# APLICACIÓN DE ALGORITMOS DE LLAVE PÚBLICA PARA CERTIFICAR LA SOBREVIVENCIA DE PENSIONADOS EN EL EXTRANJERO DE EL SALVADOR

Mayra L. Molina Morán[1], Alma Y. Mendoza Delgado[2],
Rocío B. Melgar Flores[3] y Lourdes López García[4]

***Resumen*—La comprobación de la supervivencia de salvadoreños residentes en el extranjero se realiza de forma manual, lo que implica el traslado de la información impresa en papel, de cierto país a El Salvador, expuesta a la modificación o al acceso no autorizado. En este trabajo, se propone un protocolo que certifica la comprobación de supervivencia y garantiza que tanto la generación, el envío y la verificación de la documentación digitalizada sea protegida usando algoritmos criptográficos como las firmas digitales, las funciones picadillo y las estampas de tiempo. De tal manera que la información pueda ser transmitida vía correo electrónico y que la parte receptora tenga los mismos mecanismos de seguridad para confirmar la fiabilidad de la información recibida.**

***Palabras clave*—Firmas digitales, funciones hash, estampa de tiempo, servicios de seguridad.**

## Introducción

Actualmente, los pensionados salvadoreños que viven en el extranjero requieren asistir al Consulado de El Salvador en su país de residencia para realizar el trámite de comprobación de sobrevivencia; este trámite es personal, y tiene como objetivo principal validar que se encuentra con vida el asegurado para seguir siendo sujeto del pago de pensión.

El procedimiento inicia cuando el pensionado se presenta en el consulado con su documento de identidad y solicita la comprobación de sobrevivencia a efecto de su pensión. El notario público válida la identidad y genera una declaración jurada, la cual certifica la sobrevivencia del pensionado. En una segunda fase, la declaración original es enviada a la aseguradora que se hace cargo de la pensión. El envío puede realizarlo el mismo pensionado, un familiar o en algunos casos, el consulado.

Es importante mencionar que este proceso es totalmente manual y requiere del tiempo del pensionado para asistir al Consulado; el tiempo del notario para generar la declaración jurada; el tiempo del envío y entrega del documento original por parte de la aseguradora; finalmente, el tiempo que la aseguradora tarde en depositar la pensión al interesado. Lo anterior puede derivar en retrasos en el pago de la pensión, y ya que la documentación viaja en físico por correo postal, es vulnerable al acceso no autorizado o inclusive a la modificación. Por lo que se hace necesario implementar un mecanismo de certificación de tiempo (fecha y hora) que valide la sobrevivencia del pensionado a la fecha actual, y plantear una solución informática para que el Consulado de El Salvador en cualquier país pueda realizar el trámite de comprobación de sobrevivencia y notificación, de manera inmediata, a la aseguradora del pensionado.

Debido a lo anterior, en este trabajo se propone un protocolo que permite el envío de la declaración jurada de manera digital, protegida con una estampa de tiempo como la propuesta por Adams et. al (2001) que se encuentra firmada digitalmente, con lo cual el notario público del Consulado correspondiente, certifica la sobrevivencia. Ambas técnicas criptográficas están basadas en el algoritmo de llave pública RSA (acrónimo creado con las iniciales de los apellidos de sus creadores Rivest, Shamir y Adleman) Rivest et al. (1978).

El protocolo propuesto considera únicamente la generación digital de la declaración jurada que previamente fue realizada de manera convencional por el notario, considerando por supuesto la transmisión de la declaración jurada,

[1] Mayra L. Molina Morán es estudiante de la Maestría en Seguridad y Gestión de Riesgos Informáticos en la Facultad de Posgrados de la Universidad Don Bosco en El Salvador molina.mayra@gmail.com
[2] Alma Yanira Mendoza Delgado es estudiante de la Maestría en Seguridad y Gestión de Riesgos Informáticos en la Facultad de Posgrados de la Universidad Don Bosco en El Salvador aymrd@yahoo.es
[3] Rocio Belliny Melgar Flores es estudiante de la Maestría en Seguridad y Gestión de Riesgos Informáticos en la Facultad de Posgrados de la Universidad Don Bosco en El Salvador bellymelgar@hotmail.com
[4] María de Lourdes López García es Profesora de tiempo completo de la Ingeniería en Computación del CU UAEM Valle de Chalco de la Universidad Autónoma del Estado de México y profesora colaboradora en la Maestría en Seguridad y Gestión de Riesgos Informáticos en la Universidad de Don Bosco en El Salvador mllopezg@uaemex.mx **(autor corresponsal)**

ya que es estrictamente necesario que el pensionado o su representante legal asista al consulado. De tal manera, la aseguradora puede recibir y verificar el documento de forma electrónica, haciendo el proceso mucho más eficiente y seguro.

