Diseño e implementación de Time-Stamping bajo un servidor confiable de fecha y hora

Guillermo Andrés Paulin, Miguel Ángel Robledo, Graciela María Brusa
Universidad Nacional del Litoral

gpaulin@santafe.gov.ar, marobledo@santafe.gov.ar, grabrusa@santafe.gov.ar

Resumen.
Éste trabajo propone y analiza las actividades para proporcionar certificación de fecha y hora en el Gobierno de Santa Fe, dado que es una tecnología necesaria para muchos procesos administrativos que llevan a cabo en este ámbito. Las líneas de desarrollo en una primera fase, se basan en estudiar e implementar alternativas para la obtención de fecha y hora; y en una segunda, en configurar un servidor de certificación de fecha y hora para fortalecer las propiedades de firma digital y todas las actividades, implican la consideración de los estándares vigentes aplicables a esa tecnología.. Lo más importante que se expone en este trabajo, son los resultados obtenidos luego de una evaluación del proceso de integración de Time-Stamping (TS) en la Red de comunicaciones del Gobierno de Santa Fe. Los mismos constituyen una base que puede ser tenida en cuenta para la implementación de esta tecnología de manera definitiva.

Palabras clave: Fecha, Hora, Time-Stamping, Firma Digital, Seguridad

1 Introducción

La magnitud del crecimiento que ha tenido el mundo digital en los últimos años, produjo que muchas organizaciones hayan migrado hacia una nueva forma de concebir el trabajo. El crecimiento se debió principalmente a la expansión de las redes de datos de alta velocidad que permitieron la interconexión de lugares distantes y que conjuntamente con el apoyo de dispositivos informáticos, lograron que muchas tareas que se realizaban de manera tradicional evolucionaran hacia procesos digitalizados, abriendo nuevas propuestas y perspectivas en el ámbito laboral. Surge así el concepto de transacciones electrónicas, las cuales se basan en la transferencia de información digital con propósitos específicos, produciendo ahorros de dinero, mejor respuesta a las necesidades en tiempo y forma y por ende, más eficientes.

Como toda metodología de trabajo, no está exenta de riesgos y fraudes, tales como robo de información, suplantación de identidad, modificación de la información o repudio de la misma. Nuevas amenazas de seguridad evolucionan continuamente, por lo tanto las políticas de seguridad, también lo deberán hacer. Es por ello, que para adecuarse a la era digital de manera segura, se requiere acompañar este proceso con

una constante búsqueda de herramientas tecnológicas que brinden seguridad, confianza y respaldo a las transacciones.

Bajo este panorama mundial, diferentes organismos internacionales y nacionales, tales como, ITU/T[1], IETF[2], ISO/IEC[3], ETSI[4], ONTI[5] han desarrollado estándares para la aplicación de métodos y procesos que garanticen mayor seguridad en las operaciones digitales.

Si bien el tema de la seguridad informática en general es muy amplio y no es el objeto de estudio de este trabajo, resulta de interés analizar algunas situaciones de inseguridad que pueden presentarse, para las cuales esta propuesta de trabajo presenta alternativas para mitigar el riesgo. En este marco, pueden mencionarse todas aquellas situaciones en las cuales dos personas que se comunican por medios digitales necesitan intercambiar documentos que sellen un acuerdo entre partes.

En los procesos tradicionales donde se tiene soporte en papel, el contenido de dicho acuerdo sólo es conocido por las personas involucradas, manteniendo la confidencialidad que se requiera al no permitir el acceso a otras personas. Por otra parte, el acto de firma del acuerdo se realiza generalmente con la presencia de las partes intervinientes y en el momento de firmar el acuerdo, se verifica la integridad del documento realizando enmiendas y volviendo a firmar en caso de que existan errores. La firma hológrafa garantiza entonces la autoría e integridad del documento, lo que sumado a la normativa explicitada en el Código Civil, otorga también el atributo de no repudio a dicho documento firmado.

