Máster Universitario en

Ingeniería **C**omputacional y **S**istemas **I**nteligentes

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Konputazio Zientziak eta Adimen Artifiziala Saila –
Departamento de Ciencias de la Computación e Inteligencia Artificial

K I S A

I C S I

Tesis de Máster

Ecosistema para la Creación de Firma Digital Avanzada en Movilidad y Autenticación Mediante Elemento Seguro

Iván Gutiérrez Agüero

Tutor

Álex Gracía-Alonso Montoya
Departamento de Ciencia de la Computación e Inteligencia Artificial
Facultad de Informática

informatika fakultatea
facultad de informática

KZAA
/CCIA

Septiembre 2012

RESUMEN

Con el crecimiento exponencial de terminales móviles que se está dando en el mercado internacional actual, las necesidades de los usuarios están variando tanto a nivel personal como corporativo. Al aumentar la cantidad de operaciones que un usuario puede realizar desde su dispositivo móvil, la información personal que se almacena es mayor. Si las operaciones implican un compromiso legal por parte del usuario, los datos deben ser debidamente protegidos y avalados.

Dada esta situación, se estima de vital importancia la creación de entornos que permitan al usuario identificarse de manera que su identidad no pueda ser comprometida. Un ecosistema implica la creación, gestión y distribución de certificados. Ésta es la forma tecnológicamente más avanzada actualmente para su uso desde terminales móviles.

Para almacenar los datos del usuario de forma segura, se estudian las opciones de uso de elementos seguros.

El ecosistema que se crea en este proyecto de Fin de Máster hace segura la firma de documentos digitales de forma remota mientras se está fuera de la oficina o lejos del interesado, y permitirá la investigación de nuevos elementos que contribuyan a garantizar la autenticidad de acciones y documentos.

ABSTRACT

Mobile phones' number is growing so fast in the international phone market that user needing is changing with the software matureness in both business and personal devices. Naturally, increasing user possibilities through these platforms means an increase of personal stored information inside the phone. For most of the administration operations personal data must be private, and then, correspondingly guaranteed and secured.

This situation gets to the needing of an environment creation which makes user authentication in a safe way, and his information is not compromised by any other entity. For safeness of the data, the perfect environment is a certification level authentication, involving creation and management of this environment for its use via smartphones.

Secure elements implementing Java Card OS, are supposed to be the top of investigation level storages, and nowadays the safest ecosystem known. Different hardware approaches to this solution must be investigated.

In conclusion, this project sets the outlining to make a secure environment using the mobility document signature in order to demonstrate one of this environment's purposes, advanced investigations' target.

ÍNDICE

1 OBJETIVOS 1
2 ENTORNOS PKI (PUBLIC KEY INFRASTRUCTURE) 3
2.1 CA (CERTIFICATION AUTHORITY) 3
2.2 FUNDAMENTOS Y EJEMPLOS 4
2.3 PKI Y EL CERTIFICADO DIGITAL 6
2.3.1 PKI 6
2.3.2 CERTIFICADO DIGITAL 7
2.4 FRAMEWORKS PARA CREAR NUEVAS CAs 8
2.4.1 EJBCA 8
2.4.2 GNOMINT 8
2.4.3 OPENCA 9
2.4.4 XCA 9
2.4.5 OPENSSL 9
2.4.6 JUSTIFICACIÓN DE LA SELECCIÓN 9
2.5 IMPLEMENTACIÓN DE UNA CA 9
3 ELEMENTOS SEGUROS 15
3.1 TIPOS DE ELEMENTO SEGURO 15
3.1.1 MICRO SD SEGURA 15
3.1.2 (U)SIM 16
3.1.3 EMBEDDED SECURE ELEMENT 16
3.1.4 ARM TRUSTZONE 17
3.2 ELECCIÓN DE UN ELEMENTO SEGURO 17
3.3 INTEGRACIÓN DE UN ELEMENTO SEGURO 20
4 IDENTIFICACIÓN MEDIANTE CERTIFICADOS DIGITALES 27
4.1 RELACIÓN CON EL RESTO DE ELEMENTOS ESTUDIADOS 27
4.2 CERTIFICADOS DIGITALES Y SUS POSIBILIDADES 28
4.3 ECOSISTEMA GENERAL DE CERTIFICACIÓN 29
4.3.1 CONTENIDO DE UN CERTIFICADO 30
4.3.2 ECOSISTEMA DE LOS CERTIFICADOS DESDE EL PUNTO DE VISTA DEL USUARIO 31

4.3.3 PROCEDIMIENTOS PARA LA CONSULTA DEL ESTADO DE LOS CERTIFICADOS 32
5 FIRMA DIGITAL EN MOVILIDAD 35
5.1 TIPOS DE FIRMA DIGITAL 36
5.1.1 LO QUE NO ES UNA FIRMA DIGITAL 38
5.2 TIPO DE FIRMA DIGITAL IMPLEMENTADO 40
5.3 QUÉ Y QUIÉN INTERVIENE EN UNA FIRMA SEGURA EN MOVILIDAD 41
5.4 IMPLEMENTACIÓN DE UN PROCESO DE FIRMA 42
5.5 VENTAJAS QUE APORTA LA INVESTIGACIÓN LLEVADA A CABO 44
6 CONCLUSIONES 47
7 BIBLIOGRAFÍA 49

ÍNDICE DE FIGURAS

Figura 1. Infraestructura de Clave Pública 7
Figura 2. HSM. Contenedor de CAs y funcionalidades 10
Figura 3. Composición de una CA..... 11
Figura 4. Proceso básico de generación de un certificado 12
Figura 5. Tarjeta micro SD segura utilizada en el proyecto 18
Figura 6. Petición de credenciales (erróneo, original y correcto) 20
Figura 7. Arquitectura de un elemento seguro (GlobalPlatform) 21
Figura 8. Comunicación con el elemento seguro mediante APDUs..... 22
Figura 9. Comunicación entre aplicación y elemento seguro 23
Figura 10. Diseño de los elementos que componen una tarjeta SD de acceso seguro.... 24
Figura 11. Interacción de los elementos seguros con el usuario..... 25
Figura 12. Solución a la problemática de confianza 29
Figura 13. Un tercero en el que las dos partes confían 30
Figura 14. Infraestructura de firma segura con certificados 32
Figura 15. Clasificación de los diferentes tipos de firma 38
Figura 16. Dispositivo digitalizador de firmas manuscritas 39
Figura 17. Aspecto del sello de una firma digital 41
Figura 18. Elementos de un ecosistema de firmas..... 42
Figura 19. Diagrama de la firma realizada por la aplicación..... 43
Figura 20. Pantalla principal de firma 44

1 OBJETIVOS

En este documento se van a tratar una serie de elementos gran innovación tecnológica, a los que se les añade una componente de investigación. Esta componente permitirá avanzar hacia nuevos productos de software. La tarea investigadora llevada a cabo se organiza en cuatro pilares.

1. Analizar y experimentar tecnologías para la creación de una **Certification Authority (CA)** que goce de todos los módulos que son necesarios en toda Autoridad de Certificación real y reconocida.
2. Estudiar y testear **elementos seguros**. En este campo una gran cantidad de investigadores continúa trabajando.
3. Una vez creado un ecosistema (CA y elementos seguros). La CA creada puede generar **certificados** a nombre del usuario. Este certificado único, personal e intransferible puede ser utilizado por el usuario como identificación unívoca, bajo la supervisión de la propia CA que ha expedido el certificado, el cual es avalado por ella.
4. Tras generar el entorno de credenciales del usuario, se investiga la generación de un **sistema de firmas** que va a utilizar el certificado generado a nombre del usuario como identificación unívoca. El objetivo de este punto es estudiar el posible traslado de una aplicación al mundo de la movilidad. El acceso a la aplicación móvil estará controlado por el elemento seguro elegido como parte del segundo objetivo marcado.

La constitución de estos objetivos permite disponer de un framework para seguir avanzando en la implantación de sistemas de firma digital en movilidad. Se verificará la unión que de todos ellos se hace a lo largo del proyecto, y como colofón en la aplicación resultante del mismo.

Hasta ahora no se ha presentado con éxito ninguna solución estable que conjunte en un mismo dispositivo toda la funcionalidad requerida para un entorno de firmas digitales en movilidad. Cada una de las partes o sub-proyectos que conforman el total de este proyecto presentan soluciones innovadoras en los mundos de la seguridad digital y de la movilidad. Ambos ámbitos son de gran importancia en la era de la información.

Los cuatro objetivos descritos en esta introducción se corresponden con un capítulo de los que forman la memoria. En la siguiente lista se describe el contenido de cada uno de los capítulos:

Capítulo 1: "Sistemas PKI". Este capítulo trata sobre la creación de una autoridad de certificación capaz de emitir certificados basada en la estructura PKI.

Capítulo 2: "Elementos seguros". En este capítulo se estudian las diferentes posibilidades que se están investigando para almacenar información de forma segura y su funcionamiento.

Capítulo 3: "Certificados digitales: ¿por qué usarlos?". Capítulo en que se analiza el entorno de los certificados digitales, necesarios para identificar al usuario que realiza la firma.

Capítulo 4: "Firma digital en movilidad". Último capítulo en el que se utilizan los conocimientos adquiridos en los anteriores y se investiga la creación de un entorno móvil capaz de producir firmas digitales en documentos PDF desde el mismo dispositivo.

2 ENTORNOS PKI (PUBLIC KEY INFRASTRUCTURE)

En este capítulo del proyecto se comienza dando una visión general del ecosistema encargado del almacenamiento y la gestión de identidades digitales de los usuarios, ya sean personales (ciudadano, trabajador…) o corporativas. Así se comienza introduciendo las CAs, citando los ejemplos más importantes en el ámbito nacional, y se introducen las infraestructuras de PKI y los certificados digitales.

Una vez conocido el entorno, se estudian diferentes frameworks que permitirán la creación de nuevas CAs, y se expone la implementación de uno de ellos. Este es el primer paso hacia la creación del ecosistema objeto de este proyecto.

2.1 CA (CERTIFICATION AUTHORITY)

En criptografía, una Autoridad de Certificación, más conocidas como *Certification Authority* (CA), es una entidad emisora de certificados digitales. Con estos certificados digitales se garantiza la posesión de unas claves que identifican a su dueño. Gracias a esta identificación, terceras partes pueden confiar en las firmas del emisor.

En este modelo de relaciones de confianza la CA actúa como una tercera parte de confianza entre el emisor y el receptor de la información, ya que es una entidad de confianza para ambas partes. Comúnmente, los esquemas que hacen uso de esta estructura de certificaciones son conocidos como infraestructuras de clave pública (PKI).

Hay autoridades de certificación de amplio reconocimiento que son automáticamente reconocidas y de confianza para la mayor parte de los navegadores y aplicaciones. Por otra parte, una gran cantidad de instituciones gubernamentales en distintos países manejan sus propias CAs.

Por lo tanto, las CAs deben asegurar la validez de la información enviada por el emisor, así como identificar al emisor, evitando que en otro momento pueda renegar de haber enviado dicha información. Esta comprobación habitualmente se lleva a cabo automáticamente desde servidores electrónicos que contienen la información de todos los certificados y del estado de los mismos. Cuando las credenciales del emisor son válidas, se da validez a la firma. En caso de que se hayan revocado, el certificado pasa a una lista negra, por lo que se detectará su invalidez en la comprobación, y la firma del documento se dará por invalidada.

2.2 FUNDAMENTOS Y EJEMPLOS

La Autoridad de Certificación nos va a proveer de los mecanismos necesarios para establecer la relación de confianza necesaria para que la firma digital que se va a llevar a cabo sea totalmente válida. Las firmas emitidas gozarán, por tanto, de la misma validez legal que una firma manuscrita emitida por el emisor del documento de su puño y letra.

En el estado español hay un conjunto de Autoridades de Certificación que poseen los permisos necesarios para emitir certificados digitales de forma legal, los cuales pueden ser utilizados con total confianza y cuyo uso es asegurado por diferentes cantidades de dinero para evitar robos de identidad y así verificar su validez y originalidad.

Las Autoridades de Certificación habitualmente distribuyen los certificados digitales a través de tarjetas criptográficas dentro de las que incluyen un archivo donde vienen escritos los datos del usuario, su clave pública que todo el mundo podrá conocer y la clave privada que va a utilizar para firmar de una forma segura los documentos que necesite firmar. El modelo más habitual en que estas tarjetas criptográficas se hacen realidad, es decir, como más acostumbrados están los usuarios a reconocerlas es en forma de DNI electrónico distribuido por la Dirección General de Tráfico o tarjetas microSD criptográficas que pueden emitir empresas como Izenpe.

Por lo tanto, el usuario de un certificado digital emitido por una Autoridad de Certificación legal posee un certificado que le identifica unívocamente y que incluye las claves necesarias para llevar a cabo cifrado y autenticación de una manera legal, y de forma que una tercera parte de confianza, pero independiente a las entidades o individuos que toman parte en el intercambio de información, puede asegurar que ese intercambio se ha llevado a cabo de forma correcta y que las entidades que han tomado parte en el proceso realmente son quienes dicen ser.

Entre las distintas Autoridades de Certificación que de un modo u otro emiten certificados digitales a usuarios o empresas, hay una serie de ellas que son comúnmente adoptadas y más ampliamente aceptadas a nivel nacional. A continuación se nombran las CAs que más fuerza tienen a nivel nacional y que por tanto, como se acaba de mencionar, son aceptadas en casi todos los ámbitos de identificación dentro del estado.

- *Fábrica Nacional de Moneda y Timbre (FNMT)*

La Fábrica Nacional de Moneda y Timbre, a través del proyecto llamado Ceres comienza a contemplar la certificación de los ciudadanos. Provee certificados de ciudadano, así como la renovación y revocación y revocación de dichos certificados digitales. Para las empresas, proporciona la firma de distintos tipos de documento, permite la emisión de certificados y les da la posibilidad de recibir su certificado en una tarjeta criptográfica. Los certificados pueden ser solicitados usando los datos y las claves almacenados en el DNI electrónico que identifica al usuario en cuestión.