El resto de este artículo se organiza como sigue. En la sección 2, se presenta el proceso de comprobación de sobrevivencia, según las leyes salvadoreñas. En la sección 3 se indican las herramientas criptográficas utilizadas. En la sección 4 se muestra la funcionalidad del protocolo propuesto, mientras que la sección 5 indica el flujo de información entre las entidades participantes y un análisis de seguridad. Por último, se presentan las conclusiones.

## Proceso de comprobación de sobrevivencia

La normativa vigente emitida por la Superintendencia del Sistema Financiero de El Salvador, en el Extracto del Instructivo para la Prestación de Pensiones por Vejez SAP 01-2003 incisos b y c, especifica lo siguiente en la Superintendencia del Sistema Financiero de El Salvador (2015):

***b.*** *Pensionados residentes en el extranjero: Para la comprobación de sobrevivencia en el caso de pensionados residentes fuera del país, el pensionado deberá presentarse ante la Oficina del Consulado Salvadoreño en el país de residencia y solicitarle efectuar la Declaración Jurada ante sus oficios, la cual deberá redactarse de acuerdo a las prácticas notariales de El Salvador.*

En caso de no existir Consulado de El Salvador en el país de residencia, el pensionado podrá comprobar su sobrevivencia a través de la declaración jurada, la cual deberá realizarse ante los oficios de un notario público (residente en el mismo país domiciliar del pensionado) que esté autorizado por la Corte Suprema de Justicia de El Salvador.

Alternativamente, la declaración jurada podrá otorgarse ante los oficios de la persona que ejerza la función del notariado en el país de residencia del pensionado, la cual tendrá validez en El Salvador, siempre y cuando ésta se realice en idioma castellano, y lleve las auténticas de firma requeridas por las leyes salvadoreñas y tratados internacionales suscritos por El Salvador. En este caso la declaración jurada podrá realizarse en acta notarial, siempre y cuando cumpla con los requisitos establecidos por la Ley de Notariado de El Salvador. En ningún momento un apoderado puede firmar la comprobación de supervivencia del pensionado que representa. Si el pensionado no se presenta en la fecha indicada por la aseguradora, se le suspenderá el pago de ésta, a partir del mes de cumplimiento del aniversario. Dicho pago se reiniciará con efecto retroactivo, una vez el pensionado o su representante legal, se presente a comprobar la referida supervivencia.

El formato del formulario queda a discreción de la aseguradora, sin embargo, deberá contener la siguiente información:

- Nombre del afiliado causante de pensión
- NUP del afiliado (Número Único de Previsional)
- Tipo de pensión
- Datos del pensionado: nombre, nombre y número de documento de identidad personal, dirección y teléfono, tanto particular como del trabajo.
- Información del apoderado o representante legal: nombre, nombre y número de documento de identidad personal, dirección y teléfono.
- Información relacionada con la escritura pública, tales como: número de escritura, número de protocolo y nombre del notario.
- Información del Banco en que el pensionado desea se le pague la pensión (nombre, número de cuenta, sucursal), si el pago es mediante abono a cuenta.
- Nombre y firma de la persona que recibe el formulario, nombrada o autorizada por la aseguradora, nombre y firma del pensionado, si no sabe firmar, la huella digital, nombre, firma y documento de identidad de la persona que firma a ruego, cuando el pensionado no sabe firmar, nombre y firma del representante legal.

**c.** *Las AFP (Administradora de Fondo para Pensiones) podrán llevar un control de la sobrevivencia de sus pensionados residentes en El Salvador y en el extranjero, sean éstos afiliados o beneficiarios, a través de un equipo Biométrico, para que, de forma expedita y segura puedan realizar una efectiva revisión de la sobrevivencia de sus pensionados; y que permita dar continuidad a los pagos realizados a través de éstas, de los beneficios otorgados por el Sistema de Ahorro para Pensiones.* Nota: El literal (c) fue adicionado conforme a Reforma 01/2011 (01) del 7 de enero 2011.

