UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

DESARROLLO DE UN PASAPORTE DIGITAL BASADO EN FIRMAS AGREGADAS

PARA OPTAR AL GRADO DE MAESTRO EN

SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

DRA. MARIA DE LOURDES LÓPEZ GARCÍA

PRESENTADO POR:

DAVID ELISEO MARTÍNEZ CASTELLANOS

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.

Enero de 2017

Desarrollo de un Pasaporte Digital Basado en Firmas Agregadas

Martínez Castellanos David Eliseo
UNIVERSIDAD DON BOSCO
ANTIGUO CUSCATLAN, EL SALVADOR
eliseo.martinez@gmail.com

Resumen— El presente trabajo trata del diseño de un Pasaporte Digital protegido por un protocolo criptográfico. Implementa primitivas de seguridad para cifrado de información y verificación por medio de digestión de mensajes y firma digital. El protocolo asigna el nivel de autoridades certificadoras a las entidades encargadas de emitir el pasaporte y emisión de visado. Adicionalmente se implementa el protocolo de firmas agregadas al proceso de control migratorio en las entradas y salidas del país de origen, así como las entradas y salidas de los países destino, realizando una cadena de verificación de la ruta del ciudadano poseedor del pasaporte digital.

Índice de Términos— Autoridad Certificadora, Confidencialidad, Criptografía de llave pública, Criptografía de llave privada, Disponibilidad, Firma Digital, Firmas Agregadas, Integridad.

I. INTRODUCCIÓN

El control migratorio es importante por motivos de seguridad de estado, para la lucha contra el terrorismo, crimen organizado, control de propagación de enfermedades epidémicas y para la recolección de información con propósitos económicos.

Así mismo es de interés para el propietario de un documento de viaje, la correcta verificación de su identidad como ciudadano de un país y que le facilite los trámites legales durante su viaje.

En El Salvador el documento de viaje es una libreta en papel que posee mecanismos de seguridad en físico, mientras un pasaporte digital permite el uso de criptografía como mecanismo de seguridad, proveyendo cifrado de datos y verificación de la información del pasaporte, así como de las acciones realizadas con este, de tal forma que no se pueda negar que dichas acciones fueron realizadas por el propietario del pasaporte.

En el presente trabajo se describe el funcionamiento de un protocolo de seguridad diseñado para ser utilizado como parte del funcionamiento de un Sistema de Pasaporte Digital. En este protocolo participan diferentes entidades, algunas de las cuales funcionan como autoridades certificadoras a la hora de emitir un pasaporte o una visa electrónica para el ingreso a un país.

El resto del documento está estructurado de la siguiente manera. En la Sección II se presenta el marco legal que regula la emisión de pasaportes en El Salvador, la normativa de estandarización internacional y los artículos de la Ley de Firma Electrónica de interés para el funcionamiento del Pasaporte Digital. En la sección III, se describe el detalle de las herramientas criptográficas que componen el protocolo de seguridad del Pasaporte Digital. En la sección IV, se presenta el diseño de la funcionalidad del Pasaporte Digital, la especificación formal del protocolo de seguridad y el análisis de seguridad. La sección V, describe la implementación del Pasaporte Digital como una aplicación móvil para teléfonos inteligentes basados en la plataforma *Android*. Por último, se presentan las conclusiones en la sección VI.

II. FUNDAMENTACIÓN LEGAL

Los documentos de viaje tienen gran importancia para la prueba de la identidad y nacionalidad de la persona viajante.

Cada nación posee sus leyes sobre la emisión, uso, requisitos y revalidación del documento de viaje y además existen convenios internacionales entre Estados en los que se definen normas que los países miembros deben cumplir y además se define la existencia de organismos encargados de proponer estándares los cuales los países pueden o no cumplir.

Para proveer un contexto legal al pasaporte digital se identifican a continuación artículos de las leyes nacionales de Expedición y Revalidación de Pasaportes, Firma Electrónica de El Salvador y del Convenio Sobre Aviación Civil Internacional.

A. Ley de Expedición y Revalidación de Pasaportes

En El Salvador, la emisión de pasaportes se encuentra regulada por el decreto No. 1020, Ley de Expedición y Revalidación de Pasaportes y Autorizaciones de Entrada a la República, la cual describe los tipos de documentos emitidos en El Salvador, los requisitos para cada tipo de documento, así como las instituciones del estado encargadas de la emisión de cada tipo de pasaporte.

Considerando la emisión de pasaporte ordinario, los artículos relevantes de esta ley son [1]:

Art. 1. El pasaporte es el documento de viaje aceptado internacionalmente y constituye en el Extranjero uno de los medios de prueba de la Nacionalidad e Identidad de las personas salvadoreñas.

Art. 20. El Pasaporte Ordinario será expedido por las autoridades competentes a toda persona salvadoreña que lo solicite previa su identificación, y el registro y calificación de los documentos que en el artículo siguiente se indicarán y cumplidos los demás requisitos establecidos en la presente Ley.

Art. 21. La persona que desee obtener Pasaporte Ordinario en el país, deberá comparecer personalmente ante la Dirección General de Migración o a sus dependencias o Delegaciones y cumplir con los siguientes requisitos:

a) Llenar, firmar y entregar el formulario que se le suministre, proporcionando los datos de su filiación y demás que se le requieran;

b) Inciso suprimido en Reforma del 5 de febrero de 1997, Decreto legislativo No. 959.

c) Presentar los documentos comprobatorios de su nacionalidad salvadoreña;

d) Presentar la Cédula de Identidad Personal o cualquier otro documento, que a juicio de la Dirección General de Migración establezca la identidad del interesado; y,

e) Tratándose de personas incapaces deberá acreditarse la autorización de quienes ejerzan sobre ellos el cuidado personal, tutela o curatela general.

Art. 23. La Dirección General de Migración empleará en la expedición de Pasaportes, el sistema que resulte más adecuado a sus funciones, procurando que ello redunde en beneficio del público usuario.

B. Convenio Sobre Aviación Civil Internacional

El Convenio Sobre Aviación Civil Internacional surge con el fin de que la aviación civil internacional pueda desarrollarse de manera segura y ordenada y que los servicios internacionales de transporte aéreo puedan establecerse sobre una base de igualdad de oportunidades y realizarse de modo sano y económico [2].

Este convenio posee los siguientes artículos relevantes para el uso de pasaportes y control migratorio:

Art. 13. Las Leyes y reglamentos de un Estado contratante relativos a la admisión o salida de su territorio de pasajeros, tripulación o carga transportados por aeronaves, tales como los relativos a entrada, despacho, inmigración, pasaportes, aduanas y sanidad serán cumplidos por o por cuenta de dichos pasajeros, tripulaciones y carga, ya sea a la entrada, a la salida o mientras se encuentren dentro del territorio de ese Estado.

Art. 22. Cada Estado contratante conviene en adoptar, mediante la promulgación de reglamentos especiales o de otro modo, todas las medidas

posibles para facilitar y acelerar la navegación de las aeronaves entre los territorios de los Estados contratantes y para evitar todo retardo innecesario a las aeronaves, tripulaciones, pasajeros y carga, especialmente en la aplicación de las leyes sobre inmigración, sanidad, aduana y despacho.

Art. 37. Cada Estado contratante se compromete a colaborar, a fin de lograr el más alto grado de uniformidad posible en las reglamentaciones, normas, procedimientos y organización relativos a las aeronaves, personal, aerovías y servicios auxiliares, en todas las cuestiones es que tal uniformidad facilite y mejore la navegación aérea.

A este fin, la Organización de Aviación Civil Internacional adoptará y enmendará, en su oportunidad, según sea necesario, las normas, métodos recomendados y procedimientos internacionales que traten de:

a) Sistemas de comunicaciones y ayudas para la navegación aérea, incluida la señalización terrestre;

b) Características de los aeropuertos y áreas de aterrizaje;

c) Reglas del aire y métodos de control del tránsito aéreo;

d) Otorgamiento de licencias del personal operativo y mecánico;

e) Aeronavegabilidad de las aeronaves;

f) Matrícula e identificación de las aeronaves;

g) Compilación e intercambio de información meteorológica;

h) Diarios de abordo;

i) Mapas y cartas aeronáuticos;

j) Formalidades de aduana e inmigración;

k) Aeronaves en peligro e investigación de accidentes;

Y de otras cuestiones relacionadas con la seguridad, regularidad y eficiencia de la navegación aérea que en su oportunidad puedan considerarse apropiadas.

Art. 38. Cualquier estado que considere impracticable cumplir, en todos sus aspectos, con cualesquiera de tales normas o procedimientos internacionales, o concordar totalmente sus reglamentos o métodos con alguna norma o procedimientos internacionales, después de enmendados estos últimos, o que considere necesario adoptar reglamentaciones o métodos que difieran en cualquier aspecto particular de lo establecido por una norma internacional, notificará inmediatamente a la Organización de Aviación Civil Internacional las diferencias entre sus propios métodos y lo establecido por la norma internacional.

C. Ley de Firma Electrónica de El Salvador

La Asamblea Legislativa de El Salvador, considerando que el Estado debe crear instrumentos legales que propicien el uso de tecnologías de información y comunicaciones y que debe existir un marco legal que brinde seguridad a los usuarios de las comunicaciones electrónicas y a las transacciones autorizadas mediante las aplicaciones de la tecnología, decreta la Ley de Firma electrónica de El Salvador, decreto No 133 [3].

Se consideran de interés los siguientes artículos de la Ley de Firma Electrónica para la implementación del Pasaporte Digital:

Art. 8. Los documentos de soporte electrónico utilizando firma electrónica, tendrán el mismo valor que los consignados de manera tradicional. Quedan excluidas aquellas actuaciones que para su perfeccionamiento requieren formalidades y solemnidades especiales.

Art. 9 Los documentos públicos emitidos por las instituciones estatales podrán estar contenidos en soporte electrónico y tendrán el valor asignado por el ordenamiento legal para esta clase de documentos.

Art. 24. La firma electrónica certificada tendrá igual validez y los mismos efectos jurídicos y probatorios que una firma manuscrita en relación con los datos consignados en un documento o mensaje de datos electrónicos en que fuere empleada.

En todo caso, al valorar la fuerza probatoria de un documento electrónico, se tendrá presente la

confiabilidad de la forma en la que se haya generado, archivado, comunicado, y en la que se haya conservado la integridad de la información.

III. HERRAMIENTAS CRIPTOGRÁFICAS

En esta sección, se describen las herramientas criptográficas utilizadas por el Pasaporte Digital, las cuales se utilizan para lograr los objetivos de seguridad pertinentes a un documento de viaje y de identificación personal, servicios criptográficos o protocolos intermedios y una discusión sobre los algoritmos específicos adoptados para la implementación del Sistema de Pasaporte Digital.

A. Seguridad Informática

La seguridad informática es la protección proporcionada a un sistema de información automatizada con el propósito de lograr los objetivos de preservar la integridad, disponibilidad y confidencialidad de los recursos de información, los cuales incluyen *hardware*, *software*, *firmware*, datos/información y telecomunicaciones [4].

Esta definición introduce 3 objetivos claves de la seguridad informática [5]:

1) Confidencialidad: Este término cubre dos conceptos relacionados:

- **Confidencialidad de datos:** Asegura que la información privada o confidencial no sea revelada a individuos no autorizados.
- **Privacidad:** Asegura que los individuos tengan el control sobre qué información personal puede ser recolectada y almacenada, así como por quienes y a quienes es revelada.

2) Integridad: Este término cubre dos conceptos relacionados:

- **Integridad de datos:** Se asegura que los programas y la información sean alterados sólo en la forma especificada y de forma autorizada.
- **Integridad del sistema:** Asegura que el sistema realice las funciones para las cuales fue destinado de forma inalterada, libre de manipulación no autorizada del sistema.

3) Disponibilidad: Se asegura que el sistema trabaje de forma propia y que el servicio no sea denegado a los usuarios autorizados.

B. Ataques informáticos

El Glosario de Seguridad de Internet RFC 2828 define los términos Amenaza y Ataque [6]:

- **Amenaza:** Es el potencial de una violación de seguridad, el cual existe cuando se dan las circunstancias, capacidad, acción o evento que puede infringir la seguridad y causar daño, es decir, una amenaza es un posible peligro que puede explotar una vulnerabilidad.
- **Ataque:** Un asalto a la seguridad de un sistema que se deriva de una amenaza inteligente, lo cual es, un acto inteligente que es un intento deliberado (especialmente en el sentido de método y técnica) para evadir servicios de seguridad y violar las políticas de seguridad de un sistema.

Una forma útil de clasificar los ataques a la seguridad informática es en términos de ataques pasivos y ataques activos [4]. Un ataque pasivo intenta aprender o hacer uso de la información de un sistema, pero sin afectar los recursos del sistema. Un ataque activo intenta alterar los recursos del sistema y su operación.