- *Camerfirma - Camerfirma SA*

La Cámara de Comercio de Zaragoza actúa como Autoridad de Certificación a nivel nacional, y proporciona certificados digitales a sus usuarios con validez total. Esta entidad cuenta con el soporte de WebTrust Certification Authorities, lo que le proporciona un mayor nivel de confiabilidad como tercera parte de confianza. Camerfirma, al igual que la FNMT hace posible la petición de sus certificados a través de e-dni (DNI electrónico).

- *CATCert - Agència Catalana de Certificació*

La Agencia Catalana de Certificación aparte de habilitar certificados digitales, también permite renovar, revocar o modificarlos. Los certificados expedidos por esta agencia son utilizados en administraciones públicas, tales como la administración local catalana, la Generalitat de Catalunya, instituciones comunitarias, así como algunos ministerios también contemplan su uso junto a otros. Al igual que en casos anteriores, también se hace posible la petición del certificado a través de e-dni. Esta agencia, al ser una entidad que abarca una comunidad autónoma, y no es una empresa de ámbito estatal, ha firmado un acuerdo de reconocimiento mutuo con Izenpe (perteneciente a la Comunidad Autónoma Vasca).

- *Izenpe - Euskadi.net*

Se trata de una entidad vasca que cuenta con validez nacional. Tiene el poder de proveer certificados de ciudadano, sellos de empresa (certificados a nivel de entidad empresarial), certificados de servidor seguro (SSL). Aparte de ello ofrece el servicio de firma de código para servicios o productos software implementados por empresas desarrolladoras. Afirman proporcionar apoyo técnico "a las instituciones y empresas inmersas en proyectos de firma, colaborando estrechamente con sus propios servicios informáticos para la planificación, implementación y mantenimiento de los servicios puestos en marcha."

- *Autoritat de Certificació de la Comunitat Valenciana*

Esta agencia proporciona certificados de ciudadano, a los que se refiere como Receta digital, certificados para entidades, conexiones seguras SSL y VPN, etc. Para esta entidad es necesario indicar si opera en el ámbito de la Comunitat Valenciana o en el resto de España, o si en caso de ser una empresa, se trata de una empresa privada o una entidad pública.

Otras entidades, como por ejemplo notarios, pueden expedir su propio certificado digital de acuerdo con el Ministerio de Justicia (www.safelayer.com). A nivel europeo, algunas de las CAs más reconocidas son Thawte, GlobalSign, EuroPKI o DigiCert.

2.3 PKI Y EL CERTIFICADO DIGITAL

En este apartado se van a conocer las tecnologías que van a ser utilizadas en este capítulo del proyecto. Esta sección se ha estructurado de forma que se conozca el entorno que rodea al mundo de la firma digital. Primero se va a hablar de las PKI (*Public Key Infrastructures*) y después se va a pasar a un plano más concreto para explicar el funcionamiento de los certificados digitales, también llamados certificados de clave pública, que identifican al usuario. Más adelante se hablará de las tarjetas criptográficas, en las que hoy en día es habitual que las CAs introduzcan sus certificados digitales para una distribución más segura. El hecho de la introducción del certificado en un elemento seguro que el dispositivo móvil pueda entender es uno de los puntos a investigar. En caso de que no se encuentre una solución satisfactoria para su almacenamiento y/o extracción en el elemento seguro, en este proyecto el certificado digital estará instalado directamente como elemento software en la memoria flash del teléfono.

2.3.1 PKI

El acrónimo PKI corresponde con la traducción al inglés de Infraestructuras de Clave Pública. Estas infraestructuras se basan en criptografía de clave asimétrica, de modo que en todas las operaciones que se llevan a cabo en una interacción intervienen una pareja de claves, una de ellas pública, es decir, que puede ser conocida por todo el mundo, y la otra privada, que sólo el propietario de la clave debe conocer. Los usuarios distribuyen su clave pública para poder llevar a cabo operaciones con otros usuarios, pero en caso de que "pierda" la clave privada, la seguridad de su identidad y de sus datos puede verse seriamente comprometida. Con este contexto, cualquier mensaje puede ser cifrado usando la clave pública que ha sido distribuida por el destinatario, y de este modo el contenido del mensaje sólo podrá ser descifrado por el poseedor del certificado que contiene la clave privada correspondiente.

Esta característica convierte a este tipo de criptografía en el candidato perfecto para llevar a cabo el cometido de identificar a los usuarios como emisores (o firmantes) de los documentos, hecho que se tratará en un apartado propio más adelante. Esto es así ya que sólo este firmante puede emitir firmas con su certificado digital [Chang], evitando la suplantación de su identidad. Otros servicios unidos a la firma digital mediante certificados y la criptografía de clave asimétrica son el llamado no-repudio, que garantiza que el emisor de la firma no pueda negar haber firmado ese documento, y la integridad de la información contenida en el documento, ya que ésta no ha podido ser modificada por un posible interceptor durante la comunicación desde que el emisor la firmó.

Un sistema PKI permite la creación, almacenamiento y distribución de certificados digitales que son utilizados en este proyecto. Una estructura PKI consiste en una autoridad de certificación (CA), encargada de emitir y verificar los certificados; una autoridad de registro (RA), que verifica la identidad de los usuarios; y un sistema de manejo de certificados. A continuación se muestra en la un esquema de la arquitectura que rodea a la infraestructura de clave pública.

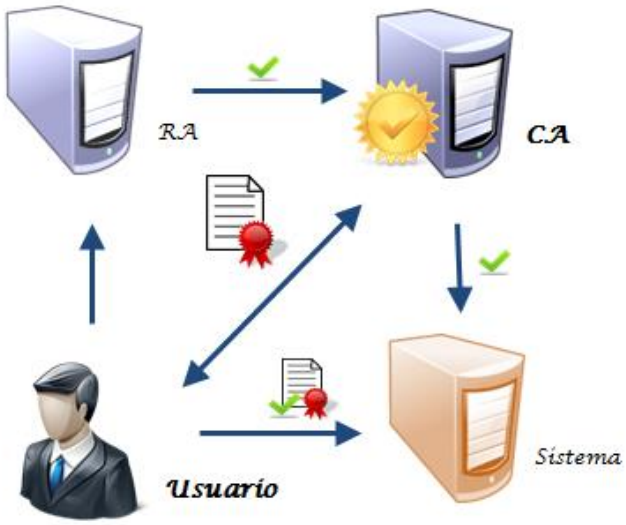

Figura 1. Infraestructura de Clave Pública

2.3.2 CERTIFICADO DIGITAL

El certificado digital es el documento que un usuario participante en un sistema PKI recibe por parte de una CA para identificarle con su firma gracias a las claves que contiene. Gracias a este mecanismo se asegura la seguridad de los servicios que se ofrece, y es parte fundamental en este proyecto.

El certificado digital vincula la identidad de un sujeto con sus claves, gracias a que existe el apoyo de una CA, que es un tercero en el que las demás entidades que interactúan con el sujeto confían. El certificado de usuario, que contiene su clave pública pero no la privada, se considera que está compuesto por información no sensible, que el usuario del certificado puede distribuir libremente.

Los certificados con los que se va a tratar en este proyecto siguen el estándar X.509, aunque existen varios formatos para certificados digitales. Dichos certificados son compuestos por la siguiente información: identidad del propietario, la clave pública asociada a esa identidad, la identidad de la entidad que expide y firma el certificado y el algoritmo criptográfico usado para firmar el certificado. Si bien esta es la información mínima, algunas CAs incluyen en los certificados que emiten alguna información extra. De los cuatro campos anteriores, los dos primeros pertenecen a su propietario y los otros dos al emisor del certificado.

Es habitual que para hacer uso de un certificado digital, el usuario deba solicitar personalmente su certificado de usuario, y deba por lo tanto acreditar su identidad con algún documento legal en una oficina de registro habilitada para este cometido. En el momento que el usuario reciba el certificado puede comenzar a hacer uso del mismo. En caso de tratarse de una empresa, el representante asignado por la misma debe poseer los datos y la acreditación necesaria.

2.4 FRAMEWORKS PARA CREAR NUEVAS CAs

A las Autoridades de Certificación expuestas en el punto anterior las distingue el alcance de la expedición de certificados, es decir, su ámbito; la cantidad de dinero por la que aseguran la validez, unicidad y seguridad de sus certificados; el modo en que expiden sus certificados; y el precio del mantenimiento de la validez legal de los mismos.

En nuestro caso, la Autoridad de Certificación que se quiere utilizar no tiene que estar necesariamente aceptada como legal a nivel nacional, ya que se va a tratar de una relación de confianza interna. Si se da este caso y no se desea invertir una cantidad determinada de dinero en la adquisición y mantenimiento de los certificados digitales que se quiere poseer para que identifiquen a los usuarios que intervienen en este caso, existe una serie de sistemas software que proporcionan los mecanismos necesarios para crear y mantener una entidad de certificación, con cadena de certificación pero sin validez legal alguna. Estas CAs "*out-of-the-box*" estudiadas tienen la posibilidad de emitir certificados digitales a los usuarios del sistema, y crear su propia base de usuarios, otorgando a sus certificados un tiempo de expiración, o revocándolos (dándolos de baja) en caso de que sea necesario, por ejemplo pérdida o robo.

Actualmente existen varios frameworks que permiten la creación de Autoridades de Certificación propias. En los siguientes apartados se describen los más importantes con licencia libre.

2.4.1 EJBCA

EJBCA (*Enterprise Java Bean Certificate Authority*) es uno de ellos, gratuito y de fácil implementación. EJBCA es un conjunto software para el despliegue y mantenimiento de infraestructuras de clave pública (PKI) implementado en Java EE que soporta la mayoría de los estándares asociados a PKI y algoritmos de cifrado, como RSA y algoritmos SHA.

EJBCA ha sido diseñado para ser independiente de la plataforma y para aceptar los tipos más comunes de certificado, así como los protocolos de creación y de verificación más extendidos. De este modo, acepta los habituales certificados construidos según el estándar X.509, la creación de listas de certificados revocados CRL, además de su comprobación, y el mantenimiento y consulta online del estado de los certificados (OCSP).

2.4.2 GNOMINT

Se trata de una herramienta de uso de Autoridades de Certificación X.509 mediante una interfaz que facilita su uso. Este sistema maneja certificados, firma de certificados por parte de la CA y CRLs, pero abarca muchos menos aspectos que EJBCA, ya que no toca partes interesantes del uso y mantenimiento de las CAs que EJBCA sí tiene en cuenta, y que pueden ser necesarias en un futuro.

2.4.3 OPENCA

OpenCA PKI Research Labs es un proyecto colaborativo que pretende desarrollar una Autoridad de Certificación de funciones plenas. El software que proporciona es de código abierto, y apoyado por Apache Project. Permite el desarrollo de software relacionado con sistemas PKI y la preparación y mantenimiento de una CA propia. El sistema es robusto, pero abarca aspectos que no nos interesan y la implantación de todo su entorno no es tan sencilla como resulta con la CA seleccionada, que contempla el sistema PKI como un todo. Este proyecto es el que más similitudes comparte con la CA que adoptada en este proyecto, pero es cierto que EJBCA está mucho más documentado.

2.4.4 XCA

XCA es un sistema multi-plataforma que proporciona una interfaz de usuario capaz de crear gráficamente claves con los algoritmos más comunes usados en criptografía, firma de certificados y CRLs. Esta interfaz también proporciona interacción con las funcionalidades del estándar PKCS#11 a través de OpenSC. Hay escasa documentación rodeando a este proyecto, que por otra parte no resuelve la necesidad que este proyecto pretende cubrir.

2.4.5 OPENSSL

OpenSSL es una implementación libre de los protocolos SSL y TLS escrita en C, pero no es una CA como tal, aunque sí toca aspectos relacionados con éstas y está considerablemente ligado al mundo del PKI. De todos modos se trata de una librería de seguridad muy interesante y que merece la pena conocer. Es multi-plataformas ya que existen versiones para las plataformas más ampliamente utilizadas.

2.4.6 JUSTIFICACIÓN DE LA SELECCIÓN

En el siguiente punto se detalla la implementación de una CA para este proyecto. Para llevar a cabo dicha implementación, se ha seleccionado EJBCA como candidato entre los frameworks descritos en los anteriores subapartados.

En definitiva, EJBCA ha sido elegido por las ventajas que proporciona gracias al amplio soporte que recibe, por la interoperabilidad que proporciona gracias a que permite la adopción de una gran cantidad de estándares que son ampliamente utilizados en el mundo de la certificación y firma, y por la extensa aceptación que tiene por entidades tanto públicas como privadas que ya la han adoptado en sus entornos de trabajo. Además de todas estas ventajas que se ha nombrado, EJBCA cuenta con una vasta documentación que ayuda a desplegar un sistema de certificación, así como aclarar posibles dudas que puedan surgir en su implantación o en su mantenimiento.

2.5 IMPLEMENTACIÓN DE UNA CA

Una autoridad de certificación se basa en la confianza generada por un tercero, por lo que una entidad autogenerada no gozará de plena validez a no ser que sea confianza

tanto para el emisor como para el receptor. Los usuarios del portafirmas que se ha obtenido como resultado de esta investigación van a utilizar una serie de certificados. Para la creación de dichos certificados ha generado el ecosistema del que se han obtenido posteriormente. En este punto se describe el proceso de creación de dicho ecosistema, es decir, la CA que da sentido a toda la cadena de confianza. Para ello se ha usado el framework seleccionado en el apartado anterior.

Para comenzar con una visión general de la CA, es conveniente especificar que la empresa que la custodia debe cumplir una serie de requisitos de seguridad que no sólo se limitan al campo digital, sino que hay una serie de normas establecidas por el NIST que especifican que se debe cumplir un nivel de seguridad de tipo militar (EAL5) para asegurar la integridad de los servidores (Figura 2) que contienen los datos que se encuentran almacenados en los certificados. Esta seguridad incluye normas como autenticación en tres fases o la utilización de un búnker subterráneo. Estos datos sobre la seguridad necesaria para la posesión de una CA dan al lector una imagen de la importancia que tiene la propia CA y la información que se maneja desde la misma. A su vez, esa importancia hace entrever la necesidad de tratar de manera segura las claves que encierran los certificados, y por lo tanto, el hincapié que se ha hecho a lo largo de la investigación para migrar de manera segura un portafirmas al entorno móvil, incluyendo la intervención de elementos seguros en el sistema.