La AFP será la responsable de la implementación, operación, divulgación y verificación del correcto funcionamiento de la herramienta, cerciorándose que los pensionados conozcan el método y la forma de demostrar

su sobrevivencia, así como la codificación de los mismos. La AFP deberá colocar los aparatos en lugares accesibles para los usuarios e implementar todos aquellos controles encaminados a evitar cualquier tipo de fraude que involucre un uso inadecuado del mecanismo de control.

*Problemas de seguridad detectados*

Los posibles escenarios no deseados con los cuales se puede enfrentar un pensionado o una aseguradora son los siguientes:

- Posibilidad de pérdida de la Declaración Jurada en el envío físico a El Salvador.
- Alteración a los datos contenidos en la Declaración Jurada previamente a su envío a El Salvador tales como nombre, fecha de expedición del acta, alteración al apostillado colocado por el consulado del país residente.
- Atraso en la entrega de los documentos por el *courier*, causando que el pensionado no se incluya en la planilla de pagos de pensión.
- Si el pensionado envía los documentos a sus familiares, ellos podrían retrasarse en la entrega de los mismos en la AFP.
- Negación de la AFP que ha recibido la información del pensionando, argumentando que la información jamás llego a la aseguradora.

## Herramientas utilizadas

Antes de presentar el protocolo propuesto, es necesario describir las herramientas utilizadas, las cuales son los esquemas criptográficos de firma digital, funciones hash y estampas de tiempo.

*Funciones hash*

Una función picadillo H definida en Stinson (2006) es una función computacionalmente eficiente que transforma una cadena binaria de longitud arbitraria $\{0,1\}^*$ a una secuencia $H(x)$ de longitud fija, es decir:

$H: \{0,1\}^* \rightarrow \{0,1\}^l$

Se dice que, $H(x)$ es el digesto de longitud $l$ de $x$.

Una función picadillo $H$ se considera segura, si los tres siguientes problemas son difíciles de resolver:

1. *Transformación mezclada*: un cambio a la entrada de incluso 1 bit, produce una salida diferente.
2. *Preimagen*: dado $y \in \{0,1\}^l$, encontrar $x \in \{0,1\}^*$, tal que $H(x) = y$
3. *Colisión*: dado $x \in \{0,1\}^*$, encontrar $x' \in \{0,1\}^*$, tal que $x \neq x'$ y $H(x) \neq H(x')$ y además,
4. *Eficiencia*: dado $x \in \{0,1\}^*$, es fácil de calcular $H(x)$

Las funciones hash son utilizadas en los esquemas de firma digital y en la verificación de la integridad de los datos, en donde podemos tener dos escenarios. El primero de ellos, cuando los datos son transmitidos y el canal de comunicación introduce errores en ellos. El segundo, cuando una entidad cambia maliciosamente los datos antes de que lleguen al destino. En ambos casos, la función hash garantiza que cualquier modificación realizada a los datos originales modificará el digesto de los mismos. Las funciones hash SHA1 y MD5 propuestas por Eastlake & Jones (2001) y Rivest (1992) respectivamente, son las que actualmente se utilizan en las aplicaciones donde es necesario mantener la integridad de los datos.

*Firmas digitales*

En la criptografía moderna, los cripto-esquemas de llave pública son ampliamente usados para generar firmas digitales. El concepto de firma digital es análogo al de una firma autógrafa, pero tiene el servicio adicional de proteger la información de alteraciones intencionales de alguna entidad maliciosa. La llave privada del usuario, la cual debe ser conocida sólo por su propietario, es requerida por el signatario para producir una única e infalsificable firma digital para un documento dado, mientras que la llave pública debe ser conocida por el verificador de la firma, con la finalidad de decidir si la firma del documento es válida o no. Una firma digital consta de los siguientes elementos según Trappe (2006):

- Un conjunto de mensajes $M$
- Un conjunto de firmas $S$
- Un conjunto de llaves privadas $KS$ y sus pares las llaves públicas $KV$
- Una función de firma $Firma(k_s, m) = s$, con $k_s \in KS$ y $m \in M$
- Una función de verificación $Verifica(k_v, s) \rightarrow \{verdadero, falso\}$, con $s \in S$ y $k_v \in KV$

Estrictamente hablando, una firma digital debe satisfacer las siguientes propiedades:

- Integridad. Implica que el documento recibido sea una copia idéntica del que fue enviado, es decir, el documento digital no puede ser modificado, destruido o intercambiado de alguna manera maliciosa o accidental.
- Autenticación. Asegura que el documento recibido fue creado por una determinada entidad.