C. Servicios de Seguridad Informática

Los servicios de seguridad son definidos como un servicio de procesamiento o de comunicación el cual es provisto a un sistema para dar cierto tipo de protección a los recursos del sistema; los servicios de seguridad implementan políticas de seguridad que son implementadas por mecanismos de seguridad [5].

La recomendación X.800 de la *International Telecommunication Union* divide los servicios de seguridad en 5 grupos y 14 servicios específicos [7]:

1) Autenticación: Garantiza que las entidades en comunicación son las que claman ser.

- **Autenticación de entidad par:** Utilizada de forma asociada a la conexión lógica para proveer confianza en la identidad de las entidades interconectadas.
- **Autenticación de origen de datos:** En una transferencia sin conexión, provee la garantía que la fuente de la información recibida es la que clama ser.

2) Control de acceso: Es la prevención del uso no autorizado de un recurso.

3) Confidencialidad: Protección de datos de revelación no autorizada.

- **Confidencialidad de conexión:** La protección de los datos de usuario durante una conexión.
- **Confidencialidad sin conexión:** La protección de los datos de usuario en un bloque de datos independiente.
- **Confidencialidad selectiva de campos:** La confidencialidad de campos elegidos al interior de los datos de usuario en una conexión o en un bloque de datos independiente.
- **Confidencialidad del flujo de tráfico:** La protección de la información que puede ser derivada a partir de la observación del flujo de tráfico.

4) Integridad de datos: Consiste en garantizar que los datos recibidos son exactamente los datos enviados por una entidad autorizada.

- **Integridad de conexión con recuperación:** Provee integridad para toda la información de usuario en una conexión y detecta las modificaciones, inserciones o eliminaciones en una secuencia completa de datos e intenta la recuperación.
- **Integridad de conexión sin recuperación:** De forma similar que la anterior, pero sin opción de recuperación.
- **Integridad de conexión selectiva de campo:** Provee la integridad de campos selectos al interior de datos de usuario en un bloque transferidos en una conexión y permite detectar si determinados campos han sido modificados.
- **Integridad sin conexión:** Provee integridad sobre un bloque de datos independiente y sin conexión, puede tomar la forma de detección de modificación de datos.
- **Integridad sin conexión y selectiva de campo:** Proveen la integridad de campos selectos en un bloque independiente de datos sin conexión. Toma la forma de determinación de modificaciones sobre los campos selectos.

5) No repudio: Provee protección en contra de una de las partes involucrada en la comunicación, que niegue haber participado en parte o en toda la comunicación.

- **No repudio origen:** Prueba que el mensaje fue enviado por una entidad específica**.**
- **No repudio destino:** Prueba que el mensaje fue recibido por la parte específica.

D. Criptografía y algoritmos criptográficos

Criptografía es el estudio de las técnicas matemáticas relativas a los aspectos de la seguridad de la información tales como confidencialidad, integridad de datos, autenticidad y autenticación [8].

Un algoritmo criptográfico también llamado algoritmo de cifrado, es una función matemática utilizada para el cifrado y descifrado de un mensaje [9].

Un mensaje es texto plano, algunas veces llamado texto claro. El proceso de disfrazar un mensaje de tal forma que se oculte su esencia es denominado el "cifrado". Un mensaje cifrado se denomina texto cifrado. El proceso de transformar el texto cifrado en texto plano se le llama "descifrado".

El texto plano es denotado por M, para mensaje o por P para texto plano. Puede ser un flujo de bits, un archivo de texto, un mapa de bits, etc. El texto plano puede tener el propósito de ser transmitido o almacenado.

El texto cifrado es denotado por C y también está conformado por datos binarios. La función de cifrado E, opera sobre M y produce C, o en notación matemática:

$$E(M) = C$$

En el proceso inverso, la función de descifrado D opera en C para producir M:

$$D(C) = M$$

Los algoritmos criptográficos modernos utilizan llaves para realizar las operaciones de cifrado y descifrado. El rango de valores posibles de la llave es llamado espacio de llaves.

Un criptosistema es un algoritmo más todos los posibles valores de textos planos, textos cifrados y llaves.

Hay dos tipos generales de algoritmos basados en llaves: De llave simétrica y de llave pública. Los algoritmos de llave simétrica, algunas veces llamados algoritmos convencionales, son algoritmos en los cuales la llave de cifrado puede ser calculada a partir de llave de descifrado y viceversa. En los algoritmos simétricos, la llave de cifrado y descifrado es la misma y pueden dividirse en dos categorías, algoritmos de flujo y algoritmos de bloque. Los algoritmos de flujo operan el texto plano bit a bit mientras que los algoritmos de bloque operan el texto plano en grupos de bits denominados bloques.

Los algoritmos de llave pública, también llamados asimétricos, están diseñados de tal forma que la llave utilizada para cifrar es diferente de la llave utilizada para cifrar y la llave para descifrar no puede calcularse a partir de la llave de cifrado en un tiempo razonable. Los algoritmos son llamados "de llave pública" porque la llave de cifrado puede hacerse pública.

E. Primitivas y protocolos criptográficos

Las herramientas criptográficas o primitivas son utilizadas para proveer servicios a la Seguridad de la Información. Ejemplos de estas primitivas incluyen esquemas de cifrado, funciones de digestión de mensajes y esquemas de firma digital. En la Figura 1 se presenta un esquema de las diferentes primitivas criptográficas y sus agrupaciones.

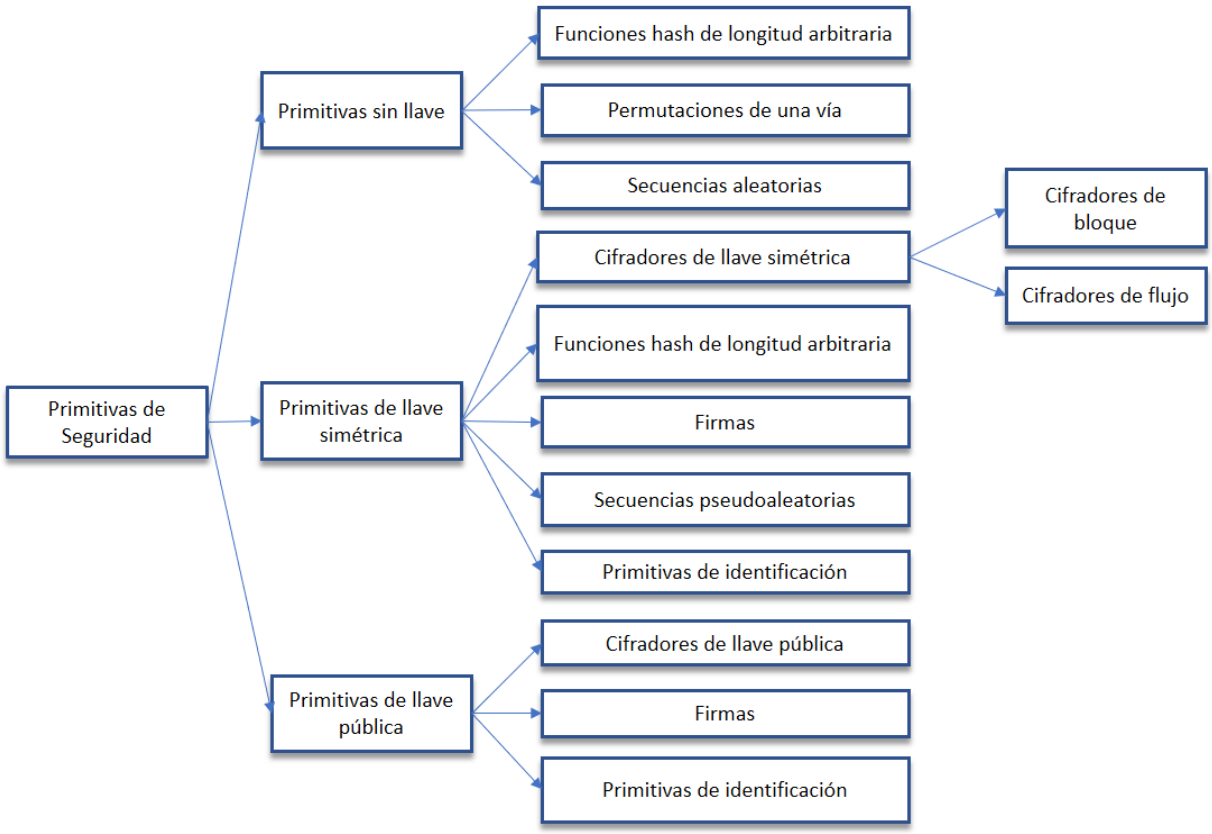

Figura 1. Taxonomía de las primitivas criptográficas [8].

Un protocolo es una serie de pasos, involucrando dos o más entidades, con el propósito de realizar una tarea. Un protocolo criptográfico es un protocolo que utiliza criptografía.

Una noción importante para la criptografía de llave pública es la de función de una vía. Las funciones de una vía son relativamente fáciles de calcular, pero difíciles de revertir, es decir, dado x es fácil calcular $f(x)$ pero dado $f(x)$ es difícil obtener x.

Una función de una vía con puerta trasera es una forma especial de función de una vía, con una puerta secreta. Es fácil calcular en una dirección, pero difícil de revertir a menos que se conozca el secreto.

Las funciones picadillo de una vía o de digestión de mensajes son otro importante bloque de construcción de protocolos. Una función picadillo es una función matemática o no, que toma un valor de longitud variable de entrada (llamada pre-imagen) y lo convierte a un valor de longitud fija llamado picadillo (*hash*), con el propósito de obtener una imagen de huella dactilar del valor de entrada. Una función picadillo de una vía trabaja en una sola dirección: Es fácil calcular el picadillo a partir de una pre-imagen, pero de difícil generar una pre-imagen que produce un valor de picadillo particular.

Un código de autenticación de mensaje (MAC) también conocido como código de autenticación de datos, es una función picadillo de una vía con la adición de una llave secreta. El valor picadillo es función tanto de la pre-imagen como de la llave secreta.

Una primitiva criptográfica que es fundamental en autenticación, autorización y no repudio es la firma digital [8]. El propósito de la firma digital es proveer los medios para una entidad de vincular su identidad a una pieza de información. El proceso de firmar implica transformar el mensaje y alguna información secreta en posesión de la entidad en una etiqueta llamada firma. A continuación, se describe su nomenclatura y disposición:

M es el conjunto de mensajes que pueden ser firmados.

S es el conjunto de elementos llamados firmas, posiblemente cadenas binarias de longitud fija.

S_A es una transformación desde un conjunto de mensajes M a un conjunto de firmas S y es llamada una transformación de firma para la entidad A. La transformación S_A es mantenida en secreto por la entidad A y será utilizada para crear firmas de mensajes desde M.

V_A es una transformación del conjunto $M\ x\ S$ al conjunto $\{verdadero, falso\}$. V_A es llamada una transformación de verificación para la firma de A, es conocida públicamente y es utilizada por otras entidades para verificar las firmas creadas por A.

Las transformaciones S_A y V_A proveen un esquema de firma digital para la entidad A.

F. Algoritmos utilizados en la implementación del pasaporte digital

La implementación del Pasaporte Digital se basa específicamente en tres algoritmos criptográficos: El algoritmo de llave simétrica AES para almacenamiento seguro, SHA-256 para digestión de mensajes y el algoritmo de llave pública RSA para firma digital simple y firmas agregadas basadas en RSA.

El Estándar de Cifrado Avanzado, AES por sus siglas en inglés, se encuentra especificado en la publicación FIPS-197 del Instituto Nacional de Estándares y Tecnología (NIST) [10]. El algoritmo AES es un algoritmo simétrico por bloques que puede ser utilizado para cifrar y descifrar información. El algoritmo AES es capaz de utilizar llaves de 128, 192, 256 bits.

Internamente, las operaciones del algoritmo AES son realizadas en un arreglo de *bytes* bidimensional llamado el Estado (*The State*). Este consiste de cuatro filas de *bytes*, cada una conteniendo Nb *bytes*, donde Nb es la longitud del bloque dividida entre 32.

Para el algoritmo AES, la longitud del bloque de entrada, la longitud del bloque de salida y el estado es de 128 bits.

Para el algoritmo AES, la longitud de la llave de cifrado K, es 128, 192 o 256 bits. El número de rondas a realizar durante la ejecución del algoritmo depende del tamaño de la llave, siendo 10 rondas para una llave de 128 bits, 12 rondas para una llave de 192 bits y 14 rondas para una llave de 256 bits.

Tanto para el cifrado como el descifrado utiliza una función de ronda que está compuesta de 4 transformaciones orientadas a *bytes*: 1) substitución de bytes utilizando una tabla de substitución llamada *S-box*, 2) Desplazamiento de filas de la matriz de Estado, 3) Mezcla de los datos en cada columna del Estado y 4) Agregación la llave de ronda al Estado.

