Proyectos	Desarrollo	Sistemas	CAU	Finanzas
	Arquitectura	Comunicaciones	Formación	Compras
Negocio	Seguridad Lógica	Gestión y mejora del Servicio	Calidad	RRHH
				Recepción y Servicios Oficina
Dirección de Proyectos	Diseño lógico de aplicaciones	Gestión de infraestructuras tecnológicas	Atención al usuario	Facturación y pagos
Consultoría	Desarrollo de aplicaciones	Gestión de servicios de comunicación	Formación a notarios y trabajadores de notaría	Compras, proveedores y contratos mantenimiento
				Recursos Humanos
Desarrollo de nuevos servicios	Firma electronica	Gestión incidental y mejora del servicio	Calidad de las aplicaciones	Gestión de oficina

Fuente: ANCERT

8.5 PLATAFORMA TECNOLÓGICA ACTUAL

8.5.1 RENO red privada notarial

ANCERT cuenta con una red de comunicaciones denominada RENO (*Rede privada Notarial*) que permite la comunicación y la prestación de servicios corporativos requeridos por los más de 3500 nodos (notarías, Colegios notariales, CGN y Serfides) y las administraciones públicas. Es una VPN gestionada con la más moderna tecnología MPLS (MultiProtocol Label Swiching).

8.5.2 La Firma Electrónica Reconocida (FEREN)

Permite al notario seguir ejerciendo su profesión en el marco de las comunicaciones telemáticas y el comercio electrónico.

ANCERT dispone de una plataforma de hardware que se divide en un sistema distribuido de más de 3.000 servidores ubicados en cada una de las notarías del territorio español complementado por un sistema central de servicios donde se almacena y procesa la totalidad de la información del colectivo notarial.

8.5.3 El servidor PLATÓN (Plataforma tecnológica de Operativa Notarial)

Es el conjunto de elementos hardware instalados en la Notaria, especialmente diseñado para el uso del Sistema Integrado de Gestión Notarial (SIGNO). El servidor Platón es el centro computacional de la notaría. Se integra directamente en la Red Notarial, tiene incorporada la aplicación SIGNO, y es el responsable del procesamiento de todos los trámites telemáticos realizados en el día a día de cada notaría. Pueden usarlo todos los usuarios para los cuales el Notario solicite el acceso a la aplicación SIGNO. Y sus características son:

- Procesador: entre 2 y 4 núcleos.
- Memoria RAM: entre 3 y 8 Gb.
- Fabricante: IMB

Se accede al servidor mediante la autenticación del usuario con tarjeta inteligente, y la seguridad aplicada consiste en el cifrado de los datos almacenados y en un firewall habilitado de forma restrictiva.

Los discos internos del servidor están configurados en RAID-1 (modo espejo), de tal forma que, si sufre una avería en un disco duro, puede continuar trabajando sin afectar al servicio. En estos casos, Ancert se pondrá en contacto con el notario para planificar la asistencia y cambiar el disco averiado.

Además, el servidor Platón realiza una copia de seguridad local en horario nocturno. Opcionalmente, el notario puede contratar, sin coste alguno, un sistema de copia remota de su servidor Platón, mediante la aplicación Copias de seguridad en Ancert, accesible dese la página de inicio del SIC.

Los Servicios Centrales hacen referencia a la infraestructura tecnológica de Ancert que permite ofrecer servicios telemáticos al colectivo notarial. Es el lugar donde se concentran gran parte de los servicios que utilizan simultáneamente notarios y otros colectivos externos. Están ubicados en Sant Cugat del Vallés (Barcelona), y se basan en una plataforma formada por diferentes soluciones tecnológicas de los mejores fabricantes.

La infraestructura informática se basa en componentes de hardware (servidores, discos duros, bases de datos, etc), software base (sistemas operativos, firewalls, antivirus, etc) y redes (cableado, ADSLs, etc) que permite el tratamiento de la información y su intercambio entre los diferentes actores que intervienen en la tramitación telemática de los expedientes notariales (notarios, Colegios Notariales, Administraciones Públicas, etc.).
Dicho de otro modo, es el centro base para el almacenamiento e intercambio de la información que se tramita diariamente en las notarías.

La componen dos tipos de servicios:

- Los de pasarela, que recogen y tratan la información enviada desde las notarías, Colegios Notariales y terceros.

- Los destinados al usuario final, como el Correo Electrónico, la intranet SIC, las webs corporativas e Intranets de los Colegios Notariales, entre otros.

Los servicios SSCC, los utilizan todas las notarías, los Colegios Notariales así como las Administraciones Públicas y privadas competentes (Ayuntamientos, Diputaciones Forales, Registros, Ministerios y Entidades Financieras).

El software que ANCERT ha desarrollado y sigue desarrollando para el colectivo notarial permite a los más de 3.000 Notarios de España, usar procesos integrados y homogéneos de trabajo en sus despachos profesionales.
Estos servicios se ubican tanto en el equipo del cliente (AGN), en servidores dedicados en el despacho notarial (SIGNO) o en SSCC accesibles mediante la WEB y son aprovechados diariamente facilitando al Notario el desempeño de sus funciones, cumplimiento de obligaciones y ampliando sus opciones de negocio.

AGN Gestión Notarial es la herramienta integrada que permite al notario realizar la gestión de su negocio, tanto de la parte pública como de la privada (confección de escrituras, minutación, facturación etc).

8.5.4 Servicios SIGNO

Se trata de un conjunto de aplicaciones informáticas que hacen posible la tramitación telemática entre notarías y Administraciones Públicas. Gracias a esta iniciativa, ciudadanos y empresas se benefician de las enormes ventajas que supone poder realizar en las notarías más de 40 tipos de trámites administrativos en línea, como liquidación de impuestos IBI o ITP y AJD, gestión de sucesiones y donaciones, remisión de información al catastro de inmediata actualización, consulta de deudas de IBI en más de 4.000 ayuntamientos integrados en el sistema, etc.

8.5.5 Base de datos corporativa (DBCORPO)

La Base de Datos Corporativa de Ancert contiene información referente a todo el colectivo notarial. Dicha información es aprovechada por otros servicios telemáticos de Ancert con objeto de facilitar datos de interés a los usuarios, tanto a nivel privado para los notarios como a nivel público para la ciudadanía.

Los diferentes servicios web del colectivo notarial ponen a disposición de los usuarios una serie de herramientas que permiten la explotación de estos datos de forma pública o privada. Principalmente, estos recursos son:

8.5.6 Guía notarial

Una herramienta de uso público (en webs colegiales) y privado (en el SIC) que, en su forma más amplia, permite las siguientes opciones para la obtención de datos:

- Buscador de notarios
- Buscador de documentos notariales
- Juntas directivas
- Localización del CGN y de las sedes colegiales
- Organización de los distritos notariales
- Notarios por poblaciones
- Notarías vacantes

Encuentra a tu notario. Una herramienta de uso público para la localización de notarios.

Directorio Europeo de Notarios. Un recurso creado por el Consejo de Notarios de la Unión Europea para la localización de notarios en nuestro continente. Ancert suministra los datos de los notarios españoles.

Localizador de protocolos. Este recurso, también de uso público, permite averiguar qué notario o sede colegial custodia un protocolo notarial de interés para el ciudadano.

8.6 TIPOS DE CERTIFICADOS CON AVAL NOTARIAL EN ANCERT

8.6.1 PERSONALES

Los Certificados Notariales Personales (CP) permiten a cualquier persona física dotarse de firma electrónica reconocida con la que podran realizar trámites con la administración y en sus tracciones privadas. Los certificados se emiten con las máximas garantías de seguridad ante Notario que realiza todo el proceso de registro. Para garantizar la máxima seguridad de los certificados y el nivel de firma reconocida establecido por la Ley de Firma Electrónica 59/2003 los certificados se entregan en tarjeta criptográfica certificada como dispositivo seguro de creación de firma.

8.6.2 PERSONA JURÍDICA

Los Certificados Notariales Corporativos (CNC) permiten a cualquier empresa, o a cualquier otra forma de persona jurídica, dotarse de firma electrónica reconocida con la que podran realizar trámites con la administración, cumpliendo así con sus obligaciones legales, y en sus tracciones privadas. Los certificados se emiten con las máximas garantías de seguridad ante Notario que realiza todo el proceso de registro. Para garantizar la máxima seguridad de los certificados y el nivel de firma reconocida establecido por la Ley de Firma Electrónica 59/2003 los certificados se entregan en tarjeta criptográfica certificada como dispositivo seguro de creación de firma.

8.6.3 REPRESENTANTE DE PERSONA FÍSICA

Los Certificados Notariales Personales de Representación Personal (CPR) permiten a un represente de una persona física dotarse de firma electrónica reconocida con la que podran realizar trámites con la administración y en sus transacciones privadas actuando en virtud de su representación.

8.6.4 REPRESENTANTE DE PERSONA JURÍDICA

Los Certificados Notariales Corporativos de Representación (CNCR) se emiten a personas físicas en calidad de representantes de personas

jurídicas. Permiten dotar al representante de una sociedad de firma electrónica reconocida con la que poder firmar documentos electrónicamente derivados de su función tanto con la administración como en tracciones privadas entre empresas.

8.6.5 REPRESENTACIÓN DE FUNDACIONES

Este producto es un Certificado Notarial de Corporativo de Representación (CNCR) que se ofrece con una tarifa especial a cargos representantes de fundaciones. Permiten dotar al representante de una fundación de firma electrónica reconocida con la que podran firmar documentos electrónicamente derivados de su función tanto con la administración como en tracciones privadas.

8.6.6 SERVIDOR SEGURO (SSL)

Los Certificados Notariales de Servidor Seguro (CNS) son certificados SSL/TLS emitidos ante Notario que actúa como Autoridad de Registro de ANCERT. La emisión del certificado ante Notario proporcionas las máximas garantías de seguridad en la verificación de toda la información de la titularidad del dominio y de los datos del certificado. Permite asegurar la autenticidad de un sitio web al que se conecta un visitante y ofrecer un canal seguro de comunicación cifrado entre cliente y servidor mediante el uso del protocolo SSL / TLS.

8.6.7 APLICACIÓN SEGURA

Los Certificados Notariales de Aplicación Segura (CNA) son certificados para la actuación automatizada a través de aplicaciones que necesitan firmar electrónicamente o autenticarse ante otras aplicaciones. La emisión del certificado ante Notario proporcionas las máximas garantías de seguridad en la verificación de toda la información de la titularidad de la aplicación y de los datos del certificado.

8.7 TIPOS DE CERTIFICADOS CORPORATIVOS EN ANCERT

8.7.1 EMPRESAS

Los Certificados Corporativos Personales son certificados de firma electrónica avanzada conforme a la Ley 59/2003 de Firma Electrónica dirigidos a empresas que buscan implantar certificados electrónicos en sus procesos internos.

8.7.2 COLEGIOS PROFESIONALES Y OTRAS ENTIDADES

Los Certificados para Corporaciones de Derecho Público son certificados de firma electrónica reconocida conforme a la Ley 59/2003 de Firma Electrónica dirigidos a Colegios Profesionales y otras entidades, con la calificación de Corporación de Derecho Público, que buscan dotar de firma electrónica a sus integrantes. Se pueden usar para la Firma electrónica reconocida de documentos electrónicos o mensajes electrónicos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido.
Los Certificados para Corporaciones de Derecho Público son aceptados para realizar transacciones con la Agencia Tributaria.

8.8 OTROS SERVICIOS

8.8.1 SELLADO DE TIEMPO

Entre el catálogo de servicios como Prestador de Servicios de Certificación ANCERT también actúa como Autoridad de Sellado de Tiempo.

El sellado de tiempo (Time Stamping) es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

Una Autoridad de Sellado de Tiempo (TSA), como ANCERT, actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

La incorporación del sellado de tiempo en los intercambios de datos automatizados permite:

- Proporcionar una prueba fehaciente del momento de creación y alteración de los documentos electrónicos.