- No-repudio. Asegura que tanto el emisor como el receptor no puedan negar haber enviado o recibido algún documento.

En firmas digitales, las funciones hash son generalmente usadas para producir digestos de mensajes. Para efectos de eficiencia, en la práctica, una firma digital es producida para el digesto de un mensaje de cualquier longitud.

La firma digital propuesta por Rivest, Shamir y Adleman en Rivest et al. (1978), llamada RSA, fue la primera realización práctica de un esquema de firma digital y hasta la actualidad sigue siendo el esquema más utilizado. Consiste de tres algoritmos descritos a continuación.

*Algoritmo 1. Generación de llaves RSA*

Entrada**:** Sin parámetros

Salida: Llave privada es $(d, n)$ y la llave pública es $(e, n)$

1. Seleccionar dos números primos grandes $|p| \approx |q| \approx 512$ bits
2. Calcular el módulo $n = p * q$
3. Calcular $\varphi(n) = (p-1) * (q-1)$
4. Seleccionar la llave pública $e$ tal que $mcd(e, \varphi(n)) = 1$ y $0 < e < n$
5. Obtener la llave privada $d = e^{-1} mod\ \varphi(n)$
6. Return $(e, d, n)$

*Algoritmo 2. Generación de la Firma*

Entrada: Llave privada $(d, n)$, el mensaje $m$, la función hash *H*

Salida: La firma $s$

1. Calcular $h = H(m)$
2. Calcular $s = h^d\ mod\ n$
3. Return $s$

*Algoritmo 3. Verificación de la firma*

Entrada: Llave pública $(e, n)$, el mensaje $m$, la firma $s$, la función hash *H*

Salida: verdadero o falso

1. Calcular $h = H(m)$
2. Calcular $h' = s^e\ mod\ n$
3. Si $h = h'$ entonces

3.1 Return Verdadero

Sino, entonces:

3.2 Return Falso

*Estampas de tiempo*

Esta herramienta provee una prueba de la existencia de un dato en un instante en el tiempo. El proceso propuesto por Adams et al. (2001) consiste en adicionar la fecha y hora en un formato específico, a la información contenida en el mensaje, con lo cual previene la corrupción de la fecha y la hora.

La estampa de tiempo debe cumplir con los siguientes requerimientos según Ma et al. (2008):

1. Independencia entre la estampa de tiempo y el dispositivo de almacenamiento, es decir, la estampa de tiempo no debe ser almacenada en la memoria física del dispositivo, ésta sólo debe estar incluida en el documento.
2. Integridad en los datos del documento, de tal manera que los datos no pueden ser modificados, borrados o alterados sin autorización o sin ser detectado.
3. No repudio, una vez que la estampa de tiempo ha sido certificada, modificarla debe ser un proceso fácilmente detectable.

Las entidades que participan en un protocolo de estampa de tiempo son el usuario que solicita la estampa; una autoridad (TSA) que certifica el mensaje con la estampa integrada y un servidor de tiempo (TS) de donde se obtiene la información de la fecha y hora.

De acuerdo con el estándar RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocols", una estampa de tiempo puede ser vista como un documento codificado que contiene tres partes: el digesto del documento, la fecha y la hora proporcionada por el ST y la firma digital de la autoridad certificadora (TSA). El algoritmo 4 muestra el uso de la estampa de tiempo integrado en la firma digital RSA.

*Algoritmo 4. Certificación de la estampa de tiempo con firma digital RSA*

Entrada: Mensaje $m$, llave privada $(d, n)$, función hash *H*

Salida: Firma $s$

1. Calcular $h = H(m)$
2. Solicitar al TSA la cadena de tiempo $t$

3. Calcular $r = H(h||t)$, donde "||" es la función de concatenar
4. Calcular $s = r^d \ mod \ n$
5. Return $s$

La empresa colombiana Gestión de Seguridad Electrónica S. A., a través de la Superintendencia de Industria y Comercio (2015), menciona que algunos de los beneficios de utilizar una estampa de tiempo son los siguientes:

- Minimiza el riesgo de modificación de la información o transacción.
- Disminuye el riesgo de adulteración de la información.
- Se eliminan factores de duda respecto del momento en que suceden acciones en relaciones de transacción.
- Transparenta los procesos para los usuarios de sistemas que tienen restricciones temporales.