Figura 2. HSM. Contenedor de CAs y funcionalidades

Cuanto mayor sea la seguridad y la disponibilidad de la entidad de confianza que mantiene la CA, más confianza genera a sus clientes. Esta confianza se blinda en muchas ocasiones con seguros, que dan valor económico a cada certificado almacenado. Tras la seguridad física, está la seguridad digital de los datos que se están tratando. La seguridad digital debe ir acorde con especificaciones físicas que se exigen, para no generar un eslabón más débil que el otro. En este análisis la parte que interesa es la que atañe al mundo digital, materializándose en la implementación para la adopción de una CA.

El servidor de CAs no está compuesto por un único nodo, es más, para la creación de la CA generada ha sido necesaria la creación de una CA genérica anterior, a partir de la cual se pueden generar nuevas CAs, que a su vez tienen la posibilidad de ejercer de nodos padre de otras (ver Figura 3).

Para la adopción de una CA se ha desplegado un servidor seguro, previamente configurado con Apache para asegurar la privacidad de la información que se ofrece y evitar recibir comunicaciones maliciosas. También se hace necesaria la integración de un módulo criptográfico que dote de fortaleza a los archivos que se manejan. En este caso, se utiliza *Java Cryptography Extension*. Una vez activo el servidor, queda configurado para la creación de las distintas CAs.

En un primer paso se ha creado un perfil para la RootCA, asignándole un password robusto; el algoritmo de cifrado; el tamaño de la clave privada, que depende del uso que se le vaya a dar; una validez, durante la cual; los certificados que estén expedidos por esa CA serán válidos, y además podrán ser comprobados contra el servidor donde está alojada la CA de forma remota; un *domain name*, que la distinguirá del resto de CAs, y las direcciones donde se encuentren la lista de revocación más actual y el servidor de comprobación online.

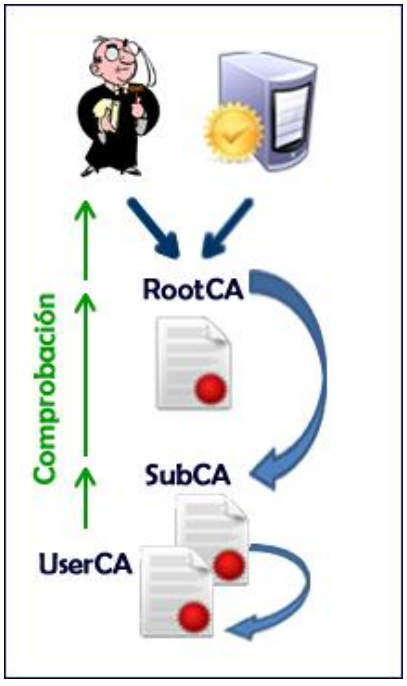

Figura 3. Composición de una CA

Al comprobar la validez de un certificado, se comprueba la CA que lo ha expedido, y si se trata de un nodo hijo, se comprueba sucesivamente la lista de validez de su nodo padre (ver Figura 3) hasta que un nodo es conocido por el receptor. A este paradigma se le conoce como cadena de certificación.

Con la CA raíz creada, se puede crear el perfil que va a caracterizar las SubCAs, CAs que en una cadena de certificación serán nodos hijo de la primera. En las SubCAs sólo

hay que indicar su validez, ya que el resto de atributos son heredados de su padre correspondiente en la cadena de certificación.

Una vez se ha realizado la configuración de las SubCAs ya es posible crear CAs para usuarios, ciudadanos, servidores, o cualquier otro perfil necesario. El resto de las CAs del sistema tendrán el perfil de SubCA y están firmadas por RootCA, que la convierte en su nodo padre.

Cuando ya existan las CAs necesarias, se deberían configurar los perfiles de certificado, que pueden ser para cifrado o autenticación. Esto dota a las claves que se generen dentro de los certificados de usos como capacidad de cifrado, no repudio, o la firma digital, elemento estudiado en este proyecto para su migración segura a movilidad. Cada perfil de certificado lleva asociado un período de expiración, como el que los investigadores de la Policía Nacional han definido de 5 y 10 años para el DNIe.

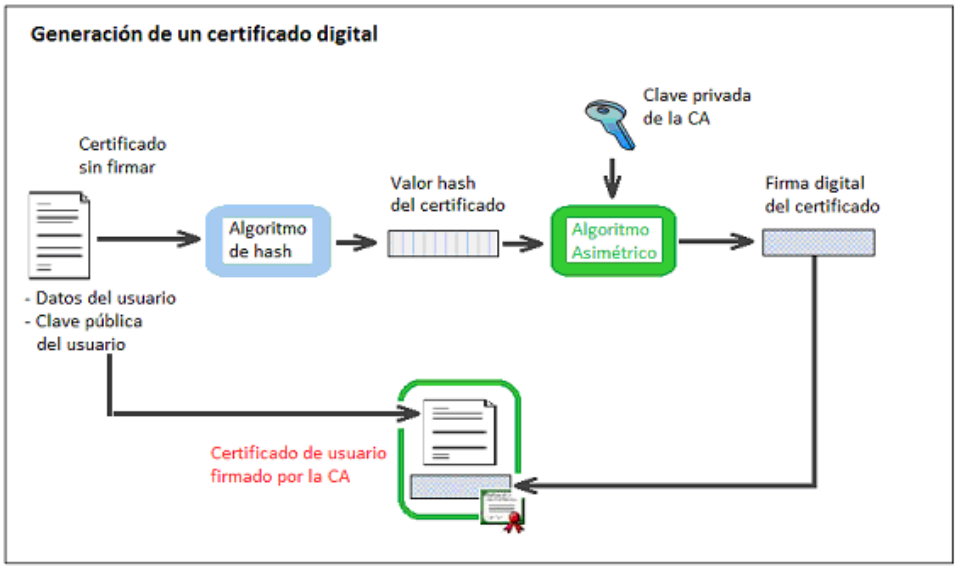

Figura 4. Proceso básico de generación de un certificado

En este momento ya se ha finalizado la preparación del ecosistema para la generación de identidades y ya es posible expedir certificados (ver Figura 4) que deben tener los siguientes campos:

- CN, Common name
- UID, Unique identifier
- O, Organization
- C, Country
- A estos campos es posible añadir alguno opcional, como el e-mail en los certificados de trabajador del Gobierno Vasco que emite Izenpe

A estos certificados les es asignado un perfil acorde al objetivo que deba cumplir, por ejemplo firma, y su RootCA, ya que se debe incluir una cadena de certificación para demostrar su validez.

De este modo ha quedado definida la creación de un ecosistema desde un punto más general hasta llegar al certificado. En un capítulo posterior se explica cómo debería ser el diseño de la consumición de dichos certificados, que en un entorno de PC es conocido, aunque aún da muchos quebraderos de cabeza a sus diseñadores y desarrolladores. Por extensión, el objetivo de este análisis es conocer si es posible generar un entorno de firmas seguras en movilidad añadiendo elementos seguros, objetivo de la investigación llevada a cabo para este proyecto.

3 ELEMENTOS SEGUROS

Los elementos seguros incluyen a las tecnologías embebidas que se utilizan en varios tipos de chips para proteger información sensible de ataques tanto hardware como software. Estos elementos serán empleados en crear soluciones *end-to-end* de confianza [Larsson et al.].

Algunos de los usos que se les da a las aplicaciones que utilizan elementos seguros incluyen funcionalidades tan interesantes como la firma digital, el cifrado de correos electrónicos, pago móvil, autenticación en SSL y VPN para redes empresariales o autenticación de clientes en aplicaciones propias. El objetivo que tiene la introducción de un elemento seguro en este proyecto es, precisamente, la autenticación que va a controlar que el acceso a la aplicación se lleve a cabo de una forma segura y controlada.

Dentro de este entorno de seguridad en el acceso a aplicaciones o terminales móviles, se hace posible la autenticación de dos factores, consistente en el acceso combinado de elemento seguro y PIN. Mediante el uso de elementos seguros se reafirma la protección de claves en caso de pérdida o robo del terminal.

En los subapartados que integran el primer apartado se van a introducir las diferentes características de los diferentes elementos seguros en desarrollo. En el segundo apartado se sopesan las características de los elementos descritos, las necesidades que requiere el proyecto, y las posibilidades de las cuales se dispone tanto tecnológicamente como económicamente, para integrar elementos seguros y garantizar de este modo la autenticación segura que se desea para el demostrador final. Finalmente, el tercer apartado muestra la integración de un elemento seguro a raíz del estudio llevado a cabo en el capítulo.

3.1 TIPOS DE ELEMENTO SEGURO

A continuación se describen los tipos de elemento seguro que en la actualidad se encuentran en proceso de diseño o desarrollo. Con este estudio se arroja luz sobre las distintas formas de almacenar datos de una manera segura y las posibilidades de cada una de ellas.

3.1.1 MICRO SD SEGURA

La tarjeta micro SD segura es un dispositivo de seguridad que combina una tarjeta de almacenamiento masivo estándar de memoria flash con un elemento seguro. Este elemento seguro está formado por un chip, con menor capacidad de memoria, y un sistema operativo *Java Card Operating System* [JavaCard] que controla el código que se puede ejecutar dentro del elemento seguro. La tarjeta micro SD segura tiene la ventaja de ofrecer la funcionalidad completa de una *smart card* en un elemento portable

estándar [Rankl&Effing], compatible con cualquier sistema operativo y host de aplicaciones SD. Además es compatible con varios móviles que se encuentran en fase de producción y con la mayor parte de PCs, por medio de un adaptador y un lector.

La seguridad que proporciona, así como las funcionalidades que ofrece, es aplicable a una gran cantidad de aplicaciones que requieren la protección de los datos del usuario o procesos de transacción seguros.

Desde el punto de vista hardware, la tarjeta micro SD ofrece las ventajas de una tarjeta de memoria SD normal con unas dimensiones más reducidas, aspecto muy útil en entornos de movilidad.

El chip integrado en este tipo de tarjetas seguras incluye una serie de algoritmos como RSA, DES, 3DES o SHA1 que facilitan el uso de aplicaciones seguras, como pueden ser transacciones bancarias y almacenamiento seguro de certificados digitales para aplicaciones de PKI.

Uno de los problemas asociados a las micro SD en cuanto a su integración total se refiere, viene determinado por la negativa de Apple a incorporarlas en sus dispositivos móviles, reduciendo significativamente su adopción generalizada.

3.1.2 (U)SIM

Las tarjetas SIM son módulos formados por circuitos integrados que albergan datos de los usuarios y de identificación, habitualmente protegidos por una clave. La información almacenada en la tarjeta SIM se almacena y gestiona de manera separada a la que se encuentra en la memoria del terminal. Como los otros elementos seguros, las SIM pueden actuar como base para la seguridad de la información que es utilizada en aplicaciones que necesiten establecer funcionalidades como cifrado de datos, autenticación o almacenamiento de claves.

El uso principal de este tipo de tarjetas se da en el ámbito de la telefonía, ya que todos los terminales móviles y algunos de los routers fijos que operan actualmente necesitan utilizar estas tarjetas para poder establecer las llamadas y las conexiones de datos. Estas conexiones y otras operaciones se llevan a cabo desde el elemento seguro, o con el acceso a través de él, habitualmente protegidas por un código PIN.

Por lo tanto, este tipo de tarjeta es ampliamente conocido, pero uno de los problemas más importantes que presenta es precisamente la influencia de los operadores de telefonía sobre este elemento. Al contener información privada sobre las redes de telefonía y los datos del cliente, no es posible acceder libremente a este elemento, por lo que otros datos que necesitan permanecer seguros, como los datos bancarios del cliente [Silvester], no pueden ser almacenados en el mismo módulo sin un permiso específico de la operadora de móvil propietaria del módulo SIM.

3.1.3 EMBEDDED SECURE ELEMENT

El elemento seguro embebido (eSE) es un elemento seguro que se incluye en el chipset del terminal, dotando al terminal de un elemento donde almacenar datos sensibles de forma segura. Este elemento seguro surge como alternativa a la cuestión que plantea quién debe tener el control del almacenamiento de la información. La solución que se da

por parte de los fabricantes de terminales es incluir el elemento seguro en el propio terminal, y así ser independiente de bancos y operadores de telefonía.

Además, los elementos seguros embebidos proveen un área protegida para aplicaciones seguras, como pagos bancarios y *ticketing* [Van Thanh] usando la tecnología NFC para interconectar esta área con elementos externos. Esta tecnología se puede aplicar a compras y otros nuevos casos de uso.

3.1.4 ARM TRUSTZONE

TrustZone es una tecnología de virtualización, en la que el procesador puede cambiar entre modo normal y modo seguro. Integra seguridad hardware y software, y posibilita trabajar utilizando sistemas empotrados de confianza. Ésta es la base de una arquitectura de ejecución segura que permite tanto a operadoras móviles como a fabricantes incorporar la seguridad en tándem con sus componentes hardware y software. El entorno seguro de ejecución ofrecido incluye servicios tales como criptografía, almacenamiento seguro e integridad que aseguran tanto el dispositivo como la plataforma.

Las aplicaciones que trabajan en el Entorno de Ejecución de Confianza (TEE) se encuentran separadas del sistema operativo para evitar ataques de software y malware. El cambio de modo en el dispositivo asegura un aislamiento del hardware, donde coexisten las aplicaciones de confianza, por ejemplo de distintas compañías de pago.

Según la arquitectura que presenta [Winter], TrustZone sirve para implementar DRMs sin influir en el funcionamiento del resto del sistema. De este modo, se puede proteger claves personales e información sensible y así evitar que se cree un ecosistema criminal en el entorno de la movilidad.