Los algoritmos de digestión de mensajes SHA-1, SHA-224, SHA-256, SHA-512, y SHA-512/256, para el cálculo de representaciones condensadas de mensajes, se encuentran especificados en la publicación FIPS 180-4 del Instituto Nacional de Estándares y Tecnología (NIST). Los algoritmos especificados por este estándar son llamados seguros debido a que es computacionalmente irrealizable 1) encontrar un mensaje que corresponda a un valor picadillo 2) encontrar dos mensajes diferentes que produzcan el mismo valor de picadillo. Cualquier cambio en el mensaje producirá, con una muy alta probabilidad, un picadillo diferente. Estos algoritmos son iterativos y de una vía [11].

Cada algoritmo puede ser descrito en dos fases: pre procesamiento y computación de picadillo. El pre procesamiento involucra el relleno del mensaje, separación del mensaje rellenado en bloques de m-bits y la inicialización de los valores para el cálculo del picadillo.

RSA es un algoritmo de llave pública, es decir, posee la propiedad de que revelar públicamente la llave de cifrado no revela la correspondiente llave de descifrado. Con RSA, un mensaje es cifrado representándolo como un número M, elevando M a un exponente públicamente conocido e, y luego tomando el residuo cuando el resultado es dividido por un producto públicamente conocido, n, de dos números primos grandes p y q, que se mantienen en secreto. El descifrado es similar, con la diferencia que se utiliza el exponente secreto d, en dónde $e\,.d \equiv 1\,(mod(p-1).(q-1))$. La seguridad del sistema se basa en parte en la dificultad de factorizar el divisor publicado n [13].

El espacio de mensaje y de texto cifrado para RSA es $Z_n = \{0,1,2,\dots,n-1\}$ donde $n = pq$ el cuál es el producto de dos números primos distintos elegidos aleatoriamente. Puesto que la transformación de cifrado es una biyección, firmas digitales pueden ser creadas revirtiendo los roles de cifrado y descifrado [8].

En el esquema de firma digital utilizando RSA cada entidad A, crea una llave pública RSA y su correspondiente llave privada, siguiendo el procedimiento:

1. Genera dos números primos aleatorios de gran tamaño, p y q.

2. Calcula $n = pq$ y $\phi = (p-1)(1-1)$

3. Selecciona un entero aleatorio e, $1 < e < \phi$ tal que $gcd(e,\phi) = 1$.

4. Utiliza el algoritmo extendido de Euclides, para calcular un entero único d, $1 < d < \phi$, tal que $ed \equiv 1\,(mod\ \phi)$.

5. La llave pública de A es (n,e) y su llave privada es (n,d).

La entidad A firma un mensaje m y cualquier entidad B puede verificar la firma de A. En este proceso se requiere el uso de una función picadillo para obtener el digesto del mensaje y producir la firma para el mismo, con lo cual se garantiza la integridad del mensaje [14].

Para firmar un mensaje m, la entidad A debe seguir el siguiente procedimiento:

1. Calcular $h = H(m)$ donde H es la función picadillo.

2. Calcular $s = h^d\ mod\ n$.

3. La firma de A para el mensaje m es s.

Para verificar la firma s de A, la entidad B debe seguir el siguiente procedimiento:

1. Obtener la llave pública de A (n,e).

2. Calcular $h' = H(m)$
3. Calcular $h = s^e \bmod n$
4. Verificar que $h = h'$, sino rechaza la firma s.

G. Protocolos Intermedios

1) Servicios de estampa de tiempo

Los servicios de estampa de tiempo proveen a los usuarios un recibo con fecha al momento de presentar un documento, el cual puede ser verificado por otros, para confirmar la existencia del documento en una fecha previa a la fecha del recibo [8].

Inicialmente, se obtiene el digesto del mensaje original, el digesto es transmitido a una autoridad de estampa de tiempo, el cual concatena el digesto a una estampa de tiempo en texto plano. La autoridad obtiene el digesto de la cadena resultante y lo firma digitalmente. El texto cifrado resultante representa la estampa de tiempo de confianza, la cual se retorna junto a la estampa de tiempo en texto plano al solicitante [15].

2) Firmas agregadas

Un esquema de firma digital agregada es una firma digital que soporta agregación: Dadas n firmas en n mensajes distintos de n usuarios distintos, es posible agregar estas firmas en una sola firma corta. Las firmas agregadas son útiles para reducir el tamaño de las cadenas de certificación [16].

3) Firmas agregadas secuenciales

En un esquema de firmas agregadas secuencial, la agregación de las firmas puede darse solamente en el proceso de firma. Cada firmante en orden agrega su firma a la firma agregada actual [17].

Operacionalmente, la agregación secuencial funciona de la forma siguiente: El usuario 1 firma M_1 para obtener σ_1; usuario 2 combina σ_1 y M_2 para obtener σ_2; y así. La firma final σ_n enlaza al usuario i a M_i para todas $i = 1, \dots, n$.

IV. FUNCIONALIDAD DEL PASAPORTE DIGITAL

El esquema criptográfico del pasaporte digital se diseña a partir de los procesos bien definidos y establecidos actualmente para el pasaporte ordinario en papel. La diferencia principal es que las interacciones son vías electrónicas sobre objetos digitales. Estas interacciones se presentan en la Figura 2.

A. Codificación de Entidades

Las entidades participantes del esquema criptográfico se codifican de acuerdo a la tabla 1.

Tabla 1. Codificación de entidades participantes en el esquema de seguridad del pasaporte digital.

Entidad	**Código**	**Observación**
Usuario del Pasaporte	U	Incluye información completa de los datos de usuario.
Dirección General de Migración y Extranjería	ME	Entidad encargada de la emisión de documentos de viaje.
Embajada Extranjera(País)	$EE(País)$	País, código de dos letras del país al que pertenece la Embajada, ej. US, BR, IN, SV
Control Migratorio (País)	$CM(País)$	País, código de dos letras del país al que pertenece la Embajada, ej. US, BR, IN, SV
Autoridad de Estampa de Tiempo	AT	
Pasaporte	P	
Visa(País)	$V(País)$	País, código de dos letras del país al que pertenece la Embajada, ej. US, BR, IN, SV
Control Migratorio (País) Entrada	$CM(País)i$	Representa el sello de entrada en el pasaporte (in)
Control Migratorio (País) Salida	$CM(País)o$	Representa el sello de entrada en el pasaporte (out)

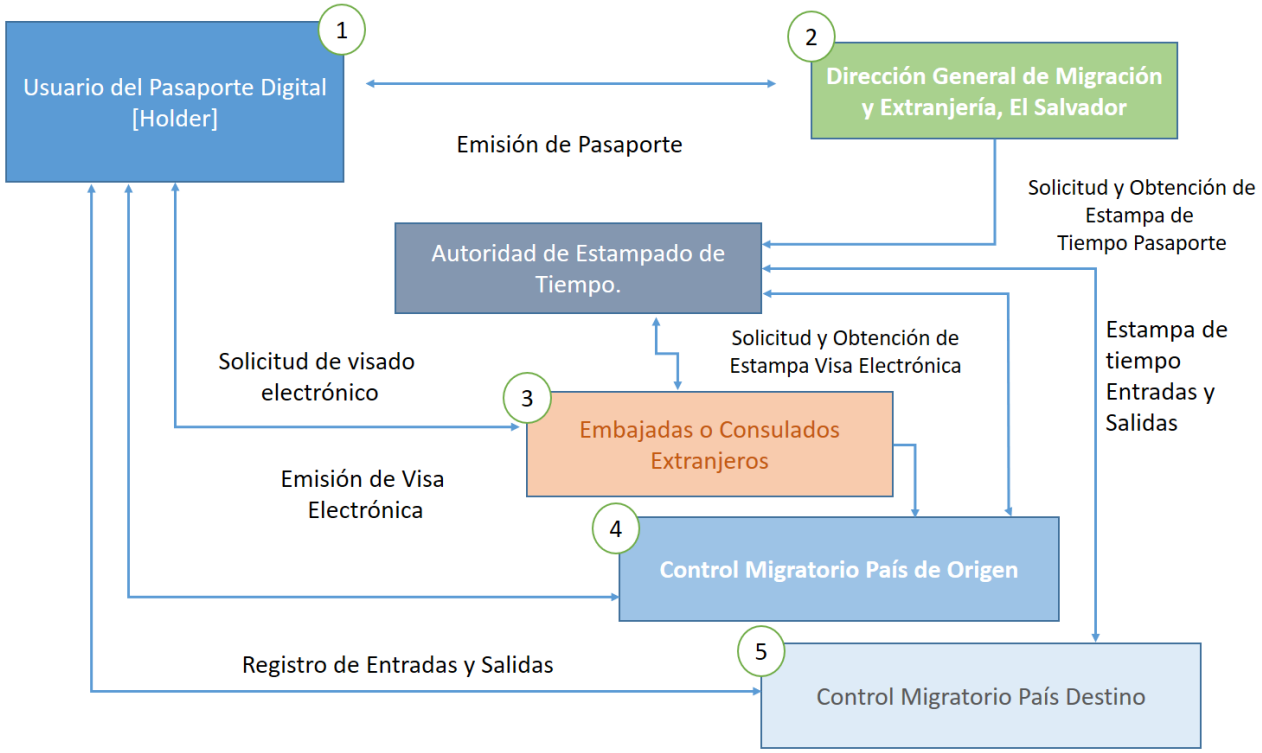

Figura 2. Entidades e intercambio de mensajes en el esquema de seguridad del pasaporte digital.

Cada entidad participante del esquema de seguridad posee un par de llaves para firma digital, estas llaves se codifican y se muestran en la tabla 2.

Tabla 2. Codificación de llaves para firma digital

Código de Entidad	**Llave Pública RSA**	**Llave Privada RSA**
U - Usuario	$K_U = \{e_U, n_U\}$	$D_U = \{d_U, n_U\}$
ME – Dirección General de Migración y Extranjería	$K_{ME} = \{e_{ME}, n_{ME}\}$	$D_{ME} = \{d_{ME}, n_{ME}\}$
$EE(País)$ – Embajada Extranjera	$K_{EE(País)} = \{e_{EE(País)}, n_{EE(País)}\}$	$D_{EE(País)} = \{d_{EE(País)}, n_{EE(País)}\}$
$CM(País)$ – Control Migratorio	$K_{CM(País)} = \{e_{CM(País)}, n_{CM(País)}\}$	$D_{CM(País)} = \{d_{CM(País)}, n_{CM(País)}\}$
AT – Autoridad de Estampa de Tiempo.	$K_{AT} = \{e_{AT}, n_{AT}\}$	$D_{AT} = \{d_{AT}, n_{AT}\}$

B. Esquema del sistema criptográfico

El esquema propuesto cuenta con tres fases, las cuales se presentan a continuación:

1) Solicitud y emisión de Pasaporte Electrónico ante la Dirección General de Migración y Extranjería de El Salvador

Para la solicitud del pasaporte electrónico por parte de un usuario es requerida la generación de su respectivo par de llaves RSA en el dispositivo que utilizará para portar su pasaporte electrónico.

En la fase de solicitud y emisión participan el Usuario, la Dirección General de Migración y Extranjería y la Autoridad de Estampa de Tiempo. La figura 3 describe la funcionalidad de esta fase.

2) Solicitud y emisión de Visa Electrónica ante embajadas y consulados extranjeros

En el caso de los países que exigen visado previo a los salvadoreños para ingresar a sus países se considera la solicitud y emisión de una visa electrónica. Se debe considerar que, aunque el resultado de la verificación del pasaporte y la estampa de tiempo sean satisfactorios, cada país es soberano y a través de sus embajadas y consulados ejerce el poder de otorgar visa o no a un ciudadano salvadoreño. La Figura 4 describe la funcionalidad de la solicitud de visa electrónica.