**Funcionalidad del protocolo propuesto**

El escenario de seguridad que el protocolo propuesto contempla es la población de salvadoreños pensionados, por una AFP, que residen en Estados Unidos y que realizan su trámite de comprobación de sobrevivencia en el Consulado de Los Angeles, en el Estado de California, y envían vía correo postal o *courier* su comprobación de sobrevivencia a la AFP o a sus familiares para que sean ellos quienes la presenten.

Las entidades para este escenario son cuatro:

1. *Pensionado en el exterior*. Solicita en el Consulado de El Salvador en los Estados Unidos que le sea elaborada una declaración jurada, la cual deberá realizarse ante los oficios del cónsul o vicecónsul. Si no existe consulado el pensionado puede solicitar a un notario público que le elabore el documento siempre y cuando este sea residente en el mismo país domiciliar del pensionado que esté autorizado por la Corte Suprema de Justicia de El Salvador.
2. *Registrador de la declaración jurada.* Es la persona responsable y asignada por el consulado para verificar la declaración jurada que presenta el pensionado, escanear el documento y realizar los procesos de estampillado de tiempo. En el protocolo se identifica como la entidad registradora: "ER".
3. *Cónsul/Vice Cónsul*. Es el responsable y designado por el Consulado de El Salvador en Estados Unidos para que de fe de la sobrevivencia del pensionado. En el sistema se identifica como la entidad certificadora "EC", y es el responsable de firmar digitalmente la declaración jurada.
4. AFP. Es la entidad responsable de recibir y verificar los documentos firmados con la estampa de tiempo.

*Políticas de seguridad*

En actualidad el hecho de estar conectados a una red en un entorno externo nos expone a la posibilidad que algún atacante irrumpa en ella, la seguridad en el ambiente de red debe tener la habilidad de identificar y eliminar vulnerabilidades. Es necesario poner atención a salvaguardar la ventaja organizacional, incluyendo información y equipo físico. Al definir la seguridad de una institución o empresa, lo que es apropiado varía de acuerdo a las necesidades de cada organización. Así que es de alta importancia que cualquier tipo de empresa con una red tenga una política de seguridad que se dirija a su conveniencia y coordinación, esté la red conectada o no, a un entorno externo, como Internet. Los diferentes tipos de amenazas que se pueden dar son como robo o destrucción de información, alterar el funcionamiento de la red, anulación del funcionamiento de los sistemas, suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, robo de dinero, estafas etc., pueden ser evitados con una correcta política de seguridad.

Las legislaciones nacionales en la mayoría de los países exigen a las instituciones privadas, empresas e instituciones públicas a implantar una política de seguridad. La protección de los datos de carácter personal y su normativa de desarrollo debe proteger ese tipo de datos, estipulando medidas básicas y necesidades que impidan la pérdida de calidad de la información o su robo. También es necesario establecer medidas tecnológicas en los sistemas informáticos que prestan servicios a los ciudadanos, de manera que cumplan con los requerimientos de seguridad acordes al tipo de disponibilidad de los servicios ofrecidos.

Siendo la información el activo más importante que poseen las instituciones o empresas, estas deben establecer técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de *barreras y procedimientos* que resguardan el acceso a los datos, y solo permiten acceder a ellos a las personas autorizadas para hacerlo. Con base en estas medidas, en el presente proyecto se definen dos tipos de políticas de seguridad:

1. Acceso a Protocolo
    - *Registro y autenticación de la entidad registradora*. La persona que el consulado delegue como responsable de registrar el proceso de sobrevivencia del pensionado será verificada como usuario del sistema por medio de los derechos asignados en el dominio de la red, ella será la responsable de realizar

en tiempo de presentación del pensionado, las operaciones de escaneo de documentación y estampillado de tiempo.

- *Registro y autenticación de la entidad certificadora*. Siendo el Cónsul o Vicecónsul la persona responsable de testificar en el sistema la sobrevivencia del pensionado, por medio de la firma digital en el documento de declaración jurada. Se realizará la validación del usuario por medio de los derechos que tiene en el dominio para acceder al sistema y será dueño de un par de llaves (pública, privada) para realizar el proceso de firma digital.
- El sistema contará con *el proceso de almacenamiento seguro* de la llave privada de la entidad certificadora con el objetivo de mantener la confidencialidad de los datos.