- Contiene información sobre los datos y el momento especifico en que el que fue creado, en un mismo paquete firmado.

- Complementar la firma electrónica alargando su período de validez, evitando el repudio del firmante pasado el período de vigencia de su certificado.

- Permite la custodia de documentos a largo plazo.

Ancert es el prestador de Servicios de Sellado de Tiempo para el Consejo General del Notariado. Particulares y empresas también tienen la oportunidad de contratar estos servicios. El servicio de Sellado de Tiempo de ANCERT se encuentra clasificado por el Ministerio de Industria, Energía y Turismo en la categoría de "Servicios de Validación Temporal".

Pasos para generar un sello de tiempo:

- El usuario desea obtener un sello de tiempo para un documento electrónico que él posee.
- Se genera un resumen digital (hash) para el documento en el ordenador del usuario.
- Este resumen conforma la solicitud que se envía a la Autoridad de Sellado de Tiempo (TSA).
- La TSA genera un sello de tiempo con esta huella, la fecha y hora obtenida de una fuente fiable (*) y la firma electrónica de la TSA.
- El sello de tiempo se envía de vuelta al usuario.
- La TSA mantiene un registro de los sellos emitidos para su futura verificación.
- ANCERT emplea una fuente segura de tiempo sincronizada conforme a UTC (Universal Time Coordinated).

El Consejo General del Notariado, a través de ANCERT, actúa como Tercera Parte de Confianza.

El Servicio de Sellado de Tiempo de ANCERT permite la obtención de sellos de tiempo (a usuarios finales y a aplicaciones) conforme a la normativa RFC 3161.

El servicio prestado por ANCERT incluye además de la emisión, la custodia en un repositorio seguro con control de integridad y la validación de los sellos de tiempo.

ANCERT en ningún caso tiene constancia del contenido del documento sellado.

ANCERT emplea una fuente segura de tiempo (Real Observatorio de la Armada) sincronizada conforme a UTC (Universal Time Coordinated).

8.9 DOCUMENTACIÓN LEGAL Y TÉCNICA

POLÍTICA DE CERTIFICACIÓN Y DPCS (ANCERT, 2015): La Política de Certificación y las Declaraciones de Prácticas de Certificación de la Entidad establecen las normas generales y específicas que rigen la emisión de certificados. Las condiciones de uso y emisión establecen sus obligaciones como suscriptor o validador de un certificado emitido por ANCERT.

Desde el 1 de Enero de 2011 todos los certificados emitidos pertenecen a la jerarquía de certificación V2. Para certificados cuya de emisión es anterior a esta fecha, se aplica la documentación de la sección V1.

CERTIFICADOS RAÍZ (ANCERT, 2015): Las cadenas de certificación son necesarias para que las aplicaciones puedan establecer la confianza en los certificados finales. Las cadenas de certificación de ANCERT son de dos niveles jerárquicos y cada una de ellas está compuesta por una Autoridad de Certificación raíz (AC raíz) y una Autoridad Subordinada (AC subordinada) de ésta.

El modelo de certificación se compone de cuatro AC raíz en función del público a quien van dirigidos los certificados finales. CGN para el colectivo Notarial, Certificados Notariales para el público general (particulares y empresas), Redes Privadas (para usos internos empresariales) y Corporaciones de Derecho Público (Colegios Profesional, Administración Pública).

VALIDACIÓN DE CERTIFICADOS (ANCERT, 2015): ANCERT pone a disposición del público general que acepta sus certificados dos métodos de consulta de estado de sus certificados: CRL y OCSP. Ambos servicios se ofrecen abiertos a todo el público y sin costes de acceso. Las direcciones de acceso a los métodos de consulta de estado se encuentran informadas en las extensiones estandarizadas para tal finalidad de todos los certificados emitidos para que las aplicaciones puedan validar automática el estado de los certificados sin intervención del usuario.

8.10 ARQUITECTURA DE SEGURIDAD DE APLICACIONES EN ANCERT

8.10.1 Componentes comunes

- Autenticación y confidencialidad de comunicaciones:
- Reverse proxy (input)
- Proxy out (output)
- Traducción de protocolos (HTTP<->HTTPS)

8.10.2 Plataforma PK

- Generación de firmas electrónicas.
- Verificación de firmas electrónicas.
- Validador de certificados.
- Sellado de tiempo.

8.10.3 Applets de firma

- Firma electrónica en el cliente (sobre navegador web)
- Custodio 2
- Conservación de firmas electrónicas. (XAdES-A)
- Service Dispatcher:
- Punto de entrada centralizado de llamadas a WebServices.WS-Security

8.10.4 Certificados electrónicos

Tipos de certificados:
Cliente: Notarios y empleados
Servidor:

- Ancert como persona jurídica (Ancert CNC)
- Certificados de aplicación (Ancert CNA)
- Firma (application servers)

Históricamente han utilizado “Ancert Security” porque no tenían un certificado específico para aplicaciones homologado.

9. ESTADO DEL ARTE CERTIFICADOS DIGITALES PARA FIRMA EN LA NUBE

La Firma digital como un servicio basado en la nube se ha convertido en un nuevo modelo de solución de ahorro de tiempo y evitar desplazamientos en cuanto a la firma de documentos se refiere. Aunque la teoría detrás de la computación en nube se basa en décadas de las tecnologías e investigaciones existentes, la respuesta entusiasta por parte de los desarrolladores y una amplia aceptación entre los usuarios confirma que el cloud computing puede desempeñar un papel aún más importante como un concepto en muchos campos de la tecnología de la información, incluido el cifrado. Firma digital basada en la nube puede ser vista como un modelo para la práctica, el acceso fiable, en demanda de la red de infraestructura de seguridad que realiza operaciones criptográficas de firma digital.

Se puede decir que el cloud computing, es un modelo de servicio enlazado con tecnología para permitir el cómodo y rápido acceso a los recursos informáticos, aplicaciones y servicios de cualquier entidad.

La firma digital en la nube es uno de los resultados de la transformación criptográfica de datos que adecuadamente implementado, ofrece los servicios de: origen, autenticación, integridad de datos y el no repudio del firmante.

La principal diferencia entre una firma digital de sistema estándar y el basado en la nube es que, mientras que la primera ópera en un medio ambiente "cerca" como un ordenador personal y enchufado en dispositivos dedicados (tarjeta de microchip y tarjeta lector), el sistema basado en la nube implica datos de la red intercambio entre firmante y firma habilitada en la nube, y para lograr este intercambio se plantea la implementación de un protocolo que garantice el intercambio seguro de estos datos y se tracen en un Software como Servicio (SaaS) en la nube que lleva a cabo la firma digital.

9.1 TIPOS DE CERTIFICADOS

9.1.1 CLASIFICACIÓN SEGÚN EL TIPO DE IDENTIDAD

Según este criterio podemos clasificar los certificados electrónicos fundamentalmente en dos:

9.1.1.1 Certificados de Persona Física.

Son los que incorporan la identidad de un sujeto físico o ciudadano. Está orientado a ciudadanos (es decir, a terceros físicos) y están fundamentalmente pensados para trámites personales aunque, en determinadas circunstancias, pueden ser usados en el ámbito profesional.

9.1.1.2 Certificados de Persona Jurídica.

Incorporan una identidad jurídica. Su uso está pensado para todo tipo de organizaciones, ya sean empresas, administraciones u otro tipo de organizaciones, todas ellas con una identidad de tipo jurídico.

9.1.1.3 Certificados de entidad sin personalidad jurídica.

Vinculan a su suscriptor unos datos de verificación de firma y confirma su identidad para ser utilizados únicamente en las comunicaciones y transmisiones de datos por medios electrónicos, informáticos y telemáticos en el ámbito tributario.

9.1.2 CLASIFICACIÓN DE CERTIFICADOS SEGÚN EL ÁMBITO DE APLICACIÓN

Según este criterio encontramos múltiples certificados, que son algunos de los que ofrecen los distintos proveedores de servicios de certificación:

- Certificado de servidor
- Certificado de pertenencia a empresa
- Certificado de representante
- Certificado de apoderado
- Certificado de sello de empresa
- Certificado de Factura Electrónica
- Certificado de Colegiado

9.1.3 CERTIFICADOS SOFTWARE Y CERTIFICADOS HARDWARE

Según este criterio, podemos clasificar los certificados electrónicos en dos categorías:

- Certificados software: Un Certificado electrónico es un documento digital que se puede guardar en una memoria USB, en un ordenador

(en el almacén de certificados) o en el disco duro. A ese Certificado se le conoce como certificado software.

- Certificados hardware: Un certificado también puede estar almacenado en una tarjeta criptográfica, que es una tarjeta que incorpora un chip electrónico. Un ejemplo claro de una tarjeta criptográfica es el DNI electrónico. En estas tarjetas es posible almacenar uno o varios certificados electrónicos, lo que se conoce como certificado hardware.

9.1.4 CERTIFICADOS DE LA LEY 11/2007

La Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos en su capítulo II establece las formas de identificación y autenticación que pueden ser usadas para la identificación de la Administración y de la actuación administrativa. De esos apartados de la Ley y de su reglamento de desarrollo, se derivan los siguientes certificados electrónicos:

9.1.4.1 Certificado de Sede Electrónica

El certificado de Sede es un certificado de Servidor que identifica y autentifica al servidor como Sede Electrónica de una Administración Pública. Las sedes electrónicas, cuando sea necesario, dispondrán de sistemas que permiten el establecimiento de comunicaciones seguras. Además, utilizarán sistemas de firma basados en certificados de dispositivo seguro o medio equivalente para identificarse y mantener una comunicación segura.

9.1.4.2 Certificado de Sello Electrónico

Según la Ley, es el certificado usado para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada. Esto quiere decir que el Sello Electrónico es el que debe usarse para todos los trámites administrativos que se realizan por medios telemáticos, tanto para la identificación de los servidores y la firma de los documentos electrónicos, como para el establecimiento de comunicaciones seguras entre máquinas.

9.1.4.3 Certificado de Empleado Público

Son los certificados que cada Administración Pública puede proveer a su personal para la identificación y autenticación del ejercicio de la competencia de la Administración Pública.

Identifican de forma conjunta al titular del puesto de trabajo o cargo, y a la Administración u órgano en la que presta sus servicios.

9.2 CERTIFICADOS DIGITALES EN UN SERVIDOR CENTRALIZADO

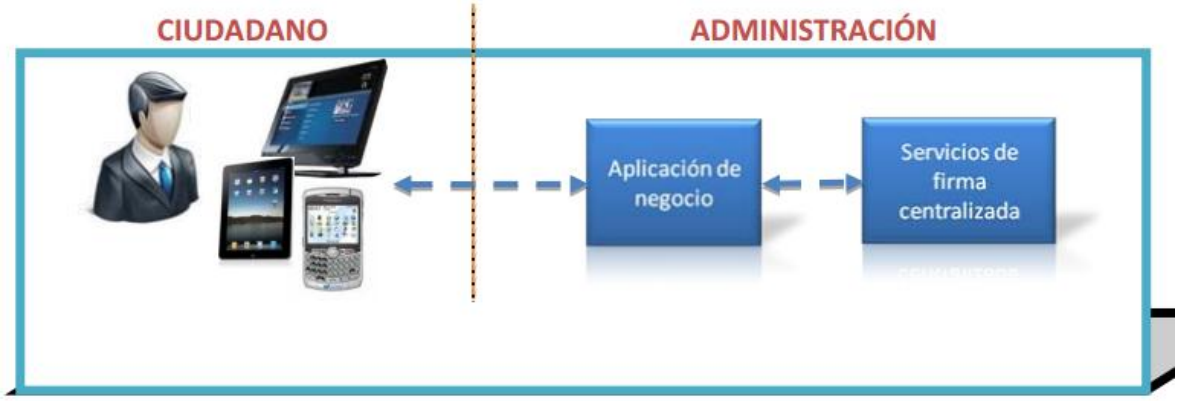
Independiente de la ubicación del sistema de gestión de la firma, los certificados de autenticación se alojan en un servidor centralizado custodiados con fuertes medidas de seguridad.