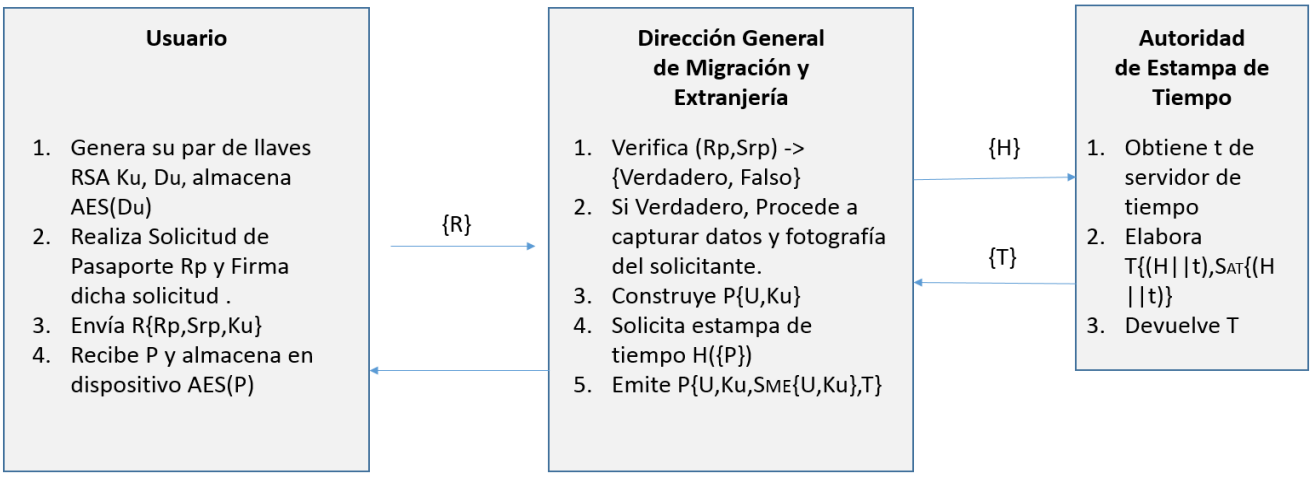

Figura 3. Funcionalidad de Solicitud y Emisión de Pasaporte Electrónico.

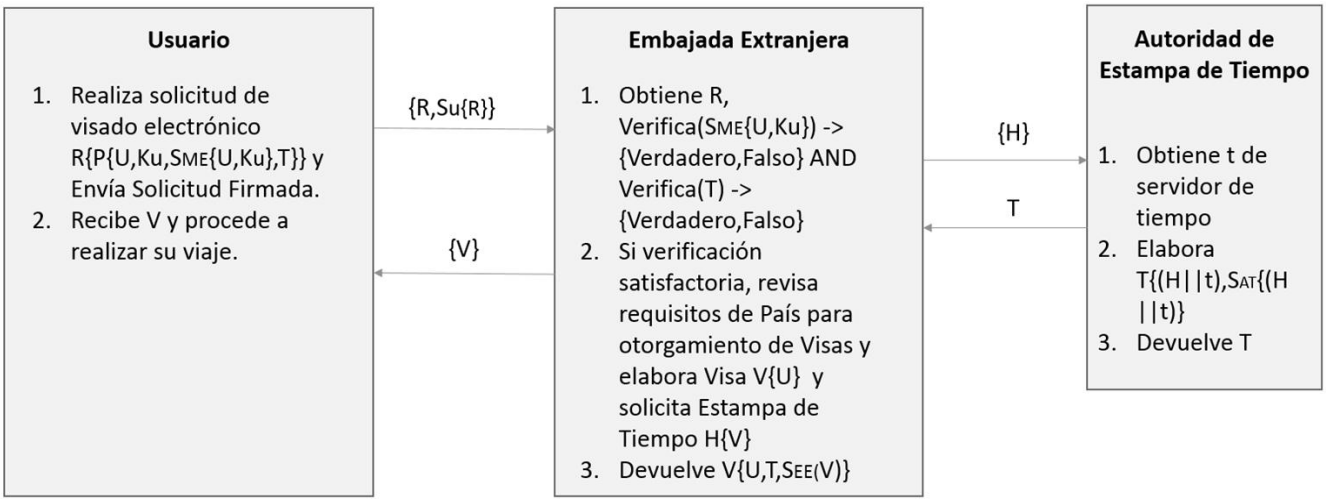

Figura 4. Funcionalidad de Solicitud y Emisión de Visa Electrónica.

3) Registro de entradas y salidas en los controles migratorios del país de origen y países destino

Al momento de pasar por uno de los controles migratorios, sea país de origen o país de destino, el usuario deberá presentar el dispositivo donde posee el pasaporte digital para su verificación y registro de la entrada o salida del país según sea el caso. En las Figuras 5 y 6 se muestra el funcionamiento del proceso. En los controles migratorios las firmas se van agregando según la ruta que siga el portador del pasaporte digital.

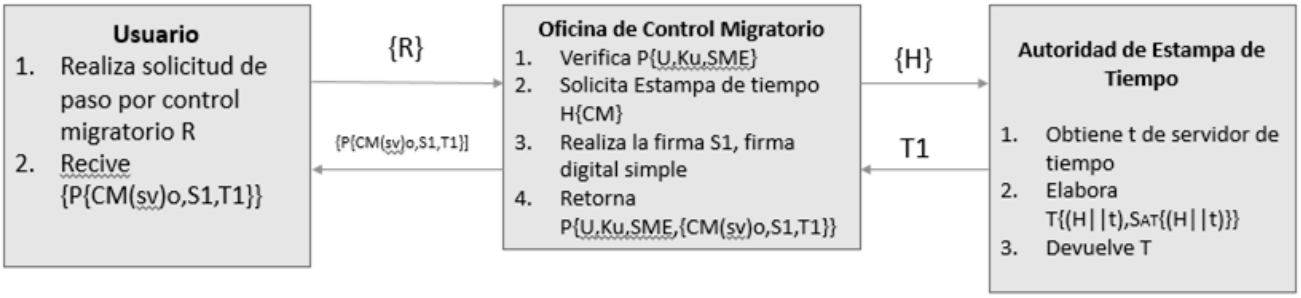

Figura 5 Control Migratorio, país de origen

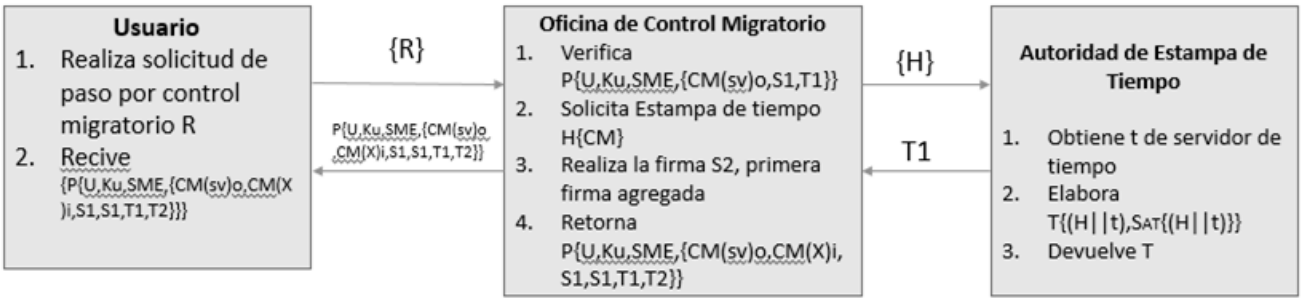

Figura 6. Control migratorio, país de destino.

C. Especificación formal del esquema y protocolos participantes

La especificación formal se realiza en términos matemáticos y se divide en tres fases.

1. *Solicitud y emisión de Pasaporte Electrónico ante la Dirección General de Migración y Extranjería de El Salvador*

Para dar inicio, el usuario genera su par de llaves RSA en su dispositivo móvil obteniendo $K_U = \{e_u, n_u\}$, $D_U = \{d_U, n_u\}$, almacena de forma segura D_U utilizando AES en modo de cifrado $AESc(D_U)$, el usuario inicia el protocolo generando una solicitud de pasaporte R conteniendo el número de solicitud de pasaporte R_p asignado por ME y lo firma:

$$SR_p = H(R_p)d_u \bmod n_u$$

La solicitud de pasaporte es dada por $R = \{R_p, SR_p, K_u\}$ y es recibida por ME para su verificación. Nótese que se envía la llave pública K_u a ME para poder validar la firma del usuario:

$$Verifica(SR_p) = Si\ {SR_p}^{eu} \bmod n_u\ es\ igual\ H(R_p)$$

$$entonces\ "Verdadero"\ sino\ "Falso"$$

Si el resultado de la verificación es "$Verdadero$" se procede a la captura de información del solicitante y toma de fotografía. Con esta información se construye el pasaporte $P\{U, Ku\}$ siendo U la colección de datos de identidad del usuario y su fotografía. La firma digital del usuario se incluye en el cuerpo del pasaporte para certificarse como parte del proceso de emisión del pasaporte. ME firma P utilizando su llave privada y sirviendo como autoridad certificadora de confianza:

$$S_{ME} = H(P\{U, Ku\})^{dME} \bmod n_{ME}$$

ME obtiene el *hash* h del pasaporte y solicita la estampa de tiempo ante la Autoridad de Estampa de tiempo:

$$h = H(P\{U, K_u\})$$

La autoridad de estampa de tiempo obtiene el tiempo t del servidor de tiempo, elabora y devuelve T:

$$T = \{S_{AT} = H(h||t)^{DAT} \bmod n_{AT}, t\}$$

ME obtiene T de la Autoridad de Estampa de tiempo y genera el Pasaporte conteniendo $\{U, K_u, S_{ME}, T\}$ y lo entrega al solicitante para su almacenamiento cifrado en el dispositivo:

$$AESc(P\{U, K_u, S_{ME}, T\})$$

2. Solicitud y emisión de Visa Electrónica ante embajadas y consulados extranjeros

Para la solicitud de una Visa Electrónica ante la Embajada de un País extranjero el usuario del pasaporte lo extrae del almacenamiento seguro descifrando con AES en modo descifrado.

$$AESd(P_c\{U, K_u, S_{ME}, T\})$$

De forma similar a la solicitud de pasaporte obtiene un número de solicitud de visa R_v y firma R_v:

$$SR_v = H(R_v)^{du} \bmod n_u$$

Usuario envía $R\{R_v, SR_v, P\{U, K_u, S_{ME}, T\}\}$ para verificación por parte de embajada extranjera. Esta verificación comienza con el pasaporte digital:

$$Verifica(S_{ME}) = Si\ {S_{ME}}^{eME} \bmod n_{ME}\ es\ igual\ a\ H(U, K_u)\ entonces\ \text{“}Verdadero\text{”}, si\ no, \text{“}Falso\text{”}$$

Si el resultado es $Verdadero$ se Verifica la estampa de tiempo $T\{S_{AT}, t\}$:

$$Verifica(T) = Si\ {S_{AT}}^{eAT} \bmod n_{AT}\ es\ igual\ a\ H(H(U, K_u)\ ||\ t) entonces\ \text{“}Verdadero\text{”}, si\ no, \text{“}Falso\text{”}$$

Si el resultado es $Verdadero$ se procede con la verificación de la solicitud de visa:

$$Verifica(SR_v) = Si\ {SR_v}^{eu} \bmod n_u\ es\ igual\ a\ H(R_v)\ entonces\ \text{“}Verdadero\text{”}, si\ no, \text{“}Falso\text{”}$$

Luego de realizar estas verificaciones, realiza la emisión de la Visa Electrónica de acuerdo a los requerimientos y legislaciones del país emisor, en todo caso esta emisión suele ir acompañada por una captura de datos, fotografía, asignación de tipo de visa, número de entradas, etc. Estos datos se almacenan en la Visa Electrónica V. La embajada obtiene el *hash* h de la Visa y solicita la estampa de tiempo de ante la Autoridad de Estampa de tiempo:

$$h = H(V)$$

La autoridad de estampa de tiempo obtiene el tiempo t del servidor de tiempo, elabora y devuelve T:

$$T = \{S_{AT} = H(h||t)^{dAT} \bmod n_{AT}, t\}$$

La Embajada Extranjera firma la Visa Electrónica:

$$V_{EE(País)} = V^{dEE(País)} \bmod n_{EE(País)}$$

Entrega al usuario solicitante:

$$V_{(país)}\{V, V_{EE(país)}, T\}.$$

El usuario solicitante recibe:

$$V_{(país)}\{V, V_{EE(país)}, T\}$$

y lo almacena de forma segura en su dispositivo:

$$AESc(P\{U, K_u, S_{ME}, T, \{(país)\{V, V_{EE(pais)}, T\}\}\})$$

3. Registro de salida en Control Migratorio

Para la salida del país a través de un control migratorio, el usuario del pasaporte lo extrae del almacenamiento seguro descifrando con AES en modo descifrado.

$$AESd(Pc\{U, K_u, S_{ME}, T\})$$

La autoridad migratoria verifica el pasaporte digital:

$$Verifica(S_{ME}) = Si\ {S_{ME}}^{eME}\ mod\ n_{ME}\ es\ igual\ a\ H(U, K_u)\ entonces\ \text{“}Verdadero\text{”}, si\ no, \text{“}Falso\text{”}$$

Si el resultado es $Verdadero$ se Verifica la estampa de tiempo $T\{S_{AT},\ t\}$:

$$Verifica(T) = Si\ {S_{AT}}^{eAT}\ mod\ n_{AT}\ es\ igual\ a\ H(H(U, K_u)\ ||\ t)\ entonces\ \text{“}Verdadero\text{”}, si\ no, \text{“}Falso\text{”}$$