2. Información

- El protocolo de seguridad no valida el contenido de los datos de la declaración jurada presentada por el pensionado, ya que de ésta es responsable la entidad que lo emite, en este caso, será el consulado.
- El estampillado debe realizarse en el tiempo que el pensionado presenta la información en forma oportuna, con el fin que el estampillado digital sea coherente con el tiempo del documento físico.
- El protocolo de seguridad recibe el documento de verificación de sobrevivencia del pensionado en un archivo digital, con formato PDF (portable document format), el cual es generado por la ER.
- El estándar para el nombre de los archivos resultantes de la digitalización de la declaración jurada firmada por el pensionado y notario deben ser codificadas de la siguiente forma: NUP del solicitante y la fecha de la comprobación de sobrevivencia.
- Los archivos de las declaraciones juradas escaneadas deben ser almacenadas en una carpeta denominada "Declaraciones".
- El archivo de declaración jurada será firmado digitalmente por el Cónsul o Vicecónsul, quien dará la certificación de la presentación de la sobrevivencia del pensionado, dicho archivo se deberá almacenar en formato de PDF.
- El Cónsul o Vicecónsul será la entidad responsable de notificar a la AFP y enviar vía correo electrónico la documentación que certifica la sobrevivencia de la entidad llamada "Pensionado".
- Las AFP autorizadas serán las únicas responsables de verificar la integridad de la declaración jurada y firmada por el EC.

*Fases*

La protección de un documento digital requiere de varios procesos que permiten la certificación y verificación del mismo. En el área de la criptografía, las firmas digitales son la herramienta principal para autenticar a un usuario, es decir, confirmar que es realmente quién dice ser. Además, las estampas de tiempo sellan un tiempo determinado, para este caso, la generación de la firma, con lo cual es posible validar la fecha de comprobación de la sobrevivencia.

Las fases que contempla este protocolo propuesto se describen en el Cuadro 1. Como puede observarse, la primera fase es el proceso normal que debe realizar el pensionado al asistir al consulado en la fecha estipulada por la AFP y del Cónsul, al verificar la documentación presentada por el pensionado y al realizar el documento en físico firmado y sellado.

Las fases 2 y 3 son las relacionadas para brindar la seguridad necesaria en la transmisión de la información a la aseguradora. Los procesos de estampado y firma digital se realizan en estas fases, donde el Cónsul o notario público autorizado tiene la responsabilidad total.

La fase 4, la desarrolla la aseguradora, quién previamente en el sistema contiene las llaves públicas de todas las entidades autorizadas para realizar una firma digital con estampa de tiempo, esto con la finalidad de verificar cada documento firmado recibido de los diferentes consulados o notarias públicas autorizadas.

En la misma fase, la AFP responde a la EC con un acuse de recibido firmado que indica si la declaración fue recibida correctamente o si hubo algún error que provocó que la firma del EC fuera inválida. Por lo anterior, cada AFP contiene un par de llaves (pública y privada) con lo cual firmará el acuse de recibido. Este proceso ayudará a brindar el no repudio, ya que ambas entidades usan una firma digital que permite la autenticación de sus respectivas entidades, con lo cual es posible validar que fue enviado y recibido tanto la declaración jurada como el acuse de recibido.

| Fase | Acción principal | Entidad(es) | Descripción | Resultado |
|---|---|---|---|---|
| 1 | Comprobación | Pensionado, ER | El pensionado entrega la documentación requerida y el notario público redacta, imprime, firma y sella la declaración jurada de la sobrevivencia (de forma manual). | Declaración jurada impresa. |
| 2 | Digitalización | ER | El notario digitaliza el documento . | Documento digital de la declaración jurada. |
| 3 | Certificación | EC | 1.- El notario solicita una estampa de tiempo al Servidor de Tiempo<br>2.- Recibe la estampa y la adjunta al documento digitalizado<br>3.- Firma el documento junto con la estampa | Declaración sellada y firmada. |
| 4 | Verificación | AFP | 1.- La aseguradora recibe la declaración sellada.<br>2.- Verifica la firma del notario púbica en la declaración jurada.<br>3.- Verifica la información de la estampa de tiempo.<br>4.- Recibido y verificado el mensaje de la EC, la AFP crea y envía un acuse de recibido a la EC. | Verificación válida o inválida. |