Para acceder al certificado digital, el titular necesita autenticarse con usuario y contraseña e introducir un código que se usa una sola vez y es enviado como mensaje de texto al mismo teléfono del usuario, es decir que tiene dos niveles de autenticación.

La firma se realiza en el servidor y no en el equipo del usuario.

El ciudadano no tiene que preocuparse de la gestión de los certificados, de esto se encarga la tercera parte denominada entidad de certificación y puede firmar desde cualquier dispositivo.

Figura 11 Esquema de autenticación en servidor centralizado



FUENTE: (Rafael Pérez Galindo)

Para contextualizar un poco más de que se trata este tipo de firma y la seguridad que se debe garantizar es importante mencionar lo siguiente: para crear la solicitud de autenticación del certificado se utilizan los siguientes datos: identificación solicitante, IP de internet, fecha y hora, con esta información el sistema de gestión envía la solicitud al servidor de la autoridad de certificación que contenga el certificado del usuario y se inicia el proceso de autenticación, el sistema autenticador rellena la solicitud de certificado con los datos disponibles y en algunos casos para validar la identidad de las

partes, el sistema de gestión de la entidad certificadora pide al usuario datos adicionales para la verificación de la firma.

Esta automatización de la generación de solicitud de certificado de autenticación minimiza el número de solicitudes de certificados de autenticación malformados. Además, el sistema de gestión del certificado de autenticación es capaz de ser instalado en una base compartida, en el que múltiples servidores y / o múltiples servicios se proporcionan con el certificado de autenticación de una fuente centralizada. El sistema de gestión certificado de autenticación genera automáticamente la fecha de caducidad del certificado de autenticación y también asegura el almacenamiento seguro del par de claves de cifrado que generalmente se basan en el algoritmo criptográfico RSA, así como el certificado de autenticación generado.

Los certificados de autenticación incluyen el uso de un cifrado para el par de claves público-privada con el criptosistema RSA e información clave que distingue y garantiza la identificación precisa del solicitante. El solicitante genera el par de claves de cifrado público-privada RSA, los datos del solicitante se transmiten a la autoridad de certificación, la autoridad de certificación revisa los datos recibidos, verifica la identidad del solicitante y luego emite el certificado de autenticación firmado a la parte solicitante en forma encriptada para su uso en el servidor del solicitante.

9.3 CERTIFICADOS DIGITALES ALOJADOS EN EL NAVEGADOR

Otra forma de validar la firma electrónica es instalando los certificados digitales en el navegador WEB. Estos usan una conexión segura entre el Servidor y el Navegador puede ser usando el protocolo SSL, están firmados por una autoridad de certificación (CA), debe incorporarse el certificado de la CA al navegador.

Para firmar con el certificado que se instala en el navegador del ordenador o dispositivo es necesario que se tenga alguna aplicación que sirva para este fin.

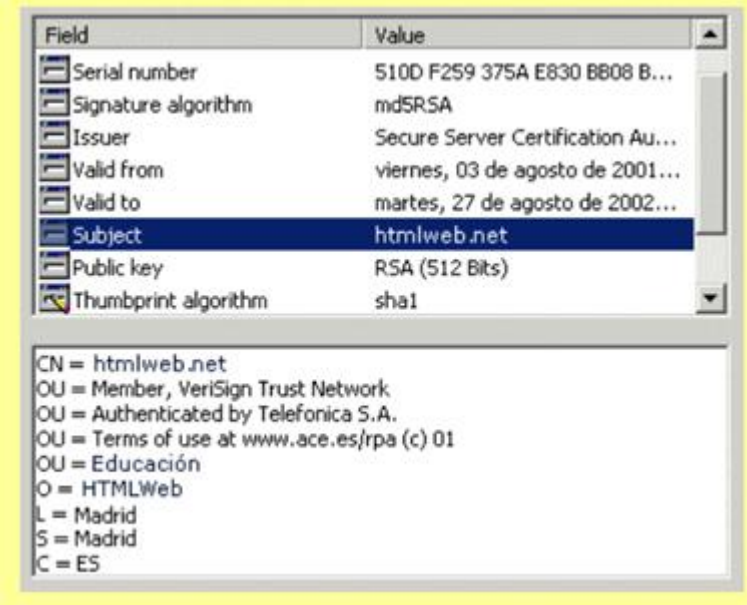
Los datos que figuran generalmente en un certificado de navegador web son:

1. Versión: versión del estándar X.509
2. Número de serie: número identificador del certificado, único para cada certificado expedido por una AC determinada.
3. Algoritmo de firma: algoritmo criptográfico usado para la firma digital.
4. Autoridad Certificadora: datos sobre la autoridad que expide el certificado.

5. Fechas de inicio y de fin de validez del certificado. Definen el periodo de validez del mismo, que generalmente es de un año.
6. Propietario: persona o entidad vinculada al certificado. Dentro de este apartado se usan una serie de abreviaturas para establecer datos de identidad.

Por ejemplo: CN nombre común del usuario, OU información varia, O organización, L ciudad, S estado (provincia), C país, E correo electrónico, UID ID de usuario.

Figura 12 Certificado digital de navegador



FUENTE: (Moreno, 2003)

7. Llave pública: representación de la llave pública vinculada a la persona o entidad (en hexadecimal), junto con el algoritmo criptográfico para el que es aplicable.
8. Algoritmo usado para la misma para obtener la firma digital de la Autoridad Certificadora.
9. Firma de la Autoridad Certificadora, que asegura la autenticidad del mismo.
10. Información adicional, como tipo de certificado, etc.

El certificado Digital vincula a una persona o entidad con una llave pública, y mediante el sistema de firma digital se asegura que el certificado que

recibimos es realmente de la persona que consta en el mismo. El sistema de firma digital liga un documento digital con una clave de cifrado.

9.4 VALIDACIÓN DE LA FIRMA ELECTRÓNICA

Las validaciones de firmas electrónicas se orientan a dos tipos:

1. Entidades. Para la cual debe implementarse un webservice que realiza validaciones de firmas electrónicas avanzadas con las diferentes soluciones de firma comerciales.

2. Ciudadanos. Para la cual debe implementarse una aplicación de acceso que permita a los ciudadanos validar las firmas electrónicas avanzadas.

9.4.1 WEBSERVICE DE VALIDACIÓN DE FIRMA AVANZADA

La entidad certificadora debe implementar un webservice ojala basado en XML, en este caso ANCERT debe alojarlo en su propia infraestructura de servidores, donde los diferentes notariados adquieran el servicio web de validación de firma avanzada para los diferentes documentos notariales. La invocación al webservice se realizará utilizando un certificado en la aplicación comercial de firma electrónica, que permitirá identificar a la entidad o notariado demandante del servicio. Es recomendable que el servicio web tanto de ANCERT como de las aplicaciones comerciales, y los mismos servicios del notariado estén securizados con certificados SSL para que establezcan canales seguros de comunicación entre los ciudadanos y los servicios de las diferentes partes actuantes en el proceso.

9.4.2 CAPA DE CONEXIÓN SEGURA SSL

Encriptación SSL: SSL significa "Secure Sockets Layer". SSL Definición, Secure Sockets Layer es un protocolo diseñado para permitir el intercambio de información segura entre aplicaciones, establece un canal seguro entre las partes. Las aplicaciones que utilizan el protocolo Secure Sockets Layer están diseñadas para dar y recibir claves de cifrado con otras aplicaciones, así como cifrar y descifrar los datos enviados entre los dos.

9.4.3 FUNCIONAMIENTO DEL SSL

Algunas aplicaciones que están configuradas para ejecutarse con el protocolo seguro SSL incluyen navegadores web como Internet Explorer y Firefox, los programas de correo como Outlook, Mozilla Thunderbird, Mail.app de Apple, y SFTP (Secure File Transfer Protocol) programas, etc. Estos programas son capaces de recibir de forma automática SSL conexiones.

El webservice deberá realizar como como mínimo lo siguiente:

- Validará si la entidad propietaria del certificado (entidad notarial) tiene permiso de uso del servicio.
- Realizará la validación de la firma avanzada del documento o texto.
- Registrará el uso en las estadísticas de uso.

La aplicación de firma deberá validar como mínimo:

La aplicación solicitará el XML que contiene el documento y la firma avanzada con la aplicación autorizada devolviendo la siguiente información:

- Resultado de la validación de la firma, es decir los datos del firmante (nombre y apellidos, DNI, teléfono etc.)
- Datos de validación de la firma.
- El documento o texto firmado.

9.4.4 PROTOCOLO OCSP

Este protocolo se describe en el RFC 2560 (IETF, 1999) y especifica un método para determinar el estado de revocación de un certificado digital x.509 usando otros medios que no sean por el uso de CRL (Listas de Revocación de Certificados).

Los mensajes OCSP se codifican bajo la notación ASN.1 y por lo general se transmiten sobre el protocolo HTTP. Se conocen como servidores OCSP aquellos con peticiones y respuestas OCSP.

Una de las ventajas que presenta OCSP frente a CRL es que mientras más tiempo pase sin actualizarse una CRL, se hace menos confiable la información que nos brinde, porque pueden haberse revocado algunos certificados entre actualizaciones, este hecho también demuestra que para el uso se requiere de conexión con el “OCSP responder”. Otro punto de vista de comparación entre OCSP y CRL es el ancho de banda, mientras la curva que describe el uso del ancho de banda contra el número de peticiones es logarítmica en el caso de CRL, para OCSP es de tipo exponencial.

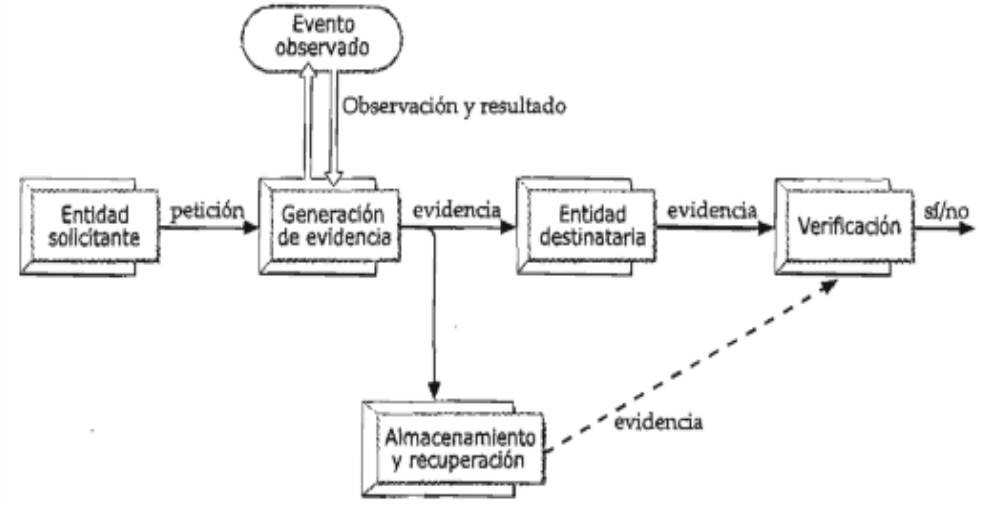
9.5 GENERALIDADES SOBRE EL SERVICIO DE NO REPUDIO

Para (Carracedo Gallardo, 2004) es un servicio que sirve para proteger a los usuario de las redes telemáticas contra el hecho que alguien niegue falsamente haber participado en algún evento u acción que haya tenido lugar. Dentro se destaca tres ámbitos de comunicación que hay necesidad de este tipo de servicio:

1. en las relaciones comerciales y contractuales a través de redes telemáticas resulta imprescindible que se puedan establecer garantías sobre la autoría de un documento.
2. en las relaciones de las administraciones públicas con los ciudadanos, las prácticas consagradas por la costumbre y respaldadas por el ordenamiento jurídico dan una gran importancia, en multitud de actos administrativos, a la obtención de justificantes que avalen el haberlo llevado a cabo.
3. en las relaciones personales a través de las redes telemáticas también pueden ser necesarias algunas de las garantías.