Si el resultado es $Verdadero$ se procede con la elaboración del registro de salida $CM(SV)o$ y se solicita la estampa de tiempo:

$$h\ =\ H(CM(SV)o)$$

La autoridad de estampa de tiempo obtiene el tiempo t del servidor de tiempo, elabora y devuelve T:

$$T\ =\ \{S_{AT}\ =\ H(h||t)^{dAT}\ mod\ n_{AT}\ , t\}$$

La autoridad migratoria realiza firma digital del registro migratorio de salida:

$$S1\ =\ H(\{CM(SV)o\ ||\ T1\})^{dCM(SV)}\ mod\ n_{CM(SV)}$$

El usuario solicitante recibe $\{CM(sv)o, S1, T1\}$ y lo almacena de forma segura en su dispositivo:

$$AESc(P\{U, K_u, S_{ME}, \{CM(sv)o, S1, T1\}\})$$

4. Registro de entrada en Control Migratorio

Para el ingreso a un país extranjero a través de un control migratorio, el usuario del pasaporte lo extrae del almacenamiento seguro descifrando con AES en modo descifrado.

$$AESd(Pc\{U, K_u, S_{ME}, T\ \})$$

La autoridad migratoria verifica el pasaporte digital:

$$Verifica(S_{ME}) = Si\ {S_{ME}}^{eME} mod\ n_{ME}\ es\ igual\ a\ H(U, K_u)\ entonces\ \text{“}Verdadero\text{”}, si\ no, \text{“}Falso\text{”}$$

Si el resultado es $Verdadero$ se Verifica la estampa de tiempo $T\{SAT,\ t\}$:

$$Verifica(T) = Si\ {S_{AT}}^{eAT}\ mod\ n_{AT}\ es\ igual\ a\ H(H(U, K_u)\ ||\ t)\ entonces\ \text{“}Verdadero\text{”}, si\ no, \text{“}Falso\text{”}$$

La autoridad migratoria realiza la verificación del control de salida, a este nivel del protocolo, aún es verificación de firma digital simple:

$$Verifica(CM(SV)o, S1, T1) = Si\ {S_{cm(sv)}}^{ecm(sv)} mod\ n_{cm(sv)}\ es\ igual\ a\ H(CM(SV)o, S1, T1)\ entonces\ \text{“}Verdadero\text{”}, si\ no, \text{“}Falso\text{”}$$

En caso de que el resultado de la verificación sea $Verdadero$ se solicita estampa de tiempo para el control migratorio de ingreso $CM(X)i$ donde X es el país al que se está ingresando:

$$h\ =\ H(CM(X)i)$$

La autoridad de estampa de tiempo obtiene el tiempo t del servidor de tiempo, elabora y devuelve $T2$:

$$T2\ =\ \{S_{AT}\ =\ H(h||t)^{dAT}\ mod\ n_{AT}\ , t\}$$

Una vez obtenida la estampa de tiempo para el ingreso al país extranjero se procede a agregar la firma digital como primera firma agregada:

$$S2\ =\ (H\ (CM(SV)o\ ||\ CM(X)i\ ||\ T1\ ||\ T2) + S1)^{\ d2CM(X)}\ mod\ n2_{CM(X)}$$

El usuario solicitante recibe:

$$\{CM(sv)o, CM(X)i, S1, S2, T1, T2\}$$

y lo almacena de forma segura en su dispositivo:

$$AESc(P\{U, K_u, S_{ME}, \{CM(sv)o, CM(X)i, S1, S2, T1, T2\}\})$$

D. Análisis de la seguridad

Como parte de los requerimientos de seguridad, el usuario posee un par de llaves, una pública y una privada, ésta última es conocida solo por el usuario.

El usuario generará las llaves desde su teléfono utilizando RSA, el cual basa su seguridad en el problema de factorización de números enteros. La llave pública generada se comparte posteriormente con ME al enviar la solicitud.

Se considera que el esquema planteado para el pasaporte digital cumple con las características fundamentales para su uso como un documento de viaje. Estas características se detallan a continuación:

- *Integridad de información*

El pasaporte electrónico posee mecanismos de verificación de la integridad de los datos contenidos en él como la verificación de la firma de la entidad emisora del pasaporte ME y la obtención de la estampa de tiempo al momento de emitir el pasaporte. Lo anterior garantiza que los datos son válidos ya que son certificados por ME.

Las firmas agregadas hacen posible validar la integridad de los controles migratorios garantizando que el registro de salidas y entradas de un usuario no pueda ser alterado ni modificado; mientras que las firmas digitales también hacen posible validar información de las visas de cada país.

- *Almacenamiento Seguro*

Los datos del pasaporte, visas y controles migratorios se almacenan de forma segura en el dispositivo utilizando el cifrado de llave simétrica por bloques AES con llaves de 128 bits utilizando un mensaje elegido por el usuario como llave.

- *Autenticación de usuario*

El pasaporte electrónico contiene toda la información del usuario: datos personales, número único de identidad, nacionalidad, etc. Además, contiene la llave pública del mismo junto con el certificado de la entidad emisora del documento (ME).

Esto es posible ya que el proceso se hace de manera presencial y se envían los datos de la solicitud firmados por el usuario y se incluye la llave pública del usuario para que la entidad emisora la pueda certificar ($R\{Rp, Srp, Ku\}$).

- *Unicidad*

La entidad emisora del pasaporte ME asigna un número único de identidad y le agrega una estampa de tiempo que solicita a la autoridad de estampa de tiempo AT. El pasaporte estará compuesto de la siguiente forma:

$$P\{U, K_u, S_{ME}(U, K_u), T\}$$

- *Trazabilidad y disponibilidad*

El pasaporte electrónico permite trazar todos los movimientos del usuario al salir o entrar de un país determinado. Esto es posible gracias al uso de firmas agregadas en donde cada uno de los controles migratorios CM agrega su firma, mensaje y estampa de tiempo de modo que queda registrado.

Este registro queda almacenado en el dispositivo de manera cifrada permitiendo que los datos estén disponibles y accesibles en cualquier control migratorio de cada país $CM(país)$.

- *No repudio*

Gracias a la capacidad de firma del usuario desde su dispositivo, el sistema cuenta con el servicio de no repudio de las solicitudes y movimientos realizados con el pasaporte electrónico.

V. IMPLEMENTACIÓN Y PRUEBAS

La implementación del Pasaporte Digital requirió la definición y creación de varias herramientas, así como la configuración de diferentes servicios para las herramientas desarrolladas y la aplicación móvil del Pasaporte Digital. La arquitectura de estas herramientas y servicios que componen el Sistema de Pasaporte Digital se muestra en la Figura 7.

Como se observa en la Figura 7, parte del funcionamiento del pasaporte digital requiere la configuración de un servicio de envío de mensajes SMS y la configuración de un equipo a funcionar como Autoridad de Estampa de Tiempo, este último desarrollado para trabajar de forma compatible con

el resto de aplicaciones que participan en el protocolo.

La Dirección General de Migración y Extranjería contará con una aplicación para la generación de las llaves, y el usuario contará con una App que se instalará en su Smartphone la cual servirá para almacenar el Pasaporte Digital (una App es una aplicación de software que se instala en un dispositivo móvil, para ayudar al usuario con una tarea específica).

Para la generación de llaves RSA (Figura 8) se elaboró un programa que permite indicar el nombre de la entidad y la ubicación donde se desea almacenar la llave privada (d, n). La llave pública (e, n) se almacena en un servidor que puede ser accedido por el resto de entidades durante la ejecución del protocolo. El programa almacena la llave cifrada (Figura 9) utilizando el algoritmo AES-128, por lo que solicita la definición de una palabra clave y finaliza con la generación de las llaves (Figura 10).

La generación de las llaves de entidades se realiza siguiendo la nomenclatura de codificación de entidades (tabla 1).

La llave privada de la entidad se almacena como una cadena en formato $\{'d','n'\}$ la cual se cifra antes de ser almacenada.

El programa de generación de llaves realiza la firma de la llave pública de cada entidad con la respectiva llave privada.

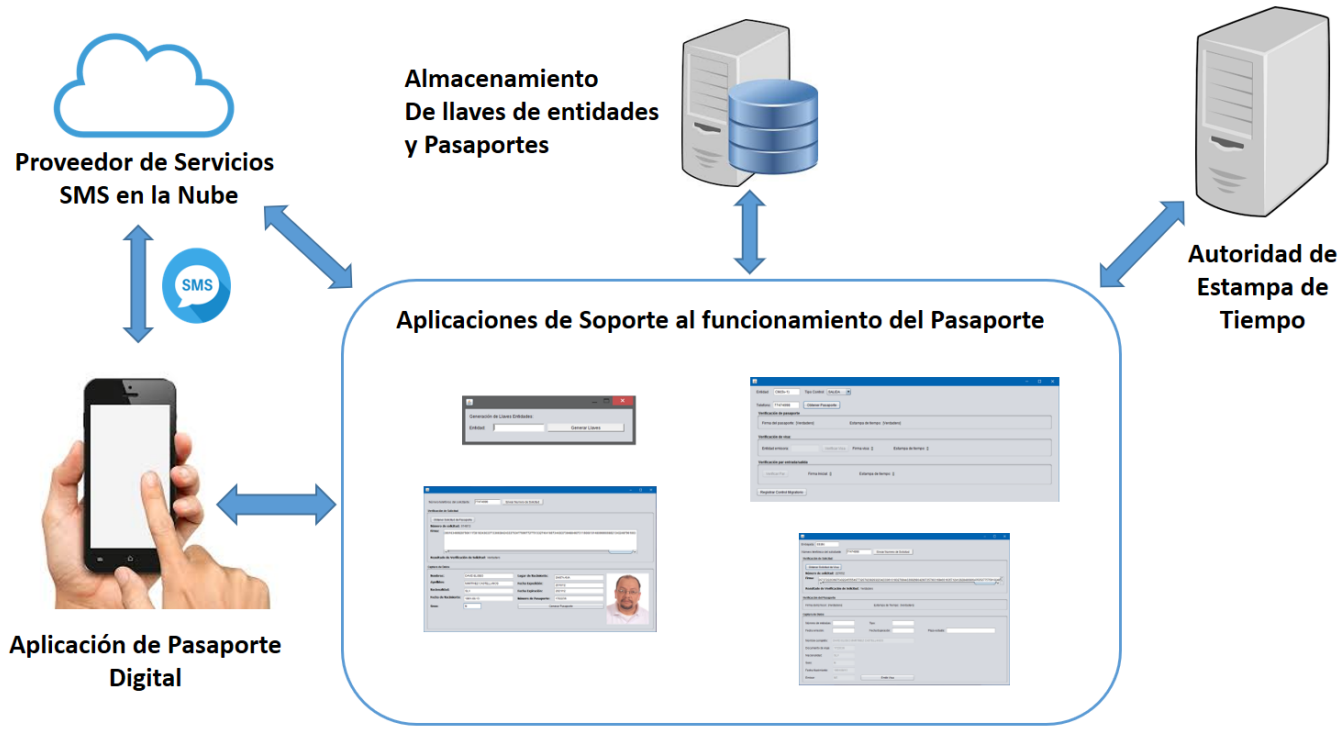

Figura 7. Arquitectura del prototipo desarrollado.

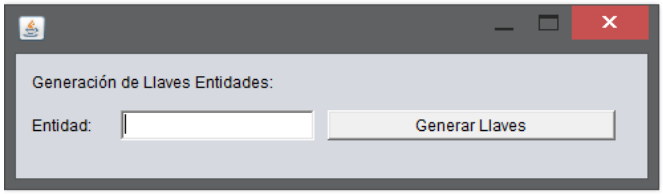

Figura 8. Generación de llaves entidades.

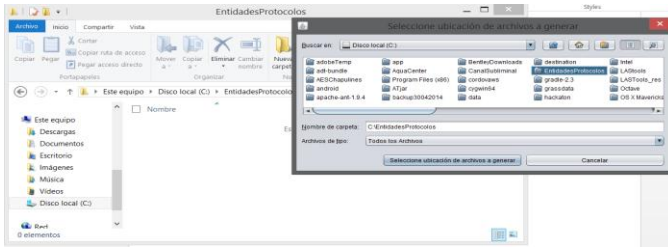

Figura 9. Almacenamiento de llaves por entidad

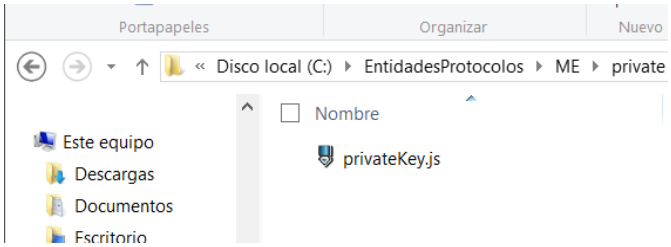

Figura 10. Resultado de la generación de llaves

A. Solicitud de Pasaporte

La solicitud de pasaporte comienza cuando el usuario solicitante proporciona su número celular al oficial de migración encargado de la emisión del pasaporte, quien utiliza la aplicación de emisión de pasaporte electrónico para enviar el código de solicitud al teléfono del solicitante por medio de un mensaje SMS (Figura 11) para validar su identidad (el código de solicitud se usará para iniciar el proceso).