Cuando el escenario cambia al soporte digital, se tiene un documento electrónico que va a ser firmado por las partes intervinientes, quienes no se encuentran en el mismo lugar, la distancia que los separa puede ser cualquiera así como también el momento en que se firma por cada uno es diferido. Como elemento adicional, dicho documento debe transmitirse a través de la red desde un actor a otro. Toda esta situación genera las siguientes necesidades:

- Se requiere contar con un mecanismo que cumpla la función de la firma hológrafa, garantizando las propiedades de autoría e integridad. En caso contrario, podrían darse situaciones de suplantación de identidad y/o alteración del contenido del documento.
- En algunos casos, también se podría requerir contar con un mecanismo que asegure fecha y hora de la firma de manera fehaciente, especialmente en aquellas operaciones que implican realizar una presentación en una fecha y hora determinada para tener validez.

Las situaciones descriptas anteriormente son las que dieron origen a nuevas tecnologías y herramientas que permiten resolver los requerimientos planteados. Así surge una herramienta tecnológica que ha tenido gran impulso y que brinda los atributos de autoría, integridad y no repudio a las transacciones electrónicas, denominada Firma Digital[6].

1 ITU/T - International Telecommunication Union - http://www.itu.int/
2 IETF - Internet Engineering Task Force - http://www.ietf.org
3 ISO/IEC - International Organization for Standardization - http://www.iso.org/
4 ETSI - European Telecommunications Standards Institute - http://www.etsi.org
5 ONTI - Oficina Nacional de Tecnologías de Información - http://ca.pki.gov.ar
6 Jefatura de Gabinete de Ministros - http://www.pki.gov.ar

La firma digital es un algoritmo criptográfico que asocia la identidad de una persona a un mensaje o documento, utilizando la tecnología de clave pública para cifrar el mensaje. De este modo, quien posea el mensaje original y la clave pública del firmante puede establecer fehacientemente que dicho mensaje fue encriptado con la clave privada asociada para determinar su autoría y también mediante un procedimiento determinado, comprobar su integridad.

Si bien su desarrollo y aplicabilidad tiene diferentes grados de avances en el mundo, la tendencia general es su incorporación en el corto y mediano plazo. Surge así, un sistema de seguridad basado en el uso de certificados digitales [1], teniendo cada firmante un certificado asociado, que le permite ser identificado dentro de las operaciones en las que utilice firma digital.

Para garantizar la operatividad, validez y seguridad de las transacciones y aplicaciones que utilicen certificados digitales, se necesita de una infraestructura adecuada que cuente con leyes, normativas, políticas, personal capacitado, hardware, software, estándares tecnológicos y procedimientos de seguridad. La misma recibe el nombre de Infraestructura de Firma Digital o Infraestructura de Clave Pública, cuya sigla en inglés es PKI (Public Key Infrastructure) [2] y hace referencia a las tecnologías utilizadas para la generación de los certificados digitales, temas que serán desarrollados oportunamente.

2 Situación actual

2.1 Situación Nacional

En nuestro país, las actividades relativas a la firma digital en el Estado, se inician en el año 1998, mediante la definición de los estándares tecnológicos aplicables en la Administración Pública Nacional[7] y se formalizan en el año 2001 con la sanción de la Ley N° 25.506[8] y su decreto reglamentario N° 2628/02[9] que formalizan la Infraestructura de Firma Digital de la República Argentina (IFDRA)[10]. A partir de febrero del 2007, se completa el esquema que garantiza la operatividad de los certificados digitales, al establecer el marco normativo para el otorgamiento y revocación de las licencias a los certificadores que lo soliciten, mediante la Decisión Administrativa JGM N° 6/07[11].

7 Resolución SFP Nº 194/98 -, http://infoleg.mecon.gov.ar/infolegInternet/anexos/50000-54999/54714/norma.htm

8 Ley Nacional de Firma Digital N° 25.506 -, http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

9 Decreto Reglamentario 2628/02 -, http://infoleg.mecon.gov.ar/infolegInternet/anexos/80000-84999/80733/norma.htm

10 Infraestructura de Firma Digital de la República Argentina -, http://www.sgp.gov.ar/contenidos/onti/productos/firma digital infraestructura.html

11 Decisión Administrativa 6/2007 -, http://infoleg.mecon.gov.ar/infolegInternet/anexos/125000-129999/125115/norma.htm

Como resultado, se tiene actualmente que la Secretaría de la Gestión Pública, dependiente de la Jefatura de Gabinete de Ministros del Gobierno Nacional, es la autoridad de aplicación de la Ley N° 25.506.