Según (Carracedo Gallardo, 2004) define el servicio diciendo que consiste en la generación, verificación y almacenamiento de evidencias que puedan decir de pruebas (demostrables ante terceros) para garantizar que un determinado evento u acción ha sucedido, dicho proceso se puede observar en la figura 13.

Figura 13 proceso de generación y verificación de evidencias.



Fuente: (Carracedo Gallardo, 2004)

9.5.1 Diferentes tipos de no repudio

En la norma ISO/IEC 7498-2 *Security Architecture* se distinguen solamente dos tipo de servicio de no repudio (de origen y de entrega), clasificación que se mantiene, ligeras variantes, en la ISO/IEC 10181-4 (ITU-T X.813). Para (Carracedo Gallardo, 2004) amplia más los tipos de no repudio.

1. No repudio de Origen (Non-Repudiation of Origin)
2. No repudio de Envío(Non-Repudiation of Sending)
3. No repudio de Depósito (Non-Repudiation of Submission)

4. No repudio de Trasporte (Non-Repudiation of Transport)
5. No repudio de Entrega (Non-Repudiation of Delivery)
6. No repudio de Creación (Non-Repudiation of Creation)
7. No repudio de Conocimiento (Non-Repudiation of Knowledge)

9.6 ESTRUCTURAS DE LA FIRMA

9.6.1 CAdES (CMS Advanced Electronic Signatures)

Es la evolución del primer formato de firma estandarizado. Es apropiado para firmar ficheros grandes, especialmente si la firma contiene el documento original porque optimiza el espacio de la información. Tras firmar, no podrás ver la información firmada, porque la información se guarda en forma binaria.
Es un conjunto de extensiones de datos firmados con sintaxis de mensajes criptográficos (CMS) por lo que es adecuada para la firma electrónica avanzada.

Mientras el formato CMS es un marco general para firmar documentos digitalmente, tales como E-Mails (S/MIME) o PDF, CAdES específica perfiles precisos de datos firmados con CMS para su uso con firma electrónica avanzada en el marco de la Directiva Europea 1999/93/CE.

Un beneficio destacado del formato CAdES es que los documentos firmados electrónicamente pueden seguir siendo válidos durante largos períodos.
El principal documento que describe este formato es el ETSi TS 101 733 Firma Electrónica e Infraestructura (ESI) - CMS Adavanced Electronic Signature, dicho formato tiene definidos 6 perfiles diferentes, según el nivel de protección ofrecido. Cada perfil incluye y mejora al anterior, la descripción de cada perfil se puede observar en la tabla 1.

Tabla 1 detalle de las diferentes versiones de CAdES

CAdES	Forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada
CAdES-T (*time stamp*)	Se le incorpora información el campo de sello de tiempos para proteger los datos de un posible repudio
CAdES-C (*complete*)	Es un CAdES-T al que se le añade referencias sobre los certificados y listas de revocación y listas de revocación utilizadas para permitir la validación en el futuro (sin almacenar los datos actuales de verificación)

CAdES-X	Es un CAdES-C al que se le añade información sobre la fecha y hora de los datos introducidos para la extensión C.
CAdES-X-L (*extended long-term*)	Es un CAdES-X al que se le incorporan los certificados (sólo clave pública) y las fuentes de validación que se usaron. Garantiza la validación *off-line* a largo plazo incluso si la fuente original no estuviera disponible.
CAdES-A (*archivado*)	Este formato incluye toda la información anterior pero incluye meta-información asociada a políticas de refirmado. Una política de refirmado establece un periodo de caducidad de la firma digital, y superado este tiempo, se procede a un refirmado. El escenario ideal para este formato de firma son aquellos documentos cuya validez sea muy elevada: hipotecas, títulos universitarios, escrituras, etc. 15, 20, 50 años, etc.

fuente viafirma

Acorde con la Tabla 1 detalle de las diferentes versiones de CAdES el formato extendido CAdES-C incorpora dos atributos:

1. Complete-certificate-references: contiene referencias a todos los certificados de las cadenas de confianza necesaria para verificar la firma.
2. Complete-revocation-references: contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de la firma.

El formato CAdES-X Long además de la información incluida en CAdES-C, incluye dos nuevos atributos certificate-values y revocation-values que incluyen:

1. Referencias a la información de validación.
2. Cadena de confianza completa.
3. CRL o respuesta OCSP obtenida en la validación

En el caso que se desee incorporar a la firma esta información de validación, la validación mediante OCSP favorece la obtención que las propiedades certificate-values y revocation-values son de menor tamaño.

Por tanto, según el tipo validación, se recomienda el uso de los siguientes formatos:

1. En el caso que la validación se realice mediante consulta OCSP: los formatos CAdES-X Long type 1 o CAdES-X Long type 2, que añaden

un sellado de tiempo a la información incluida en una firma CAdES-X Long. En este caso se incorporan los atributos certificatevalues y revocation-values puesto que la respuesta a una consulta OCSP no ocupa mucho espacio.

2. En el caso que la validación no pueda realizarse mediante OCSP y se realice mediante consulta a una CRL: los formatos CAdES-X type 1 o CAdES-X type 2, que incluyen un sellado de tiempo a la información incluida en una firma CAdES-C, es decir, a las referencias a las CRL consultada y los certificados de la cadena de confianza. No se recomienda incluir los atributos certificate-values y revocation-values ya que pueden ser muy voluminosos.

En el caso que se esté próximo a la caducidad del sello de tiempo añadido para construir la firma longeva, se puede transformar la firma CAdES-X Long type 1 o CAdES-X Long type 2, en una firma CAdES-A, añadiendo un sellado de tiempo de archivo a la firma anterior.

9.6.2 XAdES (XML Avanzado)

Dentro del formato de firma XAdES, el formato extendido XAdES-C incorpora dos propiedades no firmadas:

1. CompleteCertificateRefs: contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma, excepto el certificado firmante.
2. CompleteRevocationRefs: contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de los certificados.

En el caso que se desee incorporar a la firma esta información de validación, se recomienda utilizar el formato XAdES-X, que añade un sello de tiempo a la información anterior.

El formato XAdES-X, que añade un sello de tiempo a la información anterior.
El formato XAdES-XL, además de la información incluida en XAdES.X, incluye dos nuevas propiedades no firmadas: CertificateValues y RevocationValues que incluyen:

1. Referencias a la información de validación.
2. Cadena de confianza completa.
3. CRL o respuesta OCSP obtenida en la validación.
4.

En el caso que se desee incorporar a la firma esta información de validación, se recomienda usar el formato XAdES-A, que añada un sello de tiempo a la información anterior. En este caso se recomienda usar validación mediante

OCSP, ya que mediante este método las propiedades CertificateValues y RevocationValues son de menor tamaño.

9.6.3 PAdES (PDF Avanzado)

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. Con los formatos anteriores esto no es posible si no se utilizan herramientas externas.

En caso de forma PAdES, la guía de aplicación de la norma técnica de interoperabilidad de política y de certificados de la administración recomienda el uso del formato PAdES-Long Term e igual que en los casos anteriores recomienda usar validación mediante OCSP, ya que el tamaño de la información de validación a añadir es menor.

Además se podría añadir un sello de tiempo que incluyese dicha información de validación, ya que la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva.

9.6.4 OOXML

Formato de firma que utiliza Microsoft Office.

9.6.5 ODF

Formato de firma que utiliza Open Office.

9.7 FIRMAS DIGITALES COMO SERVICIOS EN LA NUBE

El creciente desarrollo de la computación en la nube ha permitido que empresas y personas utilicen el hardware, almacenamiento y software de terceras partes también llamados proveedores de la nube sobre el cual corren su propia infraestructura de computación para (Singh & Bansode, 2015) los usuarios de la computación en la nube puede esperar los siguientes beneficios:

1. Escalabilidad
2. Disponibilidad, confiabilidad y acceso global
3. Mantenibilidad

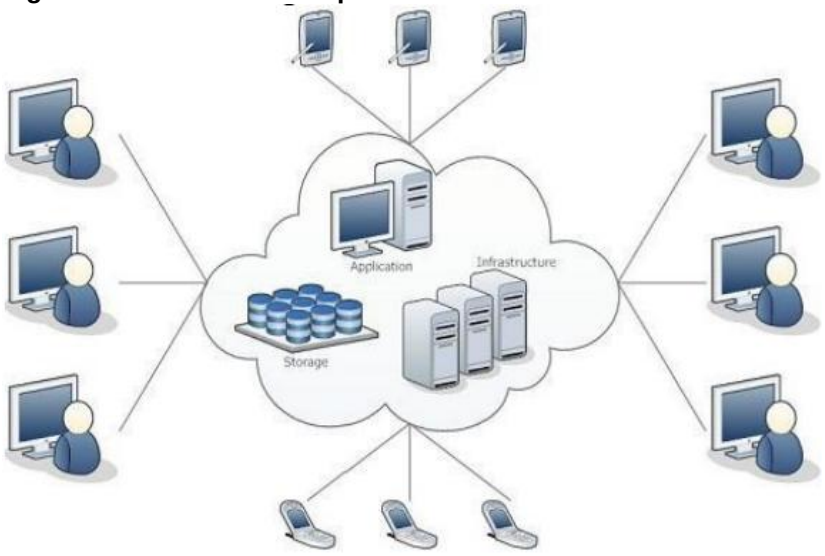
Entre los participantes en este modelo (Singh & Bansode, 2015) define:

1. proveedor de la nube (Cloud Provider)
2. consumidor de la nube (Cloud Consumer)
3. Cloud Broker es una entidad que es intermediario entre los proveedores de la nube y los consumidores de la nube. El objetivo de un servicio de intermediación es proveer al consumidor un servicio que sea más ajustado a sus necesidades.
4. Cloud Auditor un auditor de la nube es una parte independiente quien examina una pila de servicios de la nube para proveer una valoración sobre la seguridad, privacidad y su nivel de disponibilidad de los correspondiente servicios en la nube.

Acorde con el modelo de implementación y el nivel de aislamiento, (Singh & Bansode, 2015) menciona que las nubes pueden ser algunas de las siguientes 4 categorías:

1. Public Cloud: una nube pública es una nube que su infraestructura es compartida por muchos consumidores sin verificar.
2. Private Cloud: sí la infraestructura de una nube está dedicada para una organización específica.
3. Community Clouds: son nubes en el que sus servicios son accesibles para un conjunto particular de organizaciones las cuales forman una comunidad.
4. Hybrid Clouds: es una composición de dos o más tipos de nubes.

Figura 14 Modelos de computación en la nube



Fuente: (Singh & Bansode, 2015)

En contextualización al tema de firmas para poder implementar una firma electrónica como un servicio en la nube (Kinastowski, 2013) menciona algunos requerimientos básicos para los sistemas firmas electrónicas basadas en la nube, entre estos requerimientos el autor define:

9.7.1 La seguridad

Para el sistema de firma digital basado en la nube, (Kinastowski, 2013) se refiere al simple hecho de brindar protección a las llaves privadas de los usuarios sí que sean recuperados y/o utilizados sin autorización. Otras amenazas que menciona el autor (Kinastowski, 2013) están relacionadas con el uso no autorizado de la clave privada en el interior del sistema, que puede ser afectado por una modificación de los datos enviados por firmar (ataque en los datos) o ser suplantado en línea (ataque de suplantación).

Teniendo en cuenta lo anterior el autor (Kinastowski, 2013) identifica dos grandes grupos de amenazas: que el sistema pueda verse comprometido por las amenazas del software de apoyo (incluyendo el sistema operativo, navegador web, servidor web, servidor de base de datos, etc.). El otro grupo de riesgo está directamente relacionado con las vulnerabilidades en los protocolos y procedimiento (amenazas directas) del sistema, estas pueden ocurrir en cada componente del sistema y en cada etapa del proceso.