3.2 ELECCIÓN DE UN ELEMENTO SEGURO

Para experimentar en un entorno de firma digital hay que lograr que el usuario se identifique unívocamente en la aplicación, y conseguir así acceder de manera segura a la misma. Como se dijo en la introducción, éste es el segundo objetivo del proyecto. Los permisos de acceso a la aplicación se controlan mediante la utilización de uno de estos elementos seguros. El elemento seguro se elige en base a una ponderación de la serie de cualidades deseables y los inconvenientes que pueda suponer su adopción.

A través del elemento seguro que se gestiona en el demostrador del proyecto se va a controlar la entrada a la aplicación. Sólo el usuario indicado puede gozar de este permiso, ya que las credenciales del usuario que puede acceder a la aplicación se almacenan de manera segura en la Smart Card de la cual es propietario, y de la cual no existen copias. Por este motivo también se asegura que no existen copias de las credenciales que permiten al usuario su acceso a la aplicación. Por otra parte, solamente se permite que el usuario conozca el código de acceso al elemento seguro. Si cualquier otra persona o sistema intenta tener acceso a la aplicación, se le exigirá el código PIN, en caso de no conocerlo no se le da acceso, y si comete un cierto número de errores en el acceso al elemento seguro, este quedará bloqueado, bloqueando así el acceso a la

aplicación. En el caso de que se dé esta situación o que el usuario no recuerde su PIN y supere el número máximo de intentos fallidos, el usuario debe pedir/adquirir un nuevo elemento seguro con nuevas credenciales que lo identifiquen, ya que se pierde toda posibilidad de acceso a las credenciales que contenía el anterior elemento seguro. Para este proyecto se ha elegido que el número máximo de intentos fallidos en el acceso a la aplicación para que el elemento seguro quede bloqueado sea de tres accesos. El rango de accesos fallidos especificado por GlobalPlatform [GlobalPlatform] para todos los elementos seguros que sean compatibles con sus estándares varía entre 2 y 8 errores consecutivos. Por otra parte, también es importante distinguir entre el código de acceso a un elemento seguro y el código de acceso a la aplicación que lo controla o que hace uso de sus servicios. En el segundo caso estaríamos hablando de una capa de seguridad diferente, ya que aunque el acceso se realizara mediante una identificación segura, el código de la aplicación propiamente dicho no se almacena de modo seguro al quedar instalado en memoria flash, mientras que la información sensible del usuario que se encuentra almacenada dentro de un elemento seguro sí queda protegida por un elemento hardware externo.

Quedando aclarado el modo de acceso seguro a las credenciales del usuario y una vez que se han estudiado todas las posibilidades existentes actualmente en el mercado en cuanto a elementos seguros se refiere, se debe elegir uno de ellos para la consecución de este proyecto. Repasando las características y posibilidades de cada elemento seguro, la opción que se ajusta mejor a las posibilidades de este proyecto es la adopción de tarjetas micro SD. La tarjeta micro SD segura que se utiliza en el proyecto proviene de la firma alemana Giesecke & Devrient (ver Figura 5) empresa dedicada a la fabricación de estas tarjetas, así como de otros elementos seguros y el desarrollo a bajo nivel de sistemas relacionados con ellas. En esta tarjeta, la información segura queda almacenada en un tipo memoria, de pequeño tamaño y con acceso restringido, mientras que la tarjeta no pierde su funcionalidad de almacenamiento masivo, conservando la mayor parte de la memoria flash que posee comúnmente una tarjeta SD de características comunes. Gracias a esta particularidad, el móvil con ranura micro SD que se va a utilizar en el desarrollo del proyecto combina el acceso seguro con el almacenamiento de la información de aplicación en un fichero ubicado en la raíz de la propia SD.

Figura 5. Tarjeta micro SD segura utilizada en el proyecto

Los motivos que han llevado a la elección de la tarjeta micro SD como elemento seguro para llevar a cabo el demostrador han sido varios. El primero de ellos es el estado actual

de la tecnología, que permite la utilización de tarjetas micro SD como elementos seguros. Muchos de los terminales móviles que actualmente se encuentran en el mercado disponen de ranura micro SD en su interior, el que se va a utilizar en el demostrador entre ellos.

Para la introducción de datos que se desea almacenar dentro del elemento seguro, la elección de la micro SD nos proporciona la libertad necesaria para tener acceso a la misma sin depender del fabricante ni de credenciales de acceso. En este sentido, tanto TrustZone como los sistemas operativos que deben integrarlo para gestionar los cambios entre mundo seguro y mundo de aplicaciones normales están aún en fase de definición, comenzando su despliegue para realización de pruebas, pero sin una integración demasiado amplia en el mercado de la movilidad.

Los elementos seguros embebidos se incluyen hoy en día en varios terminales móviles (como el Google Nexus S) pero su futuro es incierto en estos momentos debido a la guerra entre fabricantes de terminales y operadoras de telefonía móvil. En otro lado se encuentran las tarjetas SIM, que se gestionan de manera similar a las tarjetas micro SD seguras, pero cuentan con la gran desventaja de que han sido blindadas por las MNO's a través de permisos de acceso. Con lo cual, si no se es una operadora de telefonía, no es posible el acceso a la escritura de datos en elementos de este tipo.

Por último, la disponibilidad de terminales ha influido, ya que el material disponible incluye un teléfono que no dispone de eSE ni de chip con hardware TrustZone, pero sí contiene una ranura para inserción de tarjetas SD.

La utilización de un elemento seguro en este proyecto garantiza un nivel de seguridad elevado, identificado como EAL5. La seguridad se basa en la combinación de (i) "algo que tengo", el elemento seguro que no es accesible excepto si se accede con la clave indicada, y (ii) "algo que sé", indicado por la propia clave introducida por el usuario. Dicha clave no puede ser conocida por nadie más.

En la aplicación que va a actuar de demostrador se van a ver claramente estas particularidades (mostrado en la Figura 6). Al iniciar la aplicación se muestra una pantalla en la cual se va a exigir un código PIN, que va a dar acceso al elemento seguro. En caso de que el código sea erróneo o que no se introduzca ningún código y se intente continuar con la ejecución de la aplicación, esta lo detecta y deniega el acceso a la misma. La seguridad se aumenta evitando el acceso recursivo a la autenticación en la aplicación, ya que tras un cierto número de intentos, la aplicación se cierra y guarda un *flag* de sesión que se mantiene activo hasta que el terminal móvil haya sido reiniciado, teniendo que cerrar y abrir tanto aplicación como sistema operativo cada vez que se supera ese número máximo. En caso de querer añadir una seguridad de mayor nivel, se debería implementar un bloqueo del chip seguro, el cual es definitivo. En ese caso, habría que expedir una tarjeta completamente nueva con los credenciales del usuario, ya que la anterior habría quedado completamente inutilizada. Esta situación se da con las tarjetas de crédito dadas de baja o los chips de los DNIs caducados. Por otra parte, y atendiendo a la parte principal que influye en este capítulo, en el momento que se introduce el PIN y se desee continuar hacia la parte principal de la aplicación, cuando la misma detecte que no se ha introducido la tarjeta correcta, que sus datos han sido corrompidos, o simplemente que no se encuentre una tarjeta en la ranura dedicada a las

micro SD, se muestra un mensaje de error y se prohíbe el acceso al resto de la aplicación.

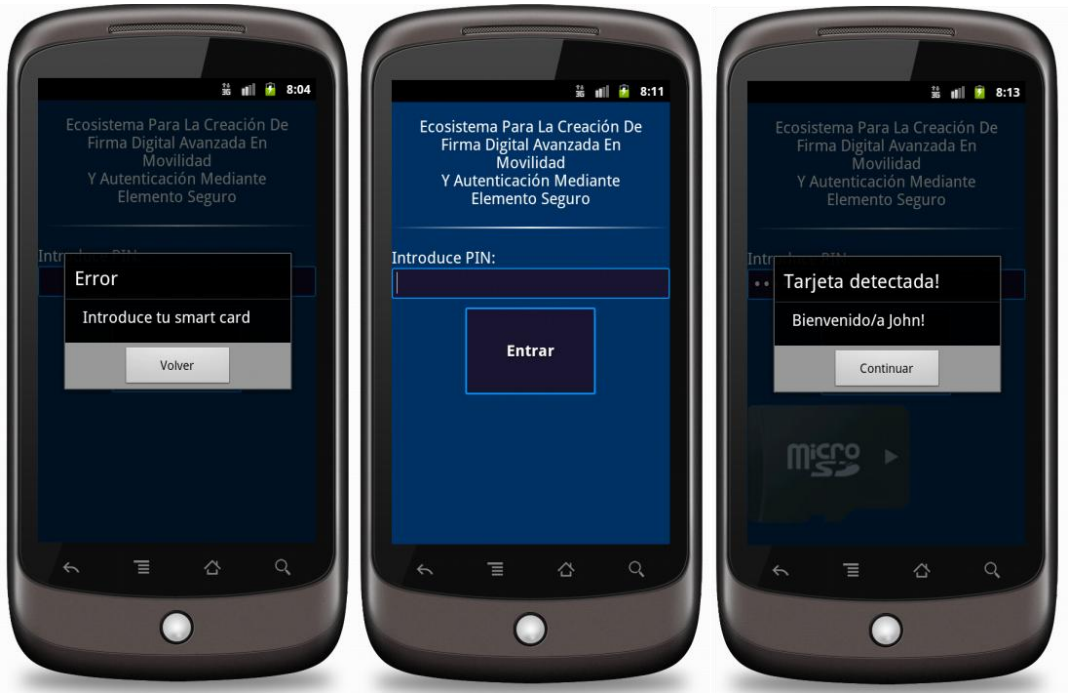

Figura 6. Petición de credenciales (erróneo, original y correcto)

Atendiendo a la distribución del sistema de firma con acceso seguro, la adopción por parte del usuario del elemento seguro para su acreditación es tan sencilla como introducir la tarjeta micro SD que le ha sido otorgada personalmente en la ranura correspondiente de su dispositivo móvil. La entrega ha de ser presencial y por medio de la identificación pertinente, puesto que de este modo se asegura que nadie más que él conoce la clave que se encuentra en su interior. En el desarrollo de la aplicación se ha incluido la librería que permite al terminal comunicarse con la parte segura de la tarjeta criptográfica, con lo cual, una vez se introduce la tarjeta correcta, la aplicación leerá los datos que contiene cuando se requiera, si el acceso es correcto.

3.3 INTEGRACIÓN DE UN ELEMENTO SEGURO

En este apartado se despliega de modo muy general la forma en se ha diseñado la integración de un elemento seguro. En primer lugar se muestra la arquitectura de la interacción de los elementos seguros con el resto del ecosistema móvil que lo rodea. Como punto final a este capítulo, se va a explicar la forma en que datos sensibles han sido almacenados y manejados para su explotación, quedando protegida la información que se desea que no sea expuesta al exterior [Schwiderski-Grosche] [Scheuermann]. Recordamos se puede tratar de datos como claves privadas, datos bancarios, semillas para generadores de claves, etc.

Disponer de una implementación es necesario para la creación del ecosistema. Posteriormente se podrá realizar una labor investigadora comparando diferentes implementaciones.

Se ha utilizado la arquitectura de este tipo de tarjeta, detallada en la Figura 7, de manera que se aprovecha su característica de poseer memoria flash, gestionada de forma habitual como un dispositivo de almacenamiento masivo, pero también cuenta con una zona segura, controlada por el sistema operativo JavaCard. En un directorio almacenado en la raíz de la memoria flash se han incluido datos de la aplicación tales como el certificado que el usuario va a usar para realizar sus firmas digitales, datos visuales de la propia firma, o los documentos que se van a firmar o ya se han firmado. Si el certificado se encuentra dentro del elemento seguro, se dice que está en un contenedor hardware. Se habla de contenedor software de certificados en caso contrario.

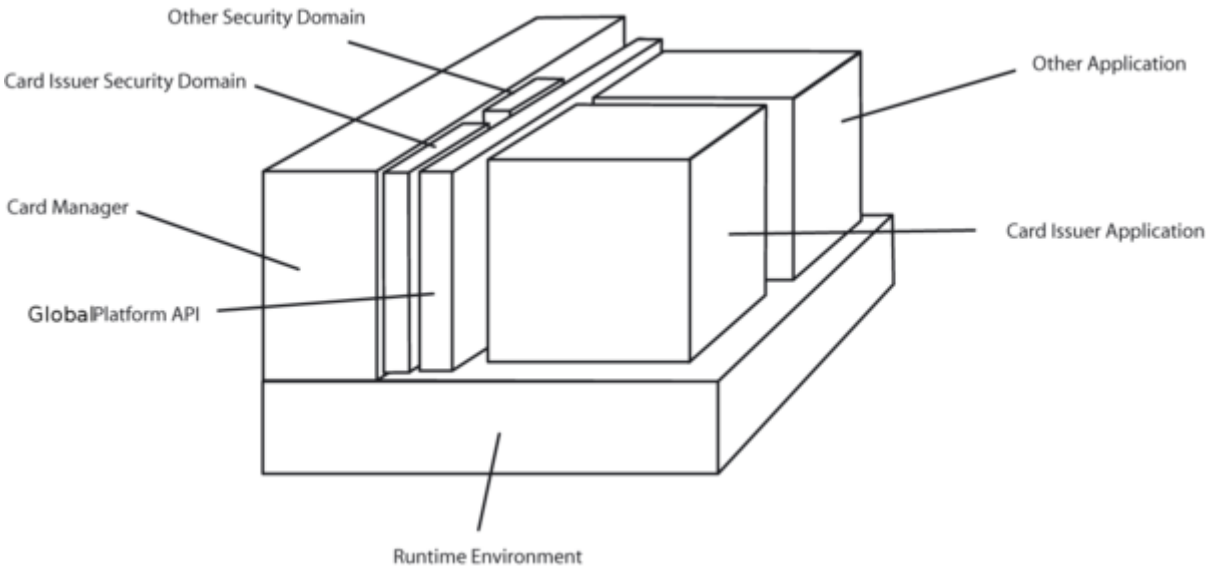

Figura 7. Arquitectura de un elemento seguro (GlobalPlatform)

En la parte segura de la tarjeta micro SD se ha instalado el applet que permite al usuario realizar el acceso a la aplicación de modo seguro. Tanto los datos de acceso como el proceso se realizan, por lo tanto, dentro de la parte segura, quedando totalmente inaccesible cualquiera de estos elementos desde el exterior sin la clave de acceso que sólo el usuario conoce, y dotando de esta forma de total seguridad al sistema de firma.