Es importante recalcar que el proceso de solicitud de pasaporte se hará de manera presencial por la persona que lo solicita, de esa forma se certifica su identidad.

Luego de ingresar el código (Figura 12) debe presionar el botón "Procesar Solicitud de Pasaporte". La Solicitud de pasaporte implica la generación de llaves RSA en el dispositivo y la firma del código recibido para proceder a la captura de datos del solicitante.

El color de fondo de la aplicación de pasaporte digital, obedece el color oficial de los pasaportes ordinarios de El Salvador y Centroamérica.

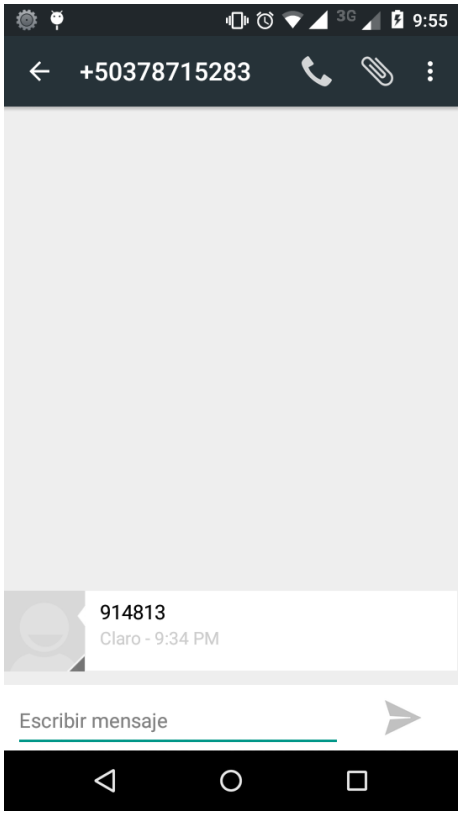

Figura 11. El usuario recibe código de solicitud vía SMS.

Luego de que la solicitud ha sido enviada desde el dispositivo, el oficial de migración procede a verificar por medio de la aplicación (Figura 13).

Una vez que se ha verificado la firma del código de solicitud, se procede a la captura de datos del usuario (Figura 14).

Al presionar el botón "Generar Pasaporte", el programa solicita la estampa de tiempo a la entidad autoridad de estampa de tiempo, por lo que se genera un *hash* de los datos y de la fotografía en un solo objeto. Cabe mencionar que la autoridad de estampa de tiempo se implementó en la forma de un servicio web.

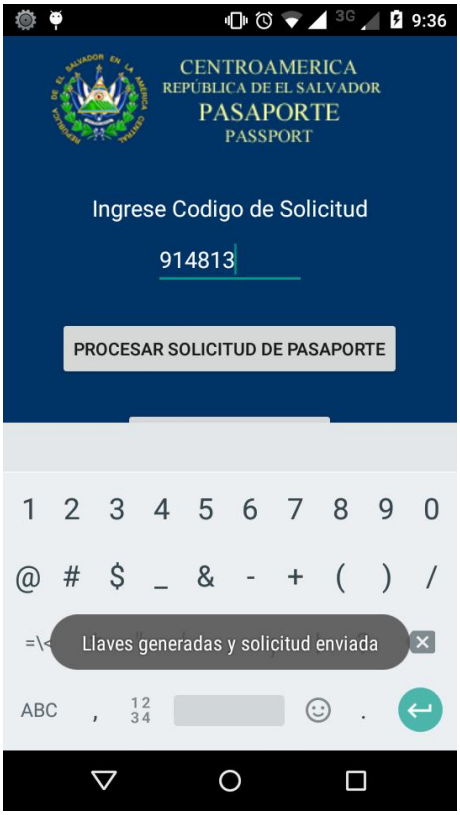

Figura 12. Ingreso de código de verificación.

Al momento de presionar "Generar Pasaporte" se solicita la clave o frase clave para poder descifrar la llave secreta de la entidad ME para poder firmar el pasaporte que será emitido. Este procedimiento lo hace el representante de la entidad ME.

Una vez que el pasaporte ha sido firmado, este es recuperado en el dispositivo del usuario mediante el uso del botón etiquetado "Obtener Pasaporte"; el pasaporte es cargado en el celular y almacenado en una cadena cifrada con AES-128 incluyendo firmas y fotografía. La visualización del pasaporte en el dispositivo móvil se muestra en la figura 15.

El pasaporte contiene la estampa de tiempo y la firma digital del emisor en formato de enteros RSA. Estos se muestran en la Figura 16.

Internamente el pasaporte digital posee una estructura definida como un objeto *JSON* por su facilidad de uso en diferentes plataformas de programación, además de ser un formato fácil de comprender. Este objeto *JSON* se muestra en la Figura 17.

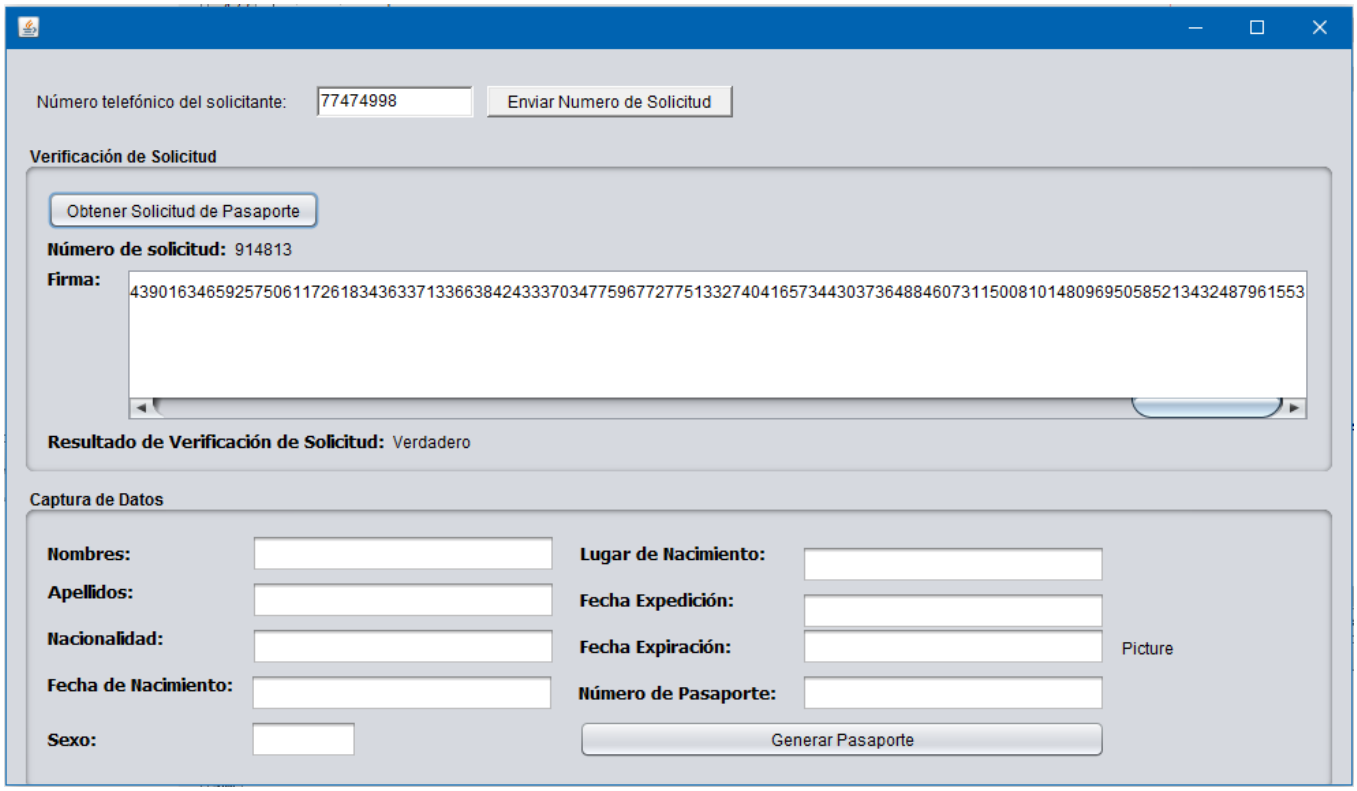

Figura 13. Verificación de solicitud de pasaporte.

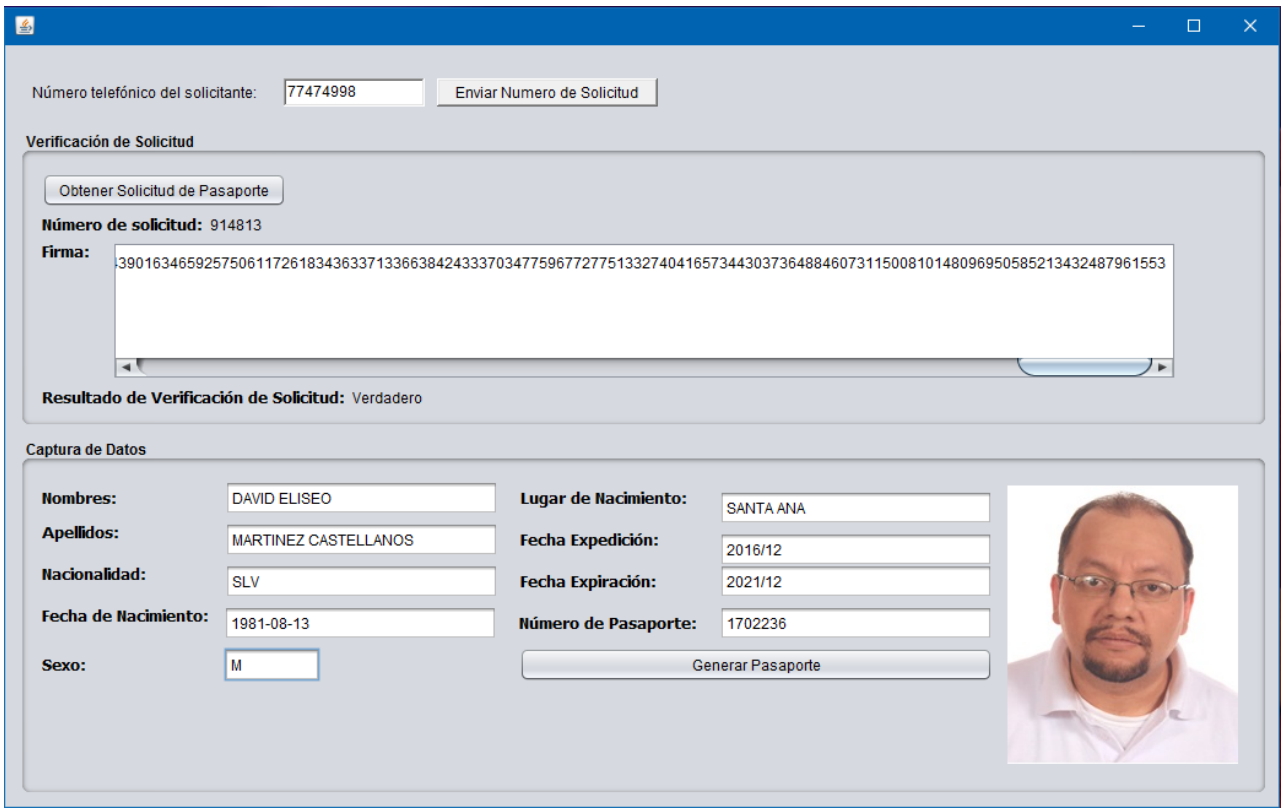

Figura 14. Captura de datos incluye una fotografía.

Figura 15. Página de datos personales.

Figura 16. Estampa de tiempo y Firma digital del pasaporte.

La firma digital del pasaporte por parte de Migración y Extranjería se realiza sobre la sección de datos personales incluyendo la fotografía del propietario del pasaporte digital. Posee una sección con el detalle de la estampa de tiempo, así como secciones de visas y controles migratorios, que a su vez son arreglos de objetos "visas" y "controles migratorios". La fotografía del Usuario del Pasaporte Digital se almacena como una cadena de texto codificado BASE64, de esta forma, el pasaporte digital se almacena como un solo elemento el cual es sujeto a digestión de mensaje, firma digital y almacenamiento cifrado.