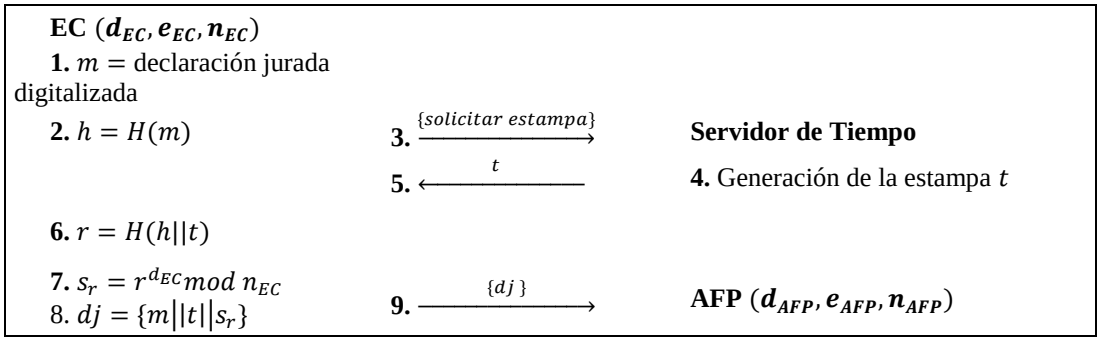
Cuadro 1. Fases del protocolo propuesto

**Flujo de datos del protocolo propuesto**

El flujo de datos del protocolo propuesto se exhibe en el Cuadro 2. La primera fase no se considera, ya que es realizada de manera manual, dada la prestación de pensiones por vejez mencionada en la sección 2.

Como puede observarse, es necesario generar un par de llaves, una pública y otra privada, para cada una de las entidades certificadoras, y la distribución de las llaves públicas junto con sus certificados digitales, de acuerdo a lo indicado por Cooper et al. (2008), para las AFP que corresponda el pensionado. De igual manera, cada AFP requiere un par de llaves con las cuales se podrá realizar la autenticación tanto de la entidad emisora como de la receptora.

Para la implementación de este protocolo se recomienda que el sistema que lo integre realice las validaciones correspondientes de los usuarios que estarán realizando los procesos. Para realizar el proceso de estampillado, la ER que ha realizado el escaneo del documento de la declaración jurada deberá validar sus permisos en el sistema. En el proceso de firma digital, la entidad certificadora (EC) valida en su cuenta de usuario los derechos para firmar, si el usuario es nuevo en el sistema, debe proceder a la generación de la información de sesión (usuario y contraseña) para el control de acceso al sistema; y la generación de un par de llaves para la certificación, si no es nuevo y cuenta con los derechos procede a la generación de firma digital.



| | | |
|---|---|---|
| | | **10.** $h = H(m)$<br>**11.** $r = H(h\|\|t)$<br>**12.** $h' = s_r^{ECC} mod\ n_{ECC}$<br>**13.** Si $r = h'$<br>**13.1** ACK="la firma es válida"<br>Sino<br>ACK="la firma no es válida"<br>**14.** $h = H(ACK)$<br>**15.** $s_{ACK} = ACK^{d_{AFP}} mod\ n_{AFP}$ |
| | **16.** $\{ACK, s_{ACK}\}$ ⟵ | |
| **17.** $h = H(ACK)$<br>**18.** $h' = s_{ACK}^{e_{APF}} mod\ n_{APF}$<br>**19.** Si $h = h'$<br>La firma es válida<br>Sino<br>La firma es inválida | | |

Cuadro 2. Flujo de datos del protocolo propuesto.

*Análisis de seguridad*

El protocolo propuesto entre las entidades EC y AFP cumple con los servicios de seguridad de autenticación e integridad. La *autenticidad* se cubre gracias a la firma digital RSA que garantiza que quien certifica el documento es la persona autorizada para ello ya sea el Cónsul o un notario público. La *integridad* se cumple por el uso de la función hash, que garantiza que tanto la información del documento jurado como la estampa de tiempo no sean modificadas sin que se detecte en la verificación de la firma. El *control de acceso* es cubierto con el uso de sesiones para cada usuario registrado, quien será dueño de un nombre de sesión y una contraseña. Es importante notar que el protocolo en realidad no cubre este requerimiento, es más bien un requisito obligatorio en la implementación del sistema. El *no repudio* se cumple con el uso de certificados digitales, los cuales, vinculan la entidad EC con su respectiva llave pública. De tal manera que el Cónsul o notario público autorizado no pueda negar su participación en la comprobación de supervivencia del pensionado. Del lado de la AFP también es requerida una firma digital en la recepción de la información, con este hecho se garantiza que la documentación llegó a su destino y que fue verificada por la respectiva AFP. Así, la autenticación es doble, y se puede garantizar que la información fue enviada y recibida en ambas partes de la comunicación.

La estampa de tiempo es agregada al mensaje para considerar el tiempo en que se realizó la comprobación de supervivencia, con lo cual se puede cotejar el tiempo de retraso que la entidad EC envía a la AFP la información del pensionado y tener más control sobre el proceso.

