UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

TESIS:

"DISEÑO Y CONSTRUCCIÓN DE UN ARTEFACTO PARA LA DISTRIBUCIÓN Y ENTREGA DE CERTIFICADOS DIGITALES X.509"

PARA OBTENER EL GRADO ACADÉMICO DE MAESTRO EN CIENCIAS EN INGENIERÍA ELECTRÓNICA CON MENCIÓN EN TELEMÁTICA

ELABORADO POR:

Ing. RONALD RICARDO MARTINEZ CHUNGA

ASESOR:

Dr. ALVARO ERNESTO CUNO PARARI

LIMA – PERÚ

2020

DEDICATORIA

Dedico la presente tesis de maestría a mi salvador el Sr. Jesús, a mi ayuda idónea Janet, a mis queridos padres Ana María y Ricardo, y a mi querida Alma Mater la Universidad Nacional de Ingeniería.

AGRADECIMIENTOS

Primero agradecer a mi Sr. Jesús, porque es él quien ha permitido que este trabajo se realice; en seguida, un agradecimiento muy especial a mí asesor de Tesis el Dr. Alvaro Ernesto Cuno Parari por el profesionalismo, la paciencia y el rigor colocados en las diversas etapas en la elaboración de este trabajo; su dirección, así como el apoyo brindado de manera permanente han sido determinantes en la consolidación de este trabajo. Asimismo, un agradecimiento especial a mis jefes inmediatos en el RENIEC, el Ing. Fernando Antonio Zapata Miranda y el Ing. Ricardo Javier Enrique Saavedra Mavila, por brindarme todo el apoyo para la realización de este trabajo. No menos importante, un agradecimiento al profesor M. Sc. Ing. Roberto Rubén Ramírez Arcelles, director de la unidad de postgrado de la FIEE UNI por las facilidades otorgadas en la defensa de este trabajo; finalmente, a mi Alma Mater de ayer, hoy y siempre, que a través de los estudios de posgrado me han permitido contribuir con soluciones reales a las problemáticas tecnológicas de relevancia práctica en nuestro País.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

Esta tesis se enmarca en uno de los problemas más desafiantes del Internet actual: la verificación telemática de la identidad de las personas que interactúan de manera remota con entornos no presenciales. En particular, se aborda el problema de la distribución y entrega de certificados digitales X.509 v3 a usuarios finales en computadoras personales y teléfonos inteligentes, describiendo el diseño, la construcción y la evaluación de un artefacto, como una alternativa para contribuir en la solución de esta problemática. Siete meta-requerimientos fueron definidos, los cuales han sido instanciados en un artefacto, que, a su vez, ha sido evaluado empíricamente. La evaluación del artefacto ha demostrado su eficacia sobre la base de su uso real y la facilidad percibida en su uso. Los resultados de este trabajo contribuyen con posicionar a las computadoras personales y los teléfonos inteligentes como una alternativa al uso de los módulos criptográficos tales como las tarjetas inteligentes o los tokens criptográficos en escenarios específicos.

Palabras claves: PKI, certificados digitales, módulos criptográficos, tarjetas inteligentes, tokens criptográficos, teléfonos inteligentes.

ABSTRACT

This thesis is part of one of the most challenging problems on the Internet today: the telematic verification of the person's identity who interact of remote way with not presential environments. In particular, the raised problem is the distribution and delivery of X.509 v3 digital certificates to end users on personal computers and smartphones, describing the design, construction and evaluation of an artifact with which it is possible to solve it. Seven meta-requirements were defined, which have been instantiated into an artifact, which in turn has been empirically evaluated. The evaluation of the artifact has demonstrated its effectiveness based on actual use and perceived ease of use. The results of this work contribute to positioning personal computers and smartphones as alternative cryptographic modules to chip cards or cryptographic tokens for some usage scenarios.

Keywords: PKI, digital certificates, cryptographic modules, smartcards, tokens, smartphones.

INTRODUCCIÓN

En los últimos años, el uso de dispositivos criptográficos en formato personal se ha venido tornando cada vez más popular, tanto por usuarios del sector privado como del sector público. Esto se debe, principalmente, a la seguridad y protección que éstos ofrecen frente a la suplantación de la identidad y al fraude electrónico. Por ejemplo, la mayoría de los bancos alrededor del mundo han dejado de utilizar las tradicionales tarjetas de banda magnética y las han reemplazado por tarjetas inteligentes que incorporan un chip criptográfico mejor conocidas como tarjetas bancarias Europay MasterCard VISA (EMV), especificación que representa un conjunto de reglas que buscan asegurar la interoperabilidad y la aceptación a nivel mundial de transacciones de pago seguras utilizando tarjetas inteligentes que incorporan un chip criptográfico para identificar a sus clientes.

Asimismo, en el sector público, diversos países se encuentran emitiendo para sus ciudadanos tarjetas inteligentes para fines de identificación; por ejemplo, es el caso de Uruguay, España, Estonia, Bélgica y Alemania por citar algunos. Lo que estos países buscan es darles a los ciudadanos un mecanismo que les permita identificarse de forma segura en el ciberespacio, en particular, cuando accedan a plataformas digitales para la realización de trámites ante el Estado de manera remota.

No obstante, el uso de estas tarjetas, debido a su tecnología subyacente (Infraestructura de llave pública), no ha alcanzado los resultados esperados ni ha logrado masificarse a escala mundial. A pesar de que las diferentes barreras han sido identificadas años atrás, muchas de ellas aún permanecen como problemas pendientes de resolver y se mantienen como desafíos para la comunidad científica [20], [22] y [30]. Para el usuario final, una de estas barreras es, además de tener que portar físicamente la tarjeta inteligente, tener que disponer de un dispositivo lector de tarjetas, de un computador personal y tener que instalar paquetes de software especializados (i.e. drivers, middlewares y librerías), en otras palabras, hablamos de su bajo nivel de usabilidad.

Sin embargo, también existe la posibilidad de contar con computadoras personales o teléfonos inteligentes de propiedad de los usuarios, que pueden ser utilizados como dispositivos alternativos que incorporan hardware o software confiable capaces de suministrar de forma alternativa infraestructura segura como la necesaria para otorgar identidad digital a los ciudadanos, los dispositivos, e incluso los Sistemas de información, otorgando garantías de seguridad mínimas.

Este trabajo contribuye con la presentación de un diseño que resuelve un problema de relevancia práctica, el que es verificado mediante la construcción o implementación de un artefacto de software que gestiona hardware de seguridad especializado. Este hardware es denominado también módulo criptográfico, el cual, a través de los mecanismos que provee, entre las operaciones más importantes, resguarda la integridad de los datos sensibles (como la identidad digital de una entidad final) que alberga, asegura las comunicaciones de extremo a extremo autenticándolas, otorgando también confidencialidad a los datos intercambiados, y puede generar evidencias de manifestación de voluntad (mediante la capacidad de generar firmas digitales). En otras palabras, para otorgar seguridad y confianza a las transacciones electrónicas críticas (que de forma nativa no tienen) que circulan en plataformas de acceso libre como el Internet, es vital el entendimiento de estas funcionalidades, revelando su importancia.

El diseño presentado es concebido utilizando estos mecanismos de seguridad, y es plasmado en el artefacto cuyo propósito es entregar y distribuir certificados digitales en contenedores seguros a través de diferentes plataformas determinadas por el alcance de este trabajo, dotando a la propuesta desarrollada, la relevancia técnica presente en los desafíos que incorpora una solución debidamente protegida desplegada en Internet.

CAPÍTULO I
ANTECEDENTES Y DESCRIPCIÓN DEL PROBLEMA

1.1 Antecedentes bibliográficos

Actualmente, diversos sistemas de información gestionan la identificación de sus usuarios a través de múltiples tecnologías que proveen identidad digital, tecnologías como las credenciales que hacen uso de un usuario y contraseña, la autenticación con contraseña de un solo uso, la biometría, los certificados digitales sobre la base de Infraestructura de llave pública (PKI: Public Key Infraestructure), entre otras. Múltiples implementaciones internacionales, así como en el Perú, han elegido como una de las formas más seguras para tal cometido a la certificación digital sobre la base de PKI.

Diversos investigadores [12], [18], [19], [20], [22], [30], [37], [38] y [42] han identificado las barreras y dificultades del despliegue de las PKI y las han clasificado en: técnicas, económicas, sociales y legales. Entre éstas destacan aquellas denominadas como las de "complejidad técnica" para el usuario final, que se refieren a las limitaciones en la usabilidad de las tarjetas inteligentes. Sin embargo, es importante destacar que existen casos de éxito del uso de esta tecnología, como es el caso de Korea, donde en las transacciones en línea con el sector privado y con el sector público es inevitable el uso de la firma digital [27]. Otro ejemplo para destacar es Estonia; de acuerdo con la Autoridad de Sistemas de Información de Estonia (https://www.id.ee/), a la fecha, se tienen en estado activo (en manos de sus ciudadanos) más de 1.3 millones de tarjetas inteligentes y desde su introducción en el 2002 hasta la fecha se han generado más de 500 millones de firmas digitales.

Si bien existen algunos casos de éxito en la adopción de la tecnología PKI con el uso de tarjetas inteligentes, en general, su masificación a nivel global aún no ha sido posible [15], [21], [28] y [36]. Entre las razones de su impopularidad se destaca la necesidad de tener que contar con dispositivos lectores y el hecho de tener que instalar drivers y realizar configuraciones particulares en el computador del usuario. Una primera iniciativa de solución a los problemas de usabilidad de las tarjetas inteligentes es el uso de contenedores compatibles con el formato PKCS#12. Sin embargo, su adopción no es

recomendada debido a que, al no estar debidamente protegidos (pues no cuentan con alguna certificación de seguridad), los datos de creación de firmas podrían ser copiados, lo que genera potenciales casos de suplantación.

Otra de las propuestas de solución a la limitación de las tarjetas inteligentes es la denominada firma remota (Server Signing). Aquí, lo que se busca es realizar una gestión centralizada de los datos de creación de firmas, lo cual reduce y simplifica los requisitos y responsabilidades en el lado del cliente. Varias plataformas que implementan esta propuesta requieren que el usuario tenga apenas un teléfono inteligente. La desventaja de esta propuesta es que, al estar los datos de creación de firmas en manos de un tercero, se requiere que estas plataformas cuenten con una certificación de seguridad específica para que las firmas digitales generadas tengan un valor similar a las manuscritas [7] y [16].

También es de destacar la propuesta que promueve el uso del Entorno de Ejecución de Confianza (i.e. Trusted Execution Environment, en adelante TEE) que pueden ser incorporados en los teléfonos inteligentes tanto de manera nativa (por hardware) como artificial (por software) [1]. Lo que se busca aquí es aislar los datos de creación de firmas y hacer que los datos intercambiados con el usuario no puedan ser interceptados. La limitación original de esta propuesta está en la necesidad de tener que contar con la participación de los fabricantes tanto para la activación de algunas de estas tecnologías propietarias, como para la estandarización aún emergente de las soluciones desarrolladas sobre estas plataformas [32], también conocidas como zona segura.

Otra iniciativa importante de tener en cuenta es la propuesta basada en criptografía con umbral (Threshold Cryptography). La idea es particionar los datos de creación de firmas en partes que son inutilizables de forma aislada. Para generar una firma digital se requiere la participación simultanea de las partes (del teléfono inteligente del usuario y de un sistema centralizado) [3]. Esta propuesta no requiere adquirir dispositivos criptográficos, ni tampoco la habilitación de funcionalidades por parte de los fabricantes.

1.2 Descripción de la realidad problemática

Como ya se ha citado, a nivel global la entrega y distribución de certificados digitales emitidos por las jerarquías PKI de Entidades de Certificación Digital orientadas a usuarios finales, mantiene diferentes tipos de limitaciones ya identificadas, y con una antelación importante. En este trabajo analizaremos esta problemática en el contexto del estado peruano.

La distribución y entrega de certificados digitales emitidos por la Entidad de Certificación del Estado Peruano del RENIEC (ECEP-RENIEC) en el contexto del estado peruano, empezó en el año 2012, con la emisión de certificados digitales a través de la interfaz web suministrada por la herramienta de gestión de Autoridades de Certificación (*CA: Certification Authority*) denominada ®EJBCA SE mediante la cual se generaban los certificados digitales para usuarios finales en módulos criptográficos tales como computadoras personales, tarjetas inteligentes o tokens criptográficos.

Inicialmente, los certificados digitales eran generados en dos módulos criptográficos de hardware de diferentes marcas, los cuales requerían una gran cantidad de pasos, así como, el tiempo invertido en su ejecución; cuando por diferentes motivos, la generación no era posible directamente desde la interfaz web, se utilizaban contenedores de software para garantizar la generación del certificado digital, y luego, el material criptográfico contenido en el contenedor (no seguro) era importado al módulo criptográfico del usuario.

Aunque los módulos criptográficos del tipo tarjeta inteligente o token criptográfico para usuarios finales cuentan con niveles de seguridad superiores en comparación de una computadora personal, el uso de certificados digitales contenidos en este segundo tipo de módulos es superior, y en gran medida. Esto se debe a que hay que tener también en consideración que hoy en día la gran mayoría de los usuarios ya cuentan con un computador personal a su alcance (sea en su casa o en su centro laboral), así como, con un teléfono inteligente personal o perteneciente a una red empresarial.

La implementación inicial del Sistema de entrega y distribución de certificados digitales del RENIEC tuvo como principal característica que, en todos los modelos presentados, las operaciones sensibles se realizaban en el lado del servidor de la Plataforma, lo que desde ya representa un potencial riesgo de seguridad no solo en el objetivo de crear el material criptográfico del usuario, sino también, en el resguardo de la integridad de la Plataforma de Generación de certificados digitales. Estos modelos vistos desde el punto de vista del cliente o navegador web son:

1.2.1 Google Chrome

El modelo descrito en la Figura 1 presenta el caso de este navegador que utilizó un applet de Java que fue inhabilitado desde la versión 45 del navegador, esto debido a la inseguridad que representaba la ejecución de un applet que requiere la tecnología NPAPI documentado en https://java.com/en/download/faq/chrome.xml. Asimismo, el navegador no permite establecer una contraseña para generar material criptográfico en un contenedor de software como el utilizado por los sistemas operativos Ms. Windows® (revisado en

detalle en el numeral 2.6.3), representando un riesgo de seguridad para el usuario titular de los datos de generación de firma digital.

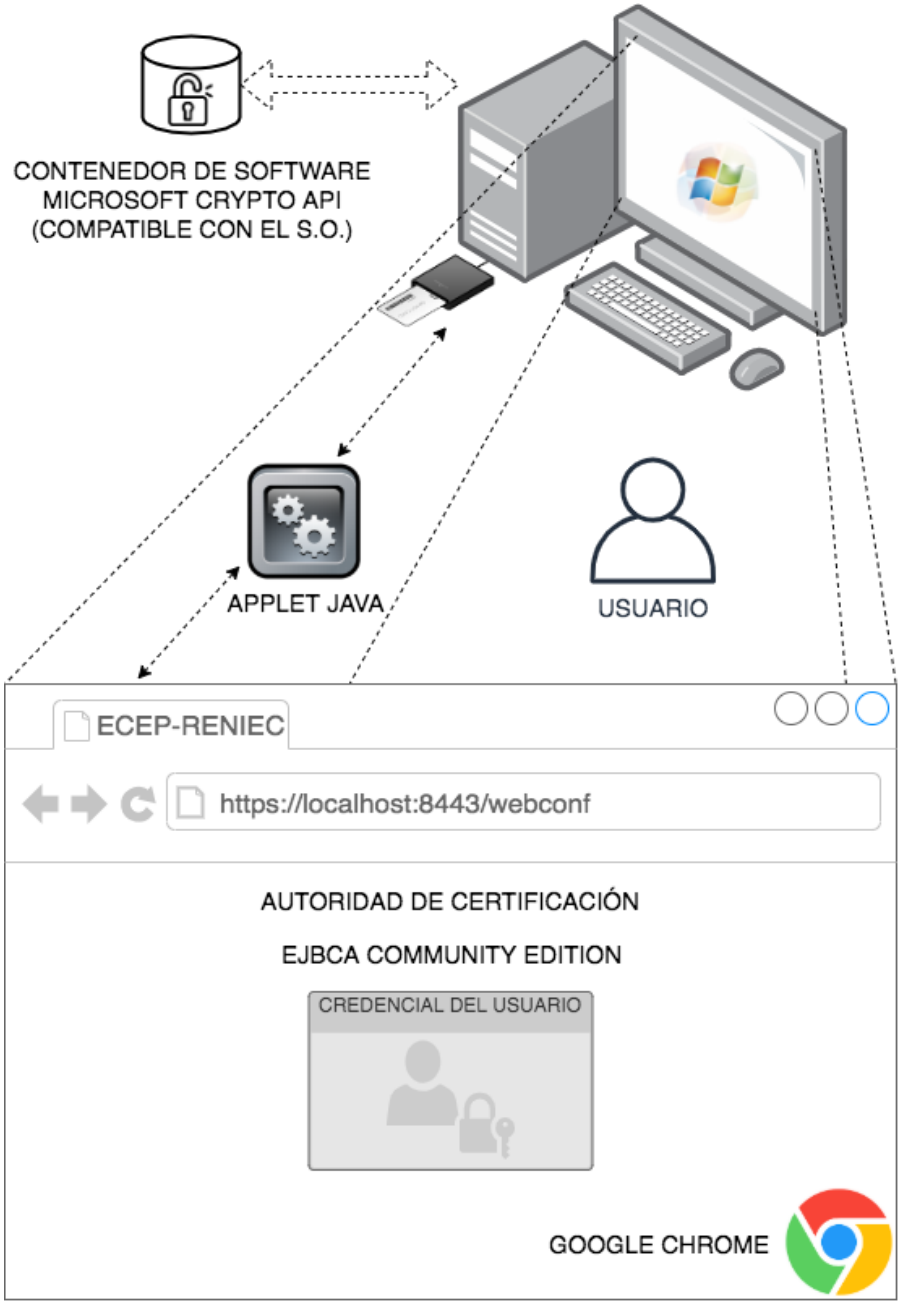

FIGURA 1. CASO DE USO CON EL NAVEGADOR GOOGLE CHROME

1.2.2 Mozilla Firefox

El primer inconveniente con este navegador recae en que cualquier material criptográfico que se intente crear en un contenedor de software podrá ser generado en el repositorio exclusivo del navegador, restringiendo al Sistema Operativo el uso de los datos de creación de firma digital del usuario. Es decir, cualquier sistema de generación de firma

digital (en la etapa de uso) que generalmente accede al repositorio de certificados digitales del sistema, no podrá encontrar los datos de creación de firma del usuario, pues estos se encuentran albergados dentro del repositorio exclusivo del navegador.

Así también, algunos módulos criptográficos de hardware compatibles con el estándar PKCS#11 mantenían una comunicación inestable entre el navegador y el módulo, debido a que los parámetros de configuración para la creación de material criptográfico mediante el estándar PKCS#11 no son accesibles, debido a que el navegador no provee una interfaz para adecuar estos parámetros por cada implementación en particular de cada modelo por fabricante. La Figura 2 describe el caso de uso.

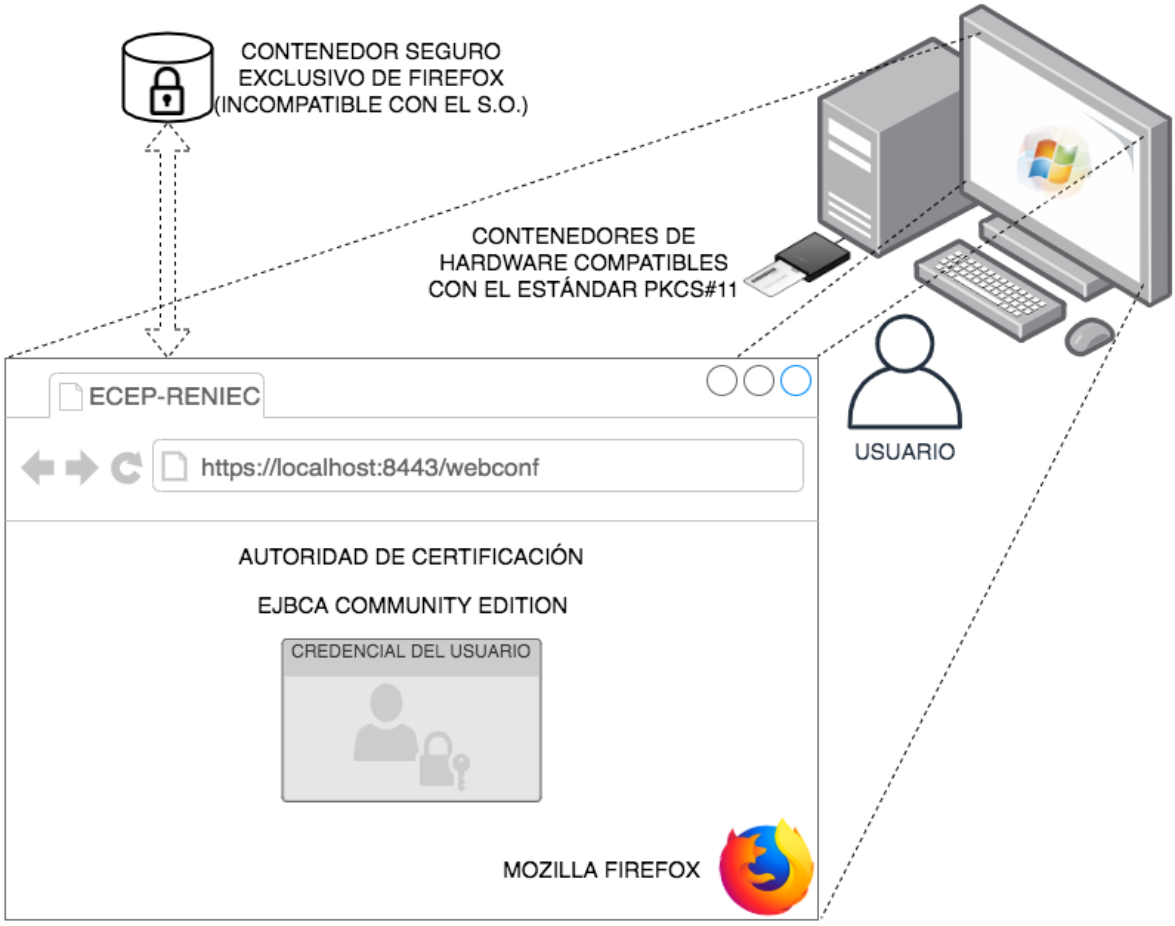

FIGURA 2. CASO DE USO CON EL NAVEGADOR MOZILLA FIREFOX

1.2.3 Internet Explorer

Desde la versión 7.0 de este navegador se incluyen características de filtrado de controles Active X, esta fue la respuesta para prevenir el intento de aprovechar las vulnerabilidades de ejecución en este tipo de plugin también conocido como Add-on. La plataforma de descarga utilizaba de acuerdo con el modelo mostrado en la Figura 3, un

Control Active X para la generación del material criptográfico del usuario, lo que representaba una potencial falla de seguridad que ponía en riesgo la generación de los datos de creación de firma que representan al usuario final.