B. Visa Electrónica

Para la solicitud de visa electrónica se creó un proceso similar. Se creó un formulario (Figura 18) diseñado para ser utilizado con las diferentes Embajadas creadas para la prueba de protocolo. Adicionalmente, posee una sección que muestra los resultados de las verificaciones tanto de la firma del pasaporte como de su estampa de tiempo. En este formulario, si el resultado de la verificación es *Verdadero*, se cargan automáticamente los datos personales del propietario del pasaporte.

Como se muestra en la Figura 19, se deben completar los campos de información de la visa a emitir, entre los que se encuentran: Número de entradas, tipo de visa, fecha de emisión, fecha de expiración y plazo de estadía. Para la selección de estos campos se consideraron los formatos de visas de Brasil, Estados Unidos e India.

El proceso de solicitud de visa es similar al de solicitud del pasaporte ya que el usuario recibe un código en su celular el cual ingresa en la pantalla de solicitud. Primero ingresa al menú de la aplicación haciendo uso del menú que se muestra en la Figura 20. Al ingresar a "Solicitud de Visa", se muestra la actividad de la Figura 21.


```
{ ⊟
  "userdata":{ ⊟
    "nombres":"DAVID ELISEO",
    "apellidos":"MARTINEZ CASTELLANOS",
    "nacionalidad":"SLV",
    "fechanac":"1981-08-13",
    "sexo":"M",
    "lnac":"SANTA ANA",
    "fechaexpedicion":"2016/12",
    "fechaexpiracion":"2021/12",
    "numeropass":"1702236",
    "picture":"/9j/4AAQSkZJRgABAgAAAQABAAD2wBDAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEw8UHRofHh0aHBwgJC4nICIsIxwcKDcpLDAxNDQ0Hyc5PTgyPC",
    "e":"65537",
    "n":"190917344172085603323169254519730954478286262506443875254742821735109586975650685901640289831476903423931044560882447355152318027
  },
  "T":{ ⊟
    "t":"Sun Dec 04 21:45:53 CST 2016",
    "r":"8eb9d73b9edd76d8d4dd77246a4dbd7235adfc26f9cf51582e60dea533cff918|Sun Dec 04 21:45:53 CST 2016",
    "s":"252036996461335816163606316177143984350844045001773193529805778205306940114446268821630717290470370439993064541055147157780223777
  },
  "userdata_signature":"253216260183518851984372604862639985202331878783524295057487910135553221468214391255673155131066737247297618374671
  "visas":[ ⊟

  ],
  "controles":[ ⊟

  ]
}
```


Figura 17. Estructura interna del Pasaporte Digital.

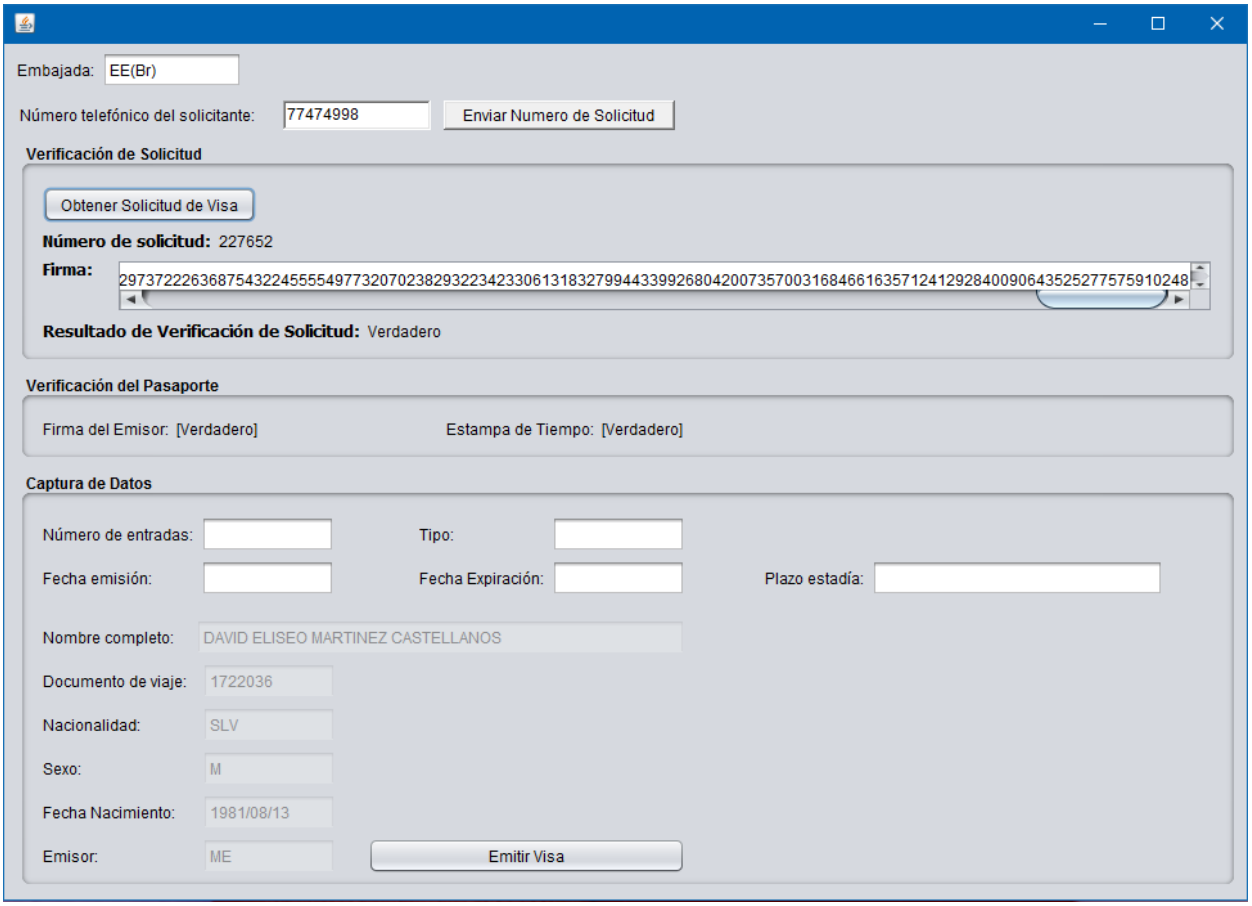

Figura 18. Solicitud de Visa Electrónica ante embajada país extranjero.

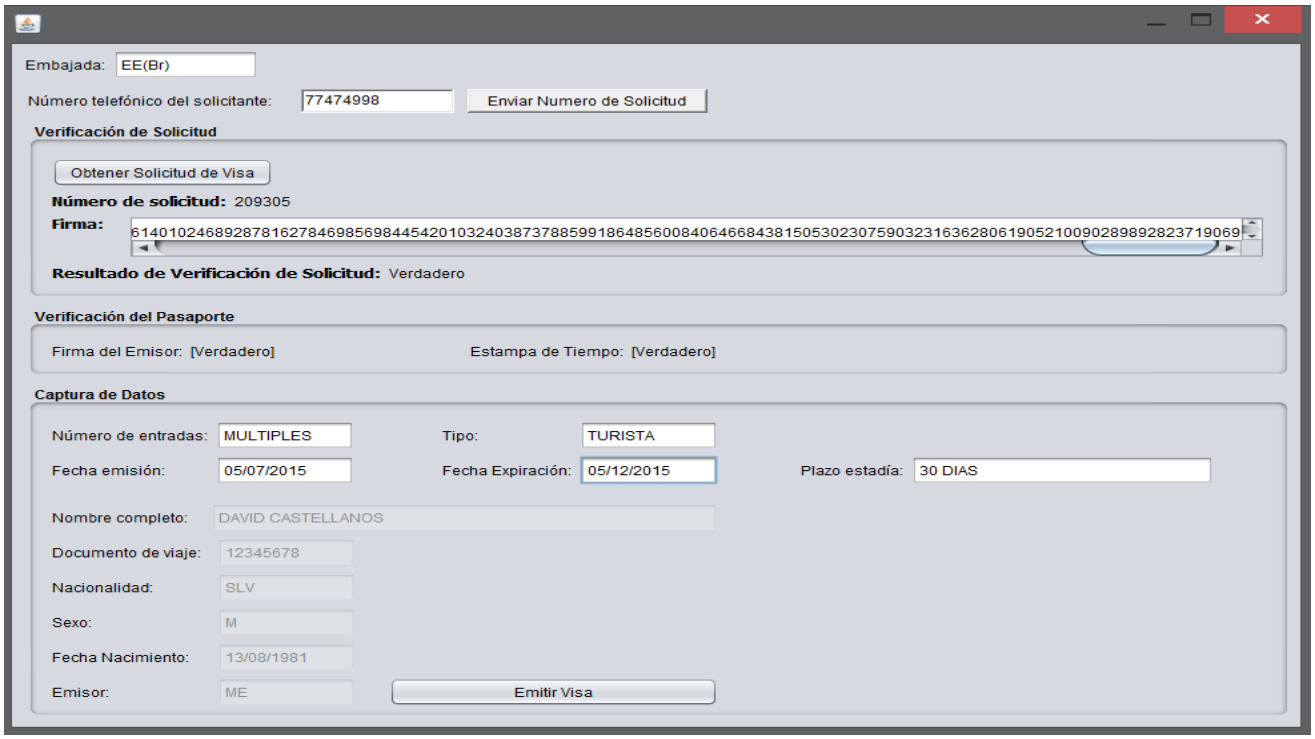

Figura 19. Captura de datos para Visa Electrónica.

Figura 20. Menú solicitud de Visa.

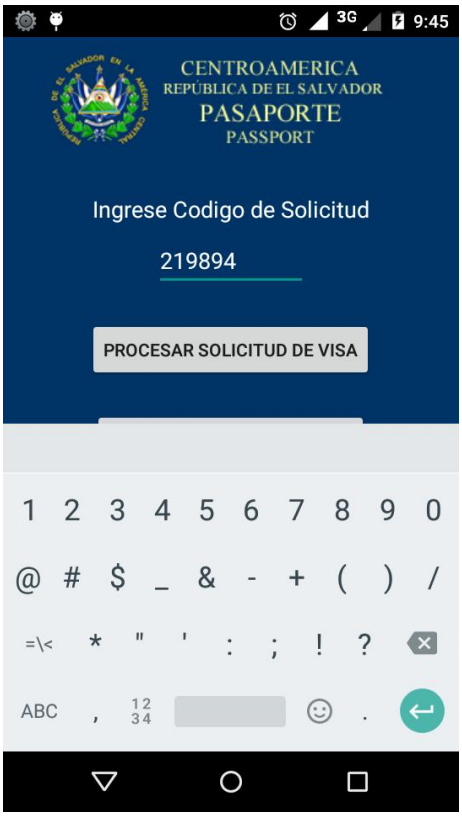

Figura 21. Procesar solicitud de Visa desde la App de Pasaporte Digital.

Para enviar la solicitud de visa, se obtiene la llave privada del usuario solicitante, contenida en el dispositivo móvil, descifrando con AES-128 y se firma con RSA la solicitud.

Al presionar el botón "Emitir", se solicita la estampa de tiempo para la visa, se firma con la llave privada de la embajada, y se actualiza el pasaporte del solicitante en la sección de visas. El solicitante presiona el botón "Obtener Visa" con lo que obtiene su pasaporte actualizado con la visa emitida.

En la Figura 22, se muestra en la aplicación móvil del pasaporte digital, la representación de la visa electrónica, muestra la firma digital de la embajada emisora en forma de un entero grande RSA.

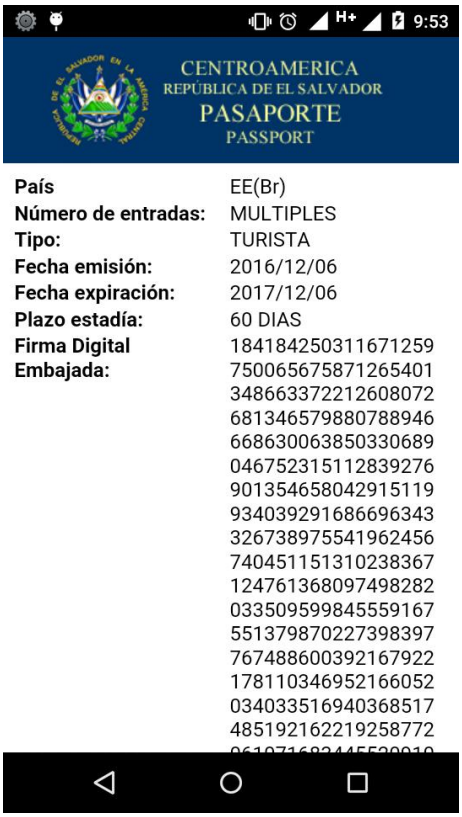

Figura 22. Visualización de la visa electrónica en el celular.