El applet creado se encuentra escrito en código Java, quedando almacenado en un archivo con extensión ".cap". La comunicación con el exterior se realiza a través de APDUs, una serie de pares de bytes, especificados en hexadecimal, que ordenados de forma correcta y enviados a través de un canal seguro (naranja en la Figura 8), son procesados en el elemento seguro de la smart card donde se genera una respuesta (verde en la Figura 8), que es enviada de vuelta al exterior. El formato de este tipo de comunicación se muestra en la siguiente porción de código (Figura 8).

```
Log.d("SmartCard","Getting Session from the first reader...");
Session session;
byte[] respApdu = null;
try {
      session = readers[0].openSession();
      // Select the applet which contains the credentials
      Log.d("SmartCard","Getting logical channel from the
      session...");
      Channel channel = session.openLogicalChannel(new byte[] {
            (byte)0x01, (byte)0x02, (byte)0x03, (byte)0x04,
            (byte)0x05,
            (byte)0x06, (byte)0x07, (byte)0x08, (byte)0x09,
            (byte)0x00, (byte)0x00  });

            // Send "open" command
            Log.d("SmartCard","transmit()");
            respApdu = channel.transmit(new byte[] {
                  (byte) 0x90, 0x00 });
                  channel.close();
            }
      }
} catch (IOException e) { e.printStackTrace(); }
```

Figura 8. Comunicación con el elemento seguro mediante APDUs

En caso de que la respuesta sea correcta, se devuelve el código 90 00. Otra posible respuesta que el elemento seguro puede enviar es una cadena de bytes hexadecimales que contengan los datos solicitados. En caso de error, el elemento seguro responde con un código de error en el que se indique el tipo de error encontrado, ya sea de comunicación, de gestión, de procesamiento, etc.

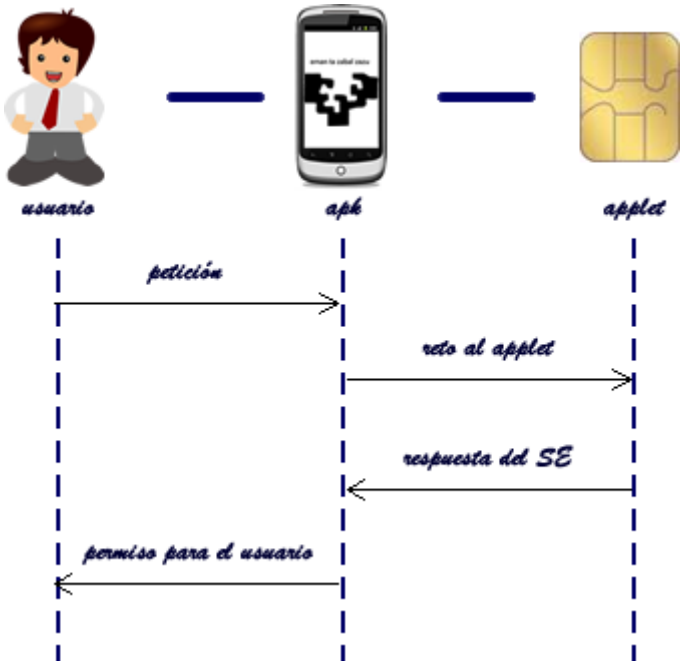

Figura 9. Comunicación entre aplicación y elemento seguro

Desde un dispositivo móvil solamente se permite la lectura de datos del elemento seguro, ya que la escritura tanto de applets como de certificados se debe llevar a cabo a través de un *handshake* de APDUs con el que se obtiene el acceso en modo escritura. En muchas ocasiones, aunque los códigos de acceso para este *handshake* no sean privados, son suficientemente largos como para que se encapsulen en programas software que los propios fabricantes de elementos seguros proporcionan o venden al adquirirlos.

Programáticamente es posible el acceso al sistema operativo Java Card en modo lectura, de forma que se puede consumir la información que contienen los applets, pero no modificarla. En el proyecto se utiliza el código para consultar si el reto el que el usuario pretende utilizar para acceder a la aplicación de forma segura es correcto (ver Figura 9). En caso de serlo, el applet descrito, al que se accede desde la aplicación devuelve un código 90 00, que como se ha explicado en este punto, comunica el permiso de acceso.

Como se puede observar en la Figura 8, para acceder al applet que se identifica por un identificador de aplicación que es único, al igual que los bytes que constituyen su nombre, es necesario abrir un servicio que establece a su vez un canal seguro. A través de ese canal, que puede ser lógico o físico, se llama al applet y se espera la respuesta a los datos que se le envían encapsulados en códigos APDU. El applet creado para este proyecto se almacena en el elemento seguro a través del software de desarrollo que proporciona G&D. No hay que confundir un applet clásico de Java con un *Java Card Applet*, recordando que este último se refiere a un programa con identificador único que se ejecuta dentro del elemento seguro.

Para llevar a cabo el proceso descrito se hace uso de un servicio proporcionado por un grupo de desarrolladores llamado "*seek-for-android*". Este grupo de Google Code se

encuentra centrado en la creación de entornos seguros y marca una referencia en este campo.

En definitiva, en el demostrador se han incluido, aparte de la aplicación de firmas, el entorno necesario que permite el acceso a la parte segura del elemento seguro, y la aplicación de acceso seguro ya instalada dentro de la parte segura de la micro SD. Estas partes se pueden distinguir en el diseño en la Figura 10 [ASSD], donde la memoria flash (en rojo) queda claramente diferenciada por un controlador (en azul) de la memoria que contiene las aplicaciones seguras (en verde). Este ecosistema permite securizar la aplicación y prevenir el acceso a la misma de usuarios no permitidos y que tengan intenciones que puedan perjudicar al dueño de la aplicación.

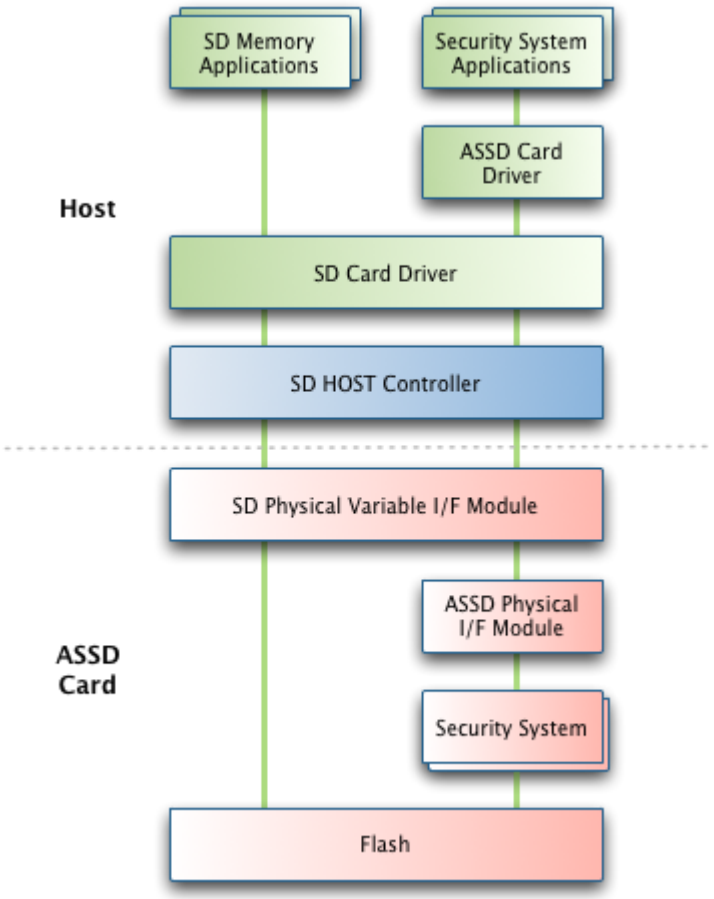

Figura 10. Diseño de los elementos que componen una tarjeta SD de acceso seguro

Finalmente, la micro SD segura permite realizar las mismas funciones que el resto de elementos seguros que se han descrito en este capítulo. Por este motivo, la información almacenada en el elemento seguro puede variar y es posible ejecutar un pequeño programa, o como en este caso almacenar la identidad de un usuario para llevar a cabo un control de accesos. El propio control de acceso que se almacena en el applet de Java Card puede ir desde un identificador, como es el caso en este proyecto, hasta un certificado de ciudadano con validez legal, el cual en este proyecto queda almacenado

en un almacén software de certificados, aunque tampoco se comprueba su validez legal, ya que los certificados generados son creados por una autoridad de certificación que emula el funcionamiento de una CA real. Si las credenciales de acceso que se crean para este proyecto contuvieran un certificado digital, se podría realizar firma, cifrado o cualquier otra operación que requiera de una identificación estándar, segura y reconocida. Este caso se da con cualquiera de los elementos seguros de la misma manera (Figura 11), ya que todos siguen las pautas marcadas por los estándares definidos por *Global Platform*.

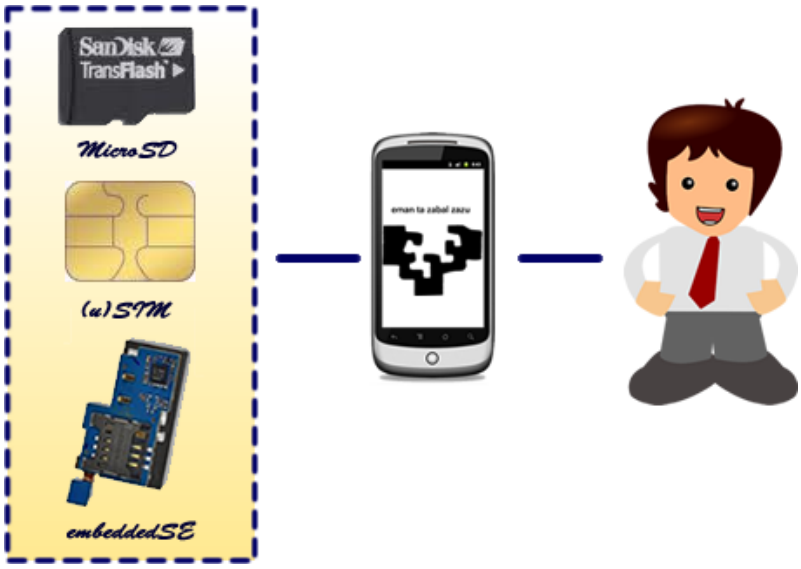

Figura 11. Interacción de los elementos seguros con el usuario

El trabajo realizado en este capítulo se verifica al integrar el sistema completo que se describe en los siguientes capítulos.

4 IDENTIFICACIÓN MEDIANTE CERTIFICADOS DIGITALES

El certificado digital es usado para identificar entidades (personas físicas, empresas…) de forma unívoca y de este modo puede entre otras cosas, identificarse dentro de un sistema determinado. Este capítulo del estudio trata sobre cómo autenticar de forma segura al usuario final de una aplicación móvil, y así poder confirmar su identidad y evitar que pueda repudiar haber firmado o dado su visto bueno sobre un determinado documento, como si de una firma manuscrita presencial se tratara. Este aporte ofrece la posibilidad de acelerar un gran número de trámites, ya que si la exploración aporta un resultado positivo y la firma es robusta, su validez es legal.

En los dos capítulos anteriores se ha estudiado y experimentado con las CA y los elementos seguros. Se ha expuesto cómo implementar un sistema seguro. Este capítulo expone el proceso que garantiza transacciones seguras: los certificados digitales. Los conocimientos que se exponen en este capítulo facilitan la comprensión del sistema de firma digital que se expone en el capítulo siguiente.

La aplicación de los certificados al mundo de la movilidad es uno de los puntos que actualmente están evaluando diferentes expertos en seguridad a día de hoy, lo que puede observarse en las numerosas publicaciones científicas que desde los últimos dos años comienzan surgir [Blythe] [Martínez-Peláez et al.] [Toorani & Beheshti]. Así pues, la bonanza de la aplicabilidad de dichas tecnologías en los dispositivos móviles es algo bien sabido tanto por los expertos en seguridad como de movilidad, pero a día de hoy los desarrollos en la práctica sobre la materia no están aportando grandes éxitos. Esto se debe en gran parte a no existir un soporte universal para su custodia en movilidad.

4.1 RELACIÓN CON EL RESTO DE ELEMENTOS ESTUDIADOS

En el primer capítulo se ha hecho una descripción teórica de los certificados digitales. También se ha detallado el entorno que culmina con su expedición. Pero el enfoque proporcionado en el segundo capítulo, "ENTORNOS PKI", los contempla desde el punto de vista del emisor de los certificados. En cambio, este capítulo está más centrado en el uso del certificado por parte del usuario y el ecosistema que une el certificado con la firma digital, la cual es tratada en el capítulo quinto, "FIRMA DIGITAL EN MOVILIDAD", y muestra un claro ejemplo de un uso de los certificados con gran significado. El hecho de conocer y utilizar certificados digitales no es en sí motivo de innovación. Pero sí lo es el modo en que se hacen uso en este proyecto y el acercamiento a un sistema de firma digital en movilidad.

En medios más controlados, y que llevan más largo tiempo en desarrollo, como es el caso de los entornos de escritorio, es habitual encontrar aplicaciones de firma, sobre todo al entrar en contacto con administraciones públicas y entidades bancarias, e.g. [Herzberg]. Estos cuerpos, que constituyen una punta de lanza hablando de seguridad,

dada la relevancia de los datos que ambas manejan, dan una gran importancia a la seguridad de los mismos. Es por tanto que no debe quedar en el olvido la seguridad en la rápida migración a entornos móviles que la sociedad actual está sufriendo. En consecuencia, el uso de los certificados de una forma segura es uno de los avances buscados en el resultado final del estudio que ocupa a este proyecto.