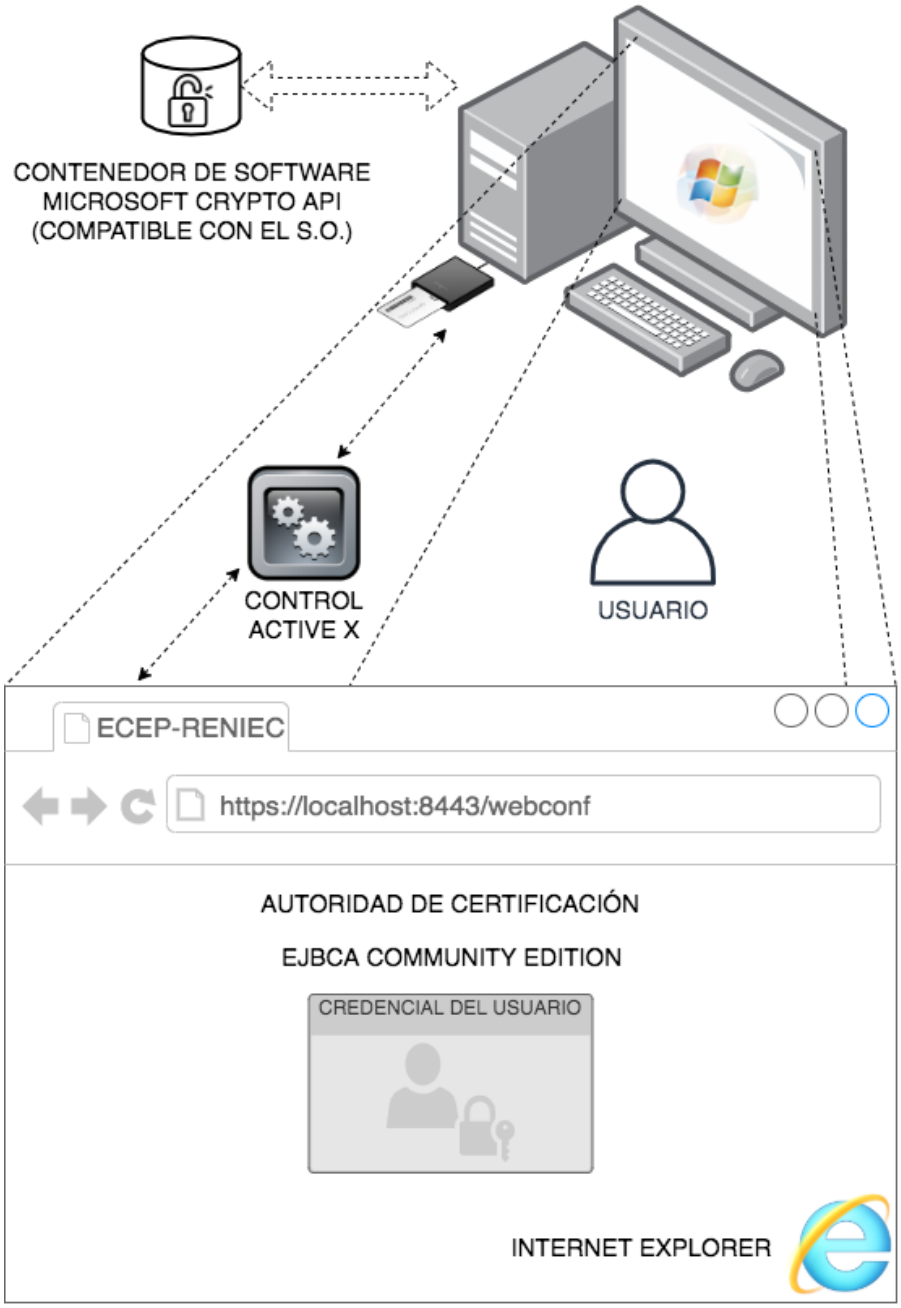

FIGURA 3. CASO DE USO CON EL NAVEGADOR INTERNET EXPLORER

1.3 Formulación del problema

Dicho lo anterior, resulta importante saber si es factible pensar en utilizar los módulos criptográficos de naturaleza personal incorporados en las computadoras personales y los teléfonos inteligentes como módulos alternativos a las tarjetas inteligentes. A diferencia de

estas últimas, que se entregan ya configuradas para realizar operaciones de firma digital (es decir, con certificados digitales), la computadora personal y el teléfono inteligente no cuentan con esta configuración de forma nativa o predeterminada. Entonces, un desafío a enfrentar se traduce en la búsqueda de la manera de entregar certificados digitales en dispositivos disímiles de propiedad del usuario final. Para indagar en esta cuestión planteamos la siguiente pregunta de investigación:

¿Cómo diseñar un artefacto informático que permita distribuir y entregar de forma efectiva y eficiente certificados digitales en diferentes tipos de módulos criptográficos de naturaleza personal?

1.4. Justificación e importancia de la investigación

La justificación de la investigación puede ser presentada bajo la visión de tres aspectos, descritos a continuación:

1.4.1 Justificación teórica

Las transacciones en el Internet representan tecnológicamente una realidad óptima donde los sistemas están conectados entre sí, generando colaboración inteligente entre ellos desde cualquier lugar y en cualquier momento. Hoy en día, el diseño de esta arquitectura en sus diversas capas aún trata con incertidumbres sobre la seguridad que incorporan aquellas implementaciones. Para mitigar las amenazas que una solución debe enfrentar, se ha identificado [17] que se debe considerar los siguientes requisitos de seguridad:

- Autenticidad
- Autorización
- Confidencialidad
- Integridad y
- Disponibilidad

Asimismo, estos requisitos motivan los siguientes desafíos de seguridad, como son:

- Interoperabilidad
- Recursos limitados
- Volúmenes de datos
- Protección de privacidad
- Escalabilidad y
- Control automático

Desafíos que deben ser incorporados en el desarrollo de una solución.

Con respecto a la seguridad en las capas externas en una arquitectura desplegada en Internet, entre las recomendaciones hechas en [39], se destaca el uso de procesamiento criptográfico como uno de los principales mecanismos de seguridad para los datos recopilados, procesados y transmitidos por los extremos. Incluir estas operaciones garantiza el cumplimiento de los requisitos citados, incluyendo cifrado y descifrado, generación de llaves simétricas y asimétricas, generación de resúmenes (representación única de cualquier dato digital), y la generación de firma digital de resúmenes, así como su verificación.

El procesamiento criptográfico (servicios criptográficos) es provisto por diferentes tecnologías seguras, que son implementadas en módulos criptográficos que toman en cuenta las prestaciones a suministrar y los recursos disponibles. La revisión de los mecanismos incorporado en la gestión y operación de los diversos tipos de módulos (tanto de las tecnologías convencionales como de las más recientes) es una necesidad que toma mayor rigor cada vez más en los diferentes ámbitos de nuestra sociedad de información, en particular, claramente presente en aquellos disponible en Internet.

Por ejemplo, En el 2009 un Drone militar americano fue hackeado por insurgentes iraquíes durante el conflicto entre Irak, Afganistán y Paquistán, donde se pudieron grabar varias horas de video transmitido en vivo por el drone, evidenciando un claro vacío de seguridad del arma americana al revelar su trayectoria; esto fue realizado utilizando una herramienta de software rusa que tenía un costo de 26 dólares americanos. Este es un claro ejemplo donde una solución online (objeto drone teledirigido que registra video), debe implementar mecanismos de autenticidad, confidencialidad e integridad incorporando módulos criptográficos en el drone que permitan asegurar las diferentes capas de procesamiento de datos (de comunicación, de control, y de datos como la posición y el video, por citar algunos de ellos).

La selección de los algoritmos criptográficos más adecuados y de mejor performance que se incorporan en los diferentes tipos de módulos criptográficos es constantemente revisada por instituciones referentes en seguridad, como el NIST en Norte América y Canadá, así como, el ETSI en la Unión Europea por mencionar un par de ellas. Estas instituciones mantienen equipos de investigación dedicados a actualizar las recomendaciones referidas a los servicios seguros que pueden ser implementados por los módulos para satisfacer sus requerimientos de uso; estas recomendaciones son públicas para que puedan ser acogidas por cualquier organización que esté interesada en

incorporar soluciones confiables en los diversos ámbitos tecnológicos de seguridad, entre ellos, Internet. Conocer el estado de arte relacionado a las capas de seguridad que implemente cualquier sistema, es esencial en el proceso del diseño a fin de realizar la elección más adecuada con los recursos de hardware disponibles.

1.4.2 Justificación práctica

Los fabricantes e integradores de módulos criptográficos ofrecen una diversidad de tipos de dispositivos de hardware y software que tienen relación directa con el tipo de aplicación o caso de uso en el cual el módulo va a ser integrado, ejemplos clásicos, están presentes en el sector de la Internet de las cosas (IoT), el sector financiero, el sector gubernamental o el sector de productos digitales con derechos de autor, como el video streaming, todas ellas ejecutándose en la plataforma de acceso libre, Internet.

Cada sector exige ciertas particularidades que deben ser suministradas por el módulo de interés, así mismo, las buenas prácticas en seguridad invitan a los fabricantes a implementar módulos criptográficos sobre la base de estándares de seguridad, tanto en las interfaces físicas como lógicas que incorporen los módulos, contar con certificaciones de seguridad ampliamente aprobadas y aceptadas; por último y no menos importante, dependiendo de la entidad final (Usuario o Sistema de Información) que va a hacer uso del módulo, el formato de presentación que satisfaga los requerimientos solicitados.

Por ejemplo, es diferente contar con un módulo que provea servicios seguros para transacciones financieras, que un módulo que suministre servicios de llave electrónica para un automóvil, o que un módulo que asegure canales de comunicación, o que un módulo que ofrezca servicios seguros de identidad digital para un usuario final. Como se puede distinguir, conocer los aspectos prácticos para la selección de un módulo criptográfico que provea servicios seguros es importante para toda organización que desee incorporarlas en los Sistemas de Información de su interés.

1.4.3 Justificación económica

La tecnología segura por su complejidad tanto en su implementación física como lógica es una tecnología que requiere ser evaluada, esto permitirá seleccionar la mejor opción disponible que equilibre las prestaciones ofrecidas, la usabilidad y el costo del módulo de interés. Este trabajo pretende contribuir con la implementación de un artefacto diseñado para incorporar los servicios criptográficos proveídos por módulos criptográficos destinados a usuarios finales en sus diferentes presentaciones, tales como, las tarjetas inteligentes, los tokens criptográficos, las computadoras personales y los teléfonos

inteligentes, plataformas que son parte del alcance de este trabajo y que representan una muestra entre las diversas plataformas que son alcanzas por la Internet.

Esto permite abrir el mercado generando la libre competencia de este tipo de productos, puesto que, el artefacto va a demostrar ser capaz de poder utilizar módulos criptográficos de diferentes marcas y modelos, distribuyendo los certificados digitales en las diferentes plataformas que son parte del alcance de este trabajo, dando al usuario final la garantía de poder elegir cualquiera de los módulos gestionados por el artefacto, otorgando al usuario la facilidad de solo preocuparse por las prestaciones adicionales que el caso de uso en particular requiera, así como, la libertad de elegir de acuerdo con su nivel adquisitivo.

1.5. Objetivos

1.5.1. Objetivo general

Diseñar un artefacto informático que permita distribuir y entregar de forma efectiva y eficiente certificados digitales en diferentes tipos de módulos criptográficos de naturaleza personal.

1.5.2. Objetivos específicos

Los objetivos específicos de este trabajo son:

a. Analizar los requerimientos funcionales y no funcionales que el artefacto informático debe satisfacer para la distribución y entrega de los certificados digitales de interés, en los diferentes tipos de módulos criptográficos.
b. Construir el artefacto informático diseñado en diferentes plataformas.
c. Evaluar la eficacia y eficiencia del uso del artefacto informático construido.

1.6. Hipótesis

1.6.1. Hipótesis principal

El diseño de un artefacto informático permitirá distribuir y entregar de forma efectiva y eficiente certificados digitales en diferentes tipos de módulos criptográficos destinados a usuarios finales.

1.7. Variables e Indicadores

1.7.1. Variable independiente

a. El artefacto informático que permitirá la distribución y entrega de certificados digitales.

1.7.2. Variables dependientes

a. La distribución efectiva de certificados digitales en diferentes tipos de módulos criptográficos.

   Indicadores:

   - El número de certificados digitales generados en los diferentes módulos criptográficos.

b. La distribución eficiente de certificados digitales en diferentes tipos de módulos criptográficos.

   Indicadores:

   - El tiempo requerido en el proceso de generación de certificados digitales en los módulos criptográficos.
   - La usabilidad percibida por el usuario final al generar el certificado digital en el módulo criptográfico de su propiedad.
   - El número de plataformas disponibles donde se implementó el artefacto.
   - El número de solicitudes atendidas por el servicio de mesa de ayuda para dar soporte técnico al procedimiento de generación de certificados digitales utilizando el artefacto.

1.8. Unidad de análisis

Los usuarios finales que solicitaron certificados digitales para persona natural (Clase 1) y persona jurídica (Clase 3) emitidos por la ECEP-RENIEC, en el periodo considerado en el numeral 1.10.

1.9. Tipo y nivel de investigación

El método de investigación utilizado en este trabajo es el de la Ciencia del Diseño, el cual permite obtener conocimiento y entendimiento de un dominio del conocimiento mediante la construcción y uso de artefactos artificiales. La diferencia primordial entre la ciencia tradicional y la ciencia del diseño es que mientras la tradicional busca entender la realidad, la ciencia del diseño busca crear objetos artificiales (soluciones) que sirven para resolver problemas reales de los seres humanos [13], [23] y [35]. De acuerdo con la literatura, entre los posibles artefactos a ser producidos por la ciencia del diseño se pueden distinguir los siguientes:

- Constructos: Lenguaje especializado utilizado para describir y razonar en referencia a un dominio del conocimiento; son utilizados para describir problemas y especificar sus soluciones.
- Modelos: Es un conjunto de proposiciones que expresan la relación entre los constructos. Típicamente representa de forma abstracta a alguna entidad natural o artificial.
- Métodos: Conjunto ordenado de pasos para realizar una tarea, transformando un modelo en otra representación con el objetivo de realizar una tarea.
- Instanciaciones: Artefactos implementados que representan de manera operativa el propósito común de los constructos, modelos y métodos.

Un aspecto adicional para considerar bajo el enfoque de la Ciencia de Diseño es la identificación del problema. Descubrir un problema relevante está distinguido por la pertinencia de la aplicabilidad práctica de un artefacto o conocimiento al obstáculo identificado (problema), para transitar de un estado actual a un estado deseado.

Dos tipos de problemas pueden ser distinguidos: de conocimiento y prácticos; La resolución de un problema de conocimiento, implica recolectar hechos, literatura, observación, consultar a especialistas en el tema, etc., y, sobre todo, no alterar el objeto de conocimiento. En la otra mano, la resolución de un problema práctico implica especificar o diseñar un cambio que será aplicado en la naturaleza, alterando su estado original.

Identificar ante qué tipo de problema nos enfrentamos es importante, por ello, en [41], el autor resume las distinciones más importantes entre ambos tipos de problema, presentado en la Tabla 1.

TABLA 1 – DIFERENCIAS ENTRE LOS PROBLEMAS DE CONOCIMIENTO Y LOS PROBLEMAS PRÁCTICOS

(FUENTE: ADAPTADO DE LA REFERENCIA [41])

Problema de conocimiento	Problema práctico
Encontrar la verdad	Hacer algo útil
Evitar alterar el mundo	Interferir en el mundo
El objetivo es el conocimiento	El objetivo es cambiar el mundo
Cualquier cambio en el mundo es un efecto colateral para minimizar	Cualquier cambio obtenido es un efecto colateral para apreciar
Las reglas éticas no son aplicadas a la respuesta	Las reglas éticas son aplicadas a las respuestas

Otro aspecto importante en torno a la Ciencia de Diseño es la evaluación del artefacto, puesto que, una vez construido es importante que sea puesto en acción y pueda ser observado para conocer más sobre su uso y comportamiento. Moody en [24], propone un modelo teórico para la evaluación de métodos de diseño en sistemas de información. La propuesta incorpora dos dimensiones para determinar el éxito de un modelo:

- Eficiencia real: si el método mejora el desempeño de la tarea.
- Adopción en la práctica: si el método es utilizado en la práctica.

Sin importar si el método mejora el desempeño o no, a menos que éste sea utilizado en la práctica, su beneficio no podrá ser aprovechado.

La Figura 4, presenta el modelo de evaluación de métodos propuesto por el autor, el diagrama muestra la relación entre los constructos y las relaciones causales entre ellas.

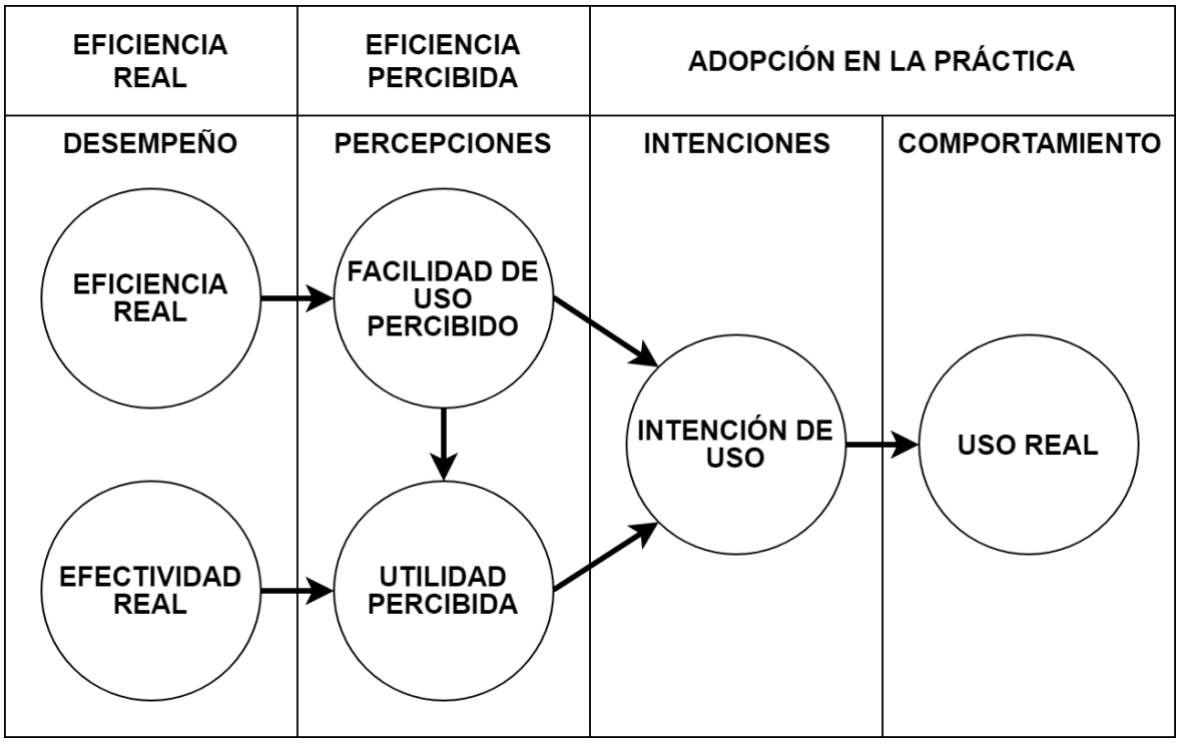

FIGURA 4. MODELO DE EVALUACIÓN DE MÉTODO

(FUENTE: ADAPTADO DE LA REFERENCIA [24])

Los constructos de este modelo son:

- Eficiencia real: El esfuerzo requerido para aplicar un método.
- Efectividad real: El grado con el que un método alcanza su propósito.

- Facilidad de uso percibido: El grado en el que una persona cree que, utilizando un método particular lo librará de esfuerzo.
- Utilidad percibida: El grado en el que una persona cree que un método particular será efectivo en alcanzar su propósito.
- Intensión de uso: La medida en la que una persona tiene la intención de utilizar un método en particular.
- Uso real: La medida en la que un método es utilizado en la práctica.

El presente trabajo de investigación busca diseñar y crear un artefacto de tipo instanciación que permita resolver el problema práctico de "la distribución y entrega de certificados digitales en módulos criptográficos destinados a usuarios finales", tales como, las computadoras personales, teléfonos inteligentes y, además, tokens criptográficos con interfaz USB y tarjetas inteligentes. Después de diseñar y construir el artefacto propuesto, se procederá a evaluar la propuesta y obtener los resultados de su inmersión en el problema, utilizando algunos de los constructos recientemente citados.

1.10. Periodo de análisis

En el alcance de este trabajo, la distribución de certificados digitales emitidos por la ECEP-RENIEC se ha registrado en los periodos establecidos en la Tabla 2.

TABLA 2 – PERIODOS DE ANÁLISIS DE LOS RESULTADOS EN LA EVALUACIÓN DEL ARTEFACTO

Módulo criptográfico	Periodo
Computadoras personales con S.O. Windows	Entre marzo 2012 y septiembre 2019
Tarjetas inteligentes y tokens criptográficos	Entre julio 2017 y septiembre 2019
Teléfonos inteligentes con S.O. Android	Entre agosto y septiembre 2019

1.11. Fuentes de información e instrumentos utilizados

Las fuentes de información han sido recolectadas de artículos y publicaciones de instituciones internacionales del ámbito científico como tecnológico, entre ellos IEEE, Research Gate, Academia, Springer, Semantic Scholar, Science Direct, Scientific Research, tesis de maestría y doctorales de Universidades e Institutos tecnológicos internacionales, entre otras; la información recopilada está relacionada a la problemática del despliegue de soluciones PKI (que generan Firma Digital) en módulos criptográficos seguros; así también, se revisaron las recomendaciones de las principales Instituciones Internacionales competentes tanto en la seguridad proveniente de los módulos criptográficos, como en su integración en Sistemas de Información que utilizan tecnología

PKI; estos módulos pueden ser elementos seguros, plataformas de módulos de confianza, entornos de ejecución de confianza, entre los más desplegados.

Además, para la implementación del artefacto en sus diferentes versiones se utilizaron las herramientas presentadas en la Tabla 3.

TABLA 3 – HERRAMIENTAS UTILIZADAS EN LA IMPLEMENTACIÓN DEL ARTEFACTO

Tipo de Herramienta	**Producto**
Middlewares de integradores y fabricantes de módulos criptográficos	CryptoVision Bit4ID Longmai SafeNet Athena SmartCard Sagem Orga Morpho Safran ACS Feitian Oberthur
SDK	Java Development Kit Trustonic
Servidor de Aplicaciones web	WildFly
API	Sun PKCS#11 MSCAPI
IDE	Net Beans Android Studio
Lenguajes de programación	C Java
Software Controlador de versiones	GitLab

1.12. Técnicas de recolección y procesamiento de datos

Los datos recolectados y presentados en este trabajo han sido obtenidos desde los datos estadísticos generados por la Planta de Certificación Digital del Estado Peruano gestionadas por la Sub Gerencia de Certificación e Identificación Digital del Registro Nacional de Identificación y Estado Civil.

CAPÍTULO II
MARCO TEÓRICO Y MARCO CONCEPTUAL

Los principales conceptos teóricos y conceptuales relacionados con este trabajo son abordados a continuación.

2.1 Criptografía

Los autores en [26], destacan que, para empezar a comprender la criptografía, debemos primero referirnos a un término más general aún, la **Criptología**, ciencia que está dividida en dos ramas principales, como lo muestra la Figura 5.

La **Criptografía** es la ciencia de la escritura oculta, ciencia que tiene como objetivo ocultar el significado de un mensaje con diferentes propósitos.

El **Criptoanálisis** es la ciencia de decodificar o quebrar Criptosistemas, el cual es de vital importancia para los criptosistemas modernos, puesto que, sin equipos de personas que intenten romper estos métodos criptográficos que conforman el criptosistema, no se podría conocer si los sistemas son seguros o no. Debido a que el Criptoanálisis es la única forma de asegurar que los sistemas criptográficos sean seguros, ésta es una parte integral de la Criptología.

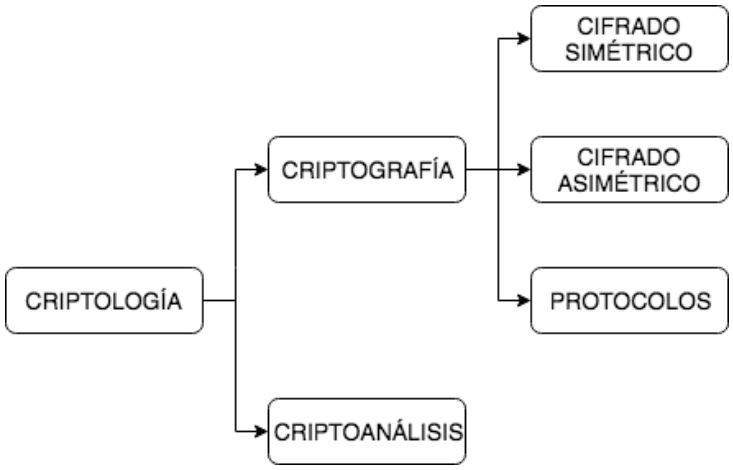

FIGURA 5. LA CRIPTOLOGÍA Y SUS CAMPOS

(FUENTE: ADAPTADO DE LA REFERENCIA [26])

Retornando al área de nuestro interés, la criptografía también está categorizada principalmente en las tres vertientes presentadas en la Figura 5, las que pasamos a describir en breve.

2.1.1 Algoritmos simétricos

Los algoritmos simétricos son entendidos por la mayoría de personas como lo que la criptografía es, donde dos partes comparten métodos de cifrado y descifrado, así como una llave secreta, e intercambian mensajes que solo ellos pueden leer. Estos algoritmos fueron los primeros en la historia de la criptografía, y aún hasta la actualidad son utilizados en cifrado de datos, así como en la verificación de la integridad de mensajes, dentro de casi todo aquel sistema que contemple una capa mínima de seguridad. Un cifrado simétrico trabaja utilizando las siguientes dos transformaciones, presentadas en la Tabla 4.

TABLA 4. SISTEMA DE CIFRADO SIMÉTRICO

$$c = e_K(m),$$ $$m = d_K(c)$$
Donde:
m es el texto plano,
e es la función de cifrado,
d es la función de descifrado,
K es la llave secreta,
c es el texto cifrado.

La Figura 6 representa de forma simplificada un proceso de cifrado simétrico (que usa algoritmos simétricos) para la transferencia de un dato (un documento electrónico, por ejemplo) de forma confidencial entre la entidad origen (Bob), y la entidad destino (Alice). Se puede observar que Bob utiliza la llave simétrica (secreta) común para ambos, para cifrar simétricamente el dato que Bob quiere enviar a Alice de forma confidencial, y una vez recibido por Alice, ella utiliza la llave simétrica (que solo ellos poseen) para descifrar simétricamente el dato cifrado, y recuperar el dato original.