9.7.2 La usabilidad

LA ISO (ISO, s.f.) define usabilidad como “La medida en que un producto puede ser utilizado por los usuarios especificados para alcanzar los objetivos específicos con efectividad, eficiencia y satisfacción en un contexto de uso.” el autor (Kinastowski, 2013) menciona la creencia de que la alta usabilidad es siempre en desacuerdo con el requisito de alto nivel de seguridad.
El autor (Kinastowski, 2013) propone un método radical para garantizar una alta usabilidad, eliminando dispositivos dedicados para firma digital (tarjetas de microchip, lectores de tarjetas. además que mediante la transferencia lógica de procesamiento con el proveedor de la infraestructura y proporcionar una interfaz de acceso simple, el proceso de firma digital puede ser reducido a la autenticación estándar y la transferencia segura de datos.

9.7.3 Cross-Platform y capacidad de integración

A fin de que cualquier tipo de sistema digital pueda ser considerado multiplataforma, debe ser capaz de operar en cualquier configuración de hardware y software. El hardware dedicado en soluciones de firma digital convencional impone requisitos del sistema obligatorio. Hace que portar el sistema a la nueva plataforma (por ejemplo, dispositivos móviles) sea muy complicado. También hace que sea difícil de integrar los servicios de firma

digital con otros servicios electrónicos. El autor (Kinastowski, 2013) propone que se debe proporcionar una interfaz de servicios de firma digital a través de protocolos de red estándar tiene capacidades multi-plataforma, tanto a nivel de hardware y software. Transferencia de la lógica de procesamiento en nube también ofrece grandes oportunidades para la integración con otros servicios electrónicos que residen en la nube.

9.7.4 Entidades básicas del protocolo para firma electrónica:

(Kinastowski, 2013) identifica cuatro entidades básicas de protocolo:

9.7.4.1 Firmante

Es el cliente del servicio de la firma, cuya clave privada se restaura en la nube en el proceso de firma digital. Teniendo en cuenta la complejidad del proceso de firma digital, los requisitos del sistema para los firmantes non mínimos. Abarcan un dispositivo móvil con una tarjeta SIM activa y con acceso a internet. Estos requisitos muy básicos permiten el procesamiento.

9.7.4.2 Emisor

El emisor es una entidad que posee o crea datos firmados por el firmante en el proceso de firma electrónica. El modelo más básico, sume que el emisor y el firmante son el mismo usuario. Sin embargo, debe tenerse en cuenta que existen más modelos complejos que definen la separación de estas funciones y pueden ser presentados de forma independiente.

9.7.4.3 Proxy

Proporciona la interfaz para el servicio de firma digital en la nube. El dispositivo consiste en un único servidor o un grupo de servidores con el software que soporta el protocolo de comunicación HTTP, sistema de gestión de base de datos y aplicaciones dedicadas. El papel del servidor proxy se reduce a la gestión y el seguimiento de acceso de los usuarios a un módulo de seguridad de hardware (HSM), donde se implementan las operaciones criptográficas de firma basada en la nube. La gestión de procesos incluye la autenticación del usuario, así como la recolección y de formato de datos enviados al HSM.

9.7.4.4 Módulo de seguridad de hardware

El HSM es un dispositivo con una función de criptoprocesador seguro dedicado a la gestión de claves criptográficas y llevar a cabo operaciones criptográficas de firma digital basada en la nube.

El HSM certificado por NIST (National Institute of Standards and Technology, 2013) se considera-resistente a la manipulación, por lo que se supone que el

medio ambiente de esta entidad de protocolo seguro tanto en la capa física y lógica. Como se mencionó anteriormente, el modelo básico de servicio de la firma basada en la nube supone que la firma del firmante de datos que posee. El modelo describe la interacción de las tres entidades (Firmante / Emisor, Proxy y HSM). Firmante / Emisor y proxy se comunican con el protocolo HTTP. Con el fin de proporcionar un mayor nivel de seguridad, esta comunicación debe hacerse por un canal TLS seguro. HSM puede conectarse al Proxy como un dispositivo integrado (por ejemplo, dispositivo PCI) o residir como un servidor de cifrado independiente. La configuración detallada del entorno de nube (Proxy y HSM) está más allá del alcance de este documento.

9.7.5 Complementos de protocolo de firma electrónica

El usuario, en adición al nombre de identificador único y contraseña, tiene un teléfono móvil con la tarjeta SIM activa y número de teléfono correspondiente. Este dispositivo para recibir mensajes de texto, enviados desde el sistema de firma, que contiene el valor de la contraseña de una sola vez (OTP).

En orden de firmar documentos, los siguientes son los pasos propuestos por (Kinastowski, 2013)

1. El usuario se conecta al proxy y se pre-autentica. A fin de mantener el protocolo lo más simple posible, firmante utiliza solo una contraseña en el sistema. Aunque el proceso de pre-autenticación se utiliza principalmente para la identificación del número de teléfono, utiliza la misma contraseña que protege la llave privada de los usuarios. es por eso que los requisitos de seguridad para este proceso deben estar flexibles, por ejemplo, mediante el uso de funciones *collision-rich* (Christianson & Malcolm, 2010). Otra idea es permitir a los clientes comprobar la validez de autenticar a los servidores mediante *zero-knowledge proofs* como lo describe (Feige, Fiat, & Shamir, 1998).

2. El servidor identifica el número del móvil del usuario autenticado e inicia el proceso de proveer el código de única vez (OTP).

3. El usuario descarga el software, necesario para el protocolo de comunicación, como un sitio web dinámico. Usando un algoritmo de implementación de generación, una especificación formal se puede observar en la figura 15.

Figura 15 Generación de la clave y documento

$$\widehat{doc} = Sym^{enc}_{Gen(pass|OTP)}(doc)$$

$$\widehat{pass} = Asym_{k^{hsm}_{pub}}(pass)$$

Fuente :(Kinastowski, 2013)

Posteriormente se envía el nombre de usuario, el documento y clave generada hacia el proxy.

4. El proxy envía la contraseña y el documento generado recibidos del usuario junto con la clave del usuario y lo establece para la autenticar al usuario en el módulo de seguridad (HSM).

5. HSM restaura la contraseña generada, el documento generado y el código OTP como se puede apreciar en la figura 16:

Figura 16 Restauración de datos recibidos de parte del proxy

$$pass = Asym_{k^{hsm}_{prv}}(\widehat{pass})$$

$$OTP = Gen_{OTP}(\hat{k}^{user} \parallel OTP_{secret})$$

$$doc = Sym^{dec}_{Gen(pass|OTP)}(\widehat{doc})$$

$$k^{user}_{prv} = Sym^{dec}_{Gen(pass)}(\ Sym^{dec}_{K}(\hat{k}^{user}))$$

Fuente :(Kinastowski, 2013)

La operación confirma la integridad y la autenticidad del documento y la validez de la contraseña de única vez.

6. El módulo de seguridad de hardware (HSM) firma el documento usando la llave privada del usuario, protege los datos de firma, como se puede apreciar en la especificación de la figura 17.

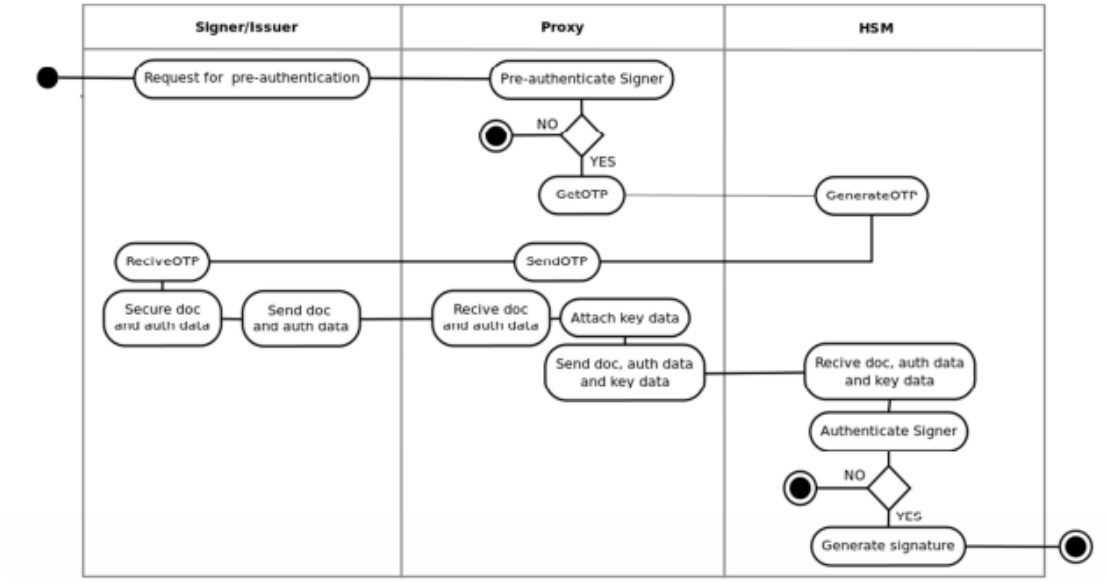
Figura 17 firma del documento

$$doc_{sign} = Sign_{k_{priv}^{user}}(doc)$$

Fuente : (Kinastowski, 2013)

El diagrama de la figura 18 da una entendimiento global acerca del proceso de firma.

Figura 18 Diagrama de actividades del proceso de firma

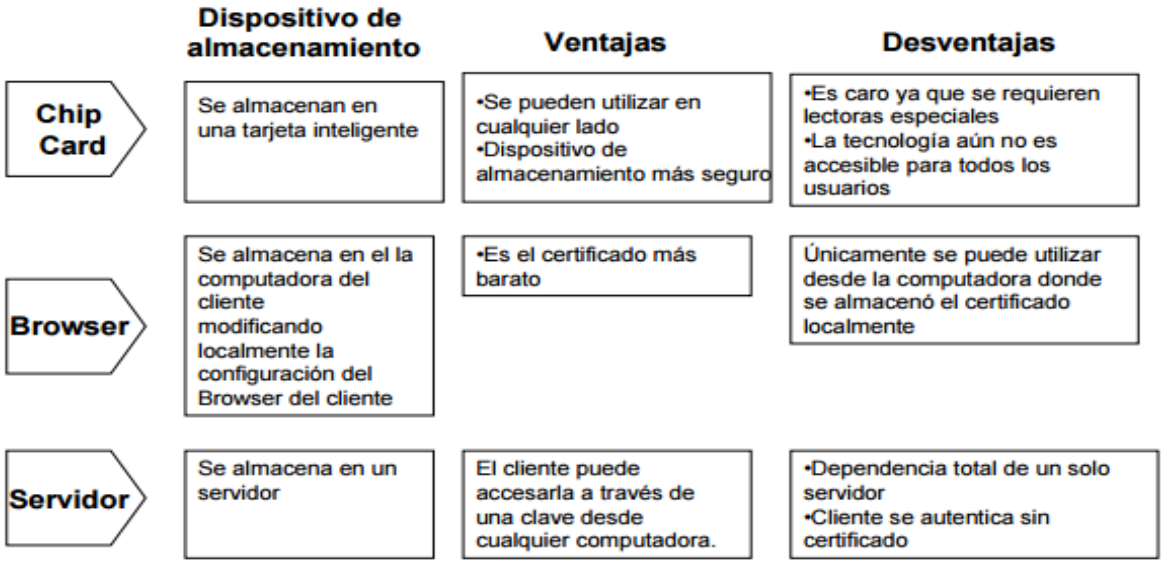


Fuente :(Kinastowski, 2013)

9.8 DISPOSITIVOS FÍSICOS PARA EL ALMACENAMIENTO DE CERTIFICADOS DIGITALES

Existen diferentes dispositivos para el almacenamiento de certificados, desde certificados personales hasta certificados de autoridades certificadoras.

Figura 19 Dispositivos físicos de almacenamiento de certificados



Un Smart Card o Chip Card es un dispositivo con forma de tarjeta de crédito con un chip en su interior. Un Smart Card requiere de un lector para poder hacer uso de él.