Otra infraestructura que ha cobrado magnitud es la desarrollada en la Provincia de San Luis[12], quienes han desarrollado una infraestructura completa, brindando diferentes servicios a la comunidad utilizando certificados digitales.

Por otra parte, existen iniciativas privadas basadas en certificados digitales emitidos por empresas radicadas en el país que cuentan con la infraestructura para la operatividad de los mismos en diferentes aplicaciones.

2.2 Situación de la Provincia de Santa Fe

En el ámbito Provincial de Santa Fe, en el año 2005 se sancionó la Ley N° 12.491[13] de adhesión a la Ley Nacional de firma digital, y cuenta con una Infraestructura provincial, creada por el Decreto Reglamentario N° 1573/2008[14]. Esto ha permitido desarrollar aplicaciones de firma digital en circuitos específicos de la administración con el objetivo de despapelizar, optimizar tiempos y procesos. Sin embargo, aún no se han iniciado actividades para implementar certificación de fecha y hora como una tecnología complementaria y necesaria para muchos procesos administrativos.

2.3 Propuesta

Este proyecto se desarrolló dentro de la Infraestructura de Firma Digital de la Provincia de Santa Fe, la cual depende de la Secretaría de Tecnologías para la Gestión del Ministerio de Gobierno y Reforma del Estado y a partir del análisis de la estructura existente se propuso la evaluación y diseño de un proceso de implementación piloto de certificación de fecha y hora, brindando los lineamientos necesarios para su implementación definitiva.

Como toda nueva tecnología, se necesitó que la misma fuera estudiada, evaluada y analizada para determinar si se adaptaba o no a la realidad provincial.

2.4 Justificación

Consideremos un ejemplo donde el concepto “tiempo” juega un rol importante en las actividades humanas, como es el escenario de un Concurso público de Ofertas para la licitación de una obra.

---

12 Instituto de Firma Digital de la Provincia de San Luis -, http://www.pki.sanluis.gov.ar/

13 Ley de la Provincia de Santa Fe de Firma Digital N° 12.491. -, http://www.santafe.gov.ar/index.php/web/content/view/full/64084

14 Decreto Provincial de Santa Fe 1573/08 -, http://www.santafe.gov.ar/index.php/web/content/view/full/64099

A partir del momento que se hace el llamado a la licitación, se desarrolla un proceso con diferentes etapas en las cuales se deben respetar tiempos estrictos, ya sea para la fecha de publicación del pliego, los períodos en el que pueden realizar consultas técnicas, se responden las consultas, se evalúan las ofertas, se pueden presentar impugnaciones, se realiza la adjudicación, se realizan ampliaciones o cambios en los productos ofertados, se emiten los respectivos documentos administrativos, se entregan los productos, se realiza el pago a proveedores, se ejecuta la garantía, etc.

Cada una de estas etapas tiene procedimientos establecidos con plazos fijos e inamovibles que requieren de un estricto control de fecha y hora que evite fraudes y aporte legalidad, transparencia y agilidad al proceso completo. Para el ejemplo citado, la Provincia de Santa Fe, cuenta con la infraestructura necesaria para garantizar la validez jurídica de las notificaciones y documentos que se hayan firmados digitalmente, pero carece de un mecanismo válido y certero para certificar la fecha y hora de cada una de las etapas detalladas.

Al no disponer de la tecnología específica para ello, los trámites existentes y las nuevas operaciones, firmadas o no digitalmente, que requieren una certificación de fecha y hora fehaciente, tales como voto electrónico, movimientos de expedientes, presentaciones ante la justicia, concursos de personal, etc., se encuentran limitadas en su implementación.

En este contexto, se consideró necesario la evaluación y el diseño de una Infraestructura de Certificación de Fecha y Hora en la provincia de Santa Fe, que se basara en estándares internacionales, atendiendo a necesidades expuestas.

3 Marco Teórico

3.1 Time-Stamping

Time-Stamping (TS) [3] es la tecnología que permite demostrar que una serie de datos han existido y no han sido alterados desde una fecha y hora determinada. Esto es válido de aplicar en operaciones electrónicas, movimientos, modificaciones y/o consultas de información dentro de un sistema informático.