Algunos de los algoritmos simétricos más conocidos por su uso, son:

- AES (Advanced Encryption Standard)
- Blowfish
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- RC5

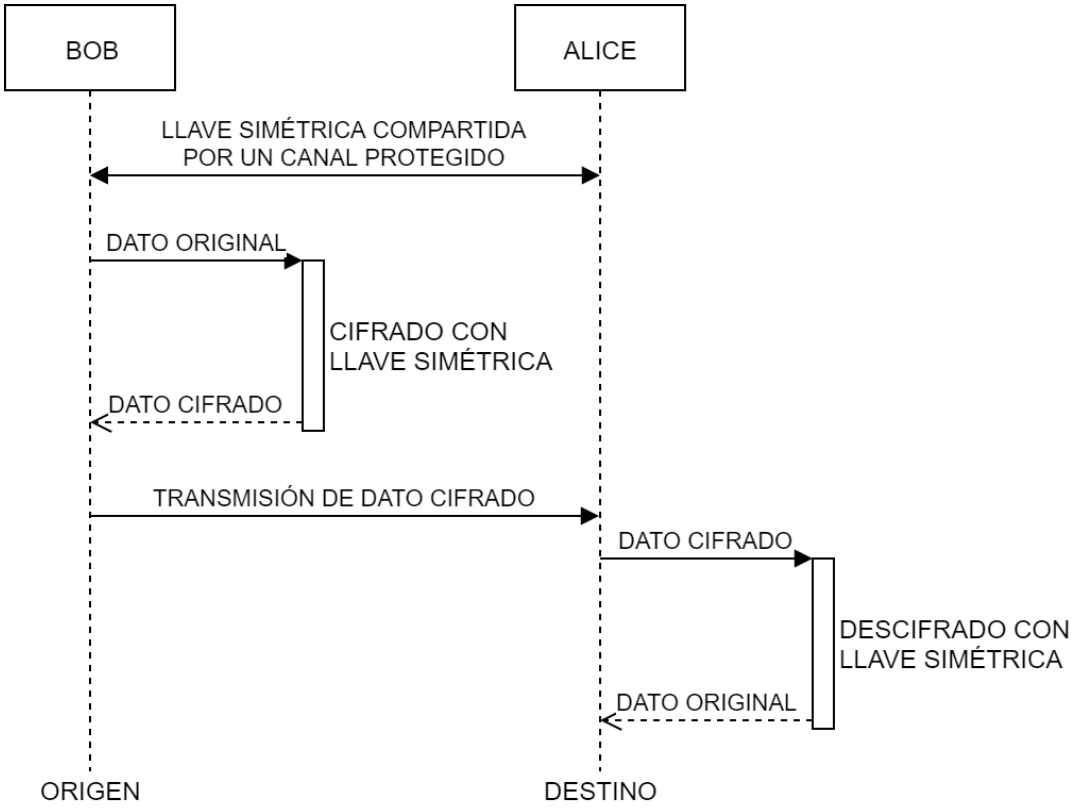

FIGURA 6. CIFRADO SIMÉTRICO

2.1.2 Algoritmos asimétricos

Los algoritmos asimétricos son presentados públicamente en 1976, como un tipo de cifrado completamente diferente al existente (simétrico). Los investigadores Whitfield Diffie y Martin Hellman de la Universidad de Standford, presentan en [4] la criptografía de llave pública. Esta propuesta presenta a un usuario que posee una llave secreta (ahora denominada llave privada) como en el caso de la criptografía simétrica, y, además, una llave pública. Estos algoritmos dieron paso a la implementación de aplicaciones importantes hoy en día, tales como la generación de las Firmas Digitales, así como la implementación del protocolo de establecimiento de llaves, entre otras aplicaciones clásicas. La Tabla 5 presenta un sistema de cifrado asimétrico conformado por tres transformaciones.

La Figura 7 representa de forma simplificada un proceso de cifrado asimétrico (que usa algoritmos asimétricos) para la transferencia de un dato de forma confidencial entre la entidad origen (Bob), y la entidad destino (Alice). Se puede observar que Bob utiliza la llave pública de Alice para cifrar asimétricamente el dato que Bob quiere enviar a Alice de forma confidencial, y una vez el dato cifrado es recibido por Alice, ella utiliza su llave privada (que solo ella posee) para descifrar asimétricamente el dato cifrado, y recuperar el dato original. Alice podría necesitar enviar un dato de respuesta a Bob, para esto, ella utiliza la llave

pública de Bob para cifrar su respuesta, le envía el dato cifrado, y Bob utiliza su llave privada para obtener la respuesta (dato original) enviada por Alice.

TABLA 5. SISTEMA DE CIFRADO ASIMÉTRICO

$$G() \rightarrow \{p_K, s_K\},$$
$$c = E(p_K, m),$$
$$m = D(s_K, c),$$
$$D\big(s_K, E(p_K, m)\big) = m$$

Donde:

$G()$ es un algoritmo no determinístico que genera o retorna un par de llaves $\{p_K, s_K\}$,

$E()$ es un algoritmo no determinístico que cifra texto plano m y retorna el texto cifrado c,

$D()$ es un algoritmo determinístico que descifra c y retorna el texto plano m.

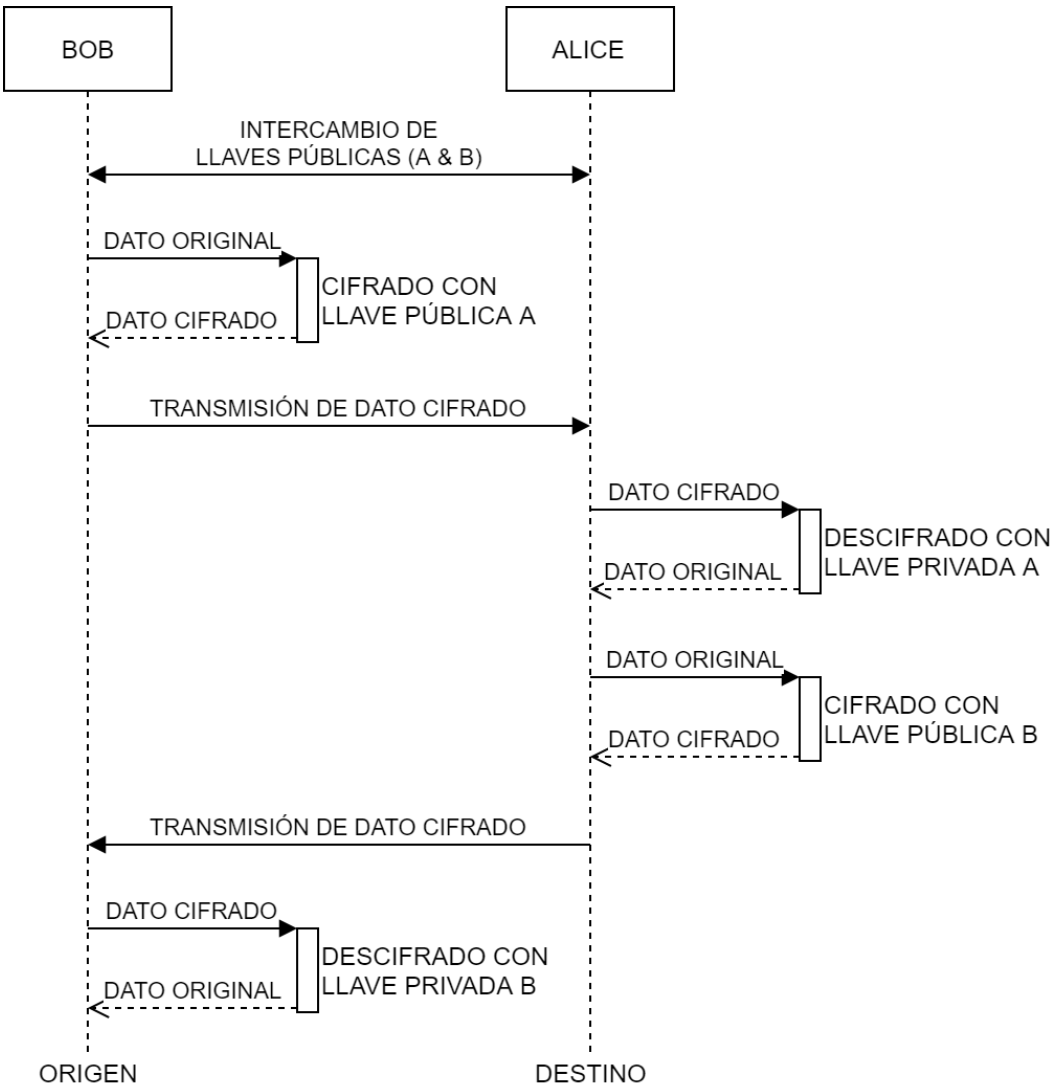

FIGURA 7. CIFRADO ASIMÉTRICO

Entre los cripto-sistemas más conocidos desarrollados sobre la base de cifrado asimétrico, se tienen:

- RSA (Rivest, Shamir y Adleman)
- Diffie-Hellman
- DSS (Digital Signature Standard)
- ECC (Elliptic Curve Cryptography)

Estos algoritmos de generación de llaves criptográficas crean el material criptográfico con los cripto-sistemas antes citados, los que están más allá del alcance de este trabajo.

2.1.3 Protocolos criptográficos

Los protocolos criptográficos se ocupan de la aplicación de los algoritmos criptográficos. Desde el punto de vista de un protocolo, estos algoritmos pueden ser vistos como bloques que permiten implementar aplicaciones tales como la comunicación segura a través de la Internet, denominada como el esquema de seguridad de la capa de transporte (*TSL: Transport Secure Layer*), esquema que es utilizado en casi todos los navegadores web actuales, y que ejemplifica a un protocolo criptográfico.

2.2 Infraestructura de Llave Pública

Para la mayoría de las personas que tienen alguna noción de PKI, ésta se trata de la infraestructura de llave pública que se usa en Internet. Sin embargo, las aplicaciones reales de PKI son mucho más amplias. PKI empezó siendo un término genérico que significaba un conjunto de servicios que utilizan criptografía de llave pública. Sin embargo, PKI se ha explotado en muchas aplicaciones o protocolos, como en (*SSL: Secure Sockets Layer*), (*S/MIME: Secure Multimedia Internet Mail Extensions*), (*IPSec: IP Security*), (*SET: Secure Electronic Transactions*), y (*PGP: Pretty Good Privacidad*), entre los más conocidos.

Por otro lado, el uso masivo del certificado digital X.509 v3 como uno de los elementos importantes en una PKI, ha sido uno de los problemas de estandarización más abordados en el comercio electrónico. Desde 1995, el grupo de trabajo PKIX del (*IETF: Internet Engineering Task Force*) comenzó a involucrar completamente los certificados X.509 v3 en los estándares PKI, logrando que PKI tenga un uso más práctico dentro de las lógicas de negocios críticas en Internet. El estándar del grupo de trabajo IETF PKIX se ha convertido en el más aceptado.

Así también, los autores en [5] presentan una relación de diversos países donde se vienen implementando trámites electrónicos vía Internet con la finalidad de ofrecer un mejor servicio a los ciudadanos y a las empresas. Reemplazar los trámites presenciales con éstos

sería muy fácil si no hubiese, en ciertos casos, la necesidad de determinar con certeza cuándo fueron realizados, quiénes los solicitaron, quiénes los atendieron, entre otros. Para esto, los países han implementado el uso de las firmas digitales y los sellos de tiempo sobre la base de tecnología PKI, buscando dotar al trámite electrónico de cuatro características que de forma natural no tiene: autenticidad, integridad, no repudio y fecha cierta. Con estas características, es posible: saber el origen del trámite (autenticidad), el momento en que se efectuó (fecha cierta), garantizar que no ha sido modificado (integridad) y garantizar que las partes no puedan negar su autoría (no repudio).

En el contexto del presente trabajo, la firma digital sobre la base de tecnología PKI es aquella generada utilizando criptografía asimétrica y en la que la llave privada se encuentra en posesión y control del firmante.

2.2.1 Elementos participantes en una PKI

Son diversos los elementos de hardware y software que conforman una PKI, la Figura 8 presenta los más importantes que son descritos a continuación.

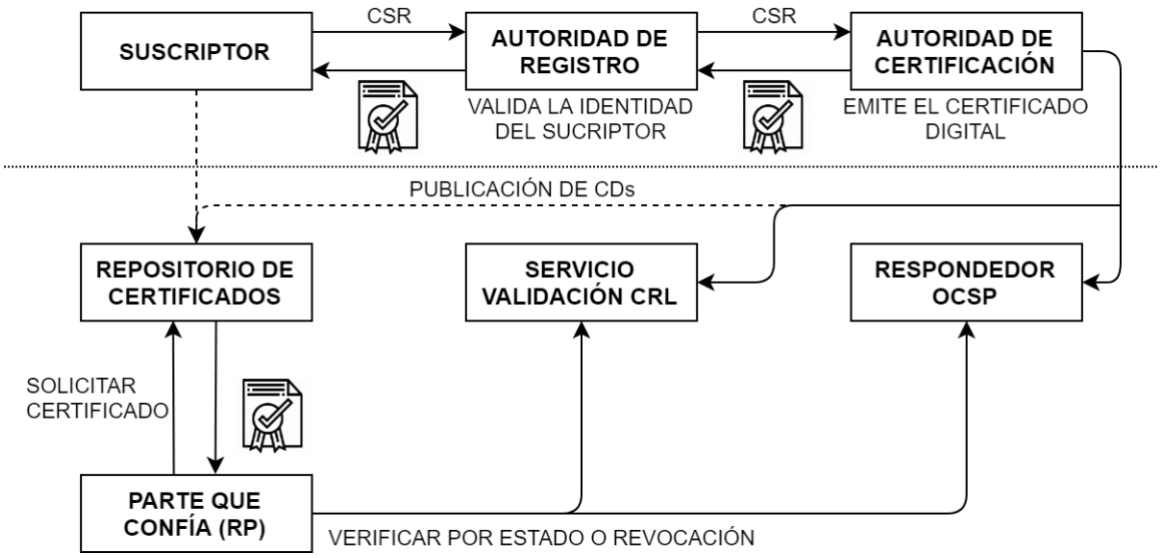

FIGURA 8. CICLO DE VIDA DE UN CERTIFICADO DIGITAL PERTENECIENTE A UNA JERARQUÍA PKI

Suscriptor. Es el usuario final también conocido como entidad final, el cual solicita un certificado digital.

Autoridad de Registro. Es la encargada de gestionar las funciones relacionadas a la emisión de certificados. Es decir, debe realizar la validación de la identidad necesaria antes de solicitar a la CA la emisión de un certificado digital.

Autoridad de Certificación. Es el tercero de confianza o en el que se confía, encargada de emitir (generar) los certificados digitales a los suscriptores que han validado su identidad previamente ante la RA.

También son encargados de gestionar los servicios relacionados a la información actualizada de los estados de los certificados digitales, mediante los servicios CRL y OCSP que publica, de tal manera que algún tercero pueda verificar que los certificados digitales pertenecientes a aquella jerarquía de certificación aún están vigentes.

Parte que confía. Es el tercero que confía o el consumidor de servicios de certificación digital, los que por lo general son Sistemas de información que dentro de sus procesos requieren la validación de certificados digitales.

Elementos adicionales en la Figura 8 son tratados con mayor detalle a continuación.

2.2.2 Certificado Digital

El Certificado digital, es un documento digital que contiene una llave pública, además de información asociada con la entidad solicitante, y una firma digital del certificado emisor. Es decir, es un empaquetado que permite intercambiar, almacenar, y utilizar llaves públicas. Ellos son el bloque básico de construcción de una PKI.

Según lo indicado en [14], la estructura básica del certificado digital es la presentada en la Tabla 6, cuyos campos más utilizados son descritos a continuación:

Versión (version). Existen 3 versiones; la primera (1) con valor 0, soporta solo campos básicos, la segunda (2) con valor 1, que agrega identificadores únicos, y la tercera (3) con valor 2, incluye extensiones. Los certificados emitidos hoy, son de la versión 3.

Número de serie (serialNumber). Debe ser un número no secuencial con una longitud de al menos 20 bits de entropía. Identifica a un certificado emitido por una CA.

Algoritmo de firma (signatureAlgorithm). Especifica el algoritmo utilizado con el que se generó (firmó) el certificado. Es colocado en el certificado para ser protegido por la firma, y es especificado de acuerdo con el RFC3279.

Emisor (issuer). Contiene el nombre único (DN: Distinguesh Name) que identifica a la entidad que ha firmado el certificado. Este campo se define de acuerdo con el estándar X.501 y mediante la estructura ASN.1.

Vigencia (validity). Define el intervalo de tiempo durante el cual el certificado es válido, y es representado con dos valores: la fecha de inicio y la fecha de término.

Sujeto (subject). Es el nombre único de la entidad para el cual el certificado es emitido. Certificados autofirmados tienen el mismo DN en los campos issuer y subject.

Llave pública (subjectPublicKeyInfo). Contiene la llave pública.

TABLA 6 – CAMPOS BÁSICOS DEL CERTIFICADO DIGITAL

(FUENTE: REFERENCIA [14])

```
Certificate  ::=  SEQUENCE  {
        tbsCertificate       TBSCertificate,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }

   TBSCertificate  ::=  SEQUENCE  {
        version         [0]  EXPLICIT Version DEFAULT v1,
        serialNumber         CertificateSerialNumber,
        signature            AlgorithmIdentifier,
        issuer               Name,
        validity             Validity,
        subject              Name,
        subjectPublicKeyInfo SubjectPublicKeyInfo,
        issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
        extensions      [3]  EXPLICIT Extensions OPTIONAL
                             -- If present, version MUST be v3
        }

   Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

   CertificateSerialNumber  ::=  INTEGER

   Validity ::= SEQUENCE {
        notBefore      Time,
        notAfter       Time }

   Time ::= CHOICE {
        utcTime        UTCTime,
        generalTime    GeneralizedTime }

   UniqueIdentifier  ::=  BIT STRING

   SubjectPublicKeyInfo  ::=  SEQUENCE  {
        algorithm            AlgorithmIdentifier,
        subjectPublicKey     BIT STRING  }

   Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

   Extension  ::=  SEQUENCE  {
        extnID      OBJECT IDENTIFIER,
        critical    BOOLEAN DEFAULT FALSE,
        extnValue   OCTET STRING
                    -- contains the DER encoding of an ASN.1 value
                    -- corresponding to the extension type identified
                    -- by extnID
        }
```

2.2.3 Repositorios de Certificados

Los certificados son revocados cuando sus llaves privadas asociadas están comprometidas o ya no son necesarias. En ambos casos, por seguridad es conveniente revocarlos, los protocolos y procedimientos de revocación están diseñados para comunicar la revocación a los usuarios. Dos estándares de revocación son implementados.

Repositorio de Certificados. Es un servicio de directorio sobre una red, una de sus implementaciones más habituales es el Directorio Activo del fabricante Microsoft.

Lista de certificados revocados (*CRL: Certificate Revocation List*). Es una lista que contiene los números de serie de los certificados revocados que no han expirado aún. Las CA mantienen una o más de estas listas. Cada certificado debe contener la localización del correspondiente CRL en la extensión "*CRL Distribution Points certificate*".

Protocolo de verificación del estado de los certificados en línea (*OCSP: Online Certificate Status Protocol*). Permite a los usuarios (terceros) obtener el estado de revocación de un único certificado a la vez, y en un momento dado. Los servidores OCPS son conocidos como "*OCSP responders*". La localización de un OCSP responder de una CA está codificada en la extensión "*Authority Information Access certificate*".

2.3 La PKI Nacional del Estado Peruano

Se ha documentado en [5], el caso de la implementación de la PKI nacional del Estado Peruano vigente, el artículo presenta el diseño y los detalles de implementación de la jerarquía que fue diseñada con la finalidad de superar las limitaciones de sus predecesoras. Presenta el contexto normativo sobre la cual fue implementada, lo que es de vital importancia en la implementación de una PKI para la adopción de la Firma Digital.

2.3.1 La Infraestructura oficial de firma electrónica (IOFE)

En el Perú, la IOFE, creada en el Reglamento de la Ley N° 27269 de Firmas y Certificados Digitales vía el Decreto Supremo Nº 052-2008-PCM, es un sistema confiable, regulado, supervisado y cuyos Prestadores de Servicios de Certificación (PSC) requieren acreditarse. Dentro del marco de la IOFE es posible generar firmas digitales que gozan de la misma validez y eficacia jurídica que las firmas manuscritas.

La gestión de la IOFE fue encargada a una organización independiente, denominada Autoridad Administrativa Competente (AAC), que tiene como una de sus funciones principales acreditar a los PSC, como condición para su ingreso a la IOFE. Los PSC pueden adoptar cualquiera de las siguientes modalidades: (1) Autoridad de Certificación, (2) Autoridad de Registro y/o (3) Prestador de Servicios de Valor Añadido.

La Figura 9 presenta una ilustración de los principales componentes de la IOFE. El lado derecho, reservado para el sector público, está conformado por una única CA raíz, administrada por una organización denominada Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), bajo la cual únicamente las entidades públicas del Estado Peruano acreditadas como CA pueden operar de forma subordinada. El lado izquierdo, reservado para el sector privado, está conformado por múltiples raíces de CA del sector privado.

La interoperabilidad tecnológica entre las CA del sector público y privado es lograda mediante el uso de una única lista de confianza oficial (TSL), la cual es actualizada cada vez que un PSC es acreditado por la AAC. La parte inferior está conformada por los suscriptores de certificados digitales obtenidos a través de las RA vinculadas a las CA.

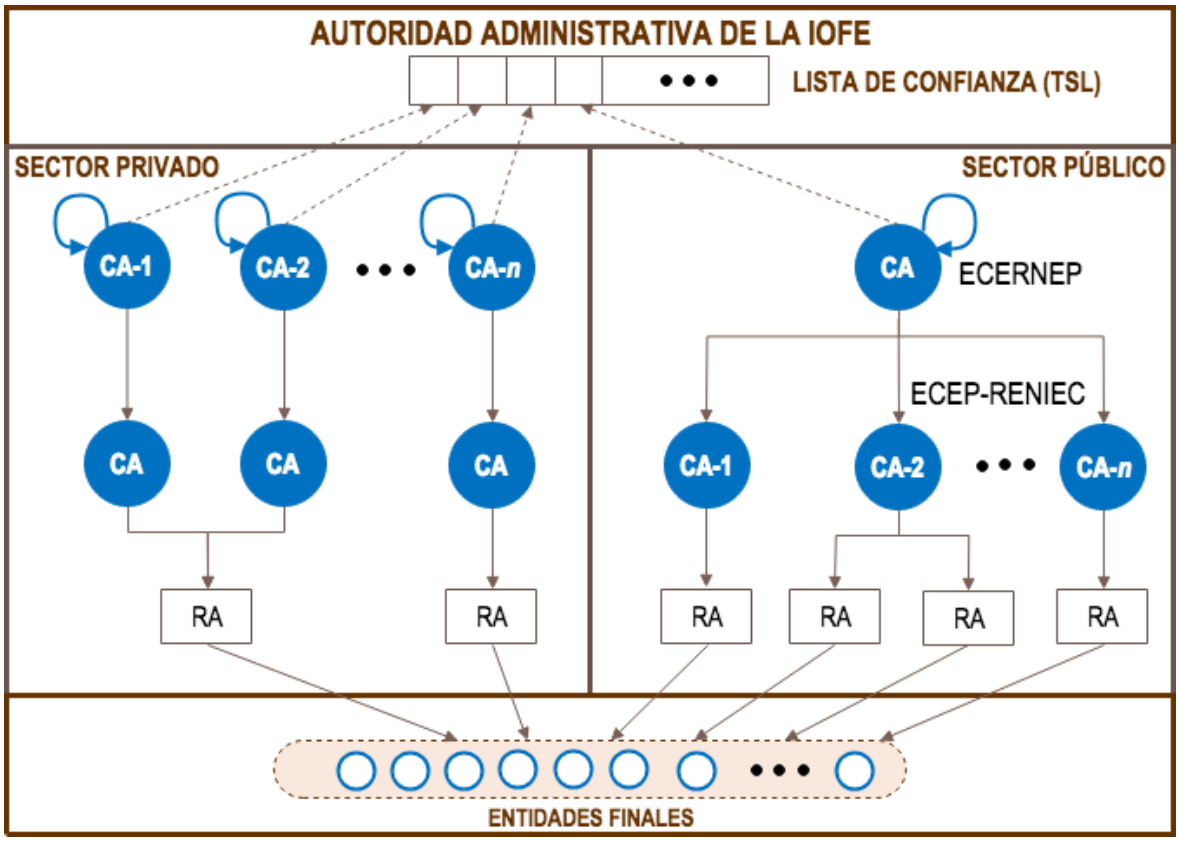

FIGURA 9. PRINCIPALES COMPONENTES DE LA IOFE DEL PERÚ

(FUENTE: REFERENCIA [5])

2.3.2 Jerarquía de certificación digital del estado peruano

La jerarquía descrita en la Figura 10, es la jerarquía de certificación digital vigente del estado peruano. Tiene en el nivel 1 a la raíz (ECERNEP PERU CA ROOT 3); el nivel 2 está destinado a acoger los certificados digitales emitidos para nuevas CA que se acrediten en el marco de la IOFE en el sector público, de este nivel, se distingue a la ECEP-RENIEC,

como la actual autoridad de certificación del estado peruano. Además, en este nivel reside la CA para el prestador de servicio de valor añadido en su modalidad de sellado de tiempo (TSA), denominada la EC-PSVA, emisor de TSU para el servicio de TSA.