La clave privada (PKI) de un usuario puede ser almacenada en un Smart Card donde internamente todas las funciones criptográficas se realizan, incluyendo firma digital, y descripción de las claves de sesión. Las Smart Cards son pequeñas, fáciles de transportar y difíciles de replicar. Las aplicaciones que usan esta tecnología van desde identificación de telefonía móvil a controles de televisión por satélite. Las Smart Cards tienen sus desventajas como los demás productos. Conectar los lectores a los sistemas puede consumir mucho tiempo. Un estudio realizado por militares de Estados Unidos indica que aproximadamente se instala y configura un lector en 30 min. Otra opción para almacenar la clave privada pudieran ser los Smart Tokens.

Los Smart Tokens usan una tecnología idéntica a las Smart Cards, con la diferencia de su forma y su interfase. Los Smart Tokens son del tamaño de una clave de auto o de la casa y usan el Universal Standard Bus (USB) como interfase. Los Smart Tokens basados en USB dan ventajas en los escenarios de IT. Los lectores no son necesarios dado a que los smart tokens se conectan directamente a los puertos USB que se encuentran en la mayoría de los sistemas de cómputo actuales. De todos los dispositivos de autenticación, los llamados “Smart” son los que son aceptados y usados para su integración con aplicaciones PKI dado a que pueden dar autenticación “siempre activa”.

Para las Agencias Certificadoras, existen las **tarjetas de almacenamiento de certificados**, de tal manera que el certificado se almacena dentro de la tarjeta y no en el disco duro. El certificado digital se respalda en dos “Smart Cards” o “Tokens” de una manera que el certificado se divide dentro de los dispositivos para que el certificado no sea almacenado o custodiado por una sola entidad.

10. PRODUCTOS COMERCIALES PARA LA IMPLEMENTACIÓN DE FIRMAS ELECTRÓNICAS

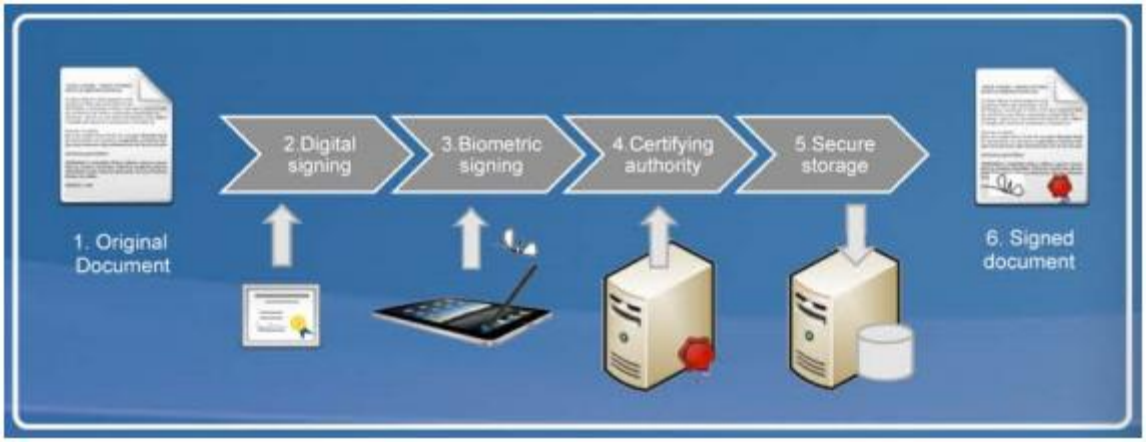
10.1 MOBBSIGN

Es una aplicación MobbSing permite firmar documentos utilizando la firma manuscrita, con validez legal, desde un dispositivo móvil (ipad, tablets, smartphones).

Funcionamiento

El dispositivo recibe el documento, donde el usuario utiliza su firma manuscrita para firmarlo. Las características biométricas de la firma se encriptan y almacenan dentro del documento. Una vez ha sido enviado al servidor, el documento es firmado digitalmente por una autoridad certificadora para asegurar la integridad del documento, esto se puede observar en la figura 19.

Figura 20 proceso de firmado y autenticado con Mobbsign



Validez legal

La validez legal de la firma biométrica del documento se logra a través de dos procedimientos:

- La identidad del autor del documento puede ser determinada manualmente (por un experto) o automáticamente, con un alto nivel de certeza.
- La firma se encuentra incrustada en el documento y no puede eliminarse, excepto por mandato judicial.

10.1.1 Plataformas que soporta

La aplicación móvil está disponible para iOS, Android, Windows Phone y Windows Store (smartphones y tablets).

10.2 VIAFIRMA MOBILE

Es una aplicación cliente de la plataforma de autenticación de firma electrónica de la empresa española Viafirma. A través de Viafirma Mobile SDK, las aplicaciones móviles nativas pueden integrarse con el cliente de firma electrónica móvil Viafirma Mobile y con Viafirma Platform, permitiendo ofrecer a sus usuarios autenticación y firma electrónica avanzada.

La solución de Viafirma Mobile permite incluir autenticación y firma electrónica con certificados digitales software (en formato PKCS#12) o incluso smartcards en aplicaciones web o aplicaciones móviles nativas. Por ello, resulta sencillo "movilizar" cualquier aplicación web que ya en la actualidad tenga firma electrónica.

10.2.1 Funcionamiento

Esta aplicación permite hacer uso de los certificados digitales del cliente previamente instalados en el dispositivo y utilizarse con aquellas aplicaciones web que ya usen los servicios de autenticación y firma electrónica de Viafirma.

10.2.2 Soporte de formatos de firma

CMS/PKCS#7, XMLDSig, XAdES (llegando a los perfiles de firma longeva como X-L o A), PDF Signature, PAdES, etc.

10.2.3 Plataformas que soporta

Actualmente se soporta la firma electrónica en dispositivos Apple iOS (como iPhone 3G, iPhone 3GS, iPhone 4, iPad, iPod Touch, etc.), Android, Windows Phone 7 y BlackBerry.

10.3 @FIRMA, PLATAFORMA DE VALIDACIÓN Y FIRMA ELECTRÓNICA

@firma es la solución tecnológica en la que se basa la implementación de la Plataforma de validación y firma electrónica del Ministerio de Hacienda y Administraciones Públicas. Es una solución basada en software libre, estándares abiertos y en java: servidores web Apache, JBOSS, Sistema Operativo Linux, AXIS, etc.

10.3.1 Cliente@Firma Móvil.

Esta aplicación es Integrable de forma transparente para los usuarios del Miniapplet. (BETA). Necesario uso del servidor intermedio (Proxi ClienteMovil). Disponible para plataformas: Android 4.0 y posteriores, iOS 6 y posteriroes, y Windows RT y 8 con interfaz de nueva generación.

Permite la realización de firma electrónicas para la realización de trámites desde el navegador Web de su dispositivo, en las páginas Web compatibles con el Cliente @firma.

10.3.1.1 Características

Debe disponer de un certificado reconocido de firma electrónica con su respectiva clave privada instalado en su dispositivo Android. Consulte con la documentación de su sistema operativo y con su proveedor de servicios de certificación para la obtención de este certificado figura 20 y el modo de instalación de este.

Figura 21. Tipos de certificados a escoger

Fuente : playstore de Google ®

10.3.2 Portafirmas

Portafirmas es el aplicativo móvil de Ministerio de Hacienda y Administraciones Públicas para acceder a sus servicios de portafirmas. Desde este aplicativo móvil se podrá:

- Acceder a las solicitudes de firma que tiene pendientes y las que ya ha atendido.
- Filtrar sus listados de solicitudes.
- Revisar los documentos que debe firmar.
- Aprobar las solicitudes que necesitan su visto bueno.
- Firmar las solicitudes pendientes.

El acceso al servicio se realiza mediante autenticación con certificado para mayor seguridad.
Deberá ser usuario de Portafirmas para hacer uso de esta aplicación.

Es decir que portafirmas esta mayormente dedicada a la infraestructura de seguridad y gestión de identidades, Servicios horizontales para las AA.PP y Soporte a la tramitación electrónica para las entidades estatales.

10.4 SOLUCIÓN CAMERFIRMA GESTIÓN DE CLAVES CENTRALIZADA

Carmerfirma se basa en servicios de firma electrónica avanzada con almacenamiento centralizado, esto implica que la posibilidad de que un usuario pueda firmar desde cualquier lugar a través de cualquier dispositivo: portátil, móvil, tablet, etc. El usuario podrá acceder al certificado digital custodiado por los sistemas de Camerfirma, dicho acceso se puede hacer a través de internet con su clave de acceso: PIN, OTP, etc

Alineación con los marcos legales

La solución de Camerfirma cumple ampliamente con las regulaciones del Nuevo Reglamento Europeo de Certificación Digital: Certificación Digital en la Nube el cual fue publicado el 3 de abril de 2014, dicho reglamento regula la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, derogando la Directiva 1999/93

10.5 SAFELAYER- TRUSTEDX UNA PLATAFORMA COMPLETA DE IDENTIFICACIÓN Y FIRMA ELECTRÓNICA

Los productos de firma de Safelayer ofrecen diferentes opciones para la integración de procesos de identificación y firma electrónica, desde configuraciones orientadas al ámbito corporativo a Prestadores de Servicios de Confianza (TSP) y ciudadanos.

Los beneficios que aporta la propuesta de Safelayer son los siguientes:

- Dinamización del desarrollo de aplicaciones y la movilidad de los procesos de firma. Facilita el desarrollo de casos de uso con mecanismos de integración actuales y ampliamente difundidos y nuevos contextos de uso cada vez más presentes, como las aplicaciones web o los dispositivos móviles.
- Mejora de la experiencia de uso para usuarios. Proporcionan mecanismos de uso sencillos para los usuarios (orientados tanto a los corporativos como a los ciudadanos), tales como el empleo de dispositivos móviles actuales y tecnologías web que no requieren la instalación de plugins o aplicaciones Java.
- Protección contra el fraude de identidad. Provee mecanismos de autenticación y firma que aportan niveles altos de seguridad. Reconoce otros mecanismos de eID, gestionando el nivel de confianza que proporcionan.
- Estrategia de mejora de la marca. Contribuye a la estrategia de mejora de marca, con un componente personalizable, para los dispositivos móviles de los usuarios/ciudadanos, que permite autenticarse y firmar (Mobile ID de Safelayer).

10.5.1 TrustedX eIDAS de Safelayer

Plataforma de identificación, autenticación y firma electrónica para entornos Web. Proporciona aseguramiento de la identidad basada en autenticación adaptativa y el reconocimiento de identidades, ya sean corporativas, reconocidas o sociales:

Aglutina las funcionalidades de autenticación, inicio de sesión único (SSO) y federación de identidades. Proporciona un conjunto de mecanismos de autenticación basados en contexto, biometría del comportamiento, claves de un solo uso, certificados digitales y dispositivos móviles.