En este proyecto se desea utilizar certificados digitales y arquitecturas PKI para la resolver el reto de la seguridad y confidencialidad de los datos tratados por la plataforma [Hiltgen]. La temática es un reto en sí misma y se aspira a adoptar las últimas tecnologías y desarrollos realizados por centros tecnológicos y universidades a nivel internacional para facilitar dicha adopción. A continuación se resume brevemente la tecnología, que a día de hoy es altamente recomendada en servidores seguros y que se quiere trasladar al mundo de los smartphones.

4.2 CERTIFICADOS DIGITALES Y SUS POSIBILIDADES

Los certificados se podrían definir como una forma de distribuir las claves públicas, esto se da gracias a que son firmados digitalmente por una Entidad Externa Confiable, también conocida con su nombre inglés, *Trusted Third-Party*, que actúa de emisor de los certificados. Esta entidad es llamada también Autoridad de Certificación, CA o *Certificación Authority*. Un certificado emitido mediante el proceso que recoge en esta investigación, garantiza que la CA confía en la identidad de la persona a la que pertenece el certificado. Esto se implementa firmando el certificado con la clave privada de la CA (que sólo ella conoce) y adjuntándola al final del mismo. Con esto se permite que cualquiera pueda verificar utilizando la clave pública de la CA del firmante que el certificado ha sido firmado por una CA en concreto. Existen diferentes tipos de certificados entre los cuales tenemos:

- X.509 (Identity Certificate)
- Certificados SPKI
- Certificados PGP
- ACs (Attribute Certificates)

Por motivos de estandarización se usa el primer tipo de certificado, que guarda la estructura exigida para que un certificado pueda generar firmas avanzadas o robustas. La generación de una entidad digital capaz de expedir firmas con validez legal debe reflejar una serie de datos que la identifiquen, tales como información del propietario del certificado, información de la entidad que lo expide y el tipo de algoritmo criptográfico utilizado . De esta forma, el estándar X.509 cumple con los objetivos propuestos en esta investigación.

Se hace uso de la clave pública de un certificado digital para asegurar las funciones de identificación y autenticación del usuario, lo que comúnmente es conocido como firma digital. Dado que sólo el titular del certificado conoce la clave privada que está asociada a la clave pública del certificado con que se firma, se considera que la información

contenida en el mismo (excluyendo la clave privada) puede ser libremente distribuida sin comprometer la integridad del usuario que se identifica.

Este tipo de certificados es ampliamente utilizado en seguridad de alto nivel para firma de documentos, autenticación contra servidores, envío de correos, transacciones, etc. El objetivo último de la investigación que se lleva a cabo es contemplar la migración a la movilidad de estas funcionalidades que tan alto valor aportan a muchas empresas de varios entornos, ya que cada vez un mayor número de trabajadores disponen de un smartphone, ya sea a nivel personal, de organización, o dedicado a seguridad gubernamental (como máximo exponente de su uso). Esto coloca las pretensiones de la investigación como un componente de máximo interés para todas las entidades que se encuentren en dicha situación.

4.3 ECOSISTEMA GENERAL DE CERTIFICACIÓN

Los certificados digitales se encuentran habitualmente almacenados en documentos con formato .p12, extensión dada porque cumplen con el estándar PKCS#12 [PKCS]. Este estándar define el formato del archivo, protegido por una contraseña de clave simétrica. El estándar que define la interfaz de los *tokens* criptográficos es el PKCS#11. En este estudio se investiga la conexión y posible integración de almacenes de certificados y elementos seguros criptográficos.

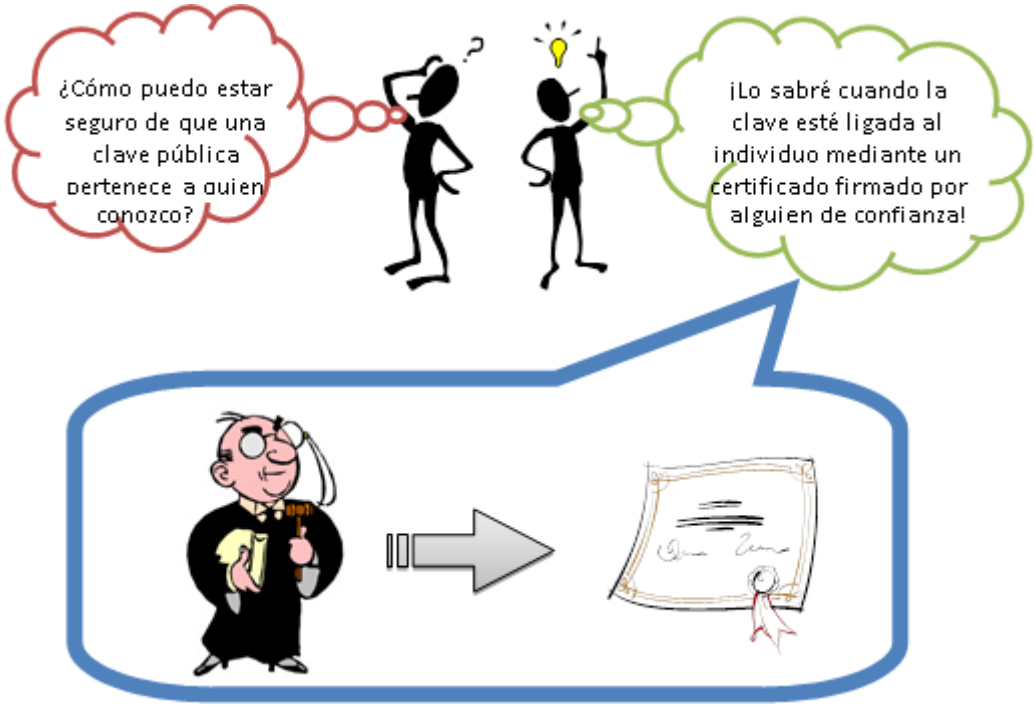

Figura 12. Solución a la problemática de confianza

Ahora bien, el resultado final que se quiere conseguir con el uso de certificados digitales es adquirir el conocimiento necesario para poder asegurar que la clave pública de un

usuario corresponde realmente a ese individuo y no ha sido falsificada por otro usuario que desee hacer un mal uso del certificado (Figura 12). Es necesario destacar que en el mundo de los dispositivos móviles hay muchas más posibilidades de que los datos y aplicaciones del usuario se vean comprometidos teniendo en cuenta el paradigma actual en el que la mayor parte de los dispositivos tienen la posibilidad de conectarse con el exterior, además de la consabida pérdida o robo que puede sufrir el terminal como tal.

En grupos pequeños de usuarios, puede ser suficiente con intercambiar las claves públicas de forma presencial. Pero cuando el ámbito es mayor, la solución consiste en recurrir a un Tercero de Confianza (Figura 13), responsable de garantizar la identidad de las personas o entidades que realizan transacciones a través del canal de comunicación.

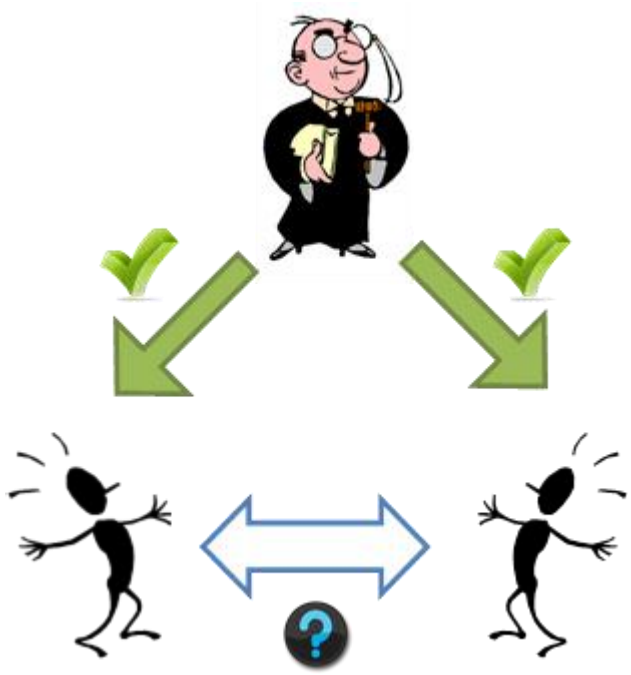

Figura 13. Un tercero en el que las dos partes confían

Esta tercera parte confiable se erige en la figura de la CA expuesta en el Capítulo 2 "ENTORNOS PKI (PUBLIC KEY INFRASTRUCTURE)", encargada de vincular cada clave pública a la identidad de su titular. Esta vinculación se lleva a cabo dentro del certificado digital. El certificado contiene información estructurada acerca de la identidad de su titular, su clave pública y los datos de la CA que lo emitió.

Al incorporar los datos identificativos y la clave pública de su titular, el certificado permite comprobar cuándo un mensaje procede de un determinado usuario. El resultado es que el certificado digital permite comunicar un usuario de forma segura con todos los clientes de una CA conociendo únicamente la clave pública de ésta.

4.3.1 CONTENIDO DE UN CERTIFICADO

En este sub-apartado se describe la estructura de campos estandarizados para X.509 que ha sido definida por la ITU-T para sistemas PKI. El tipo de certificado digital que la CA

que se genera a partir del análisis del Capítulo 2 “ENTORNOS PKI” va a crear está compuesto por los siguientes campos:

- Número de versión y número de serie del certificado
- Identificador del algoritmo utilizado para firma o cifrado
- Nombre (DN) e identificador único de la entidad emisora del certificado
- Período de validez, de modo que llegada la fecha indicada, el certificado dejará de ser válido y ningún dispositivo debería aceptarlo.
- Nombre (DN) e identificador único del titular
- Clave pública del titular
- Campos extra

4.3.2 ECOSISTEMA DE LOS CERTIFICADOS DESDE EL PUNTO DE VISTA DEL USUARIO

Tras conocer el tipo de certificado integrado dentro del ecosistema a crear, es de gran interés conocer cómo el usuario se integra e interacciona en el entorno de las entidades de certificación y cómo interactúa con otros usuarios del sistema en la creación y comprobación de firmas digitales. De esta explicación se obtiene la posición que el usuario adquiere respecto al sistema de firma en movilidad que se está estudiando.

Para interiorizar las relaciones que se establecen con el uso de certificados digitales, el funcionamiento del sistema es el que se describe a continuación:

El objetivo de los usuarios del sistema es comunicarse de manera segura. La información creada por el emisor (ya sea de un documento o en una comunicación) no puede ser alterada durante su transmisión. Y el sistema debe permitir que ambos participantes puedan demostrar que la otra parte participó en la comunicación. En el caso de un documento, toda persona que lo reciba debe poder comprobar que el emisor lo firmó. En la Figura 14 se describe la infraestructura que cumple el anterior caso de uso:

En los siguientes párrafos se describen los pasos básicos que se deben cumplir en la Figura 14 para que se cumpla el caso de uso presentado en este apartado:

1. El emisor tiene en su dispositivo un certificado que ha obtenido tras crear una solicitud de certificado. El certificado obtenido está firmado por la CA, que es de confianza para el receptor, ya que conoce la clave pública de la misma.
    a. Si el certificado es autogenerado, el usuario debe registrarse y pedir a la CA que firme el certificado. El certificado le será devuelto firmado con la clave privada de la CA.
2. El usuario tiene su clave pública confiable, por lo que al firmar con la misma, genera una firma que puede ser verificada por otros usuarios. Esta investigación

añade la ventaja de poder verificar de manera segura la firma desde el propio terminal móvil del usuario.

3. El usuario que desee verificar el documento firmado extrae la clave pública de la CA que firmó la clave pública del emisor. En caso de no conocer la CA del firmante, se debe solicitar una comprobación online para obtener su clave pública.

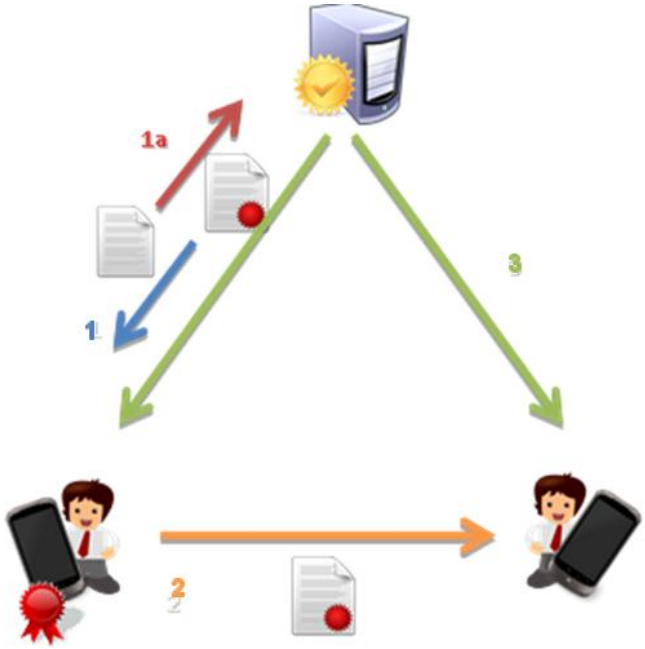

Figura 14. Infraestructura de firma segura con certificados

4.3.3 PROCEDIMIENTOS PARA LA CONSULTA DEL ESTADO DE LOS CERTIFICADOS

Tal y como se ha comentado antes, desde el punto de vista de usuario, la Autoridad de Certificación es básicamente una tercera parte confiable cuya función es la de garantizar de forma fiable que una cierta clave pública está ligada unívocamente a la identidad de una determinada persona física o jurídica. Para ello, la Autoridad de Certificación emite certificados, los publica y mantiene un registro público y actualizado del estado de los certificados, incluida su revocación.

Toda CA debe disponer de un repositorio de certificados accesible vía web u otro medio, donde se publiquen los certificados emitidos, así como las listas de certificados revocados. Hay dos formas fundamentales de almacenar los certificados emitidos y revocados, habilitando así la comprobación de la validez de los certificados utilizados por los usuarios:

- Haciendo uso de CRLs: Son listas en las que se recogen todos los certificados suspendidos y revocados. La CRL debe ser actualizada por la CA a intervalos de

tiempo ajustables dependiendo de las necesidades (o nivel exigido) de seguridad y disponibilidad de la CA.