Las CA emisoras de certificados digitales para entidades finales están distribuidas en el nivel 3, según el tipo de suscriptor: Class 1 (para usos específicos como los certificados digitales para persona naturales contenidos en dispositivos móviles), Class 2 (para Ciudadanos), Class 3 (para Trabajadores de la Administración Pública) y Class 4 (para Sistemas de Información). La emisión de CRL por clase es diaria en este nivel online (CRL consultada permanentemente por el mayor flujo de emisiones); diferente de los dos primeros niveles donde las emisiones son poco frecuentes, encontrándose en modo offline.

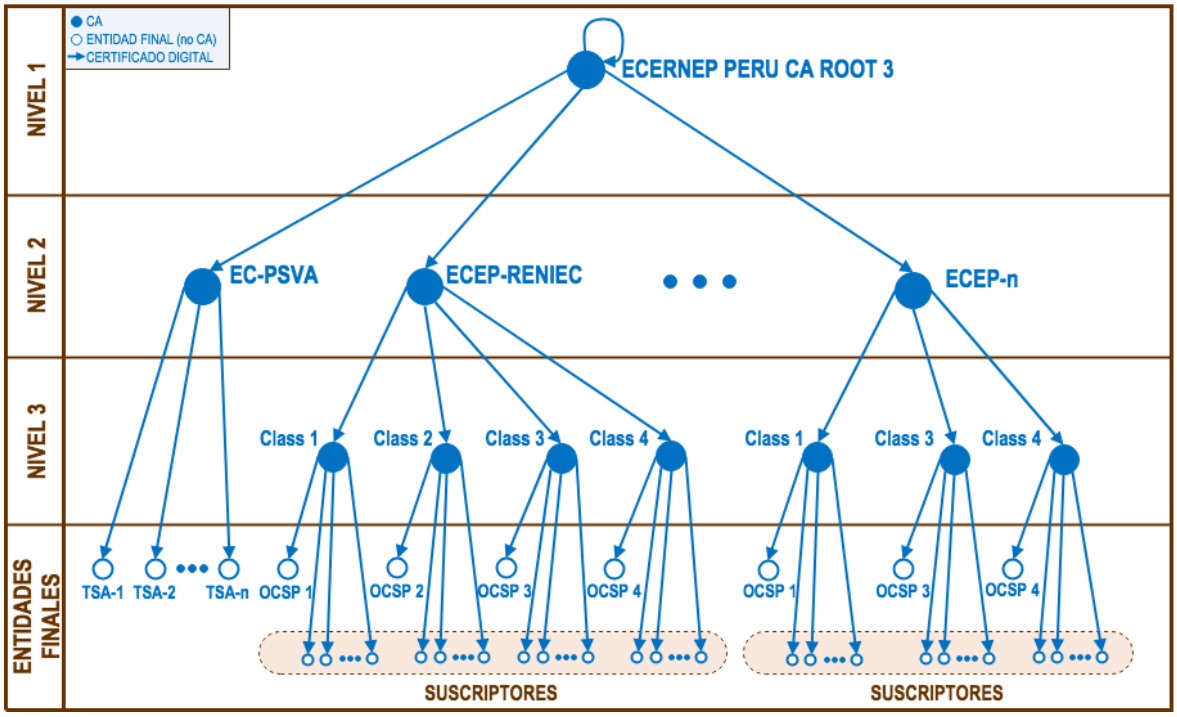

FIGURA 10. JERARQUÍA DEL ESTADO PERUANO ECERNEP PERU CA ROOT 3

(FUENTE: REFERENCIA [5])

2.4 Firma Digital

Así como la identidad digital segura es un mecanismo que permite garantizar con seguridad y confianza la identidad de una persona en medios electrónicos, también, se presenta la necesidad de que las personas cuenten con mecanismos que les permitan manifestar su voluntad, representada cuando por ejemplo asume obligaciones; mecanismos que le permitan garantizar la misma validez legal y eficacia jurídica existente en los entornos presenciales tradicionales.

Una firma digital es un dato en formato electrónico que sirve como mecanismo para verificar la autenticidad (propiedad que permite identificar el origen del dato) e integridad (propiedad que garantiza que el dato no ha sido modificado) proveniente de otro dato (referido también como dato firmado) también en formato electrónico.

Una firma digital es un tipo de firma electrónica. Ésta última es cualquier símbolo electrónico utilizado para vincularse a un dato en formato electrónico, entre ellas destacan: la firma manuscrita digitalizada, la firma biométrica, la dupla usuario contraseña, o la misma firma digital que es generada por un procedimiento criptográfico que establece una relación única y exclusiva entre el dato firmado y el firmante.

2.4.1 Operaciones de Firma Digital

Se destacan cuatro operaciones básicas dentro del alcance del uso de la firma digital: generar, verificar, extender y archivar. En este trabajo estamos interesados en revisar la primera operación que consiste en crear un dato y asociarlo a un documento de forma tal que el dato generado sea único y esté vinculado al documento, esto es, efectuar la firma digital propiamente dicha.

2.4.2 Modelo de la creación de la Firma Digital

De acuerdo con [6], el objetivo de la creación es generar una firma digital que contenga el documento del firmante, el certificado de firma o una referencia a este, así como los atributos de firma que la soportan, y su interpretación y propósito. la Figura 11 presenta los elementos que participan en la creación.

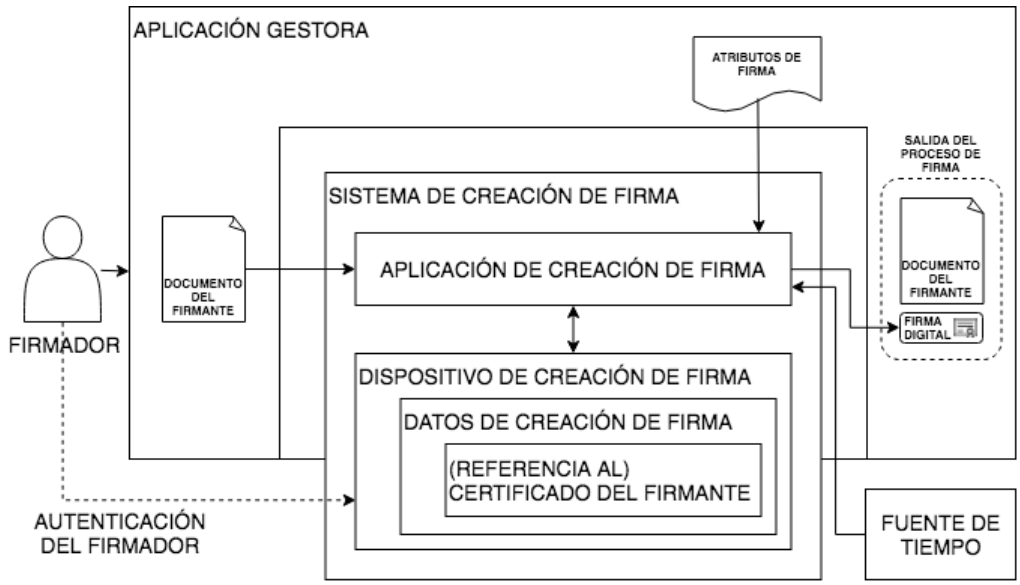

FIGURA 11. MODELO FUNCIONAL DE LA CREACIÓN DE UNA FIRMA DIGITAL

(FUENTE: ADAPTADO DE LA REFERENCIA [6])

El modelo antes presentando consta de los siguientes elementos:

Firmador: Quién desea crear una firma digital de un documento, o firmarlo suministrándolo a la Aplicación gestora. Puede ser una persona o un autómata implementado dentro de la aplicación gestora.

Documento del Firmante: Es el documento para el cual la firma digital será creada.

Aplicación gestora: Es un Sistema de información, que representa a una aplicación informática a la que el firmador tiene acceso para firmar documentos electrónicos.

Atributos de firma: Son datos que son provistos por la aplicación gestora o por el firmante, que en general forman parte de la firma digital.

Sistema de creación de firma: Software que implementa toda la funcionalidad requerida para la creación de una firma digital, y que está integrado al Sistema de información. Contiene una aplicación de creación de firma y un dispositivo de creación de firma.

Aplicación de creación de firma: Es la encargada de recibir todos los insumos del Sistema de información (Documento del firmante y los atributos de firma), prepara estos insumos, y los envía al Dispositivo de creación de firma (accediendo a los datos de creación de firma), y con la autorización previa mediante la autenticación del firmador, se genera la firma digital que es retornada al Aplicativo de creación, quién en conjunto con los datos suministrados por la fuente de tiempo de ser el caso, ensambla la firma digital resultante del documento electrónico de interés conforme con el formato de firma deseado.

Dispositivo de creación de firma: Contiene el certificado digital para generar firma digital o una referencia a él; así como, contener los datos de creación de firma correspondientes (generalmente la llave privada asociada al certificado digital); además, puede autenticar al firmador, y crear el valor de la firma utilizando los datos de creación de firma del firmador.

Fuente de tiempo: Fuente de tiempo que emite fecha y hora cierta, comúnmente implementada con una entidad de confianza que emite sellos de tiempo, que son firmas digitales generadas por una unidad de sello de tiempo, las que garantizan que el dato ha existido en un momento específico y que no ha sido alterado desde entonces.

Autenticación del Firmador: Secuencia alfanumérica conocida únicamente por el firmante que permite el uso de los datos de creación de firma.

Firma digital: Dato generado por el Aplicativo de creación de firma, y que es administrado junto con el Documento del firmante por la Aplicación gestora, la cual está vinculada tanto al documento como al firmante.

2.4.3 Clases o niveles de firma digital

La Figura 12 ilustra una estructura común que sirve como base para todos los tipos de firma digital definidas en [6]. Esta consiste en el documento del firmante, los atributos firmados, los que son requeridos para el cálculo del valor de la firma digital, el valor de la firma en sí mismo, así como cualquier otro atributo no firmado incluido en la firma por la Aplicación gestora.

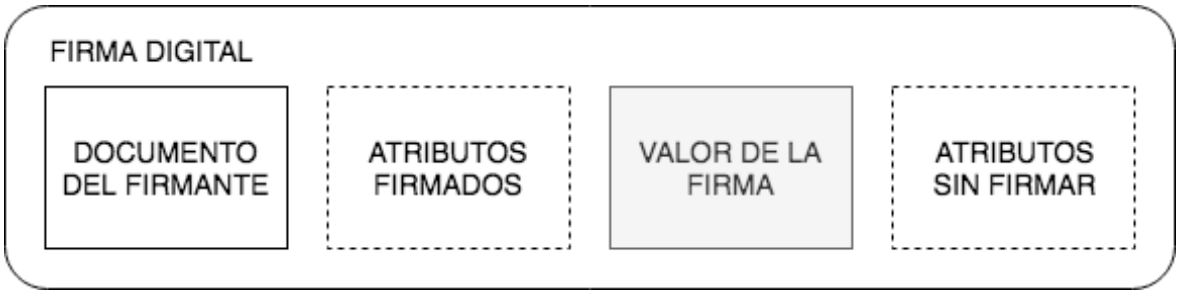

FIGURA 12. FIRMA DIGITAL

(FUENTE: ADAPTADO DE LA REFERENCIA [6])

Cada una de las clases de firma digital corresponden a una combinación de atributos agregados con la finalidad de mejorar la capacidad de validar una firma en el futuro, cuando el certificado correspondiente o cualquier otro material necesario para la validación satisfactoria puede haber expirado, ser revocado, o ha utilizado algoritmos que no tienen la suficiente fortaleza para ser de confianza.

Una **Firma básica** es una firma que puede ser validada tanto como el correspondiente certificado esté vigente (ni revocado ni expirado).

Una **Firma con tiempo** es una firma que prueba que la firma digital ha existido en punto de tiempo dado.

Una **Firma con material de validación longevo** es una firma que proporciona la disponibilidad a largo plazo del material de validación al incorporar todo el material o la referencia al material requerido para validar la firma.

Una **Firma proporciona disponibilidad a largo plazo e integridad del material de validación** está orientada a la disponibilidad e integridad a largo plazo del material de validación de las firmas digitales a largo plazo lo que puede ayudar a validar la firma más allá de eventos que limiten su validez (por ejemplo, la debilidad del algoritmo criptográfico utilizado, o la expiración de algún dato de validación).

2.4.4 Creación de una firma digital básica

Los insumos obligatorios para el proceso de creación de una Firma básica son el documento del firmador o la representación del documento de firmador y el certificado digital de firma. La salida del proceso de creación de firma básica es un objeto dato firmado que contendrá: el valor de la firma, una referencia a o una copia del certificado digital de firma como un atributo firmado, y atributos opcionales firmados o no. La Figura 13 ilustra el contenido de una Firma digital básica.

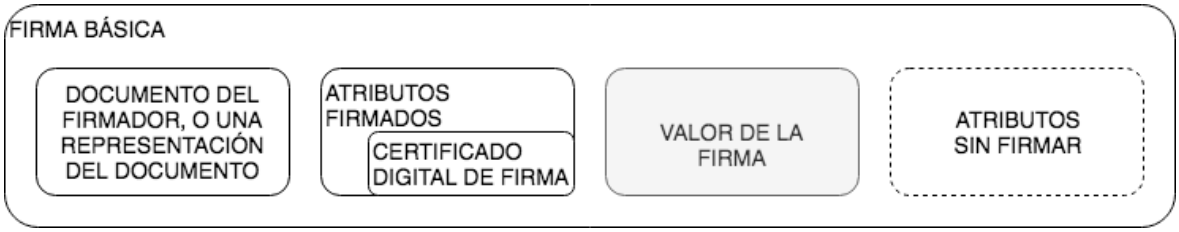

FIGURA 13. FIRMA DIGITAL BÁSICA

(FUENTE: ADAPTADO DE LA REFERENCIA [6])

2.4.5 Formatos de empaquetamiento

A fin de preservar la interoperabilidad cuando se trata de documentos firmados digitalmente, la utilización de estándares es esencial. El formato de firma digital define como se estructura los campos y los valores que la componen, entre las que se distinguen:

CMS (Cryptographic Message Syntax). Es un formato de firma genérico y de requisitos minimalistas que podría ser insuficiente para efectuar operaciones de validación de largo plazo.

CAdES (CMS Advanced Electronic Signatures). A diferencia del formato CMS, el formato CAdES establece la presencia de atributos obligatorios que permiten la verificación a largo plazo de una firma digital. Normalmente, es apropiado cuando se requiere que la firma se guarde en formato binario.

XAdES (XML Advanced Electronic Signatures). La especificación ha sido diseñada para generar firmas digitales en formato XML. El resultado es una firma en formato de etiquetas que puede ser procesada de forma eficiente por los computadores. Ejemplos de este tipo de firma son las usadas en facturas e historias clínicas electrónicas.

PAdES (PDF Advanced Electronic Signatures). PAdES fue específicamente diseñado para atribuir las mismas capacidades definidas en CAdES y XAdES a documentos PDF con firma digital.

2.5 Módulos criptográficos

Esta sección presenta las principales implementaciones en el mercado tecnológico actual, su ámbitos y aplicaciones, así como su distinción entre cada uno de ellos.

2.5.1 Hardware Security Module (HSM)

Denominado también dispositivo seguro resistente a manipulaciones que puede ser incorporado en un sistema de información y que provee servicios criptográficos tales como la gestión, generación, y custodia de material sensible. Existen diferentes modelos y factores de forma según el propósito. Por ejemplo, un HSM de alto rendimiento, que es un módulo con gran capacidad de almacenamiento y tiene una alta velocidad de atención a peticiones concurrentes Por lo general, es accesible a través de una interfaz ethernet, y es custodiado en un centro de datos. Otro factor de forma es la presentación en forma de tarjeta de expansión. Otro factor de forma es el denominado portable, debido a que es conectado directamente a su respectivo host mediante un puerto externo, y solo es utilizado a demanda; concluido su uso es custodiado en un almacén seguro.

2.5.2 Tarjeta inteligente o tarjeta con chip (Smart Card)

De forma similar al HSM, una tarjeta inteligente también es un módulo de hardware seguro. La diferencia entre ambas reside principalmente en que sus prestaciones son limitadas y están adecuadas a pequeños volúmenes, puesto que una tarjeta inteligente por lo general solo atiende a un usuario final. La tarjeta inteligente es típicamente una tarjeta de plástico PVC o de policarbonato con un microcontrolador embebido, y se comunican con un host mediante un lector de tarjetas. Una tarjeta inteligente puede exponer una interfaz de contacto, de proximidad o ambas. La familia de estándares ISO/IEC 7816 describe las características físicas de las tarjetas inteligentes de contacto, los protocolos de comunicación, y las interfaces que permiten gestionar el material criptográfico contenido. Similarmente, el ISO/IEC 14443 y el ISO/IEC 18092 describen las interfaces y protocolos de proximidad para tarjetas inteligentes. Complementando también, la especificación PC/SC (Personal Computer/Smart Card) está diseñada para integrar las funcionalidades de una tarjeta inteligente como servicios en un host (computadora personal).

2.5.3 Token criptográfico

Es un módulo de hardware seguro comúnmente utilizado por usuarios finales, cuenta con una interfaz de acceso USB como mínimo, y puede ser descrito como un producto embebido que representa al micro-controlador de la tarjeta inteligente insertado

permanentemente en un lector de tarjetas inteligentes con la interfaz USB. Este producto integrado es distribuido como el factor de forma token USB o token con interfaz USB.

2.6 Tecnologías modernas de seguridad portátiles

Se han presentado muchas propuestas diferentes en [24] sobre cómo se puede construir un entorno seguro contenido en los dispositivos móviles, estas propuestas incluyen diferentes arquitecturas como protección de software (en tiempo de compilación y endurecimiento de código en tiempo de enlace), la gestión de aplicaciones, así como, la protección de hardware, destacando las siguientes propuestas.

2.6.1 Secure Element (SE)

En concordancia con lo citado en [10], un elemento seguro (SE) es una plataforma resistente a manipulaciones (generalmente un microcontrolador seguro en un chip) capaz de albergar de forma segura aplicaciones y su datos confidenciales y criptográficos (por ejemplo, llaves criptográficas) en concordancia con la reglas y requerimientos de seguridad establecidos por Autoridades de confianza bien identificados.

Existen diferentes factores de forma para un SE: SE integrado, SIM/UICC, smart microSD, así como también tarjetas inteligentes, todos ellos para abordar requerimientos muy específicos de las diferentes necesidades del mercado. Los SEs son una evolución del chip tradicional que reside en las tarjetas inteligentes, que se han adaptado para satisfacer las necesidades de un mundo cada vez más digitalizado, necesidades presentes en los teléfonos inteligentes, las tabletas, los decodificadores, las portátiles, los automóviles inteligentes, y en diversos dispositivos IoT.

Cuando múltiples aplicaciones y sus procesos asociados están almacenados y se ejecutan dentro de un único dispositivo, es crucial contar con la capacidad de alojar aplicaciones de confianza y sus credenciales en un entorno seguro. Ejemplos de esto incluyen autenticación, identificación, firmas digitales y gestión de credenciales, todos los cuales son necesarios para diferentes servicios al consumidor y que requieren de un entorno protegido para operar de forma segura.

Los usuarios exigen cada vez más que todos sus servicios sean accesibles desde un teléfono inteligente. Por ejemplo, la seguridad a prueba de manipulaciones del SE permite que el teléfono inteligente almacene de forma segura las llaves de un automóvil, lo que es esencial debido al alto valor del artículo. El elemento seguro utiliza la interfaz NFC del teléfono inteligente, y además, permite la ejecución de operaciones seguras con los datos

relacionados a la llave del automóvil. El App del teléfono inteligente, mediante una autenticación, indica al SE contenido que utilice la llave para abrir las puertas del automóvil, encender el automóvil, o incluso compartir temporalmente la llave con otro SE (por ejemplo, utilizado por un técnico de mantenimiento).

Caso de uso: SE que alberga la Identidad Digital móvil de ciudadanos en Alemania

El último Julio de 2020 [33], el fabricante coreano de smartphones y otras tecnologías Samsung Electronics, en conjunto con la Agencia federal alemana para seguridad de información (BSI), la Bundesdruckerei (BDR), encargada de la impresión segura de tarjetas de identidad, y Deutsche Telekon Security GmbH, la compañía alemana de telecomunicaciones más grande en Europa, hacen de conocimiento público su asociación para que de manera conjunta, emitan el documento de identidad nacional alemán contenido en un SE embebido en la línea alta de smartphones Samsung Galaxy S20, a más tardar, en el tercer trimestre del presente año.

La nueva solución ha sido gestada dentro del proyecto OPTIMOS 2.0, cuyo objetivo es crear un ecosistema abierto que provea la tecnología e infraestructura para una autenticación móvil segura. La naturaleza abierta con la que fue concebida aseguraría que pueda ser masificada, y utilizada por diversos proveedores de servicios de identidad digital.

La línea de productos Galaxy S20, S20+, y S20 Ultra, son los primeros smartphones en satisfacer las exigencias del framework de seguridad para identidad digital electrónica de la BSI para uso soberano en Alemania []. Con esta tecnología los ciudadanos alemanes pronto serán capaces de verificar su identidad remotamente desde su smartphone para acceder a diversos servicios digitales, por ejemplo, para realizar transferencias de registros médicos confidenciales, transacciones bancarias, o incluso ejercer su derecho a voto.

La Figura 14 presenta la interfaz de usuario disponible en esta línea de smartphones que será proveída por BDR a través de un App descargable desde PlayStore; después de descargar e instalar el aplicativo Mobile ID, para verificar su identidad, los propietarios podrán aproximar su tarjeta de identidad nacional a su smartphone utilizando su interfaz NFC; una vez verificada la identidad del ciudadano, el eID móvil, será almacenado de manera segura en el SE, permitiendo en adelante, acceder a los servicios solo con su smarpthone.

Todo esto será posible debido a que el gigante coreano presentó en mayo [34] una solución de seguridad comprendida de un SE, el chip S3FV9RR que ofrece protección nativa para tareas críticas como: arranque seguro, almacenamiento de material sensible

aislado, autenticación de dispositivo, pagos con tecnología móvil (NFC), entre otras características de seguridad. La versión más reciente del chip ha obtenido la certificación de seguridad Common Criteria Evaluation Assurance Level (CC EAL) 6+, el nivel más alto adquirido para un componente móvil embebido en un smartphone, a la fecha.

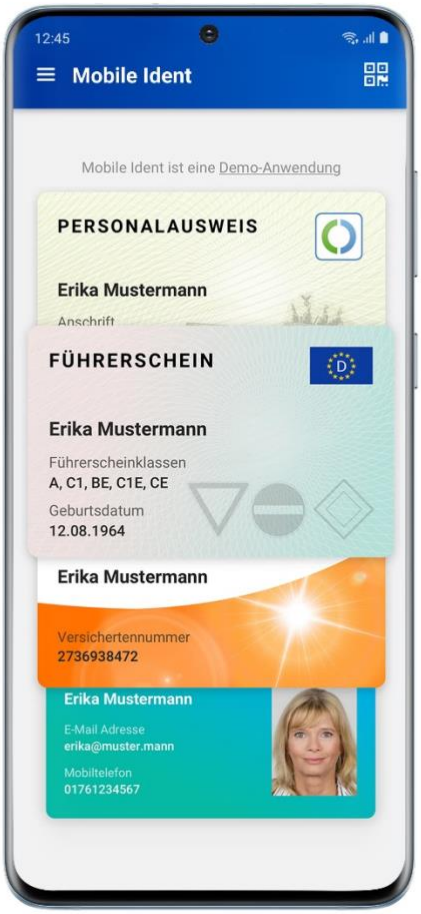

FIGURA 14. INTERFAZ DEL APP EID QUE PERMITE EL USO DE LA IDENTIDAD DIGITAL MÓVIL PARA CIUDADANOS ALEMANES, CONTENIDA EN UN SE

2.6.2 Trusted Execution Environment (TEE)

La estandarización del TEE es una iniciativa de *GlobalPlatform* de acuerdo con [11], donde se define al TEE como una primitiva de seguridad implementada en un sistema que proporciona un área segura (recursos de hardware y software aislados) del procesador principal en un dispositivo, esto garantiza que los datos sensibles son almacenados, procesados y protegidos en el entorno aislado y de confianza. De tal manera que, ofrece protección contra ataques de software generados en un entorno de procesamiento general, también referido como el entorno de ejecución enriquecido (*REE: Rich Execution*

Environment), donde la mayoría de la plataforma de software incluyendo el sistema operativo primario se ejecutan.

La capacidad del TEE de ofrecer ejecución segura de software seguro autorizado, conocido como la Aplicación de confianza (*TA: Trusted Application*), proporciona una seguridad de extremo a extremo protegiendo así, la ejecución de código autenticado, la confidencialidad, la autenticidad, la privacidad, la integridad del sistema y los derechos de acceso a los datos, mientras que, en el REE, la aplicación que interactúa con la TA es llamada una aplicación cliente (*CA: Client Application*).