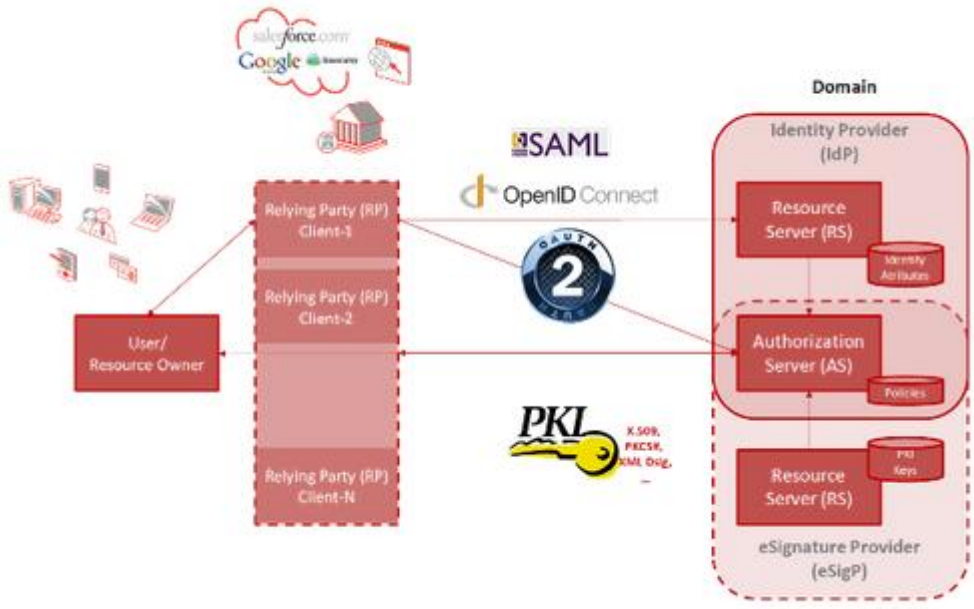
Complementa la plataforma incorporando atributos de identidad PKI para desarrollar funciones de firma electrónica. Aporta, conjuntamente con la

funcionalidad de autenticación, servicios de firma en servidor y dispositivos móviles, ofreciendo una solución integral para el despliegue de los nuevos servicios de confianza eIDAS.

10.5.2 Características

- Mecanismos de autenticación, federación y SSO adaptativos
- Integración de la organización en los medios Social, Mobile y Cloud (SoMoClo) asegurando un nivel de confianza variable ajustado a las aplicaciones.
- Autenticación adaptativa. Equilibra los vectores seguridad, riesgo/coste y conveniencia de usuario mediante la elevación de la confianza inteligente basada en información contextual y la acumulación dinámica de múltiples factores.
- Gestiona la confianza en la federación de identidades y proporciona control de inicio de sesión único (SSO) entre aplicaciones independientemente del medio y dispositivo, y adaptándose a los requerimientos de confianza variable. Mecanismos de firma electrónica
- Permite dos modalidades de integración de firma electrónica avanzada en las aplicaciones de forma sencilla y uniforme tanto remoto en servidor (p.e. cloud) como en dispositivo en posesión del usuario (p.e. mobile). Auditoría y regulaciones

Figura 22 Arquitectura TrustedX eIDAS

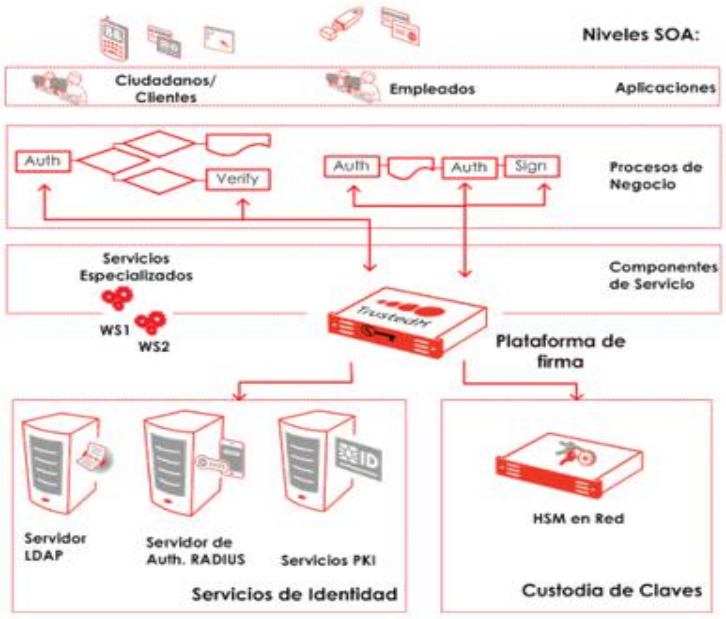


Fuente: safelayer

10.5.3 TrustedX para firma electrónica

En la figura 23 se puede aprecia cada una de las capas de servicio SOA.

Figura 23 Arquitectura



Fuente: safelayer

10.5.4 Servicios de firma:

TrustedX incorpora funciones que aportan un conjunto de mecanismos de seguridad y confianza como servicios. Dichos Servicios de Firma se pueden usar de diferentes formas, soportando diferentes estrategias de integración:

- APIs Java y .NET: Permite integrar de forma sencilla los servicios de firma en aplicaciones nativas Java y .NET (*).
- SOAP/WS: Estándar OASIS DSS como protocolo de acceso a servicios web.
- REST/WS, SOAP/WS: Usando la pasarela de integración de TrustedX que permite configurar el procesado del tráfico y de los datos mediante un lenguaje de pipelines XML.

La plataforma incluye un Applet Java para escenarios de integración de firma electrónica con tarjeta de usuario en entornos web.

El conjunto de funciones de la plataforma se agrupan en los siguientes servicios:

- Autenticación y autorización. Se encarga de la gestión de las políticas de autenticación y el control de acceso a los recursos/servicios de la

plataforma. Soporta mecanismos internos de autenticación basados en contraseña y certificados digitales, así como servicios de autenticación de terceros basados en RADIUS (TMS), SAML o en LDAP/AD.

- Gestión de entidades y objetos. Este servicio se encarga de la gestión de las entidades y objetos de la plataforma. Puede agregar repositorios externos, tales como LDAP/AD de usuarios, bases de datos, archivos y HSMs para la protección de las claves privadas.
- Validación de certificados. Proporciona funciones PKI para validar cadenas de certificados y consulta de estado de los certificados.
- Soporta OCSP/CRL y mecanismos personalizados (por ejemplo, bases de datos y la plataforma @firma).
- Generación y verificación de firmas. Genera y verifica firmas en la mayoría de los formatos estándares para documentos electrónicos, incluyendo correo electrónico y mensajería web. En concreto, los formatos soportados incluyen firmas múltiples, firmas con sello de tiempo y firmas longevas.
- Auditoría y accounting. Centraliza de manera uniforme y segura la información de log relativa a la firma electrónica. El sistema de log permite incorporar anotaciones específicas, facilitando su gestión con herramientas de terceros.
- Integración con otros componentes: TrustedX puede agregar mecanismos y repositorios externos para facilitar la integración con otras herramientas corporativas.
- LDAP/AD, RADIUS y bases de datos para propósitos de autenticación, autorización y obtención de información.
- Bases de datos y herramientas SIEM para el registro de logs centralizado.
- HSMs para la protección de las claves privadas.
- Soporte de OCSP/CRL y de mecanismos personalizados para validación de certificados.
- Opcionalmente, pueden añadirse los siguientes módulos:
- Carpetas vigiladas: Módulo que permite a usuarios y aplicaciones el uso de carpetas de red para iniciar procesos de firma desasistida de uno o varios archivos.
- TrustedX monitoriza el contenido de unas carpetas de red, ejecutando una serie de acciones sobre los archivos que se almacenan en ésta.
- Una vez procesados, TrustedXguarda las firmas en una carpeta de salida, igualmente accesible por red, incluyendo un report de los resultados.
- TrustedX destaca por soportar múltiples carpetas vigiladas y permitir la definición de acciones encadenadas
- Orientado tanto a usuarios como aplicaciones. Para firmar, basta con realizar una operación de copiar&pegar sobre una carpeta.
- Custodia de firmas electrónicas. Se encarga de mantener el no repudio de las firmas electrónicas, interactuando de forma transparente con el servicio de no repudio y gestionando los metadatos relativos a la firma electrónica y los documentos electrónicos.

10.5.5 Características técnicas

- Formato: Software appliance. Consultar para más información sobre entornos hardware o virtuales homologados.
- Monitorización de eventos: Simple Network Management Protocol (SNMP).
- Servicios de seguridad: OASIS WS-Security, DSS (Digital Signature Service) y SAML, REST, SOAP y SSL/TLS.
- Estándares de sobre digital: PKCS #7, IETF CMS, ETSI TS 101733 - CAdES, W3C XML-DSig, W3C XML-Enc, ETSI TS 101903 - XAdES, Firma para documentos PDF según IETF y S/MIME y ETSI TS 102 778) - PAdES.
- Soporte de sellado de tiempo digital: TSP de IETF – RFC 3161.
- Verificación de estado de certificados digitales: Mediante CRLs, protocolo OCSP de IETF y otros mecanismos personalizables.
- Acceso a base de datos y directorios: Oracle, Microsoft SQL Server o MySQL.
- Protocolo de acceso a directorio LDAP.
- Acceso a servicio de autenticación: Autenticación basada en LDAP/AD y
- TMS compatibles con protocolo RADIUS.
- Soporte de gestor documental: Protocolo HTTP/WebDAV y XAM.
- Soporte de HSM: Dispositivos PKCS #11 homologado por Safelayer.
- Sistemas de archivos de red soportados: SMB/CIFS y NFS.

10.6 XOLIDO ® SIGN CLOUD

Permite el tratamiento y generación de documentos para su participación en procesos de flujo de trabajo, notificaciones y circuitos con firma electrónica y sellado de tiempo. Cuenta con autenticación mediante certificado electrónico y seguridad SSL. Permite la generación de modelos de formulario y documentos PDF (opcionalmente también PDF/A) con inclusión de códigos de verificación seguros (CVE) y códigos de barras QR-Code.

10.6.1 Características

a) Multiusuario
b) Acceso seguro SSL con autenticación de usuarios mediante:
    a. Certificado electrónico.
    b. Acceso de usuario y contraseña
c) Módulo de gestión de usuarios, roles, categorías y departamentos.
d) Módulo de creación de formularios y plantillas para la generación de documentos PDF con:
    a. Generador de códigos de verificación seguros (CVS / CVE).
    b. Inclusión de códigos de barras QR-Code y asociación de metadatos.
e) Módulo de circuitos de firma y flujos de trabajo.

f) Módulo para subir y guardar documentos con:
    a. Asociación de metadatos
    b. Generador de códigos de verificación electrónica seguros (cvs / cve).
    c. Inclusión de códigos de barras QR-Code.
g) Módulo de envíos de documentos:
    a. Entre usuarios de la aplicación.
    b. A direcciones de correo electrónico definidas por el usuario.
h) Módulo de notificaciones:
    a. Avisos y alertas a email:
       Sistema de alertas recibidas en los correos electrónicos de los usuarios de la aplicación notificándoles diversos eventos, como por ejemplo la necesidad de su participación en un circuito de firma o flujo de trabajo.
    b. Notificaciones fehacientes:
       Sistema de envío para notificar la existencia de un documento que puede ser accedido en una zona de trabajo autenticada mediante certificado electrónico.
i) Módulo de operaciones de invitado, permite solicitar operaciones sobre los documentos a usuarios externos (invitados):
    a. Firma electrónica con certificado.
    b. Firma manuscrita digitalizada con sellado.
    c. Aprobación / Rechazo.
j) Firma electrónica incrustada en documentos PDF.
k) Sellado de tiempo de Autoridad Certificadora reconocida.
l) Procesos anuales de firma electrónica / sellado de tiempo y generación de documentos PDF: 12.000. (Se consideran distribuidos de forma uniforme a lo largo del periodo anual).
m) Cuenta FTP para la descarga de documentos desde el repositorio.
n) Trazabilidad de las comunicaciones certificadas y registro de Logs.
o) API Web Services SOAP para integración e interoperabilidad con sus propias aplicaciones o de terceros.
p) Manual de usuario y manual de ayuda a integradores SOAP.
q) Este servicio se proporciona con un subdominio con el nombre de tu organización de forma gratuita:
    a. Ejemplo: https://tuorganizacion.xolidosign.com

10.6.2 Costo

El costo de esta solución es de 1.200 € / año, este valor es sujeto a condiciones y restricciones:

Todos los precios son con impuestos no incluidos. Precios válidos salvo error o modificación. Las características y funcionalidades ofrecidas en www.xolido.com de los distintos Productos y Servicios son meramente

orientativas y en ningún caso tendrán la consideración de vinculantes. El Contrato de Suministro de Productos y/o Servicios determina la relación contractual con el Cliente.