C. *Controles migratorios*

Para el uso del pasaporte electrónico en un viaje, se implementó una aplicación para los respectivos controles migratorios tanto para el uso de los oficiales de migración en El Salvador como de los oficiales de migración de países extranjeros a los

cuales viajaría el usuario del Pasaporte Digital (Figura 23). La aplicación permite realizar las entradas y salidas del país al que corresponde la codificación de Control Migratorio (Tabla 1).

Para poder realizar el control migratorio es requisito la verificación del pasaporte y de su respectiva estampa de tiempo.

En el caso de la entrada a un país que requiere visado para el ingreso a su territorio, la aplicación permite la consulta de las visas electrónicas y la verificación de la firma de la embajada emisora, así como su estampa de tiempo (Figura 24).

En la aplicación móvil, el menú "Pasar por control" inicia la actividad o pantalla de la aplicación móvil, diseñada con el propósito de ser utilizada durante los controles migratorios. Esta actividad se muestra en la Figura 25.

Una vez que el oficial de migración, haciendo uso de la aplicación, aplica el sello de control migratorio, el usuario del pasaporte digital actualiza el pasaporte digital haciendo uso del botón "Obtener Sello". El sello de control migratorio puede revisarse en el móvil a través del menú "Sellos de control", el cual al activarse muestra la pantalla o actividad que se muestra en la Figura 26.

El sello de control migratorio, aparte de contener la firma digital de la unidad migratoria donde se realiza el control de salida o entrada, posee la estampa de tiempo proveniente de la Autoridad de Estampa de Tiempo.

Conforme el usuario del pasaporte digital realiza su viaje y pasa por los diferentes controles migratorios, las firmas de cada control migratorio se van agregando a la firma original, conforme a lo especificado en la descripción formal del protocolo del pasaporte digital.

Figura 23. Aplicación para control migratorio

Figura 24. Verificación de visa electrónica.

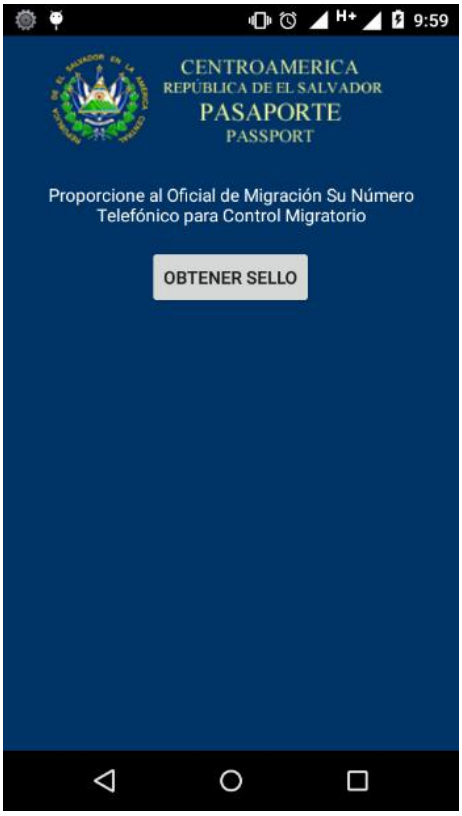

Figura 25. Paso por control migratorio.

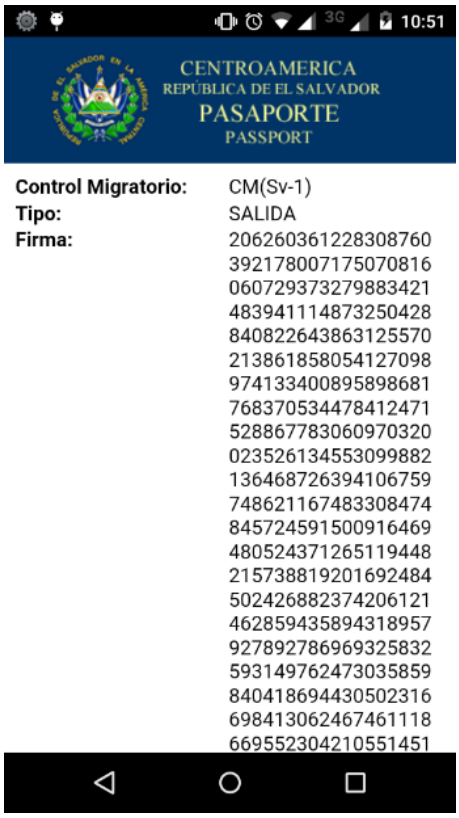

Figura 26. Sello de control migratorio.

D. Seguridad de los algoritmos implementados

La implementación del Pasaporte Digital utiliza el algoritmo AES-128 para el almacenamiento cifrado de la llave privada del usuario del pasaporte, así como para el almacenamiento cifrado del pasaporte digital. La seguridad del algoritmo viene dada por el tamaño de la llave, la cual es de 128 bits.

El algoritmo utilizado para la digestión de mensajes es SHA-256, el cual puede procesar mensajes de longitud menores a 2^{64} bits, trabaja con bloques de 512 bits y el tamaño del picadillo resultante es 256 bits.

La seguridad de una función picadillo se encuentra determinada por su resistencia a colisiones, resistencia a pre-imagen y resistencia a segunda pre-imagen, dependiendo de las propiedades que la aplicación criptográfica requiera. Si la aplicación requiere más de una propiedad de la función picadillo, entonces la propiedad más débil representa la seguridad de la función picadillo para esa aplicación. Para el caso de firma digital, se considera resistencia a colisión la propiedad que determina la seguridad para la función picadillo [12].

Las propiedades de seguridad para el algoritmo SHA-256 son:

Resistencia a colisión en bits: 128 bits.

Resistencia a pre-imagen en bits: 256 bits.

Resistencia a segunda pre-imagen: 201-256 bits.

Por lo que la seguridad de SHA-256 para la aplicación en el pasaporte digital es de 128 bits.

El algoritmo RSA fue implementado utilizando llaves de longitud 3072 bits, contando con 128 bits de seguridad real [16].

E. Características de Hardware y Software utilizado en la implementación

1) Hardware

Para la implementación del Pasaporte Digital, el Hardware utilizado se compone en 3 equipos, de los

cuales uno es una instancia virtual de *Google Compute Engine*. Estos equipos se describen a continuación:

- Servidor Web: Instancia *g1-small* de *Google Compute Engine*, 1 CPU virtual, 1.7 GB memoria *RAM*, almacenamiento persistente de 10 GB. El CPU virtual de una instancia g1-small es respaldado por un núcleo físico compartido el cual puede ser 2.6 GHz *Intel Xeon E5*, 2.5 GHz *Intel Xeon E5 v2*, 2.3 GHz *Intel Xeon E5 v3* o 2.2 GHz *Intel Xeon E5 v4*.
- Equipo de cómputo de escritorio: Procesador 1.6 GHz *Intel Core i5-4200U*, 8 GB memoria *RAM*, disco duro 1 TB.
- Teléfono inteligente: Motorola Moto E *Dual SIM* XT1022, *chipset Qualcomm Snapdragon 200*, procesador *Dual-core* 1.2 GHz *Cortex-A7*, memoria interna 4 GB, 1 GB RAM.

2) Software

El software instalado en los equipos utilizados en la implementación, se describe a continuación:

- Software del Servidor Web: Sistema Operativo *Linux Ubuntu* 15.4 *GNU/Linux 3.19.0-78-generic*, Servidor Web *Apache* 2.4.10, servidor de bases de datos *PostgreSQL* 9.4.5.
- Software del equipo de cómputo de escritorio: Sistema Operativo *MS Windows* 10, *Java Runtime Environment* 1.8, *NetBeans* 8.1 como Entorno de Desarrollo Integrado para aplicaciones *Java*, *Android Studio* 1.5.1 como Entorno de Desarrollo Integrado para aplicaciones *Android*.
- Software del teléfono inteligente: Sistema Operativo *Android* versión 5.1 (*lollipop*)

VI. Conclusiones

La elaboración de un documento de identidad digital con capacidad de firma digital es de interés no solo para El Salvador sino para otras naciones. El pasaporte digital cumple con estas características e implementa diversos controles de seguridad específicos a los procesos migratorios, desde la emisión del pasaporte digital, pasando por el proceso de obtención de visas de viaje y los pasos por cada uno de los controles migratorios, en los cuales se realizan verificaciones y se aplican sellos de control en forma de firmas digitales con estampa de tiempo.

La reciente aprobación de la Ley de Firma Electrónica de El Salvador representa una oportunidad para innovación tecnológica y para la aplicación de métodos criptográficos a procesos que requieren de mecanismos de seguridad y que no cuentan con ellos, además la posibilidad de agilizar estos procesos.

Luego de la revisión de la Ley de Emisión de Pasaportes de El Salvador, se observa que el protocolo propuesto y el prototipo elaborado, cumplen las especificaciones legales, siendo los principales requisitos, que el pasaporte ordinario sea emitido por la Dirección General de Migración y Extranjería de El Salvador y que la emisión sea realizada en persona, lo que su vez permite la certificación de la identidad de la persona.

A nivel de requisitos de estandarización internacional, la implementación del Pasaporte Digital, requiere de una notificación oficial a la Organización de Aviación Civil Internacional, expresando el uso de un documento de viaje diferente a los definidos en los estándares descritos por dicho organismo.

VII. Referencias

1) Publicaciones periódicas

[4] *National Institute of Standars and Technology, An Introduction to Computer Security*: *The NIST Handbook. NIST Special Publication* 800-12, 1995

[7] CCITT *Recommendation* X.800, *Security Architecture for Open Systems Interconnection for CCITT Applications*. Geneva 1991.

2) Libros

[5] William Stallings, *Cryptography and Network Security Principles and Practices*, Quinta Edición, ISBN 10: 0-13-609704-9.

[8] Alfred J. Meneses, *Handbook of Applied Criptography*, ISBN: 0-8493-8523-7, Octubre 1996.

[9] Bruce Schneier, *Applied Cryptography*, Segunda Edición, 1996, ISBN 978-1-119-09672-6.

[14] María de Lourdes López García, Diseño de un protocolo para votaciones electrónicas basado en firmas a ciegas definidas sobre emparejamientos bilineales, México, D.F. junio 2011.

3) Escritos presentados en conferencias (sin publicar)

[15] B. Gipp, N. Meuschke, and A. Gernandt. *Decentralized Trusted Timestamping using the Crypto Currency Bitcoin*. *In Proceedings of the iConference 2015, Newport Beach, CA, USA*, Mar. 24 - 27, 2015. URL http://ischools.org/the-iconference/.

4) Escritos publicados

[13] R. Rivest, A. Shamir and L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. *Communications of the ACM*, 21 (2), pp. 120-126, febrero 1978.

5) Legislaturas

[1] Asamblea Legislativa, República de El Salvador, Decreto No 1020, D.O No 48, Tomo No 274, 10 de marzo de 1982.

[3] Asamblea Legislativa, República de El Salvador, Decreto No 133, D.O No 196, Tomo No 409, 26 de octubre de 2015.

6) Normas

[2] *International Civil Aviation Organization*, Convenio Sobre Aviación Civil Internacional, Novena Edición, Doc. 7300/9 2006.

[10] *National Institute of Standards and Technology* (NIST), *Federal Information Processing Standards Publication* 197, *Advanced Encryption Standard*, Noviembre 2001.

[11] *National Institute of Standards and Technology* (NIST), *Federal Information Processing Standards Publication* 180-4, *Secure Hash Standard*, Agosto 2015.

[12] *National Institute of Standards and Technology* (NIST), *Special Publication* 800-107, *Recommendation for Applications Using Approved Hash Algorithms*, Agosto 2012.

7) Recursos en línea

[6] *Internet Security Glossary*, RFC2828, Mayo 2000, https://www.ietf.org/rfc/rfc2828.txt, Accedido el 28-Nov-2016.

[16] "*RSA Laboratories - TWIRL and RSA Key Size*", *Emc.com*, 2017. [En línea]. Disponible: https://www.emc.com/emc-plus/rsa-labs/historical/twirl-and-rsa-key-size.htm. [Accesado: 02- Jan- 2017].

David E. Martínez nació en San Salvador, República de El Salvador en 1981. Graduado como Ingeniero en Ciencias de la Computación ha trabajado por más de 10 años en el Desarrollo de Sistemas Informáticos. Labora desde hace 8 años en el Ministerio de Medio Ambiente de El Salvador y sirvió previamente en el Ministerio de Relaciones Exteriores de El Salvador.

Luego de los estudios realizados en la Maestría Seguridad y Gestión de Riesgos Informáticos de la Universidad Don Bosco, la Criptografía se ha vuelto su principal área de interés en combinación con el Desarrollo de Aplicaciones Móviles.