En comparación con otros entornos de seguridad en el dispositivo, el TEE también ofrece altas velocidades de procesamiento y una gran cantidad de memoria disponible. El propósito principal del entorno de ejecución aislado facilitado por el TEE, es proteger el dispositivo y los activos (TAs). El TEE puede proteger la confidencialidad, la integridad de los datos y sus estados en tiempo de ejecución de una TA de otras aplicaciones que se ejecutan en la misma plataforma.

El estándar GlobalPlatform TEE logra lo anteriormente citado, definiendo las siguientes características de seguridad:

- **Aislamiento del S.O. enriquecido (REE)**. Todas las aplicaciones de confianza y sus datos asociados están separados del entorno enriquecido.
- **Control de gestión de aplicaciones**. Cualquier modificación de la TA y el TEE puede solo ser realizada por la entidad autenticada.
- **Identificación y enlace**. Donde el proceso de arranque es vinculado al Sistema en el chip (*SoC: System on Chip*), asegura la autenticidad e integridad del TEE Firmware y de las TAs.
- **Almacenamiento confiable**. Los datos de la TA y el TEE están almacenados de forma segura para garantizar la integridad, confidencialidad y vinculación al TEE (o anti-clonado).
- **Acceso confiable a periféricos**. El TEE proporciona APIs de acceso a periféricos confiables tales como la pantalla, sensores biométricos y SEs, bajo el control del TEE.
- **Criptografía de vanguardia**. La generación de números aleatorios, la criptografía y las marcas de tiempo monotónicas son activos clave para los servicios de valor agregado.
- **Aislamiento de otros TA**. Las TA están aisladas dentro del TEE, y del propio TEE.

En un dispositivo de consumo, el TEE también puede proporcionar un mecanismo de interfaz de usuario confiable (*Trusted UI*). Este es un modo transitorio específico en el que un dispositivo móvil es controlado por el TEE para verificar que la información presentada en la pantalla del dispositivo proviene de una aplicación de confianza autorizada, y que la información proporcionada por el usuario está aislada de las otras aplicaciones en el dispositivo.

Múltiples fabricantes de chips y teléfonos ya han desarrollado y desplegado versiones propietarias de la tecnología TEE. La falta de estandarización como resultado de estos despliegues presenta al desarrollador de aplicaciones un desafío significativo que superar; cada solución TEE propietaria requiere una diferente versión de la misma aplicación para garantizar que la aplicación se ajuste a los aspectos únicos de cada tecnología. Además, si el proveedor de aplicaciones desea implementar soluciones en múltiples entornos TEE y tiene seguridad de que cada entorno proporcionará un nivel de seguridad común, entonces se deberá realizar una evaluación de seguridad en cada solución TEE. Esto llevará a un proceso de desarrollo intensivo de recursos.

Como lo muestra la Figura 15, los diversos entornos de IT empresariales implementan aplicaciones para dispositivos móviles de usuarios del tipo "Bring your own device", aplicaciones que van desde la entrega de contenido multimedia Premium, los sistemas de pago móvil, la IoT, hasta los programas de identificación empresarial y de gobierno, entre otros; los que buscan balancear la necesidad de una experiencia enriquecedora con su seguridad subyacente. El TEE aísla las TA, manteniéndolas lejos de cualquier programa maligno en el S.O. enriquecido y separadas de otras aplicaciones almacenadas en el TEE. Debido a esto, el TEE se está convirtiendo en un entorno esencial dentro de todos los dispositivos, a medida que evoluciona el mercado de servicios seguros.

GP define un proceso de calificación para un TEE, la que incluirá pruebas funcionales (conformidad) y pruebas de evaluación de seguridad (certificación). Esta certificación tiene como base la metodología de Common Criteria, y un perfil de protección TEE que ha sido validado por un laboratorio y aprobado por un cuerpo de certificación.

Las principales especificaciones que han sido desarrolladas por GP TEE a la fecha, son presentadas en la Tabla 7, y continuación, se presenta una breve descripción de aquellos estándares que son de utilidad para el desarrollador de aplicaciones.

TEE Client API. Es una interfaz de comunicación diseñada para habilitar la ejecución de una aplicación cliente en el sistema operativo enriquecido, accediendo así al intercambio

controlado de recursos con una TA ejecutándose dentro del TEE. Tales servicios pueden incluir criptografía, almacenamiento seguro, reloj seguro, TUI, interfaces a los SE, y más.

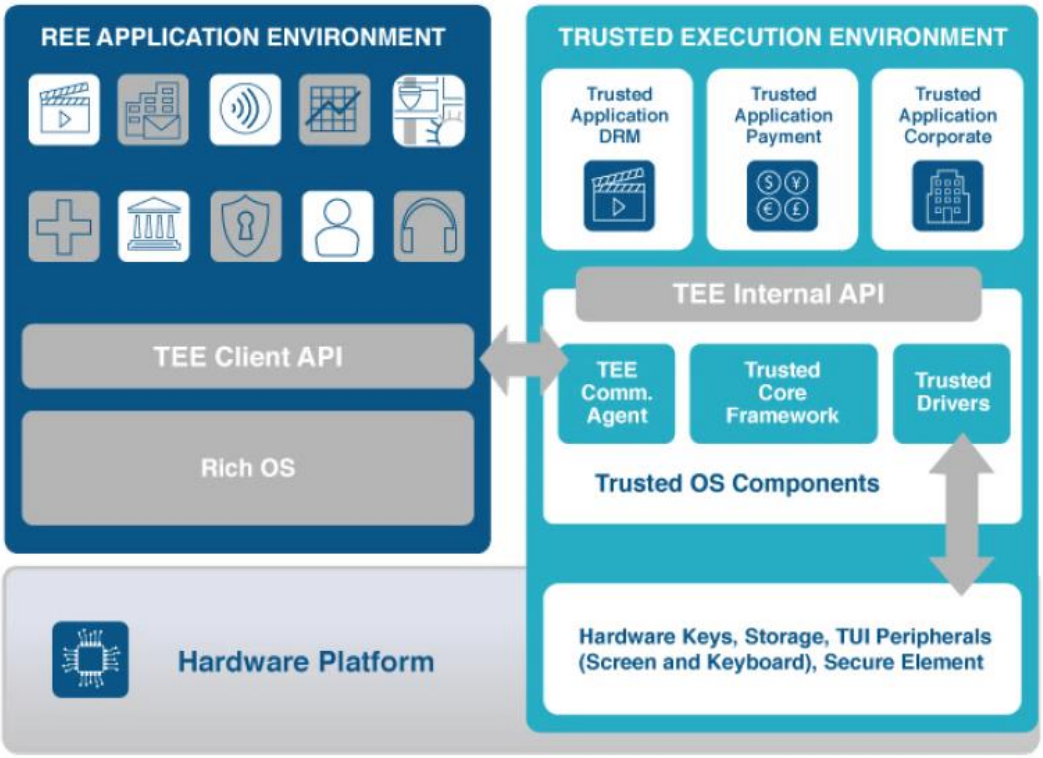

FIGURA 15. ARQUITECTURA DEL ENTORNO DE EJECUCIÓN DE CONFIANZA PROPUESTO POR GLOBALPLATFORM

(FUENTE: REFERENCIA [11])

TABLA 7 – ESTÁNDARES IMPLEMENTADOS POR GLOBALPLATFORM

Nº	ESTÁNDAR	ESPECIFICACIÓN
1	TEE Client API	1.0
2	TEE Internal Core API	1.2
3	TEE Secure Element API	1.1.1
4	TEE Sockets API	1.0.1
5	Trusted User Interface API	1.0
6	TEE System Architecture	1.2
7	TEE Internal API	1.0
8	TEE Protection Profile	1.2.1
9	TEE TA Debug	1.0.1
10	Secure Element Remote Application Manager	1.0.1
11	Secure Element Access Control	1.1

TEE Internal Core API. Es una interfaz de programación diseñada para habilitar una TA ejecutándose dentro de un TEE para realizar operaciones generales de una aplicación de seguridad. El soporte es proveído por criptografía, almacenamiento seguro, comunicación, y tareas generales, tal como cronometraje y gestión de memoria.

TEE TA Debug. Provee una simple, pero estandarizada metodología de depuración. La estandarización permite que los dispositivos desarrollados provean modos de depuración adecuados para las pruebas de compatibilidad y desarrollo, y al mismo tiempo los elimine controlada y verificablemente de los dispositivos de producción.

Trusted User Interface API. Permite que un TA muestre texto y gráficos mientras se consulta al usuario que realice una acción que va desde la navegación a la identificación con PIN o una contraseña. El TA puede proveer garantías gráficas en cuanto al estado de seguridad de la pantalla, el cual puede ser respaldado por medidas de garantía adicionales que implemente el usuario del TEE.

TEE Secure Element API. Debido a que cualquier comunicación que pase por el REE se considerará insegura, y puesto que la comunicación podría ser interceptada o manipulada por un atacante. Esta API proporciona una capa que está presente para permitir la comunicación con el SE integrado en el dispositivo dentro del cual se implementa el TEE. Además, esta API no especifica las capas físicas que se utilizan para comunicarse con el SE.

En referencia al caso de uso de identidad digital para el gobierno, hay contextos potenciales incontables para aprovechar un TEE en sector gubernamental. A continuación, se revisará un tipo general de implementación que se aplicaría en múltiples países, el caso de las tarjetas inteligentes de identificación electrónica.

Caso de uso: Asegurando las soluciones de identidad electrónica gubernamentales

En [9] se registra el siguiente escenario: Una tarjeta inteligente de identidad electrónica (eID) es una credencial de identificación emitida por un gobierno que ayuda a proveer a los ciudadanos altos niveles de seguridad y autenticación. Las aplicaciones varían según el emisor, pero ellas incluyen la verificación de identidad en el punto de entrada hacia los servicios de gobierno, o para satisfacer los requerimientos de otras autoridades. La emisión de eID se ha incrementado vertiginosamente en el Perú.

La identidad electrónica propone beneficios tanto a los ciudadanos como para los gobiernos, debido a sus características de seguridad y comodidad mejoradas. La

usabilidad es el principal impulsor detrás de muchas nuevas aplicaciones, incluyendo tanto a los servicios online gubernamentales, como a los servicios disponibles a través de los dispositivos móviles.

Desde una perspectiva de la seguridad, es importante tener en cuenta que los eID residen en su mayoría sobre la base de los SE, lo que significa que los datos almacenados dentro del propio eID (tal como la identidad del usuario, el material criptográfico, y la información del certificado utilizada para la autenticación y la autorización) están altamente protegidos. Sin embargo, hay otros activos confidenciales del usuario (tales como el PIN y la información del servicio del usuario), que no están almacenados dentro del SE.

El TEE está adecuado para proteger estos activos; y la Tabla 8 ilustra cómo diferentes tipos de datos están protegidos dentro de un eID que también implementa un TEE. Como se muestra en esta tabla, la información más confidencial de un usuario está protegida por el eID. Sin embargo, para acceder a esta información tanto para autenticación como identificación, al titular de la tarjeta normalmente se le solicita ingresar un código PIN, que debe mantenerse confidencial.

En entornos basados en PC, el PIN puede ser protegido mediante los terminales de tarjeta inteligente equipados con teclado y pantalla. Sin embargo, en escenarios basados en dispositivos móviles, donde la interfaz NFC es utilizada para comunicarse con el eID, utilizar una terminal de tarjeta externa no es a menudo factible. En este caso el TEE puede efectivamente servir como la terminal de la tarjeta inteligente suministrando la funcionalidad necesaria como parte de una TA dedicada, este escenario se muestra en la Figura 16.

TABLA 8 – NIVELES DE PROTECCIÓN (COMMON CRITERIA) PARA LOS DATOS CONTENIDOS EN UNA TARJETA DE IDENTIDAD ELECTRÓNICA

(FUENTE: REFERENCIA [9])

ACTIVO	NIVEL DE PROTECCIÓN REQUERIDA	ENTIDAD QUE ALBERGA EL ACTIVO
Datos del usuario	Strong (AVA VAN 5) EAL4+	eID Token
Llaves y certificados	Strong (AVA VAN 5) EAL4+	eID Token
2º Factor (PIN, biometría)	Enhanced (AVA VAN 3) EAL4	TEE-based Terminal
eService Data	Enhanced (AVA VAN 3) EAL4	TEE Trusted UI

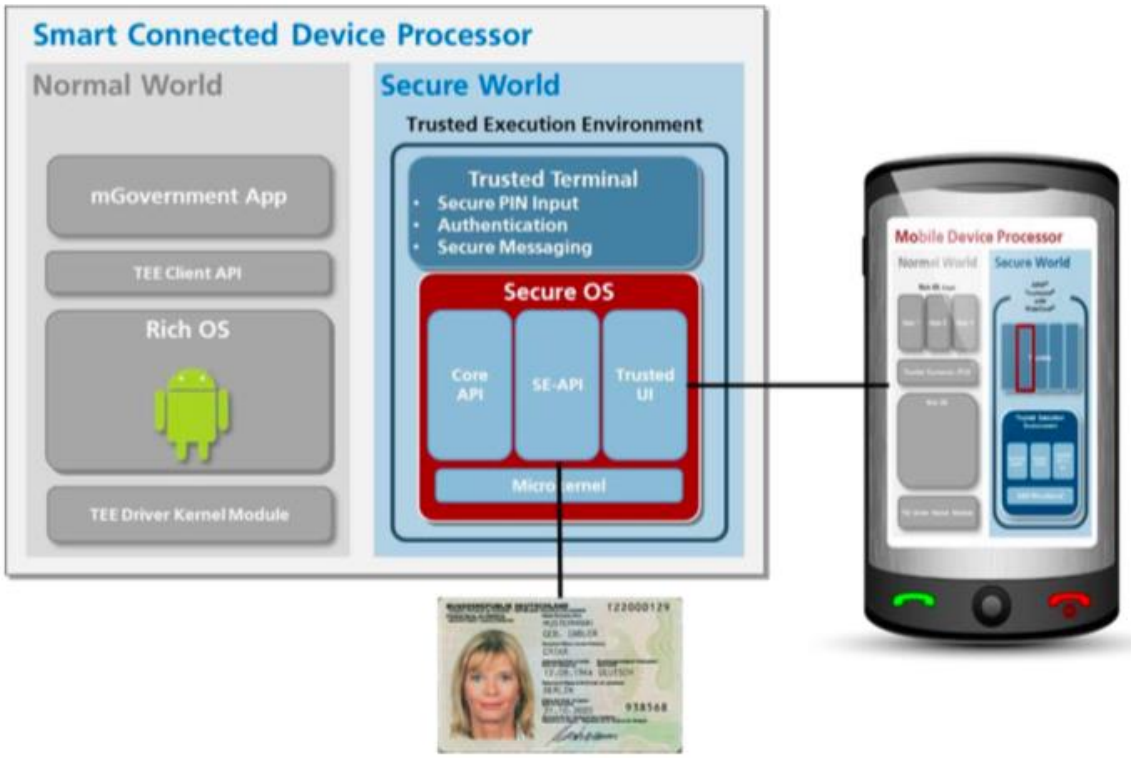

FIGURA 16. USO DEL TEE COMO UNA TERMINAL CONFIABLE PARA EN LA TARJETA DE IDENTIDAD ELECTRÓNICA ALEMANA

(FUENTE: REFERENCIA [9])

Es importante tener en cuenta que la mayoría de las soluciones eID utilizan un canal de comunicaciones de mensajería segura para proteger el canal de comunicación de proximidad. Por ejemplo, el eID alemán utiliza el protocolo de establecimiento de conexión autenticada por contraseña (PACE: Password Authenticated Connection Establishment), para asegurar el canal de proximidad y obtener el consentimiento del usuario.

En dicha implementación, el TEE provee las siguientes funciones de seguridad (con las especificaciones de GlobalPlatform aplicables, en paréntesis):

- Los componentes del eID pueden ser instaladas en el TEE de manera confiable (Framework de administración)
- El titular de una tarjeta puede ingresar de forma segura su PIN (TUI)
- Importante información de usuario puede ser recuperada desde el eID y de forma segura presentada al usuario (TUI)
- El protocolo de autenticación puede ser ejecutado de forma segura (TEE SE API, Internal Core API)
- El esquema de mensajería segura y sus llaves derivadas de forma segura pueden ser ejecutadas (TEE SE API, Internal Core API)

En este caso de uso, el TEE proporciona la mejor manera para que las implementaciones de eID garanticen que toda la información del usuario está protegida, incluidas las entradas de usuario (tales como el PIN) y los datos accedidos desde el SE. En contraste, las implementaciones eID que no aprovechan un TEE están potencialmente expuestas a vulnerabilidades de seguridad.

2.6.3 Trusted Platform Module (TPM)

Según lo indicado en [40], el (TCG: Trusted Computing Group) ha abordado el problema de la confianza, y los beneficios de seguridad relacionados, para las PCs, los servidores, los equipos de red, y los sistemas integrados durante más de una década, impulsando la especificación TPM.

El estándar TPM define una raíz de confianza de hardware ampliamente aceptada como más segura que una de software, pues esta última puede ser vulnerada con mayor facilidad por los atacantes. El TPM es utilizado con software para integrar su funcionalidad; las APIs de código abierto están disponibles permitiendo así, desarrollar software personalizado. En la mayoría de los sistemas donde se encuentre embebido un TPM, éste proporciona mediciones de integridad, comprobaciones de estado y servicios de autenticación.

El estándar TPM inicia con la versión 1.2, que ha sido incorporado en billones de PCs, Servidores, Sistemas integrados, equipos de red y otros dispositivos. La evolución de la IoT, y el incremento de la demanda de seguridad más allá del entorno de PC tradicional, llevaron a TCG a desarrollar la especificación TPM 2.0, la cual ha sido adoptada como un estándar internacional, el ISO/IEC 11889:2015.

Para una mayor flexibilidad de las aplicaciones y para permitir un uso más extendido de la especificación, TCG crea TPM 2.0 con un enfoque de "librería". Esto permite a los usuarios elegir aspectos específicos de la funcionalidad del TPM para diferentes niveles de implementación y seguridad. Además, nuevas características y funcionalidades fueron agregadas, tales como algoritmos más agiles, así como, la capacidad de implementar nuevos algoritmos criptográficos de ser necesario.

Un TPM incluye los siguientes atributos:

- Soporte para encriptación masiva en la plataforma
- Alta calidad de números aleatorios
- Servicios criptográficos

- Almacenamiento persistente y protegido para pequeñas cantidades de datos, bits fijos, contadores monotónicos y registros extendibles
- Un almacenamiento protegido pseudo-persistente para cantidades ilimitadas de llaves y datos
- Una amplia selección de métodos de autorización para acceder a llaves y datos protegidos
- Identidades de Plataforma
- Soporte para la privacidad de la plataforma
- Generación y verificación de firmas digitales (normal, anónimo, pseudo-anónimo)
- Certificación de las propiedades de llaves y datos
- Auditoría del uso de las llaves y los datos

En una Plataforma de confianza, el TPM también proporciona:

- Certificación: informe del estado de la plataforma a un tercero, de tal manera que permite autenticar al dispositivo
- Sellado: Uso del estado de la plataforma para autorizar acceso a las llaves y los datos

Cuatro tipos de TPM son populares hoy en día:

Un **TPM discreto** proporciona el más alto nivel de seguridad, como puede ser requerido, por ejemplo, para un TPM que es usado para asegurar el controlador de freno de un automóvil. El objetivo de este nivel es asegurar que el dispositivo protegido no pueda ser hackeado incluso con métodos sofisticados. Para lograr esto, un chip discreto es diseñado, construido y evaluado para el nivel más alto de seguridad que puede resistir la manipulación del chip, incluido todo tipo de ataques sofisticados.

Un **TPM integrado** es el siguiente nivel en términos de seguridad. Este nivel todavía tiene un TPM de hardware, pero está integrado en un chip que proporciona otras funcionalidades además de la seguridad. La implementación por hardware lo hace resistente a las fallas de software, sin embargo, este nivel no está diseñado para ser resistente a manipulaciones.

Un **Firmware TPM** es implementado con protección de software en una plataforma. El código se ejecuta en la CPU principal, así que un chip separado no es necesario. Mientras se ejecuta como cualquier otro programa, el código se encuentra en un entorno de ejecución protegido denominado TEE que está separado del resto de los programas

que se ejecutan en la CPU. Haciendo esto, el material sensible como las llaves privadas que el TPM puede necesitar, y que, a su vez, no debería ser accedido por otros aplicativos sin autorización, puede ser albergado en el TEE creando una ruta más difícil para los hackers. Este tipo de TPM también es conocido como una TA que se ejecuta en una plataforma TEE (TPM 2.0 en adelante).

Un **TPM de Software** puede ser implementado como un emulador de software de TPM de hardware. Sin embargo, un TPM de software está expuesto a muchas vulnerabilidades, no solo la manipulación, sino también, las fallas en cualquier sistema operativo donde se ejecute. El TPM de software tiene aplicaciones clave: Es muy bueno para probar o construir un sistema prototipo con un TPM. Para propósitos de prueba, un TPM de software podría proporcionar la solución o el enfoque correcto.

Las especificaciones del estándar TPM, definen la funcionalidad de seguridad para un módulo embebido en la plataforma de un dispositivo, permitiendo que el dispositivo implemente un sistema confiable dado que un TPM está vinculado a una plataforma de un dispositivo particular, y puede ser utilizado para identificar al dispositivo ante un tercero.

La diferencia con el TEE radica en que el TPM no permite que alguna lógica específica de una aplicación personalizada se ejecute dentro de un TPM, pues solo proporcionan interfaces para permitir que el sistema operativo y aplicaciones específicas de la plataforma del dispositivo puedan acceder a su funcionalidad.

Caso de uso: Proveedores de servicios criptográficos implementados por Microsoft (MsCAPI / CNG)

Los (CSP: Cryptographic Service Provider) son responsables de crear, almacenar y acceder a llaves criptográficas, la base de cualquier certificado digital y una PKI. La selección de un proveedor criptográfico determina qué tipo, tamaño y almacenamiento de llave se utilizará. Existe diversidad de proveedores para los diferentes tipos de módulos criptográficos ya revisados. Su enfoque básico es implementar algoritmos criptográficos de diferentes maneras, pero con una API común. Las aplicaciones gestionadas por el S.O. que usan criptografía pueden usar la API sin conocer los detalles de cómo se implementa un algoritmo y mucho menos el algoritmo en sí.

Las versiones más recientes del S.O. Ms. Windows incorporan un CSP denominado Microsoft Platform Crypto Provider (*CNG: Cryptographic Next Generation*), proveedor evolucionado desde su antecesor Ms. Crypto API o MsCAPI. Este genera y alberga llaves

en un TPM, y soporta la certificación de llaves para permitir que la AC se asegure de que la llave está contenida en el TPM.

El proveedor GNC ilustra algunas de las ventajas que ofrece un TPM, debido a que debajo de la interfaz CNG, Windows o un tercero suministran un proveedor criptográfico (es decir, una implementación de uno o varios algoritmos) desplegado solo como bibliotecas de software, o como una combinación de software y hardware del proveedor disponible, o también en conjunto con el hardware de un tercero. Si se implementa a través de un TPM de hardware, el proveedor criptográfico se comunica con el hardware detrás de la interfaz de software del CNG.

Como una referencia de la arquitectura de las primeras versiones de la interfaz de un TPM, se revisará lo citado en [2]. Debido a que al igual que con cualquier otro elemento de hardware el TPM requiere un controlador dedicado, además de una interfaz de proveedor de servicios para permitir que se integre desde el S.O. Este conjunto de servicios de soporte de plataforma confiable es denominado (*TSS: TCG Software Stack*) y constituyen una API de seguridad que proporciona la funcionalidad del TPM hacia el sistema operativo. El TSS consiste, en el nivel más bajo, del controlador de dispositivo basado en hardware que inicializa las interfaces e intercambia datos con el TPM. El siguiente nivel superior consiste en los servicios de sistema que son:

- Librería del controlador del dispositivo TPM
- Servicios Nucleo TSS
- Proveedor de servicios TSS

Estos gestionan la coordinación y los accesos múltiples al TPM, convierten los comandos API abstractos a la secuencia de datos para el TPM y preparan los servicios del sistema (incluso si ningún usuario está activo) para un acceso remoto, por ejemplo, para el administrador del sistema. Un administrador de caché almacena de forma segura los datos que exceden el área de memoria en el dispositivo de almacenamiento masivo externo, proporcionando así una capacidad de almacenamiento para llaves y datos de seguridad que está limitada solo por el tamaño del almacenamiento en disco.

La operación y las llamadas del TSS están especificadas con precisión por el Estándar TCG, ya que es solo a través de una implementación precisa y confiable que la cadena de confianza entre el sistema operativo y el TPM de hardware se mantendrá estable. La implementación de TSS varía de un sistema operativo a otro. Como algunas de las subfunciones (por ejemplo, el nivel más bajo del controlador), también, deben estar

equipadas con derechos de administrador del sistema. Normalmente, el fabricante de TPM también suministra el TSS requerido para el sistema operativo relevante.

La relación y dependencia entre los diferentes niveles que permiten suministrar los servicios de soporte a la plataforma confiable son representadas en la Figura 17.