- A través de OCSP (Online Certificate Status Protocol): Es el protocolo mediante el cual se puede realizar una consulta sobre el estado actual de un certificado concreto. Esto evita tener que almacenar, acceder y verificar toda la lista de certificados revocados, lo cual es un serio inconveniente cuando el número de certificados emitidos aumenta considerablemente.

Está demostrado que es posible utilizar estos mecanismos en movilidad, ya que su comprobación se basa en una lista almacenada en el dispositivo o una consulta online. Por este motivo queda fuera del alcance de esta investigación, pero se nombra dada su importancia en el ámbito de la seguridad de la información.

5 FIRMA DIGITAL EN MOVILIDAD

En este capítulo se expone el análisis realizado para portar firmas digitales a dispositivos móviles. De este modo, el usuario tendrá libertad suficiente para usar sus credenciales de forma cómoda y totalmente segura donde quiera que esté. Así, el usuario tiene la oportunidad de intervenir en procesos de forma remota de manera legal como, por ejemplo, al usar su DNI electrónico.

Tras estudiar los componentes que permiten la firma digital y su autentificación, este capítulo expone cómo se ha experimentado para efectuar la firma digital de documentos PDF en movilidad. La firma de documentos PDF es algo ampliamente utilizado en el ámbito empresarial, donde una gran cantidad de los documentos con los que se trabaja en muchos de sus procesos, necesitan ser firmados por operarios, por intermediarios o por responsables del proceso en cuestión.

La firma digital, aparte de la gestión remota de documentos, tiene la posibilidad de permitir al usuario de una aplicación tanto la carga como la descarga de dichos documentos. Por tanto, a través de la firma digital generada en este proyecto, el usuario tiene que ser capaz de gestionar el documento en su dispositivo móvil, de forma que el proceso al que pertenezca el documento firmado pueda continuar, y otro usuario pueda realizar las acciones que necesite sobre ese documento.

Hay otras acciones necesarias que el ecosistema generado en este proyecto debe tener, como que el usuario final tiene que ser capaz de verificar y de ejercer de firmante en el documento que se esté gestionando en cualquier momento [Sherman et al]. Cualquier otra entidad podrá comprobar una firma desde su dispositivo móvil cuando sea necesario.

El capítulo expone en primer lugar los diferentes tipos de firma digital, clasificados según la seguridad que ofrecen y comparando la dificultad que entraña su adopción. En el siguiente apartado se justifica la elección de un tipo de firma para el sistema a crear.

La sección siguiente resume el entorno del portafirmas, explicando el sistema con el que ha de interactuar el usuario.

En el cuarto punto se desarrolla la implementación del sistema de firma digital que permite al usuario firmar documentos desde su dispositivo móvil a través de un elemento seguro y utilizando su certificado, temas expuestos en capítulos anteriores.

Para finalizar el capítulo se exponen las ventajas que ofrece el sistema portafirmas implementado, en conexión con el resto de elementos estudiados en otros capítulos del proyecto.

5.1 TIPOS DE FIRMA DIGITAL

En este apartado se exponen los tres tipos de firma digital que han definido los estándares. Cada nivel de firma tiene unas características que dependen de su complejidad y de la seguridad que ofrecen.

Según el nivel de seguridad ofrecido por el certificado utilizado sea mayor o menor, en consecuencia la robustez y el valor dado por terceros a la firma creada, irá directamente en proporción. Hay que tener en cuenta que los requisitos relacionados con la seguridad del sistema quedan fuera de la definición de cada nivel de firma. A continuación se nombran los distintos tipos de seguridad que contempla la Unión Europea en cuanto a la firma digital.

- **Firma digital ligera**: Hace referencia a los datos en forma electrónica, adjuntados o lógicamente asociados a otros datos electrónicos, que sirven como un método de autenticación.

  Se utiliza para la autenticación de forma que pueda asegurarse que la persona que la utiliza es realmente el titular de la firma electrónica. Sin embargo, no se puede estar seguro de que la persona es también dueña de la clave con la que se genera la firma. El titular de la clave, se define como una entidad que puede usar la firma electrónica, mientras que el dueño de la clave es la persona que tiene el derecho explícito a utilizarla. Normalmente, un titular de la clave puede ser un servidor que crea las firmas, como por ejemplo, el software de la empresa, y el empleado sería el dueño de la clave.

- **Firma digital avanzada:** Se define cómo la firma electrónica que cumple los siguientes requisitos:

  - Está únicamente vinculada al firmante
  - Es capaz de identificar al firmante
  - Cualquier cambio en los datos a los que se refiere es detectable

  La firma electrónica avanzada tiene un valor más importante que una firma electrónica ligera, ya que garantiza la integridad del texto, así como la autenticación del firmante. Debido a este hecho, se hace necesario definir un tipo de firma digital más avanzada, de forma que pueda asegurarse la robustez de la misma, desde todos los puntos de vista.

- **Firma digital cualificada**: Este tipo de firma digital se define en base a la introducción de requisitos en la infraestructura necesaria para generar la firma digital. En dicha estructura se incluyen tanto el hardware y software utilizado, como el certificado digital necesario para realizar la firma. Por un lado, el dispositivo seguro de creación de firma debe cumplir las normas técnicas necesarias para garantizar que la clave no puede ser forzada ni reproducida en un plazo de tiempo más largo que el período de validez de la misma. Por otro lado,

el certificado digital también debe cumplir los siguientes requisitos para que una firma sea reconocida como cualificada:

- Se debe tener la certeza de que el certificado utilizado para realizar la firma se expide como un certificado reconocido.
- Se debe poder identificar la Autoridad de Certificación (CA) y el estado en el que está generado (país de procedencia).
- Se debe poder acceder al nombre del firmante para poder identificarle
- Se debe asegurar que los datos de verificación de firma, que correspondan a los datos de creación de firma, están bajo el control del firmante
- Se debe conocer el período de validez del certificado
- Se debe conocer el código identificativo del certificado
- Se debe poseer la firma electrónica avanzada de la Autoridad de Certificación

Este tipo de firma digital tiene un valor jurídico fuerte: garantiza autenticación e integridad. También proporciona el no repudio, donde, en caso de tratarse de un mensaje, el remitente no puede decir que no lo envió y a su vez, el destinatario no puede decir que no lo recibió.

Tras haber conocido los diferentes tipos de firma según su nivel de seguridad, se va a desplegar una función donde se muestra la complejidad técnica que conlleva la adopción de cada tipo de firma. Por supuesto, cuanto más alto es el nivel que se establece para los requisitos, más crece la dificultad técnica que implican tanto su desarrollo [Abdalla& Reyzin] como su implantación. Antes de mostrar el gráfico hay que tener en cuenta que cada tipo de firma tiene un propósito, y que no es posible realizar cierto tipo de operaciones bajo un nivel de seguridad, pero que tampoco conviene adoptar una firma de alto nivel para situaciones de baja seguridad debido a la complejidad que su uso conlleva. Cuanto mayor es el número de requisitos que cumple un tipo de firma, mayor es el valor legal que esta adquiere según lo establecido por la comisión de la Unión Europea.

Figura 15. Clasificación de los diferentes tipos de firma

A modo de clarificación, la firma digital ligera sólo representa una definición de lo que se entiende por firma digital. Debido a que es una definición meramente teórica, su uso a nivel práctico queda limitado a prototipos, activos experimentales, etc.

Por otro lado, la firma digital avanzada establece los requisitos para poder adoptar la firma digital en algunos dominios de aplicación. Es decir, sólo tendría validez en determinados dominios cerrados. Por ejemplo, una empresa puede hacer uso de la firma digital avanzada para las transacciones realizadas dentro de la empresa, pero la firma no tendría validez fuera de ella.

Finalmente, la firma digital cualificada establece todos los requisitos necesarios para el uso de la firma digital en cualquier dominio de aplicación. Esto es así, debido a que es el propio gobierno, el encargado de suministrar los certificados digitales, que a posteriori se utilizarán para firmar digitalmente. De esta forma, cualquier aplicación que cumpla los requisitos, podrá garantizar las características de: autenticación, integridad y no-repudio en el intercambio de datos o información digital.

5.1.1 LO QUE NO ES UNA FIRMA DIGITAL

Es común que a menudo se presente la firma manuscrita en una pantalla como una firma digital. Es muy común encontrar esta creencia en comercios y hasta en bancos, donde la seguridad debería ser extrema. En estos lugares encontramos paneles de firma como el que se observa en la Figura 16, cuyo cometido es digitalizar una firma manuscrita, almacenando dicha firma en una base de datos en vez de dejarla impresa en el recibo. La afirmación de que este tipo de firmas se trata de una firma digital es un error, puesto que la propia firma no contiene ningún dato añadido que pueda identificar al usuario, y tampoco es comprobable mediante una tercera entidad de confianza, aunque siempre ha

existido la relación de confianza de que en caso de surgir un problema, una firma manuscrita puede ser apoyada por una entidad legal.

Más allá de la confianza no existe un método legal que la distinga de una firma manuscrita corriente, y por lo tanto no goza de carácter legal como firma digital.

Por otra parte, el sistema de digitalización de firma no resulta novedoso, ya que con la firma generada se obtiene el mismo resultado que se obtiene con una firma manuscrita clásica.

Figura 16. Dispositivo digitalizador de firmas manuscritas

Si se compara una firma manuscrita, sea digitalizada o en papel, con una firma digital, se observa que una firma replicada una y otra vez por un humano siempre varía en menor o mayor medida y que, por lo tanto su falsificación resulta sencilla y que puede ser repetida por otro usuario del sistema. También se debe tener en cuenta que un usuario no tiene la posibilidad de modificar su firma digital de manera intencionada, y que en caso de querer replicarla se genera una nueva, quedando invalidada la anterior. Sin embargo, un usuario puede generar varias firmas manuscritas diferentes, con intención de utilizarlas en distintos momentos o lugares.

Otro inconveniente con que cuenta una firma digitalizada frente a una digital de valor legal, es su alcance, ya que sólo puede ser utilizada como firma y como autorización. No así para el cifrado de mensajes, ya que esto debe realizarse con la clave privada que posee el certificado digital que identifica unívocamente al usuario.

En definitiva, aunque la firma manuscrita se ha venido utilizando como método de demostración de un acuerdo mutuo, o de un contrato, incluso con valor legal, y aunque con escasa aceptación se ha intentado digitalizar este tipo de firma, con las razones mostradas en este apartado queda demostrada la insuficiente seguridad que proporciona ese tipo de firma frente a una firma digital cualificada realizada a través de un certificado expedido por una entidad de confianza con valor legal.

5.2 TIPO DE FIRMA DIGITAL IMPLEMENTADO

Hay que recordar que el objetivo de este proyecto es identificar de forma segura al usuario de unos datos con los cuales se va a firmar. Por este motivo, para el proyecto se decide utilizar la firma digital cualificada, por estar dotada del más alto nivel de seguridad que las autoridades establecen a nivel legal. El objetivo es que los datos del usuario se encuentren protegidos y estructurados correctamente, de manera que otro usuario pueda comprobar la validez de los datos con los que se ha firmado.

Los datos que se incluyen en la firma del usuario de este proyecto son:

- DN: Nombre que aparece como titular en el certificado del firmante
- Date: Fecha completa[1] en la que se ha firmado. Para que la firma sea totalmente válida se debe firmar obteniendo la hora del servidor de la CA. En caso contrario aparecerá la nota "Validez desconocida".
- Reason: Razón que se da para la firma. Este campo es opcional.
- Location: Lugar desde el que se firma. Este campo es opcional.
- Contact: Persona o grupo de contacto. Puede una división dentro de la empresa. Este campo es opcional.

El aspecto que tiene una firma generada para un documento PDF se muestra en la **¡Error! No se encuentra el origen de la referencia.**, aunque lo más importante de esta firma no es el sello que se muestra (ya que incluso es un elemento que se puede elegir no poner), sino que el valor real de una firma digital se encuentra oculto en los metadatos del documento, al que se ha incluido la parte pública de los datos del certificado de usuario. Estos metadatos, incluidos en la firma que se realiza con la aplicación resultante del proyecto, pueden ser comprobados por cualquier otro usuario que posea una herramienta estándar de comprobación de firmas, aunque no se trate de un dispositivo móvil, y de esta manera la firma queda verificada y su validez comprobada.

[1] El formato de la fecha es AAAA.MM.DD HH:mm:SS GMT

Figura 17. Aspecto del sello de una firma digital

5.3 QUÉ Y QUIÉN INTERVIENE EN UNA FIRMA SEGURA EN MOVILIDAD

El ecosistema de la firma está compuesto por una serie de elementos que deben coexistir para que todo el conjunto pueda funcionar en armonía. Los elementos que lo componen son los siguientes (ver Figura 18):

- Dispositivo de creación de firmas: El equivalente de un dispositivo de creación de firma portado a un entorno móvil. Puede encontrarse dentro de una tarjeta inteligente (por ejemplo, una tarjeta SIM).
- Aplicación de firma móvil: La aplicación que crea una firma electrónica.
- Sistema de creación de firma en movilidad: El sistema global que crea una firma móvil y que consiste en el dispositivo desde el que se crea la firma y la aplicación.

Figura 18. Elementos de un ecosistema de firmas

La aplicación se encarga de la presentación del documento a firmar, y de mostrar el resultado después de la firma, es decir, es el componente encargado de interactuar con el usuario. Al tratarse de una aplicación segura, debe encargarse también de autenticar al usuario. Por otra parte, el dispositivo de creación de firmas se debe encargar del núcleo del proceso, que es formatear, aglutinar, crear y verificar los datos a firmar.

5.4 IMPLEMENTACIÓN DE UN PROCESO DE FIRMA

Se puede definir el concepto de firma digital en movilidad como un método universal de utilizar un dispositivo móvil para confirmar el acuerdo por parte de un ciudadano con una determinada transacción electrónica.

A continuación se despliega uno de los múltiples casos en el que la aplicación puede ser utilizada para la firma de documentos, desarrollando los sucesivos pasos que se suceden en el proceso de firmado. La descripción de este escenario ayuda a la concepción de una idea más clara sobre la creación de firmas en movilidad. Por lo tanto, en el escenario descrito se puede observar el resultado del análisis llevado a cabo en los apartados de este documento.