10.6.3 Xolifo® Sign cloud bajo el dominio corporativo del cliente

Puedes utilizar un dominio o subdominio propio de tu organización del tipo https://tuorganizacion.com o https://subdominio.tuorganizacion.com para acceder a tu Xolido®Sign Cloud.

Para ello es necesario un certificado servidor SSL y una IP fija para la aplicación Xolido®Sign Cloud.

10.7 HELLOSIGN

La conexión a HelloSign es segura y cifrada mediante SSL (Secure Sockets Layer), los documentos también se almacenan y se cifran en reposo utilizando AES- cifrado de 256 bits.

La autenticación en dos fases asegura documentos confidenciales de miradas indiscretas.
La eSign es alineada con las políticas de 2000US firma electrónica en comercio global y nacional, la Uniform Electronic Transactions Act (UETA) y la directiva europea (EC/1999/93).

Soporta la firma en archivos de 17 diferentes formatos incluyendo PDF, Microsoft Word, Powerpoint, Excel entre otros.

Soporta la firma cuyo proceso se hace desde el dispositivo móvil.

Brinda un API para rápida construcción de aplicaciones que implementa firma electrónica.

Los documentos son protegidos por encriptado SSL y una infraestructura de servidor seguro, alojado en un data center con nivel de seguridad Tier III, SSAE-16, además de ISO 27001.

Flujos de trabajo flexibles permite que 1 o 20 personas firmen simultáneamente o en un orden especifico, además de ofrecer la funcionalidad de hacer copias al carbón para otras personas.

10.8 SIGNIFICANT

Es un producto de la compañía privada xyzmo con base en Ansfelden, Austria con una subsidiaria en Estados Unidos. Con 10 años de experticia en el sector de firmas Electronicas. SIGNificant ayuda a la automatización de los procesos de negocio y digitalizarlo completamente.
Para la solución existen certificados digitales (tarjetas inteligentes, token USB, certificado software, HSM).
Para enviar un documento a un destinatario externo para la firma utilizando certificados digitales para la firma aumentando el cumplimiento legal.
La seguridad en cuanto a la identidad del firmante para las transacciones online, está compuesta por autenticación por e-mail, autenticación por medio de la red social FACEBOOK, también con el envío de mensajes de texto con una clave de única vez para el dispositivo móvil del firmante.

Cuenta con una opción de traza de auditoría que se provee a quien se firma un documento, dicha traza de seguimiento guarda registros de los siguientes eventos:

- Envío de e-mails y notificaciones
- Consentimiento del firmante para usar firma electrónica
- Autenticaciones de usuario
- Creación de la firma
- Transacciones completas
- Descarga de documentos
- Cancelaciones

10.9 ANÁLISIS COMPARATIVO BENEFICIOS DE CADA APLICACIÓN DE FIRMAS

Basado en la documentación de las paginas oficiales de cada una de las soluciones de firma electrónica en la nube se construye una tabla, acorde con criterios que se encontraron a partir de las necesidades de ANCERT, que una solución no tenga una X en la Tabla 2 no necesariamente quiere decir que no la ofrezca, simplemente que dicho criterio o funcionalidad no estaba especificada en la documentación

Tabla 2 Comparativo de aplicaciones de firma electrónica

	VIAFIRMA	MOBBSIGN	CAMERFIRMA	SAFELAYER	XOLIDO	HELLOSIGN
Múltiples firmas	X					
Firmas embebidas	X		X			
Gestión de claves (privadas/publicas)	X					X
Gestión de certificados				X		
módulo HSM			X	X		
Autenticación de usuarios	X				X	
Integración e interoperabilidad con otras CA, TTPs	X		X	X		
Firma por parte de la autoridad certificadora		X				
Custodia digital	X		X			
APIs para desarrollo de aplicaciones en dispositivos móviles	X					

11. RECOMENDACIÓN DE HERRAMIENTA DE FIRMA ELECTRONICA PARA ANCERT

Antes de hacer la recomendación es importante abarcar un aspecto a tener en cuenta, y es que en todos las soluciones consultadas no se observó o no se especifica cómo es el proceso de múltiples firmas (inclusión de múltiples firmas embebidas) en un mismo documento (para aquellas soluciones que ofrecían esta funcionalidad), tan solo unas pocas lo mencionan pero no explican como seria el proceso.

En cuanto a la recomendación de las herramientas que más se acerquen a las necesidades de ANCERT se recomienda:

11.1 VIAFIRMA

Porque hace uso del protocolo OPENID lo que posibilita el intercambio seguro de identidades entre dominios; esto es un punto fuerte cuando se habla de la integración de esta solución con otros sistemas. Gracias al protocolo brinda la opción de participar en la actividad de autenticación de usuarios.

Brinda una amplia gama de formatos de cifrado, además de sus correspondientes APIs para los lenguajes de programación java y C#. Brinda soporte a los diferentes estándares de infraestructura de clave pública y tecnologías de almacenamientos de certificados.
La gran variedad de formatos de firma que soporta es otro diferenciador de esta solución sobre las demás, en su documentación mencionan los diferentes procesos de firma. El avanzado desarrollo de clientes para las diferentes plataformas de dispositivos móviles. Junto a lo anterior brinda el servicio de custodia digital donde se almacenan los documentos firmados para posterior recuperación y validación, ofreciendo diferentes tipos de almacenamiento. Confirma a: ANCERT, DNI electrónico, Camerfirma, entre otras, como autoridades de certificación reconocidas.

Con respecto a esta solución de firma móvil Viafirma los costes estimados serian los siguientes:

Existen dos modalidades para el producto de firma electrónica:

On-Premise - Licencia Stándar. Con esta opción nos referimos a la adquisición de una licencia de viafirma platform. El precio de la licencia de explotación son 15000€ (único pago sin limitación de tiempo)

On-Demand - Servicios Centralizados. En esta modalidad los pagos se realizan mensualmente según las operaciones máximas realizadas, independientemente de que sean de autenticación y/o firma electrónica. En esta modalidad los pagos son mensuales según las operaciones realizadas:

PLATFORM	Basic	Premium	Enterprise
Pago mensual	149,99 €	299,99 €	Presupuesto a medida
Operaciones (autenticaciones + firmas)	600	2.000	Consultar
Coste firma	0,25 €	0,15 €	

Ayuda integración (Bolsa horas) - Mínimo 10h	Coste Hora (40 €)

El coste de **Viafirma mobile sdk** para ambas modalidades son 3000€.

En el siguiente enlace se encuentran algunas preguntas frecuentes sobre viafirma mobile: https://www.viafirma.com/la-firma-movil

11.2 CAMERFIRMA

Esta solución comparte algunas características con VIAFIRMA, como lo son interoperabilidad con otros dominios, cifrado de datos, gestión centralizada de claves, uso de módulos de seguridad Hardware, autenticación de usuario ante la plataforma de gestión mediante diversos métodos (PIN o *Password*, huella dactilar, *Smartcard*, OTP, etc.), custodia de claves, cuentan con un servidor de sellos de tiempo, respondedor OCSP. Esta solución se ve un poco limitada frente a VIAFIRMA en la parte de API para desarrollo en dispositivos móviles, dado que en su documentación no especifican con detalle que soporte brindan para el desarrollo de aplicaciones móviles que requieran la integración con los servicios de CAMERFIRMA.

12. CONCLUSIONES

Se concluye que la firma digital es un mecanismo que garantiza la seguridad de las comunicaciones electrónicas, además permite dar cumplimiento a requisitos legales, dando la misma validez que un documento manuscrita y adicionalmente quienes ofrecen este servicio también garantizan condiciones de seguridad en sus aplicaciones que , pues su aplicación certifican que el mensaje no ha sido vulnerado.

La integración de firmas emitidas por una entidad prestadora de servicios de certificación, permitirán garantizar: la autenticidad del origen; la integridad de la información transaccional a lo largo de su ciclo de vida y el no repudio a las transacciones es decir que requiere de autoridades certificadoras, quienes aseguran que una persona y su firma son quienes dicen ser.

Firmar electrónicamente un documento tiene ventajas con son: menos papeles y más agilidad en las transacciones, sin embargo, su uso no depende de la tecnología o de las leyes, depende de la capacidad de adaptación y de confianza que los usuarios tengan con algo tan sensible como la privacidad y seguridad de sus datos.

Existen en el mercado múltiples herramientas comerciales que incluyen APP para firmar electrónicamente documentos desde cualquier dispositivo móvil, esta nueva adaptación de la tecnología posibilita la expansión comercial de las organizaciones, se reducen los costos y tiempos de trámites y rediseña las relaciones laborales y la interacción humana.

13. Bibliografía

de Matías García, L. (2013). *GESTIÓN DE RIESGO EN DISPOSITIVOS ANDROID BASADA EN ELIMINACIÓN DE VULNERABILIDADES Y DETECCIÓN DE CONTEXTOS.* Leganés: UNIVERSIDAD CARLOS III DE MADRID ESCUELA POLITÉCNICA SUPERIOR.

Rafael Pérez Galindo. (s.f.). *Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.* Obtenido de http://www.cpeig.org/portal/system/files/175/2169/04+eIDAS+VisionAGE.pdf

ANCERT. (2015). *Certificados raiz -Ancert*. Obtenido de http://www.ancert.com/liferay/web/ancert/aapp-oopp/certificados-raiz

ANCERT. (2015). *Portal de autenticacion y DPCs - ANCERT*. Obtenido de http://www.ancert.com/liferay/web/ancert/aapp-oopp/politica-de-certificacion

ANCERT. (2015). *Validación de certificados - ANCERT*. Obtenido de http://www.ancert.com/liferay/web/ancert/validacion-de-certificados1

APPLE. (2015). *APPLE*. Obtenido de http://www.apple.com/es/ios/what-is/

Carracedo Gallardo, J. (2004). *Seguridad en redes telemáticas.* Madrid: McGraw Hill.

Christianson, B., & Malcolm, J. (Marzo de 2010). *Security Protocols XVIII: 18th International Workshop.* Obtenido de https://books.google.com.co/books?id=gsujBQAAQBAJ&dq=collision-rich+security&hl=es&source=gbs_navlinks_s

Feige, U., Fiat, A., & Shamir, A. (1998). *Springer.* Obtenido de http://link.springer.com/article/10.1007/BF02351717#page-1

IETF. (Junio de 1999). *rfc2560.* Obtenido de http://tools.ietf.org/html/rfc2560

IETF. (Mayo de 2008). *rfc5280.* Obtenido de http://tools.ietf.org/rfc/rfc5280.txt

ISO. (s.f.). *International Standar Organization*. Obtenido de http://www.iso.org/iso/home.html

Kinastowski, W. (2013). *CLOUD COMPUTING 2013 : The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization.* Obtenido de Digital Signature as a Cloud-based Service:

https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCsQFjAAahUKEwicjqHF95LGAhVFkQ0KHQyaAN8&url=http%3A%2F%2Fwww.thinkmind.org%2Fdownload.php%3Farticleid%3Dcloud_computing_2013_3_20_20041&ei=nmp_VZzHO8WiNoy0gvgN&usg=AFQj

MICROSOFT . (2015). *WINDOWS PHONE*. Obtenido de https://msdn.microsoft.com/es-es/library/jj130729.aspx

Moreno, L. (2003). *educastur .* Obtenido de http://www.educastur.princast.es/fp/HOLA/hola_bus/cursos/curso17/documentos/seguras.pdf

National Institute of Standards and Technology. (Marzo de 2013). *NIST*. Obtenido de http://www.nist.gov

OASIS-OPEN. (2015). *OASIS | Advancing open standards for the information society.* Obtenido de https://www.oasis-open.org

Portal Administracion electrónica. (2015). *Portal firma*. Obtenido de http://firmaelectronica.gob.es/Home/Empresas/Tipos-Certificados.html

Singh, M., & Bansode, A. (Enero de 2015). *nternational Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE).* Obtenido de Implementation of Cloud storage Security Mechanism using: http://www.ijarcsse.com/docs/papers/Volume_5/1_January2015/V5I1-0365.pdf