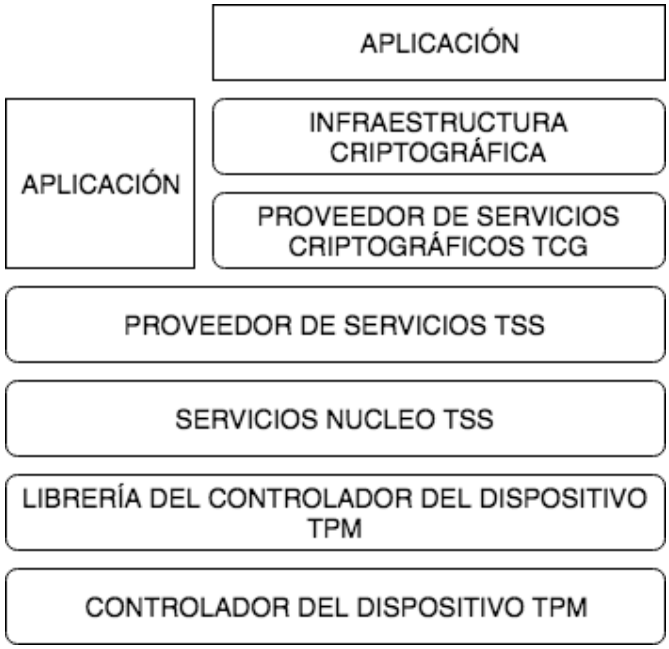

FIGURA 17. SERVICIOS DE SOPORTE DE LA PLATAFORMA CONFIABLE

(FUENTE: ADAPTADO DE LA REFERENCIA [2])

Debido a que el TSS es una API, que provee interfaces criptográficas que permiten que sus funciones de seguridad estén disponibles al S.O. es posible también proporcionar esta interfaz a otras aplicaciones de seguridad a través de un módulo de adaptación, lo que permite en particular la disponibilidad del almacenamiento seguro y los servicios de firma del TPM a las aplicaciones convencionales, aumentando significativamente el nivel de seguridad de estas aplicaciones estándar. Aunque esta funcionalidad no es requerida originalmente por el Estándar, aumenta considerablemente la usabilidad de la plataforma.

Inicialmente dos implementaciones (Aplicaciones) se realizaron sobre esta base, implementaciones que hoy en día se perfeccionan constantemente:

Microsoft Cryptographic Service Provider (MS-CSP). Varios productos de las aplicaciones de Windows (como Outlook, Explorer, Word, entre otros) proporcionan funciones de seguridad incorporadas como cifrado y firma, y gestionan estas funciones a través de la Interfaz de programación de aplicaciones criptográficas de Microsoft MS-CAPI como una interfaz criptográfica patentada. MS-CAPI puede acceder al TPM accediendo a varios proveedores de seguridad como módulos de software, tokens criptográficos o

tarjetas inteligentes, o a través del TSS como lo muestra la Figura 17. Por lo tanto, es relativamente fácil portar aplicaciones de seguridad existentes que ya usan MS-CAPI a los niveles de seguridad más altos del TPM simplemente por selección de un CSP diferente. El sistema operativo MS Windows muestra la presencia de un TPM incorporado en la tarjeta madre del hardware donde reside el S.O. a través de su Administrador de dispositivos, como se observa en la Figura 18.

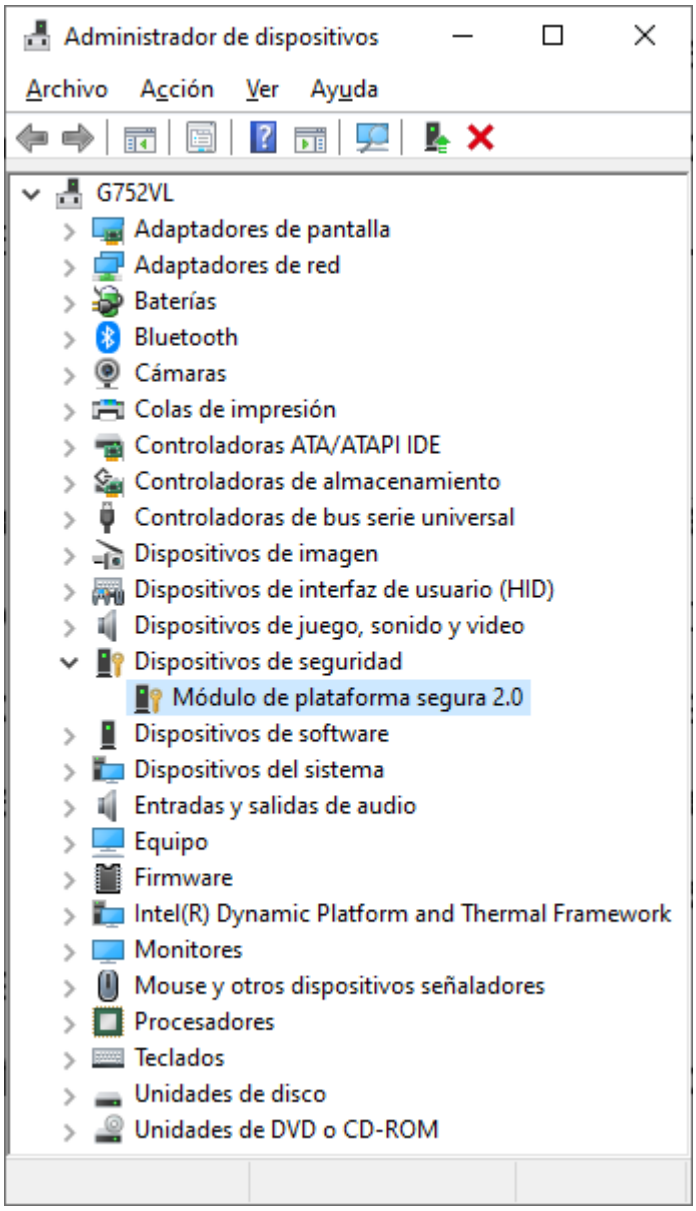

FIGURA 18. TPM 2.0 UTILIZADA POR LOS SISTEMAS OPERATIVOS MS. WINDOWS

Asimismo, el MS-CAPI dentro de las diferentes interfaces que expone, presenta una interfaz gráfica de usuario, desde donde el usuario del S.O. puede acceder al contenido criptográfico disponible para su uso desde el repositorio de certificados digitales que el S.O. gestiona, como se observa en la Figura 19.

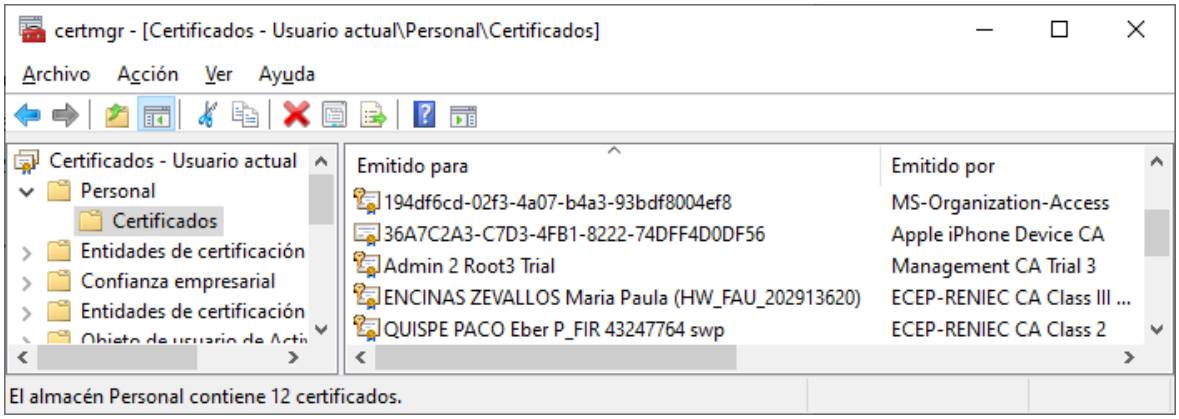

FIGURA 19. REPOSITORIO DE CERTIFICADOS DIGITALES PROVISTOS POR EL SISTEMA OPERATIVO A LOS APLICATIVOS A TRAVÉS DE LA INTERFAZ MS-CAPI

PKCS#11. Desarrollado por RSA es el estándar de interfaz criptográfica más utilizado (es revisado en la siguiente sección con mayor detalle). Éste es utilizado por ejemplo por el navegador Mozilla de Firefox, así como el visor de documentos PDF Acrobat de Adobe. Una vez más, la conversión de las llamadas de seguridad entre el PKCS#11 y el API TSS facilita considerablemente la adaptación de las aplicaciones estándar existentes. Por lo tanto, se pueden lograr soluciones para el usuario altamente seguras con un costo y complejidad de implementación mínima gestionando de forma segura los certificados digitales para navegadores y visores de documentos PDF a través de un TPM.

2.7 Estándares criptográficos de llave pública

Los Estándares de criptografía de llave pública (PKCS: Public-Key Cryptography Standards) son un conjunto de protocolos estándar que hacen posible el intercambio seguro de información en Internet utilizando una PKI. Los estándares incluyen entre otros protocolos, el cifrado RSA, el cifrado basado en contraseña, la sintaxis de certificado extendido, y la sintaxis de mensajes criptográficos para S/MIME (el estándar propuesto por RSA para correo electrónico seguro ampliamente utilizado).

Aquellos que son de nuestro interés en este trabajo, son:

2.7.1 Certification Request Syntax Standard (PKCS#10)

Este estándar en su versión 1.7 especifica la sintaxis para solicitar la firma digital o la certificación de una llave pública. Cuando una entidad requiere un certificado de llave pública, la entidad construye una solicitud de certificado (*Certificate Request*) y la envía a una Autoridad de Certificación, quién autentica a la entidad solicitante verificando la firma digital enviada; si la solicitud es validada, la Autoridad genera un certificado digital X.509

utilizando el *Distinguished Name* de la entidad, su llave pública, el nombre del emisor, el número de serie elegido por la Autoridad, un periodo de validez, y un algoritmo de firma.

2.7.2 Cryptographic Token Interface Standard (PKCS#11)

Este estándar en su versión 2.2 especifica una interfaz de programación de aplicaciones (API), de bajo nivel llamada (*Cryptoki: Cryptographic Token Interface*), para dispositivos que custodian material criptográfico y ejecutan operaciones criptográficas. Cryptoki presenta un enfoque orientado a objetos, independiente de la tecnología (cualquier tipo de dispositivo como las tarjetas inteligentes, y los tokens USB, entre otros), facilitando así, la abstracción de los detalles del dispositivo. Cryptoki presenta a las aplicaciones una vista lógica y un modelo común del dispositivo criptográfico denominado por el estándar "token criptográfico". Finalmente, Cryptoki gestiona y distribuye los recursos (múltiples aplicaciones accediendo a múltiples dispositivos).

El estándar especifica cómo se deben proveer los servicios criptográficos disponibles en un dispositivo, que requieren ser consumidos por una aplicación mediante el uso del lenguaje de programación ANSI C (1990). Cryptoki provee portabilidad, puesto que la aplicación no tiene que cambiar la interfaz para un tipo diferente de dispositivo o un diferente entorno de ejecución. Cryptoki está orientada a dispositivos criptográficos asociados con un usuario simple, así que no tiene un medio para distinguir múltiples usuarios, la atención está en las llaves de un usuario simple y lo que ocurre con un pequeño número de certificados relacionados a ese par de llaves. Cryptoki está implementada como una librería o *driver* que soporta las funciones declaradas en la interfaz. Entonces, una aplicación puede ser enlazada con Cryptoki directamente, alternativamente, Cryptoki también puede ser enlazada mediante una librería dinámica. En cualquier caso, si el enlace es directo o dinámico, la interfaz de programación entre la aplicación y la librería Cryptoki permanece igual. Algunas de las implementaciones de estas librerías desplegadas por diferentes fabricantes, son representadas en la Figura 20.

2.7.3 Personal Information Exchange Syntax Standard (PKCS#12)

Este estándar describe una sintaxis para la transferencia de información sensible, incluyendo llaves privadas, certificados digitales, entre otro material secreto y extensiones. Los sistemas operativos, las aplicaciones, los navegadores, entre otros, que soportan este estándar permiten que un usuario importe, exporte y utilice este repositorio de información utilizando cifrado (en base a llave pública o por contraseña) para proteger la información de su exposición no autorizada.

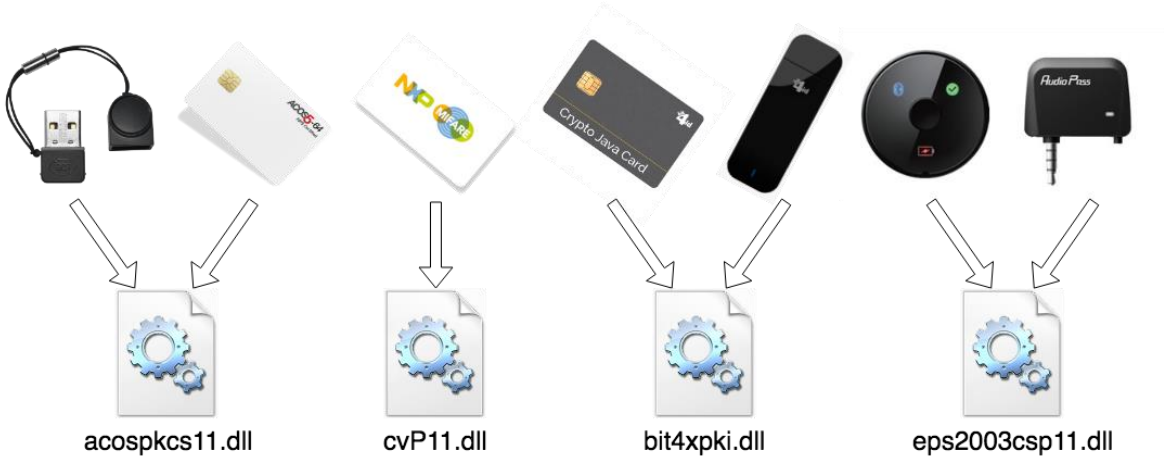

FIGURA 20. LIBRERÍAS PKCS#11 IMPLEMENTADAS PARA MÓDULOS CRIPTOGRÁFICOS

2.8 Certificaciones de seguridad

En el contexto de la regulación peruana, entre las certificaciones de seguridad para módulos criptográficos destinados a usuarios finales que son de interés en este trabajo, la AAC exige que estos módulos deben contar con al menos una de las dos certificaciones presentadas en esta sección, garantizando el valor legal de su uso en el estado peruano.

2.8.1 ISO/IEC 19790:2012

Information technology -- Security techniques -- Security requirements for cryptographic modules.

Más conocida como la certificación de seguridad FIPS 140-2, y en el Perú está regulado que el uso de un módulo criptográfico en formato personal que cuente con una certificación de seguridad de este tipo debe certificar como mínimo el Nivel 1.

2.8.2 ISO/IEC 15408:2009

Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.

Comúnmente conocido como la certificación de seguridad Common Cirteria, y en el Perú está regulado que el uso de un módulo criptográfico en formato personal que cuente con una certificación de seguridad de este tipo debe certificar como mínimo el EAL4.

2.9 Internet de las Cosas

La ITU-T Y.2060 define la (*IoT: Internet of Things*) de la siguiente manera:

“Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras.”

A la fecha, como parte de todas las comunicaciones existentes en Internet, también existe abundante literatura sobre la IoT, que excedería al contenido de este trabajo de investigación; y en cuanto a lo que nos concierne, revisaremos rápidamente lo referido a las direcciones de acción que la seguridad en la IoT tiene y tendrá en los próximos años.

2.9.1 Criptografía ligera para la seguridad en la IoT

De acuerdo con [31], este tipo de criptografía representa una dirección de investigación de gran importancia que recientemente ha ganado una atención importante anticipando su relevante rol en las técnicas de seguridad aplicables por venir en la IoT; aquí el objetivo es encontrar técnicas criptografías eficientes que puedan reemplazar a aquellas tradicionales computacionalmente costosas mientras puedan suministrar un nivel aceptable de seguridad.

Este propósito está estrechamente ligado a la performance del hardware asociado, puesto que el diseño de nuevas técnicas criptográficas va de la mano con el hardware de seguridad disponible para su implementación. Un algoritmo criptográfico ligero, implica recursos limitados para ejecutar operaciones sensibles sobre algún material criptográfico asociado. Esto implica contar con adecuado discernimiento del hardware especializado, portátil y con suficientes recursos que va a ser capaz de proveer la seguridad y la rapidez en las operaciones requeridas; siendo esto, uno de los objetivos del presente trabajo, la revisión de las tecnologías que pueden satisfacer estos requerimientos de seguridad.

CAPÍTULO III
DESARROLLO DEL TRABAJO DE TESIS

3.1 Análisis

3.1.1 Identificación del problema

En el sector gobierno, normalmente, las tarjetas inteligentes sirven para poder hacer firmas digitales, que son de reconocida importancia porque permiten garantizar con algún grado de certeza la identidad de la persona que solicita un trámite en línea (autenticidad de origen), así como garantizar que lo solicitado no sea modificado (integridad) y que posteriormente el solicitante no pueda negar haberlo realizado (no repudio).

Sin embargo, la obtención y la utilización de las tarjetas inteligentes no ha tenido amplia aceptación a nivel global por diversos motivos. Por ejemplo, para la obtención de una tarjeta que contenga un certificado digital se requiere hacer una verificación exhaustiva de la identidad del solicitante, además de pagar una tasa considerable (que incluye el precio de la tarjeta) por un periodo de tiempo no muy prolongado. Además de tener la tarjeta para su utilización, una persona requiere adquirir un dispositivo lector y tener un computador configurado adecuadamente. Todo esto hace que las tarjetas inteligentes sean catalogadas como una tecnología con alta complejidad técnica para el usuario final.

Teniendo en consideración la ubicuidad de los computadores personales y de los teléfonos inteligentes en la actualidad, surge la interrogante de saber en qué medida sería posible la utilización de estos dispositivos en reemplazo de las tarjetas con chip. Este reemplazo tendría que empezar a ser abordado considerando las etapas de obtención y utilización. En lugar de obtenerse una tarjeta que ya incluye los datos de creación de firma, es necesario concentrarse en buscar la manera de generar y cargar aquellos datos en el computador personal o en el teléfono inteligente del usuario de manera remota.

En el caso de un computador personal se descarta la utilización de ficheros sueltos, incluyendo aquellos protegidos con cifrado (contenedores PKCS#12). No es recomendable su uso debido a que, al no estar debidamente protegidos, el material criptográfico podría ser copiado indiscriminadamente, lo que generaría potenciales casos de suplantación.

Teniendo esto en consideración, el espacio de búsqueda para un mayor despliegue recae en los computadores personales con sistema operativo MS Windows, puesto que estos suministran una interfaz que provee mecanismos de protección de material criptográfico denominado MS CryptoAPI (My store), que acredita una certificación de seguridad FIPS 140-2 Nivel 1. Para el caso de teléfonos inteligentes, también se descarta el uso de ficheros sueltos, por lo que nos enfocaremos en el uso de la zona segura denominada TEE, debido a que ya es posible encontrar algunas implementaciones con certificaciones de seguridad.

3.1.2 Definición de los objetivos

Los objetivos del artefacto han sido plasmados en los requisitos funcionales y no funcionales presentados en la Tabla 9.

Se requiere que el artefacto tenga una capa de identificación para que pueda discernir entre los usuarios autorizados y no autorizados para realizar la operación de obtención de un certificado digital. También, se requiere que el artefacto pueda verificar de forma automatizada si el entorno del usuario cumple con todos los pre-requisitos necesarios y de ser posible se auto-instale todo lo que fuese necesario.

TABLA 9 – REQUISITOS FUNCIONALES Y NO FUNCIONALES

RF1	El artefacto debe tener una capa de identificación para permitir solo a los usuarios autorizados realizar la operación de obtención de un certificado digital
RF2	El artefacto debe poder verificar de forma automatizada si el entorno del usuario cumple con todos los pre-requisitos necesarios
RF3	El artefacto debe auto-instalar todo lo necesario
RF4	El artefacto debe permitir al usuario poder elegir qué tipo de módulo criptográfico utilizar
RF5	El artefacto debe notificar a las partes el resultado final de la operación
RNF1	El artefacto debe ser fácil de utilizar
RNF2	El artefacto debe ser rápido de operar
RNF3	El artefacto debe proteger los datos de creación de firma de forma similar o equivalente a como lo hacen las tarjetas inteligentes
RNF4	Cumplir el marco legal vigente

Además, el usuario debe poder elegir qué tipo de módulo criptográfico utilizar y el artefacto debe ser fácil y rápido de utilizar y debe notificar a las partes el resultado de la operación a fin de dar cumplimiento a la normativa legal correspondiente.

Finalmente, deben protegerse los datos de creación de firma de forma similar o equivalente a como lo hacen las tarjetas inteligentes.

3.2 Diseño del Artefacto

En la Tabla 10 se presentan los meta-requisitos del artefacto, los cuales fueron definidos en base a los requisitos presentados en la subsección precedente.

TABLA 10 – DEFINICIÓN DE META-REQUISITOS

N.º	Meta-requisito	Descripción
1	Basado en web	El artefacto debe estar construido de forma que pueda ser utilizado desde un navegador web o una plataforma de distribución digital, de tal manera que el usuario final no requiera realizar instalaciones de componentes ni configuraciones particulares en su computador. La interacción necesaria para utilizar el artefacto no debería ser más compleja que cuando utiliza su correo electrónico vía un navegador web.
2	Consentimiento informado	El artefacto debe presentar al usuario información relacionada a aspectos normativos y tecnológicos envueltos en la operación.
3	Autenticación de la identidad del usuario	El artefacto debe tener la capacidad para realizar la autenticación de la identidad del usuario haciendo uso de diferentes mecanismos de autenticación, dependiendo del tipo de certificado digital entregado. Para mitigar ataques, por ejemplo, de fuerza bruta, se debe contemplar el bloqueo temporal de la operación tras un número fallido de intentos.
4	Verificación automatizada de pre-requisitos	El artefacto debe realizar la verificación de pre-requisitos del entorno de forma automatizada, en la medida de lo posible, sin requerir la intervención del usuario.
5	Módulos criptográficos	El artefacto debe permitir al usuario elegir el módulo criptográfico a utilizar cuando sea necesario. El artefacto debe estar en la capacidad de poder interactuar con diferentes tipos de módulos criptográficos de naturaleza personal.
6	Generación del material criptográfico	El artefacto debe tener la capacidad de generar de forma automatizada el material criptográfico correspondiente.
7	Comunicación y notificación	Una vez que el artefacto finaliza la generación del material criptográfico se debe comunicar a las partes el resultado final.

A continuación, se describe el desarrollo de los meta-requisitos propuestos, en términos de la definición de la arquitectura del artefacto y de los detalles de su implementación.

3.2.1 Arquitectura lógica

Tal como puede verse en la Figura 21, una implementación del artefacto ha sido concebida para estar conformada por dos capas claramente definidas: *Server Side* y *Client Side*.

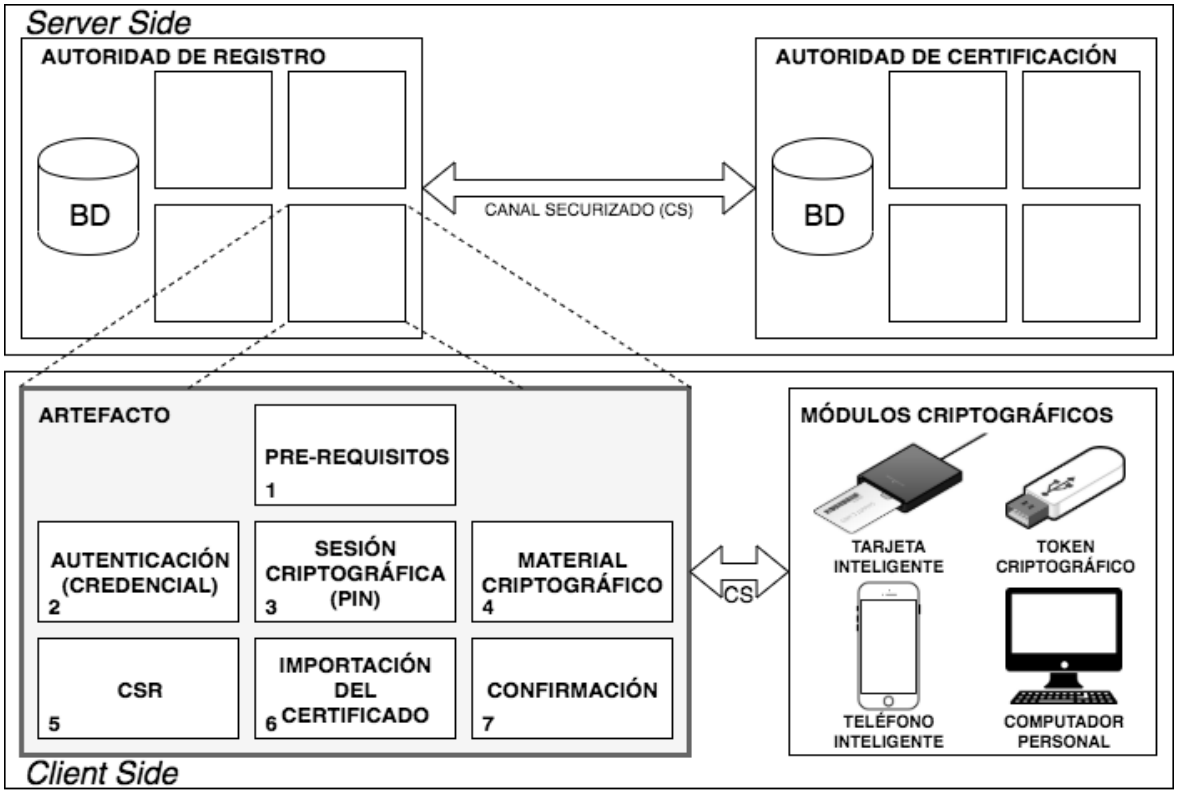

FIGURA 21. ARQUITECTURA LÓGICA DEL ARTEFACTO

En la capa *Server Side* se encuentran la plataforma de la Autoridad de Certificación (CA) y la plataforma de la Autoridad de Registro (RA). La plataforma de la CA es la fábrica de los certificados digitales, que opera sin intervención humana y puede estar asociada a varias RA como se ha visto en la Figura 9. Las plataformas RA interactúan con la CA invocando a un WS securizado expuesto por ella. La plataforma de la RA es aquella donde una persona con el rol de operador de registro da de alta a un usuario previa verificación de su identidad y de acuerdo con un protocolo preestablecido. La RA expone un WS securizado que es consumido por los aplicativos en el *Client Side*.