El usuario necesita firmar un documento que ha recibido por parte de otro usuario, y el documento recibido ha quedado almacenado en el directorio creado para la aplicación, el cual se encuentra en la raíz de la memoria flash en la tarjeta micro SD. En la aplicación se posibilita al usuario la firma de cualquier documento siempre que se encuentre en formato PDF. El documento que se va a firmar puede encontrarse dentro de un proceso de firmas, por ejemplo el visto bueno a una petición realizada por otra persona, como firma de contratos, de partes de horas, o revisión de documentos.

Si se supone que el usuario ya ha accedido a la aplicación segura, solamente tiene que seleccionar el documento que desea firmar y pulsar el botón de firma, que realiza el proceso necesario para añadir los metadatos de su certificado de usuario a los propios del documento que se ha seleccionado. En esta aplicación se sigue un proceso de firmado similar a la firma con *PDF Signature* de Java, pero migrado para dar soporte a dispositivos móviles (ver Figura 19), teniendo en cuenta que la librería de firma debe ser más ligera y que para móvil las librerías nativas de cifrado son diferentes a las existentes en un PC de sobremesa.

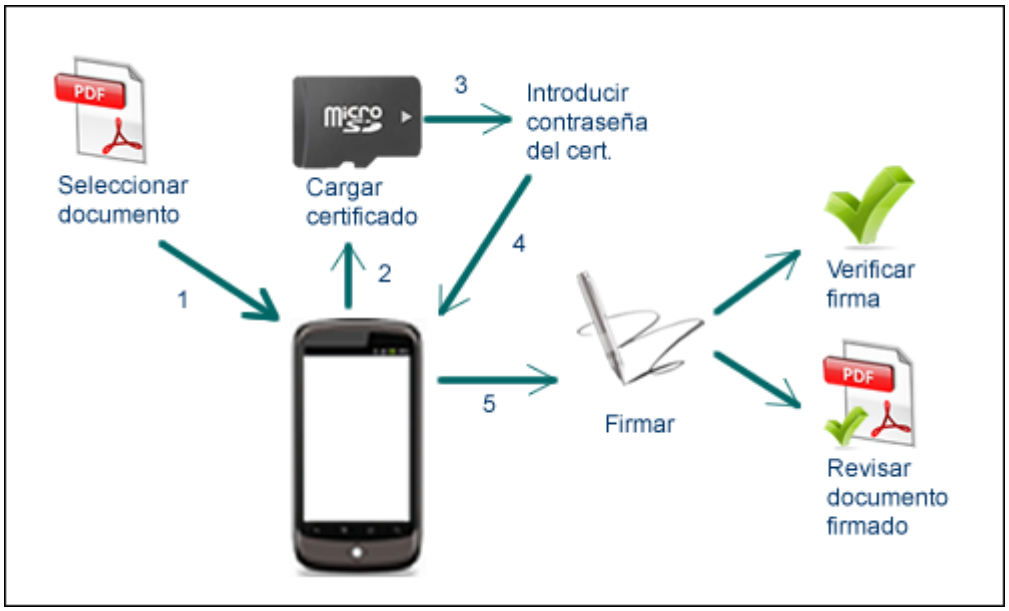

Figura 19. Diagrama de la firma realizada por la aplicación

Si el documento estaba previamente firmado, la firma se añadirá al mismo documento sin influir en la integridad de la anterior firma, creando un nuevo estado de documento. De este modo se pueden comprobar ambas firmas independientemente, y en caso de que alguna de las firmas existentes en el documento no haya sido emitida de forma correcta o no se haya emitido con el apoyo de un servidor de confianza, se podrá detectar y tener conocimiento de este hecho. En la Figura 20 se muestra la pantalla principal de la aplicación en la que se lleva a cabo el firmado del documento.

Figura 20. Pantalla principal de firma

Por supuesto, para dotar de una funcionalidad total a los componentes del escenario, cada usuario integrante del mismo debería ser capaz de ver "in situ" el documento con la/s firma/s correspondiente/s. Para realizar esta última acción (Figura 20, abajo), el usuario y el/los destinatario/s deberían contar previamente con la ayuda de un visor de documentos de tipo PDF instalado en su terminal de escritorio o en su dispositivo móvil.

5.5 VENTAJAS QUE APORTA LA INVESTIGACIÓN LLEVADA A CABO

La gran ventaja que ofrece este método de firmado frente a la firma clásica de documentos PDF ofrecida por otras aplicaciones de escritorio o la propia herramienta ofrecida por la aplicación Acrobat Reader de Adobe es la migración del portafirmas al mundo de la movilidad. Con la aplicación desarrollada para este proyecto, el usuario podrá gozar de su firma desde su propio teléfono móvil o Tablet. Si además dispone de conexión 3G o WIFI, la firma se realiza con una marca de tiempo, aportada por el servidor de firmas, que puede ser comprobada junto al resto de datos de la firma. Mediante esta comprobación se evita el fraude y la posibilidad de que se haya utilizado

un certificado (identidad del firmante) que ya no sea válido, bien sea porque ha caducado o porque se ha revocado.

Otra ventaja que ofrece el portafirmas digital de documentos PDF es que la firma del usuario va a ser comprobable, con lo que se aumenta la seguridad del documento firmado frente a una firma manuscrita convencional, ya que esta última puede ser suplantada. Sin embargo, la firma que realiza el usuario con la aplicación adjunta a este proyecto está protegida por un código PIN que sólo el usuario debe conocer. Un elemento visual puede ser añadido en este tipo de firmas, lo que ayuda visualmente a la persona o entidad que revise el documento para dar su visto bueno. La firma sigue siendo válida si no se añade esta marca de agua de la firma. Ya que puede ser comprobada con los mecanismos clásicos de comprobación de firmas digitales, y en ella pueden añadirse datos como identidad del firmante, fecha, lugar y razón de la firma, además de un sello identificativo de la empresa.

Un portafirmas localizado dentro del terminal móvil que disponga de un sistema capaz de denegar el acceso a terceros no deseados supone un gran avance. El siguiente paso natural en esta carrera por la securización de identidades digitales es el almacenamiento del certificado digital. El certificado identifica de manera única al usuario dentro del elemento seguro que se ha utilizado para controlar el acceso al propio demostrador.

En definitiva, tanto la migración a una aplicación de firma segura en movilidad, como el uso de certificados digitales y elementos seguros, suponen retos tecnológicos de alto valor añadido dentro del mundo de la seguridad digital. Esto supondrá un importante avance para la comunidad de desarrollo de aplicaciones móviles.

La protección de los datos de usuario en sus dispositivos móviles interesa tanto o más que en entornos de escritorio. La dificultad de conseguir seguridad es mayor en los móviles, ya sea (i) por la falta de drivers y lectores, (ii) por la necesidad de minimizar el número de elementos que se llevan encima, o (iii) porque el número de posibilidades de que nuestros dispositivos y aplicaciones caigan en manos de terceros se eleva exponencialmente. Por ello, el uso de elementos seguros (estudiados en el capítulo 1,”ELEMENTOS SEGUROS”) incrementa las garantías de la identificación personal y los hace muy deseables.

El almacenamiento de credenciales de usuarios físicos está dando pequeños pasos en su avance hacia la movilidad. Sin embargo, se ven entorpecidos por sus altas dificultades técnicas. En otras ocasiones se ralentiza por la incertidumbre que genera la pugna de las grandes entidades por hacerse con el control de los elementos seguros o también debido a temas políticos. Aun contando con estos inconvenientes la identificación segura desde el móvil es una meta deseada por muchas empresas que desean proteger la integridad de los datos de sus trabajadores, y en el ángulo opuesto perseguida por muchos desarrolladores que ven en este tipo de identificación, la identificación del futuro.

6 CONCLUSIONES

A lo largo de este proyecto se ha realizado un profundo estudio sobre diversos entornos, cuya combinación permite avanzar en la securización de los datos de un usuario en su dispositivo móvil, sea cual sea su ámbito.

Los elementos de investigación principales en los que se ha hecho hincapié a lo largo del proyecto son fundamentalmente tres. En las siguientes líneas se describen brevemente las conclusiones obtenidas para cada uno de los objetivos marcados al principio del proyecto. Su conjunto cierra el objetivo global de crear un ecosistema que sirva de base para seguir investigando en esta área.

En un primer lugar, se ha logrado un nivel de seguridad satisfactorio en el ecosistema de PKI implementado. El modelo de identificación tiene al usuario como objetivo de seguridad, y por lo tanto se ha validado el uso de certificados únicos para tal fin. Otro punto aclarado en el proyecto indica la portabilidad de estos ecosistemas al mundo de la movilidad, dotando de mayor seguridad a los sistemas de firma.

La disertación seguida para movilidad sobre los elementos seguros comerciales o en proceso de investigación, deja claro que estos elementos proporcionan seguridad suficiente, tanto a nivel físico como digital, para permitir el almacenamiento de datos sensibles sobre usuarios o empresas. Ésta conclusión se acentúa por la seria apuesta a nivel de investigación e innovación por parte de las grandes empresas del sector, localizadas en banca, operadoras móviles, fabricantes de hardware, universidades y los centros de investigación más importantes del mundo.

El ecosistema experimental implementado en este proyecto proporciona una base sólida para la experimentación de la firma digital segura en movilidad. Por lo tanto, se deduce que uno de los siguientes pasos que se van a dar en el mundo de la movilidad incluye la posibilidad de trasladar las necesidades burocráticas o bancarias al propio terminal del cliente. Una de las operaciones que se puede requerir al ciudadano es la firma, por ejemplo, de contratos. El estudio llevado a cabo a través de la implementación de un portafirmas experimental madura la idea de que realmente es seguro el uso de estos sistemas, pensando en nuevos usos como el almacenamiento de documentos de identidad o la banca móvil.

Como conclusión principal se deduce que, pese a las dificultades que surgen tanto en diseño, como en adaptabilidad o utilización de los diferentes elementos, estos cumplen los objetivos requeridos a nivel de seguridad y recursos para convertirse en un futuro en la referencia en el campo de la identificación.

7 BIBLIOGRAFÍA

[Abdalla& Reyzin] Michel Abdalla and Leonid Reyzin (2000). *A New Forward-Secure Digital Signature Scheme*, Advances in Cryptology - ASIACRYPT 2000, 116-129

[ASSD] SD Association, *Advanced Security SD Card* [https://www.sdcard.org/]

[Blythe] Stephen E. Blythe (2008). *Finland's Electronic Signature Act and e-Government Act: Facilitating Security in e-Commerce and Online Public Services*, Hamline Law Review

[Ceres] CERES, *Certificación Española* [www.cert.fnmt.es/]

[Chang] Kae-por F. Chang (Sep, 2001) *Authority-neutral certification for multiple-authority PKI environments*, US Provisional Application Ser. No. 60/325,835

[FNMT] Fábrica Nacional de Moneda y Timbre [http://www.cert.fnmt.es/index.php?cha=com&lang=es]

[GlobalPlatform] GlobalPlatform, *Estandarización para desarrollo, despliegue y mantenimiento de smart cards* [www.globalplatform.org/]

[G&D] Giesecke & Devrient [http://www.gi-de.com/es/index.jsp]

[Herzberg] Amir Herzberg, Bar-Ilan University (May 2004). *Payments and banking with mobile personal device*, ACM Conference on Security and Privacy in Wireless and Mobile Networks

[Hiltgen] Hiltgen, A. (2006). *Secure Internet Banking Authentication*, Security & Privacy, IEEE, Vol.4, Issue 2, 21-29

[JavaCard] Sun Microsystems, Inc. (2006). *Java Card Platform Application Programming Interface, Version 2.2.2*

[Larsson et al.] Stig B. Larsson, Christoph T. Hoffmann, Phillip C. Dimond (1991) *Smart Card Validation Method*, PCT Pub. No. WO91/17524

[Martínez-Peláez et al.] Rafael Martínez-Peláez, Cristina Satizábal, Francisco Rico-Novella, Jordi Forné (2008). *Efficient Certificate Path Validation and Its Application in Mobile Payment Protocols*, The Third International Conference on Availability, Reliability and Security

[NIST] National Institute of Standards and Technology [www.nist.gov/]

[PKCS] RSA Laboratories (2011). *What is PKCS? Public Key Cryptography Standards*, [http://www.rsa.com/rsalabs/]

[Rankl&Effing] W. Rankl, Wolfgang Effing (1997). *Smart Card Handbook*, ISBN:0471967203

[Scheuermann] Scheuermann, D. (Oct 2002). *The smartcard as a mobile security device*, IEEE Electronics & Communication Engineering Journal, 205-210

[Schwiderski-Grosche] Schwiderski-Grosche, S. (Oct 2002) *Secure mobile commerce*, IEEE Electronics & Communication Engineering Journal, 228-238

[Sherman et al.] Sherman S. M. Chow, Lucas C. K. Hui, Siu Ming Yiu and K. P. Chow (2004). *Secure Hierarchical Identity Based Signature and Its Application*, Lecture Notes in Computer Science, Volume 3269/2004, 275-279

[Silvester] Kelan C. Silvester (2004). *User authentication using a mobile phone SIM card*, US Pat. Appl. No. 10/816,104

[Toorani & Beheshti] Mohsen Toorani Ali Asghar, Beheshti Shirazi (2008). *LPKI – A Lightweight Public Key Infrastructure for the Mobile Environments*, 11th IEEE Singapore International Conference on Communication Systems. ICCS 2008.

[TrustZone] ARM, *Tecnología de seguridad móvil para servicios de valor añadido* [http://www.arm.com/products/processors/technologies/trustzone.php]

[Van Thanh] Do Van Thanh (2000). *Security Issues in Mobile eCommerce*, EC-WEB '00 Proceedings of the First International Conference on Electronic Commerce and Web Technologies, 467-476

[Winter] Johannes Winter, Graz (2008). *Trusted computing building blocks for embedded linux-based ARM trustzone platforms*, STC '08 Proceedings of the 3rd ACM workshop on Scalable trusted computing, 21-30