## Conclusiones

El proceso de automatización para la comprobación de sobrevivencia de los pensionados salvadoreños que viven en el extranjero permite que la declaración jurada, que corrobora que aún está con vida el pensionado, sea entregada de una manera segura y eficiente a la AFP donde se encuentra asegurado. La digitalización de la declaración jurada y el anexo de la estampa de tiempo son certificados a través de la firma digital RSA generada por el Cónsul o el notario público autorizado con lo cual se protege la integridad de la información y se autentica la identidad del certificador. El no repudio se cumple al realizar una autenticación tanto de la AFP como del Cónsul, esta autenticación doble le permite a cada entidad confirmar que los respectivos mensajes fueron recibidos y/o enviados por la otra entidad. La declaración jurada digital es un archivo, idealmente en formato PDF, dividido en tres secciones: la primera corresponde a la información proveniente de la digitalización de la declaración jurada impresa, firmada de forma autógrafa por el Cónsul y estampada manualmente con el sello del Consulado o la notaría pública autorizada; la segunda sección es la información de la estampa de tiempo con la fecha y hora en la que se solicitó la comprobación generada por el Cónsul a través de un Servidor de Tiempo; por último, la tercera sección cuenta con la firma digital producida también por el Cónsul para certificar la comprobación de supervivencia. El archivo generado es transmitido por correo electrónico, lo que lo hace altamente eficiente comparado con el envío de manera impresa a través de un correo postal que tardaría días o meses en llegar.

De tal manera que el proceso de comprobación usando un protocolo que es sencillo y fácil de implementar garantiza la protección del documento y la eficiencia en la trasmisión, y por tanto, la satisfacción del pensionado al tener la confianza de recibir su pago de pensión en tiempo y forma.

*Recomendaciones*

Ya que las herramientas criptográficas están integradas como biblioteca en la mayoría de los lenguajes de programación, en este trabajo se deja al lector la libertad de implementar el protocolo propuesto en el lenguaje de su elección o como mejor le convenga.

## Referencias


Adams C., Cain P., Pinkas D. y Zuccherato R."Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP), Request for Comments: 3161". *Network Working Group*. Recuperado de la página oficial de la IETF: http://www.rfc-base.org/txt/rfc-3161.txt. 2001.

Cooper D., Santesson S., Boeyen S., Housley R. y Polk W. "Internet X.509 Public key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Request for Comments. 5280". *Network Working Group*. Recuperado de la página oficial de la IETF: https://tools.ietf.org/html/rfc5280. 2008.

Eastlake D. y Jones P. "US Secure Hash Algorithm 1 (SHA1), Request for Comments 3174". *Network Working Group*. Recuperado de la página oficial de la IETF: https://tools.ietf.org/html/rfc3174. 2001.

Ma H., Hua Y. y Guo W. "Electronic time stamping safety and efficiency optimize technique research". *International Symposium on Electronic Commerce and Security*, Agosto 2008.

Rivest R. "The MD5 Message-Digest Algorithm, Request for comments 1321". *Network Working Group*. Recuperado de la página oficial de la IETF: http://www.rfc-base.org/txt/rfc-1321.txt, 1992.

Rivest R. L., Shamir A. y Adleman L. M. "A method for obtaining digital signatures and public key cryptosystems". *Communications of the ACM*, Vol. 21, No. 2, 1978.

Stinson D. R. "Cryptography: Theory and Practice" 1ra. Edición, *Chapman and Hall/CRC* 2006.

Superintendencia de Industria y Comercio "Estampa de tiempo" Recuperado de la página oficial de la *Certificadora digital Gestión de Seguridad Electrónica S.A.* de Colombia: http://portal.gse.com.co/index.php/productos/estampa-de-tiempo 2015.

Superintendencia del Sistema Financiero de El Salvador "Instructivo SAP 01/2003 para el otorgamiento de prestaciones por vejez en el Sistema de Ahorro para Pensiones". Recuperado de la página oficial *del Gobierno de El Salvador*: http://www.ssf.gob.sv/images/stories/desc_pensiones_instructivos/SAP/SAP%2001-2003%20Para%20el%20Otorgamiento%20de%20Prestaciones%20por%20vjez%20en%20el%20SAP.pdf 2015.

Trappe W. "Introduction to cryptography with coding theory" 2da. Edición *Pearson Prentice Hall* 2006.