En la capa *Client Side* tenemos los aplicativos que le permiten a un usuario final obtener un certificado digital en un módulo criptográfico de su elección: computador personal, teléfono inteligente, tarjeta inteligente y token criptográfico.

Estos aplicativos, a consecuencia de la interacción del usuario, envían peticiones de certificados a la RA realizando las operaciones descritas en la Tabla 11.

TABLA 11 – OPERACIONES GENÉRICAS REALIZADAS ENTRE LAS CAPAS

Nº	Operación	Descripción
1	Verificación de pre-requisitos	Se realizan verificaciones de pre-requisitos relacionadas al S.O., a la disponibilidad de los servicios web, y al versionamiento.
2	Autenticación	La credencial de acceso recibida por el usuario es enviada al servicio de la RA del *Server Side*, el servicio verifica que la credencial es válida y se encuentra activa notificando al aplicativo.
2	Inicio de sesión criptográfica	Se establece una sesión con el módulo criptográfico haciendo uso del PIN de protección, e invocando a las librerías correspondiente para obtener acceso al módulo criptográfico.
3	Generación de material criptográfico	Se genera un par de llaves asimétricas RSA de 2048 bits.
4	Generación del CSR	Con la llave privada se genera una solicitud de firma de certificado (*Certificate Signing Request* - CSR), la cual es empaquetada en formato PKCS#10.
5	Certificación de la llave pública	Se envía el CSR junto con la credencial verificada al servicio de la RA del *Server Side*, quién procede a la certificación de la llave pública contenida en el CSR, certificado digital que es generado en formato X.509v3.
6	Importación del certificado	El certificado digital es recibido por el aplicativo cliente y es importado en el módulo criptográfico asociándolo a la llave privada correspondiente.
7	Confirmación	El aplicativo confirma, tanto al servicio del *Server Side* como al aplicativo en el *Client Side* (usuario final), que el certificado ha sido generado (configurado) satisfactoriamente.

La secuencia de operaciones entre la capa *Server Side* y la capa *Client Side* es presentado en la Figura 22.

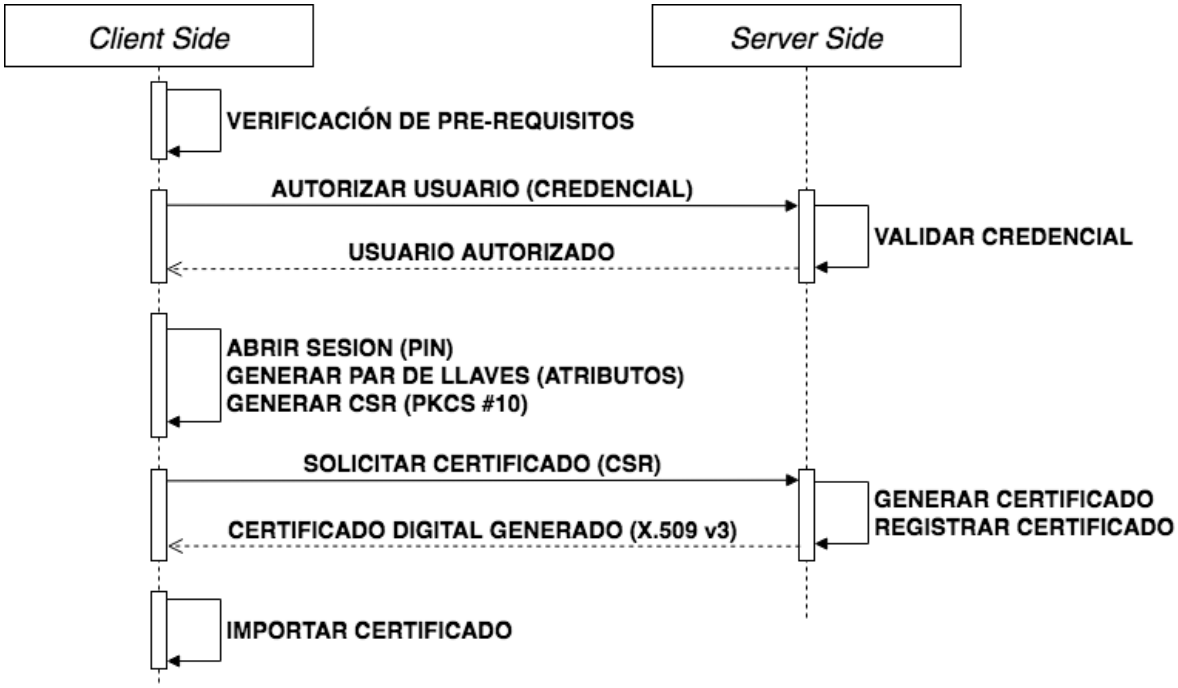

FIGURA 22. DIAGRAMA DE SECUENCIA ENTRE EL SERVER SIDE Y EL CLIENT SIDE

3.3 Implementación

3.3.1 Implementación del ServerSide

En la capa *Server Side* distinguimos a la plataforma de la RA y de la CA. La plataforma de la CA ha sido implementada mediante el despliegue del software EJBCA Enterprise Edition versión 6.15 disponible en https://www.ejbca.org/. El EJBCA es un software PKI para autoridades de certificación que está desarrollado en Java (JEE) y se despliega en un servidor JBoss. Es robusto, flexible, de alto rendimiento, escalable, independiente de la plataforma y modular. El EJBCA se integra con la RA mediante un web service SOAP, el cual es utilizado para acceder a funciones específicas de forma remota sobre una conexión HTTPS autenticada con un certificado cliente firmado por la CA de gestión del EJBCA.

La plataforma de la RA tiene un web service API REST implementado en Java que ha sido desplegado en un servidor Wildfly y cuenta con cinco métodos: test(), version(), login(), generate() y notify(). Esto métodos son invocados por los aplicativos en el ClientSide a través de una conexión HTTPS y securizada con JWT. El método test() verifica la disponibilidad del servicio, el método version() controla que los aplicativos del ClientSide se encuentre actualizados, el método login() autentica al usuario validando la credencial requerida para la generación del certificado digital, el método generate() recibe la CSR en formato PKCS#10, la valida y realiza la generación del certificado, y el método notify()

registra como exitosa la instalación de certificado digital en el módulo criptográfico y notifica a las partes la documentación correspondiente.

3.3.2 Implementación del ClienteSide para PCs con S.O. MS Windows

Es un aplicativo desarrollado en Java que funciona en arquitecturas de 32 y 64 bits y realiza las operaciones descritas en la Tabla 12.

3.3.3 Implementación del ClienteSide para teléfonos inteligentes con S.O. Android

Este aplicativo está conformado por dos componentes: el aplicativo android (AA) y el aplicativo de confianza (TA), desarrollados en lenguaje Java y lenguaje C, respectivamente. El primero se encarga de la interfaz gráfica de usuario y la comunicación con el ServerSide mediante un API REST. El segundo se encarga de realizar las tareas criptográficas relacionadas con el TEE en el teléfono inteligente. Ambos aplicativos se intercomunican utilizando el SDK de Trustonic (Trustonic's Application Protection, en adelante TAP).

El SDK incorpora el S.O. Kinibi para gestionar el TEE, y la librería criptográfica TRICX acreditada con una certificación de seguridad FIPS 140-2 Nivel 1, la que es utilizada por la TA para acceder al TEE. En esta implementación se realizan las operaciones listadas en la Tabla 13.

3.3.4 Implementación del ClienteSide para dispositivos con interfaz PKCS#11

Con la finalidad de demostrar la flexibilidad del artefacto, además de los aplicativos para PC y para teléfono inteligente, se implementó un aplicativo que permite la entrega de certificados digitales en módulos criptográficos de diferentes marcas y modelos que cuentan con interfaz PKCS#11 para usuarios finales.

La secuencia de operaciones es similar a la que realiza el aplicativo para PC con la diferencia que, en este caso, el material criptográfico se genera internamente en la tarjeta inteligente o en el token criptográfico.

Además de ello, se generó un procedimiento de homologación con la finalidad de homogeneizar el funcionamiento de este aplicativo entre la diversidad de fabricantes e integradores, considerando así también, que debían acreditar una certificación de seguridad como mínimo, ya sea Common Criteria EAL 4+ o en su defecto FIPS 140-2 Nivel 1.

TABLA 12 – OPERACIONES REALIZADAS EN EL CLIENTSIDE PARA PCS

Nº	Operación
1	Se registra el proveedor criptográfico BouncyCastleProvider() y se crea una instancia de la clase KeyStore de tipo PKCS#12.
2	La clase KeyPairGenerator es la encargada de la generación del par de llaves asimétricas. Una instancia de esta clase es creada pasando como parámetros el tipo de par de llaves a generar (RSA en este caso), y el nombre del proveedor (para este caso es BC). La generación se ejecuta con la función generateKeyPair(), y se obtiene una referencia a la llave privada con la función getPrivate(), así como el valor de la llave pública con getPublic().
3	La clase PKCS10CertificationRequest es la encargada de generar la petición firmada de certificado (CSR), pasando los siguientes parámetros: el algoritmo de firma a utilizar, la información del firmante de la petición en formato X.509, la llave pública, la referencia a la llave privada, y el nombre del proveedor. El resultado es un objeto CSR en formato PKCS#10.
4	El CSR generado y la credencial de acceso, son enviados al servicio expuesto en el ServerSide mediante un canal cifrado TLS. En el ServerSide, primero se verifica la credencial enviada y la integridad del CSR, y en caso satisfactorio, se procede a la certificación de la llave pública contenida en el CSR con la llave privada de la CA. El nuevo certificado digital en formato X.509v3 es retornado en formato DER por el mismo canal establecido al inicio de la comunicación.
5	Se procede a crear el contenedor del certificado según el estándar PKCS#12. Para ello se apertura una sesión utilizando la clase KeyStore, la cual es instanciada pasando el tipo de proveedor y el nombre del proveedor. Luego se invoca a la función setKeyEntry() de la instancia KeyStore, enviando como parámetros de importación un alias que identifica al certificado recibido, la referencia a la llave privada y la cadena de certificados.
6	El contenedor creado en el literal anterior es instalado en el MSCAPI. Para esto se hace uso de la librería JNA, que es la responsable de exponer los métodos necesarios para importar el contenedor PKCS#12. En este punto, el MSCAPI le pedirá al usuario establecer un PIN de protección para la llave privada.
7	Finalizada la importación, se comunica al ServerSide y al usuario final que la operación ha finalizado satisfactoriamente.

TABLA 13 - OPERACIONES REALIZADAS EN EL CLIENTSIDE PARA TELÉFONOS INTELIGENTES

Nº	Operación
1	La TA es instalada internamente en el teléfono inteligente tras la solicitud de la AA. Si se trata de la primera instalación, entonces se crea un PIN por defecto con la función SetDefaultPin() en la zona de confianza. Este PIN, que puede ser cambiado posteriormente con la función ChangePin(), es utilizado como parámetro de entrada en las funciones criptográficas. Además, en función de las características del teléfono (modelo y fabricante), la TA puede instalarse en modo protección por software (Software Protection, en adelante SWP) o en modo de protección por hardware (TEE).
2	Cuando el usuario solicita la descarga de su certificado digital, la AA solicita a la TA crear un par de llaves criptográficas de tipo RSA de 2048 bits con la función RSAGenerateKey(). Estas llaves son almacenadas de forma segura en la zona de confianza del teléfono inteligente.
3	Para la creación de la CSR se extrae la llave pública con la función LoadPublicKey(). Esta llave y el SubjectDN sirven como parámetros para la creación de un objeto PKCS10CertificationRequest de Java. Para firmar digitalmente la CSR se llama a la función RSASignDigest().
4	La CSR generada, junto a la credencial de acceso del usuario, son enviados por la AA hacia el ServerSide, cuyo API REST retorna el certificado digital en formato Base64. Este certificado es convertido al formato PEM, después es almacenado en el teléfono y luego es asociado a su par de llaves en el TEE a través de una referencia numérica.
5	Finalmente, la AA notifica el éxito de la operación tanto al usuario como al ServerSide.

CAPÍTULO IV
ANÁLISIS Y RESULTADOS

4.1 Descripción del escenario de las pruebas

La implementación del artefacto fue realizada en varias iteraciones. En cada iteración se probaron las funcionalidades de los tres aplicativos *Client Side* con usuarios con experiencia en el tema. Se recibieron sugerencias de mejoras funcionales que fueron incorporadas en las versiones subsiguientes.

4.2 Métodos de validación empleados y resultados obtenidos de la investigación

Para la evaluación del artefacto se realizó un estudio comparativo entre la efectividad del módulo de entrega que viene como parte de la plataforma EJBCA con la efectividad del artefacto propuesto frente al cumplimiento de los requisitos funcionales y no funcionales. Además de la eficiencia que el artefacto proporciona.

4.2.1 Módulo de entrega de la plataforma EJBCA

Se desplegó el módulo de entrega que viene como parte de la plataforma EJBCA. Este módulo tiene una interfaz gráfica de usuario especialmente diseñada para ejecutarse sobre un navegador web. Aquí se registraron un total de 51,141 operaciones de obtención de certificados digitales, algunos con ayuda del personal del equipo de soporte técnico y otros no.

Todas las operaciones fueron realizadas en computadores personales con MS Windows. Se contabilizó que, dependiendo del caso, cada operación tomó entre 15 a 20 minutos por certificado digital. Entre los principales problemas encontrados con esta forma de entregar certificados podemos destacar los siguientes:

- Demora para realizar la operación
- Procedimiento engorroso para un usuario final
- Múltiples casos por día que llegaron al servicio de soporte al cliente

- Un procedimiento diferente por cada dispositivo
- Bloqueos de seguridad efectuados por los navegadores web.

Una de las principales causas de estos problemas es que, para el caso de llaves RSA generadas en el repositorio criptográfico del S.O., los navegadores web difieren en su comportamiento, en particular, en la forma de establecer el PIN de protección. Por ejemplo, el Google Chrome no permite especificar un PIN de protección, mientras que el MS Internet Explorer si lo permite. Además, el Mozilla Firefox administra su propio repositorio de confianza y no permite utilizar el repositorio del S.O. Asimismo, es de destacar la limitación del Google Chrome y del MS Internet Explorer frente a la interfaz PKCS#11, ya que no la soportan nativamente, salvo Mozilla Firefox que sí lo hace.

4.2.2 *Client Side* para computadores personales con S.O. MS Windows

Este aplicativo cuya presentación se muestra en la Figura 23, ha sido puesto a disposición de los usuarios en la dirección web https://pki.reniec.gob.pe/dcdelivery3/. Muchos de los usuarios han sido usuarios de la herramienta descrita en la subsección precedente y otros han sido usuarios completamente nuevos. Al inicio, antes de la puesta en operaciones, fueron realizadas sesiones de capacitación, pero solamente al personal de mesa de ayuda de las organizaciones participantes. Desde su puesta en operación, se han registrado un total de 82,383 operaciones de generación de certificados digitales. Se han realizado encuestas de satisfacción a los usuarios, destacando ellos dos propiedades del artefacto: rapidez de la operación (en promedio, cada operación toma entre 1 a 2 minutos) y facilidad de uso (la mayoría de los usuarios manifiesta que la interfaz de usuario de la herramienta es intuitiva y declaran no haber necesitado de una capacitación para utilizarla). Asimismo, hemos notado que el número de tickets recibidos en la mesa de ayuda para realizar soporte técnico se han reducido a entre 1 a 2 por semana.

FIGURA 23. PLATAFORMA DISPONIBLE PARA LA DESCARGA DEL ARTEFACTO EN PC

4.2.3 *Client Side* para teléfonos inteligentes con S.O. Android

Para la evaluación de este aplicativo se realizó una prueba de campo a fin de comprobar la funcionalidad de la TA, así como de la AA en diferentes marcas y modelos de teléfonos inteligentes (en la Tabla 14 se presenta la lista de modelos y marcas de los teléfonos inteligentes utilizados). Se identificaron 51 usuarios para la prueba de campo, los cuales debían tener conocimientos o experiencia con firma digital utilizando tarjetas inteligentes. Los usuarios realizaron 51 operaciones de entrega de certificados en teléfonos inteligentes. Se realizaron encuestas de satisfacción a los usuarios, destacando la facilidad de la operación percibida. En general, los participantes en la prueba manifestaron que la operación fue "cómo instalar cualquier otro App" del Play Store (Figura 24) y hacer un login a alguna página web para generar el certificado digital. El aplicativo aún no ha sido puesto en producción, ya que aún se tiene previsto realizar una prueba de campo adicional con usuarios que no han utilizado tarjetas inteligentes y firma digital.

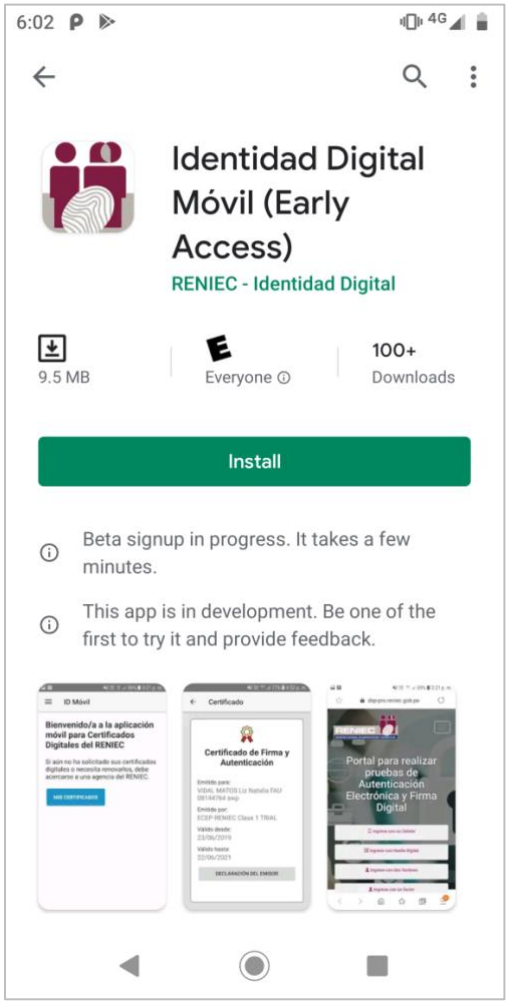

FIGURA 24. PLATAFORMA DISPONIBLE PARA LA DESCARGA DEL ARTEFACTO EN TELÉFONOS INTELIGENTES CON S.O. ANDROID

TABLA 14 - TELÉFONOS INTELIGENTES UTILIZADOS EN LA PRUEBA DE CAMPO

MARCA	Nº	MODELO	VERSIÓN DE S.O.
Asus	1	Zenfone Pegasus 3 X008DB	7.0
Huawei	2	Y5 III MYA-L03	6.0
	3	P8 Lite ALE-L23	
	4	P9 Lite DIG-L03	
	5	P9 EVA-L09	
	6	Mate 8 NXT-L09	7.0
	7	Mate 9 Lite BLL-L23	
	8	P10 VTR-L09	8.0
	9	P20 Lite ANE-LX3	
	10	Y5 (2018) DRA-LX3	8.1
	11	Y7 (2019)	
	12	P30 Pro VOG-L04	9.0
	13	P20 EML-L09	
	14	P Smart 2019	
LG	15	K8 (2017) X240DSF	6.0
	16	Q6 M700F	7.1.1
	17	K11 Alpha	7.1.2
	18	K9 LM-X210HM	
Motorola	19	G5 Plus	8.1
Nokia	20	5 TA-1027	7.1.1
Samsung	21	Galaxy A5 SM-A520F	6.0.1
	22	Galaxy J5 (2016) SM-J510MN	7.1.1
	23	Galaxy A5 SM-A520F	8.0
	24	Galaxy J7 Pro SM-J730GM	8.1
	25	Galaxy Note 9	
	26	Galaxy A50 SM-A505G	9.0
	27	Galaxy S9 Lite	
Sony	28	Xperia Z5 E6603	7.1.1

4.2.4 *Client Side* para dispositivos con interfaz PKCS#11

Este aplicativo ha sido puesto a disposición de los usuarios en la dirección web https://pki.reniec.gob.pe/dcdelivery3/ (Figura 25). Se han registrado 9,307 operaciones de generación de certificados digitales desde su puesta en operación, y así también se han detectado que el número de solicitudes de atención en el servicio al soporte técnico se ha reducido a entre 1 a 2 por semana. Se han realizado encuestas de satisfacción a los usuarios, habiendo obtenido las mismas impresiones que para el aplicativo *ClientSide* para computadores personales con MS Windows. Además, destacamos que contamos con un único procedimiento para la operación de 25 módulos criptográficos con interfaz PKCS#11 homologados a hasta la fecha listados en la Tabla 15.

TABLA 15 – MÓDULO CRIPTOGRÁFICOS CON INTERFAZ PKCS#11 HOMOLOGADOS

PRES.	INTEGRADOR	N°	MODELO	CHIP
TI.	Cryptovision	1	JCOP 2.4.2 R3	NXP P5CD081V1A
	Bit4ID	2	Crypto Java Card	NXP P5CC073V0B
		3	J-Sign	ST Microelectronics SA23YR48/80B
		4	Touch&Sign 2048	ST Microelectronics ST19WR66I
T.		5	CryptoKey	
		6	I Am	
		7	Digital DNA	ST Microelectronics SA23YR48/80B
		8	tokenME	INSIDE Secure ATVaultIC405
		9	tokenME v2	
		10	tokenME v3	AisinoChip Electronics SCC-X
	Longmai	11	mToken CryptoID	
	SafeNet	12	iKey 4000	Philips P8WE5032
		13	eToken 5100	SafeNet eToken 5100
		14	eToken 5110	Infineon SLE78CFX3000PH
		15	eToken PRO (Java)	ATMEL AT90SC25672RCT-USB Rev.D
	Athena Smartcard	16	IDProtect Key	
		17	IDProtect Key with LASER PKI	
	Sagem Orga	18	ypsID e-M Key	
TI.	Morpho Safran	19	ypsID	
T.	ACS	20	ACOS5-64	ST Microelectronics ST23YL80
		21	CryptoMate Nano	
		22	ACR101I SIMicro (CCID)	
	Feitian	23	AudioPass	ST Microelectronics ST23YT66
		24	ePass 2003	
TI.	Oberthur	25	eID Card	NXP P5CD144V0B

Nota: TI representa a una Tarjeta Inteligente y T representa a un Token criptográfico.

FIGURA 25. PLATAFORMA DISPONIBLE PARA LA DESCARGA DEL ARTEFACTO EN TARJETAS INTELIGENTES Y TOKENS CRIPTOGRÁFICOS

4.3 Aspectos de implementación encontrados

En la implementación de los aplicativos *Client Side* se han identificado diversas situaciones que, si bien podrían ser consideradas como excepcionales, consideramos que merecen ser documentadas.

4.3.1 Implementación para computadores personales con S.O. MS Windows

En las que destacamos las siguientes:

i. Cuando se le pide al usuario que establezca un PIN a efectos de proteger el acceso al material criptográfico, puede ocurrir que el usuario cancele esta acción (de manera intencionada o no intencionada), ya que el dialogo de decisión está controlado completamente por el S.O. Si bien es cierto que se tiene un número de intentos predefinido, si el usuario cancela todos estos intentos, el certificado digital no será instalado en el repositorio criptográfico gestionado por el módulo MSCAPI.
ii. Cuando el computador del usuario tiene el JRE instalado, pero no configurado de forma estandarizada se presentan problemas diversos. Esto pasa también en situaciones donde hay varias versiones del JRE instalado en el mismo computador. El aplicativo funciona perfectamente con instalaciones estandarizadas del JRE 8 de 32 o 64 bits.
iii. Cuando la contraseña de acceso al S.O. del computador personal es reseteada por una cuenta de administrador (ya sea del equipo local o de dominio), el material criptográfico creado con la contraseña anterior queda inaccesible. Esto se da por controles de seguridad del S.O. que busca garantizar que solo el usuario quién instaló el certificado digital pueda hacer uso de este. Para volver a tener acceso al material criptográfico, se tiene que restablecer la contraseña original utilizada al momento de la instalación del certificado digital.

4.3.2 Implementación para teléfonos inteligentes con S.O. Android

En la implementación del aplicativo destacamos los siguientes aspectos de implementación:

i. La sesión de acceso al entorno de confianza es fluida en modo SWP, sin embargo, en modo TEE, algunas veces, tras utilizar algunas operaciones criptográficas, ocurren excepciones que hacen que se deba volver a iniciar la sesión.

ii. El modo SWP del TAP no provee la función TEE_GenerateKey(), por lo que la generación del par de llaves RSA debe ser realizada externamente y luego exportada hacia el entorno de ejecución de confianza.
iii. Si bien las primeras pruebas realizadas en teléfonos inteligentes de gama media y alta fueron exitosas, se encontró un modelo donde a pesar de incorporar un TEE nativo, no se pudo acceder su funcionalidad y la ejecución no tuvo éxito.
iv. Como mecanismo de control de instalaciones, cada primera instalación del TA requiere acceder a un servidor de activación de aplicaciones de confianza TAM Server, el cual autoriza la instalación.
v. El tamaño del registro para almacenamiento en el entorno de confianza tiene un máximo de 4096 bytes, exigiendo que datos de mayor tamaño tengan que ser almacenados por lotes cuyo flujo debe ser implementado.
vi. Uno de los modelos listados en la Tabla 14 requirió implementar una excepción en el proceso de instalación de la TA, que no se presentó en los otros modelos. Este hecho hace pensar en la necesidad de establecer un procedimiento previo de homologación de teléfonos inteligentes a fin de evitar incidencias con los usuarios finales.

4.3.3 Implementación para dispositivos con interfaz PKCS#11

Se destacan los siguientes aspectos de implementación:

i. De los 25 módulos criptográficos para usuarios finales homologados, solamente cuatro proveen librerías PKCS#11 que se ejecutan en modo standalone; es decir, la ejecución del aplicativo no requiere la instalación previa del middleware del módulo criptográfico sobre el cual el artefacto va a operar.
ii. Se encontró limitaciones relacionadas al alias (parámetro CKA_ID) utilizado en la operación de importación del certificado en dispositivos compatibles con el estándar PKCS#15. Esta limitación sucede debido a que la escritura permitida en el parámetro PKCS#15 asociado (pkcs15-ub-identifier) supera el máximo de la longitud establecida (255 bytes). También se encontró un módulo que permite escribir solamente 38 caracteres como máximo y otro solamente 31. Otros dos módulos solamente permiten el uso de caracteres ASCII.
iii. Se han encontrado situaciones excepcionales cuando el usuario final utiliza módulos criptográficos sin haber sido inicializados.

iv. Cuatro módulos presentan una restricción relacionada a la importación de certificados. Estos solamente permiten importar el certificado asociado a la llave privada resguardada por el módulo mas no la cadena de certificación completa.
v. Dos módulos permiten iniciar sesión (ingreso del PIN requerido) solamente mediante la interfaz gráfica provista por su middleware.
vi. Debido a aspectos de compatibilidad con la mayoría de los drivers PKCS#11 de los dispositivos, la implementación requiere la utilización del JRE de 32 bits en el computador personal del usuario.

Es importante señalar que, en general, todas las implementaciones realizadas sufren de problemas cuando los usuarios están conectados bajo una red intermitente y de baja calidad o cuando se encuentran en entornos corporativos con políticas de seguridad de red bastante restringidas. En estos casos, la usabilidad del artefacto se ve impactada porque la mayoría de los usuarios finales no distinguen el origen del problema, atribuyendo la causa al artefacto.

4.4 Contrastación de la hipótesis

El postulado de la hipótesis principal es: El diseño y la construcción de un artefacto informático permitirá distribuir y entregar de forma efectiva y eficiente certificados digitales en diferentes tipos de módulos criptográficos destinados a usuarios finales.

Para la contrastación de la hipótesis, tenemos que dar respuesta a la hipótesis principal a partir de los resultados obtenidos para los cinco indicadores identificados:

i. El número de certificados digitales para persona jurídica (Class 3), y persona natural (Class 1) generados en los módulos criptográficos utilizando el artefacto informático (instancias) implementado, es presentado en la Tabla 16.
ii. El tiempo requerido por el artefacto en el proceso de generación de certificados digitales en los módulos criptográficos, es presentado en la Tabla 17.
iii. La usabilidad del artefacto percibida por el usuario final al generar el certificado digital en el módulo criptográfico de su propiedad es tabulada en la Tabla 18
iv. El número de solicitudes atendidas por el servicio de mesa de ayuda para dar soporte técnico al procedimiento de generación de certificados digitales utilizando el artefacto, es presentado en la Tabla 19.
v. El número de plataformas disponibles donde se implementó el artefacto es listado en la Tabla 20.

TABLA 16. NÚMERO DE CERTIFICADOS DIGITALES GENERADOS A SEP2019

	Interfaz de distribución original (EJBCA)		Artefacto	
Tipo de módulo criptográfico	**Cantidad de certificados digitales**	**Periodo**	**Cantidad de certificados digitales**	**Periodo**
Módulos MSCAPI (computadoras personales)	51,141	Entre marzo 2012 y junio 2017 (63 meses)	82,383	Entre julio 2017 y septiembre 2019 (26 meses)
Tarjeta inteligente y Tokens criptográficos			9,307	
Teléfonos inteligentes			51	Entre agosto y septiembre 2019 (2 meses)

TABLA 17. TIEMPO REQUERIDO DURANTE EL PROCESO DE GENERACIÓN DE CERTIFICADOS DIGITALES

Tiempo promedio requerido utilizando la interfaz de distribución original	Tiempo promedio requerido utilizando las instancias del Artefacto informático
Entre 15 a 20 minutos	Entre 1 a 2 minutos

Se realizaron encuestas de satisfacción a los usuarios, donde destacan dos propiedades del artefacto: rapidez de la operación, y facilidad de uso.

TABLA 18. CUESTIONARIO DE SATISFACCIÓN DEL CLIENTE QUE UTILIZÓ LAS IMPLEMENTACIONES DEL ARTEFACTO INFORMÁTICO

Pregunta del cuestionario	Valores	Resultado
¿Según su experiencia con el proceso de entrega de su certificado digital, que tan rápida es la herramienta?	Lento Normal Rápido	Rápido
¿Qué nivel de dificultad representó para usted el uso de la herramienta?	Fácil Normal Difícil	Fácil
¿Requirió usted capacitación para el uso de la herramienta?	Sí No	No

TABLA 19. NÚMERO DE SOLICITUDES ATENDIDAS POR EL SERVICIO DE MESA DE AYUDA

N° de solicitudes atendidas para dar soporte técnico a la interfaz original	N° de solicitudes atendidas para dar soporte técnico al Artefacto
Entre 1 y 2 por día	Entre 1 y 2 por semana

TABLA 20. PLATAFORMAS DISPONIBLES IMPLEMENTADAS CON EL ARTEFACTO

Plataformas operativas disponibles con la Interfaz original	Plataformas operativas disponibles con el Artefacto
1. Computadoras personales 2. Módulos criptográficos (02)	1. Computadoras personales 2. Módulos criptográficos (25) 3. Smartphones con S.O. Android (28)

Por los resultados obtenidos, podemos afirmar que el artefacto informático (diseñado y construido) permite una distribución y entrega efectiva y eficiente de certificados digitales en diferentes tipos de módulos criptográficos (plataformas) destinados a usuarios finales.

CONCLUSIONES

1. El artefacto diseñado e implementado permitió la distribución y entrega de certificados digitales X.509 v3 a usuarios finales en computadoras personales y teléfonos inteligentes, permitiendo a las personas, acceder a la verificación de su identidad digital de manera remota con entornos no presenciales como el Internet.

2. Se definieron siete meta-requisitos funcionales con la finalidad de generalizar la propuesta y así poder hacer una implementación modular que permitió la distribución y entrega de material criptográfico (certificados digitales y llaves criptográficas asociadas) con la siguiente distribución:

    - En 82383 módulos MSCAPI de computadores personales con MS Windows (versiones 7, 8, 8.1 y 10)

    - En 51 teléfonos inteligentes entre 28 diferentes marcas y modelos con S.O. Android listados en la Tabla 14.

    Adicionalmente, para demostrar la flexibilidad del artefacto, también se generó material criptográfico en 9307 módulos criptográficos entre 25 modelos de 10 marcas que cuentan con interfaz PKCS#11 presentado en la Tabla 15, los que fueron previamente homologados.

    Habiendo respondido la pregunta de investigación planteada, concluimos que, si es posible diseñar, construir e implantar un artefacto flexible y fácil de usar que permite la distribución y entrega de certificados digitales X.509 v3 en computadores personales y teléfonos inteligentes de propiedad del usuario final.

3. Se realizó una revisión de la literatura y fueron recopiladas casuísticas e incidentes reportados producto del uso de una herramienta profesional (®EJBCA de PimeKey Solutions AB) con usuarios reales. De esta manera se definió el problema y se identificaron los requisitos funcionales y no funcionales como objetivos del problema abordado.

4. Se realizó una evaluación de la efectividad y la eficiencia de la propuesta mediante pruebas empíricas de satisfacción del cumplimiento de los requisitos funcionales y no funcionales planteados.

5. El diseño propuesto e implementado en el artefacto informático ha permitido verificar que puede ser reproducido por plataformas operativas adicionales, garantizando la escalabilidad de la propuesta.

6. No obstante, hay algunas limitaciones que merecen ser destacadas:

    a. Es recomendable que la entrega de certificados digitales en computadores personales no sea realizada en redes abiertas, debido a que en el caso de este contenedor (incorporado en una computadora personal), el material criptográfico es protegido solo por software y no por hardware.

    b. Si bien, para la implementación del artefacto propuesto, se han tomado las medidas de seguridad del caso (que las llaves privadas sean no exportables y que estén resguardadas de forma cifrada en el S.O. del computador personal), éstas no llegan a ser comparables a los controles de seguridad existentes cuando se utiliza una tarjeta inteligente o un token criptográfico, o el TEE de un teléfono inteligente (inclusive con SWP).

    c. Es recomendable el uso de computadores personales solamente en entornos corporativos con políticas de seguridad preestablecidas, y con certificados digitales asociados a políticas de certificación de bajo riesgo.

    d. El uso de los teléfonos inteligentes (con el material criptográfico protegido por el TEE), es recomendado fuertemente, pues logra una estabilidad entre la mínima seguridad que brinda, y la facilidad de uso que ofrece a los usuarios finales, sin embargo, aún su bajo nivel de estandarización limita su incorporación en este tipo de soluciones.

RECOMENDACIONES Y TRABAJOS FUTUROS

Algunos trabajos que se desprenden como consecuencia del desarrollo del trabajo son los siguientes:

1. Sería importante estudiar la incorporación de la distribución y entrega de material criptográfico en dispositivos en el ámbito de la IoT, debido a que la tecnológica subyacente que lo permitiría es similar a la revisada y comprobada en este trabajo.

2. Una tarea pendiente y evidente es efectuar una instanciación y evaluación del artefacto en plataformas las MacOS, iOS y Linux.

3. En MacOS y iOS no debería presentarse mayor inconveniente, ya que estos cuentan con un mecanismo de seguridad denominado *Secure Enclave* que persigue la esencia funcional del TEE disponible para un teléfono inteligente con S.O. Android.

4. Sin embargo, no sucede lo mismo para el caso de Linux [29], ya que este no cuenta aún con un mecanismo nativo para el almacenamiento y uso de material criptográfico como es el caso del módulo MSCAPI de MS Windows, identificando una línea de investigación a abordar.

5. Otra actividad futura que resulta también interesante de investigar es la adopción de la criptografía con umbral (threshold cryptography) propuesta por Buldas et al. [3], la cual permitiría prescindir de la participación de los fabricantes, que es requerida cuando se utiliza el TEE de los teléfonos inteligentes.

6. Asimismo, resulta recomendable llevar a cabo estudios más exhaustivos del balance entre la seguridad y usabilidad de la propuesta.

7. Finalmente, también sería recomendable explorar el uso de múltiples factores de autenticación para verificar la identidad del usuario que va a realizar una operación de obtención de certificado digital.

BIBLIOGRAFÍA

[1] **Bouazzouni, M., Conchon, E., Peyrard, F.** (2018) Trusted mobile computing: An overview of existing solutions, Future Generation Computer Systems, vol 80, pp. 596-612, [en línea], consultado el 30/07/2020, URL disponible en: https://www.sciencedirect.com/science/article/abs/pii/S0167739X16301510?via%3Dihub

[2] **Brandl, H., Rosteck, T.** (2004) Technology, Implementation and Application of the Trusted Computing Group Standard (TCG), Infineon White paper, [en línea], consultado el 30/07/2020, URL disponible en: http://www.cs.unh.edu/~it666/reading_list/Hardware/trusted_computing_overview.pdf

[3] **Buldas, A., Kalu, A., Laud, P., Oruaas, M.** (2017) Server-supported RSA signatures for mobile devices, European Symposium on Research in Computer Security, pp. 315–333, Springer, [en línea], consultado el 30/07/2020, URL disponible en: https://research.cyber.ee/~peeter/research/esorics2017.pdf

[4] **Diffie, W., Hellman, M.** (1976) New Directions in Cryptography, [en línea], consultado el 30/07/2020, URL disponible en: https://ee.stanford.edu/~hellman/publications/24.pdf

[5] **Encinas, M., Martinez, R., Cuno, A., Gallo, A., Zapata, F., Saavedra, R.** (2018) The National PKI of Peru: a new certification hierarchy, 37th International Conference of the Chilean Computer Science Society (SCCC), [en línea], consultado el 30/07/2020, URL disponible en: https://ieeexplore.ieee.org/document/8705241

[6] **ETSI. TECHNICAL SPECIFICATION 119 102-1** (2018) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, version 1.2.1, [en línea], consultado el 30/07/2020, URL disponible en: https://www.etsi.org/deliver/etsi_ts/119100_119199/11910201/01.02.01_60/ts_11910201v010201p.pdf

[7] **European Union eIDAS Regulation**. (2014) REGULATION (EU) Nº 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic

identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC pp. 73–144, [en línea], consultado el 30/07/2020, URL disponible en: https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

[8] **Federal Office for Information Security.** (2019) Technical Guideline TR-03159 Mobile Identities Part 1: Security Requirements for eIDAS LoA "substantial", Version 1.0 Draft 2, [en línea], consultado el 30/07/2020, URL disponible en: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03159/TR-03159-1.pdf?__blob=publicationFile&v=4

[9] **GlobalPlatform, Inc.** (2015) The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market, [en línea], consultado el 30/07/2020, URL disponible en: https://globalplatform.org/wp-content/uploads/2018/04/GlobalPlatform_TEE_Whitepaper_2015.pdf

[10] **GlobalPlatform, Inc.** (2018) Introduction to Secure Elements, [en línea], consultado el 30/07/2020, URL disponible en: https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf

[11] **GlobalPlatform, Inc.** (2018) Introduction to Trusted Execution Environments, [en línea], consultado el 30/07/2020, URL disponible en: https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment-15May2018.pdf

[12] **Guida, R., Stahl, R., Bunt, T., Secrest, G., Moorcones, J.** (2004) Deploying and using public key technology: Lessons learned in real life, IEEE Security & Privacy Magazine, vol. 2, no. 4, pp. 67–71, [en línea], consultado el 30/07/2020, URL disponible en: https://ieeexplore.ieee.org/document/1324604

[13] **Hevner, A., March, S., Park, J., Ram, S.** (2014) Design science in information systems research, MIS quarterly, vol. 28, Nº 1, pp. 75–105, [en línea], consultado el 30/07/2020, URL disponible en https://www.researchgate.net/publication/201168946_Design_Science_in_Information_Systems_Research

[14] **Internet Engineering Task Force** (2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) RFC5280, [en línea], consultado el 30/07/2020, URL disponible en: https://tools.ietf.org/pdf/rfc5280.pdf

[15] **Islam, K.** (2012) Effective use of smart cards: A case study of smart cards in Sweden, Master's thesis, UMEA Universitet, [en línea], consultado el 30/07/2020, URL disponible en: http://umu.diva-portal.org/smash/record.jsf?pid=diva2%3A606154&dswid=-5232

[16] **Leitold, H. Konrad, D.** (2019) Qualified Remote Signatures – Solutions, its Certification, and Use, Proceedings of 29th SmartCard Workshop, pp. 219–231, [en línea], consultado el 30/07/2020, URL disponible en: https://graz.pure.elsevier.com/en/publications/qualified-remote-signatures-solutions-its-certification-and-use

[17] **Leloglu, E.** (2017) A Review of Security Concerns in Internet of Things, [en línea], Journal of Computer and Communications, vol. 5 Nº 1, consultado el 30/07/2020, URL disponible en: https://www.scirp.org/journal/paperinformation.aspx?paperid=73675

[18] **Linden, M., Linna, P., Kivilompolo, M., Kanner, J.** (2002) Lessons learned in PKI Implementation in Higher Education, EUNIS2002, The 8th International Conference of European University Information Systems, Portugal, pp. 246–251, [en línea], consultado el 30/07/2020, URL disponible en: https://www.researchgate.net/publication/246680597_Lessons_Learned_in_PKI_Implementation_in_Higher_Education

[19] **Lioy, A., Marian, M., Moltchanova, N., Pala, M.** (2006) PKI past, present and future, International Journal of Information Security, vol. 5, no. 1, pp. 18–29, [en línea], consultado el 30/07/2020, URL disponible en: https://www.academia.edu/10975801/PKI_past_present_and_future

[20] **Lippert, M., Karatsiolis, V., Wiesmaier, A., Buchmann, J.** (2006) Life-cycle Management of X.509 certificates based on LDAP directories, Journal of Computer Security, vol. 14, no. 5, pp. 419–439, [en línea], consultado el 30/07/2020, URL disponible en: https://www.researchgate.net/publication/220065430_Life-cycle_management_of_X509_certificates_based_on_LDAP_directories

[21] **Loo, W., Yeow, P., Chong, S.** (2009) User acceptance of Malaysian government multipurpose smartcard applications, Government Information Quarterly, vol. 26, no. 2, pp. 358–367, [en línea], consultado el 30/07/2020, URL disponible en: https://www.academia.edu/5520170/User_acceptance_of_Malaysian_government_multipurpose_smartcard_applications

[22] **Lopez, J., Oppliger, R., Pernul, G.** (2005) Why have public key infrastructures failed so far?, Internet Research, vol. 15, no. 5, pp. 544–556, [en línea], consultado el 30/07/2020, URL disponible en: https://www.researchgate.net/publication/220146887_Why_have_public_key_infrastructures_failed_so_far

[23] **March, S. Smith, G.** (1995) Design and natural science research on information technology, Decision support systems, vol. 15, no. 4, pp. 251–266, [en linea], consultado el 30/07/2020, URL disponible en: https://www.researchgate.net/publication/222484351_Design_and_Natural_Science_Research_on_Information_Technology

[24] **Moody, D.** (2003) The Method Evaluation Model: A Theoretical Model for Validating Information Systems Design Methods, ECIS. 1327-1336, [en línea], consultado el 30/07/2020, URL disponible en: https://www.researchgate.net/publication/221408322_The_method_evaluation_model_A_theoretical_model_for_validating_information_systems_design_methods

[25] **Msgna, M., Ferradi, H., Naeem, R., Markantonakis, K.** (2015) Secure Application Execution in Mobile Devices, [en línea], consultado el 30/07/2020, URL disponible en: https://www.researchgate.net/publication/290437133_Secure_Application_Execution_in_Mobile_Devices

[26] **Para, C., Pelzl, J.** (2010) Understanding Cryptography, Springer, [en línea], consultado el 30/07/2020, URL disponible en: http://swarm.cs.pub.ro/~mbarbulescu/cripto/Understanding%20Cryptography%20by%20Christof%20Paar%20.pdf

[27] **Park, D.** (2015) Social life of PKI: Sociotechnical development of Korean public-key infrastructure, IEEE Annals of the History of Computing, vol. 37, no. 2, pp. 59–71, [en línea], consultado el 30/07/2020, URL disponible en: https://www.academia.edu/25840731/Social_Life_of_PKI_Sociotechnical_Development_of_Korean_Public-Key_Infrastructure

[28] **Paul, C., Morse, E., Zhang, A., Choong, Y., Theofanos, M**. (2011) A Field Study of User Behavior and Perceptions in Smartcard Authentication. Human-Computer Interaction – INTERACT 2011, vol. Part IV, pp. 1–17, Springer, Berlin, Heidelberg, [en línea], consultado el 30/07/2020, URL disponible en:

https://www.researchgate.net/publication/221054584_A_Field_Study_of_User_Behavior_and_Perceptions_in_Smartcard_Authentication

[29] **Prabhav, S., Madhav, D., Rakshak, K., Rohan, N., Latha, NR.** (2017) Trusted execution environment and linux- A survey, International Journal of Computer Trends and Technology (IJCTT), vol. 45, no. 1, pp. 28–32, [en línea], consultado el 30/07/2020, URL disponible en: https://www.semanticscholar.org/paper/Trusted-Execution-Environment-and-Linux-A-Survey-Prabhav-Deshpande/b4e08563c5db2bb9b4197047fdefa07cfab97e4f

[30] **Price, G.** (2006) Public key infrastructures: A research agenda, Journal of Computer Security, vol. 14, no. 5, pp. 391–417, [en línea], consultado el 30/07/2020, URL disponible: https://www.researchgate.net/publication/220065341_Public_Key_Infrastructures_A_research_agenda

[31] **Rayes, A., Salam, S.** (2019) Internet of Things From Hype to Reality. The Road to Digitization, Segunda edición, Editorial Springer, [en línea], consultado el 30/07/2020, URL disponible en: https://www.springer.com/gp/book/9783319995151

[32] **Sabt, M., Achemlal M., Bouabdallah A.** (2015) Trusted Execution Environment: What It is, and What It is Not, 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, pp. 57-64, [en línea], consultado el 30/07/2020, URL disponible en: https://ieeexplore.ieee.org/abstract/document/7345265

[33] **Samsung Electronics.** (2020) Samsung, BSI, Bundesdruckerei and Telekom Security Partner to Bring National ID to Your Smartphone, Samsung Newsroom, [en línea] consultado el 30/07/2020, URL disponible en: https://news.samsung.com/global/samsung-bsi-bundesdruckerei-and-telekom-security-partner-to-bring-national-id-to-your-smartphone

[34] **Samsung Electronics.** (2020) Samsung Elevates Data Protection for Mobile Devices with New Security Chip Solution, Samsung Newsroom, [en línea] consultado el 30/07/2020, URL disponible en: https://news.samsung.com/global/samsung-elevates-data-protection-for-mobile-devices-with-new-security-chip-solution

[35] **Simon, H.** (1996) The sciences of the artificial. MIT press, [en línea] consultado el 30/07/2020, URL disponible en: https://monoskop.org/images/9/9c/Simon_Herbert_A_The_Sciences_of_the_Artificial_3rd_ed.pdf

[36] **Sorge, C.** (2015) The German Electronic Identity Card: Lessons learned, Handbook of Research on Democratic Strategies and Citizen-Centered E-Government Services, [en línea], consultado el 30/07/2020, URL disponible en: https://www.igi-global.com/chapter/the-german-electronic-identity-card/121322

[37] **Straub, T.** (2006) Usability challenges of PKI. PhD thesis, Technische Universitat, [en línea], consultado el 30/07/2020, URL disponible en: http://tuprints.ulb.tu-darmstadt.de/epda/000682/tstraub_diss.pdf

[38] **Sultan, K., Ruhi, H.** (2015) Overcoming Barriers to Client-Side Digital Certificate Adoption, International Journal of Computer Science and Information Security, Vol. 13, Nº 8, [en línea], consultado el 30/07/2020, URL disponible en: https://www.academia.edu/15236280/Overcoming_Barriers_to_Client-Side_Digital_Certificate_Adoption

[39] **Suo, H., Wan, J., Zou, C., Liu, J.** (2012) Security in the Internet of Things: A Review, 2012 International Conference on Computer Science and Electronics Engineering IEEE, [en linea], consultado el 30/07/2020, URL disponible en: https://ieeexplore.ieee.org/document/6188257

[40] **Trusted Computing Group** (2019) TPM 2.0: A Brief Introduction, [en línea], consultado el 30/07/2020, URL disponible en: https://trustedcomputinggroup.org/wp-content/uploads/2019_TCG_TPM2_BriefOverview_DR02web.pdf

[41] **Wieringa R.** (2007) Writing a Report About Design Research, University of Twente, the Netherlands, [en línea], consultado el 30/07/2020, URL disponible en: https://wwwhome.ewi.utwente.nl/~roelw/ReportingAboutDesignResearch.pdf

[42] **Zefferer, T., Krnjic, V.** (2012) Usability evaluation of electronic signature based e-government solutions, IADIS International Conference WWW/INTERNET, vol. 2012, pp. 227–234, [en línea], consultado el 30/07/2020, URL disponible en: http://www.iadisportal.org/digital-library/usability-evaluation-of-electronic-signature-based-e-government-solutions