La implementación de esta certificación se realiza a través de lo que se denomina Autoridad de Sellado de Fecha y Hora, en inglés conocida como Time Stamping Authority (TSA).

Para asociar los datos (por ejemplo archivos de documentos, videos, música, fotos, etc.) con un instante de tiempo es necesario disponer de una infraestructura adecuada, la cual requiere de un conjunto de leyes, normativa, personal capacitado, hardware, software, estándares tecnológicos y procedimientos de seguridad.

3.2 Estándares aplicables

Un estándar, como lo define la ISO[15] *"*son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito*"*. La documentación la realizan diferentes organismos internacionales, con el objetivo que los mismos sean difundidos y captados de igual manera, tanto por entidades o personas que los vayan a utilizar.

Uno de los tantos organismos internaciones de estandarización existentes es IETF[16] cuya principal función es la investigación y desarrollo de nuevas tecnologías para diseño, uso y manejo por Internet. El análisis de nuevas propuestas y la regulación de los estándares, son publicados bajo la forma de RFC[17] (Request For Comments). RFC significa "solicitud de comentarios" y consiste en un documento formal de la IETF que es el resultado de un estricto proceso de selección, elaboración y análisis que asegura su calidad y coherencia. Detalla prácticamente aspectos relacionados con la tecnología asociada a Internet, tales como, propuestas para una nueva tecnología, información acerca del uso de tecnologías y/o recursos existentes, propuestas de mejoras de tecnologías y proyectos experimentales.

Un servicio de Time-Stamping debe cumplir con los estándares internacionales vigentes, los cuales contribuyen a la interoperabilidad, siempre que las aplicaciones de software que también los utilicen.

Los estándares para Time-Stamping son:

- RFC 3161[18] "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)".
- RFC 3628[19] "Police Requeriments for Time-Stamping Authorities TSAs".

La adopción de estos estándares es porque se consideran los más utilizados y surge como consecuencia de una investigación sobre la implementación de TS en diferentes países.

A modo de ejemplo, se pueden mencionar, la implementación de TS en Costa Rica[20], el proyecto CERES[21] en España, sitios privados, tales como CECOBAN[22] en México, CERTISUR[23] en Argentina e incluso el proyecto OpenTSA[24] de Debian, el

15 International Organization for Standardization - http://www.iso.org/
16 Internet Engineering Task Force - http://www.ietf.org
17 IETF - Internet Engineering Task Force - http://www.ietf.org/rfc.html
18 RFC 3161 - http://www.ietf.org/rfc/rfc3161.txt
19 RFC 3628 - http://www.ietf.org/rfc/rfc3628.txt
20 Costa Rica, Política de sellado de tiempo del Sistema Nacional de Certificación -, http://www.firmadigital.gob.cr/Documentos/PoliticadeSelladodetiempover100.pdf
21 España, proyecto CERES -, http://www.cert.fnmt.es/index.php?cha=adm&sec=2&page=16&lang=es
22 CECOBAN - http://productos.cecoban.com.mx/productos/sellos-digitales-de-tiempo/
23 CERTISUR - http://www.certisur.com/manejo-documental-seguro
24 OpenTSA - http://opentsa.org/

modelo e-ping[25] Estándares de Interoperabilidad del Gobierno Electrónico de Brasil, el Proyecto Mercosur Digital[26], apoyado por la Unión Europea o la Plataforma de sellado de Tiempo TS@ del Ministerio de Política Territorial y Administración Pública del Gobierno de España[27].

La RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)" define aspectos acerca de proceso de Time-Stamping, incluye el formato de solicitud de sellos de tiempo (Request Format), el formato de devolución (Response Format), mecanismos de transporte (email, ftp, etc.) y aspectos de seguridad.

En detalle, la RFC 3161 referente a sellado de tiempo, define secciones, tales como una introducción al estándar, las obligaciones de la TSA, las transacciones, los formatos de solicitud y respuesta de sellos de tiempo y consideraciones de transporte. Si bien no existe ningún mecanismo obligatorio para el transporte de sellos de tiempo, la RFC detalla algunos mecanismos opcionales, tales como, basado en email, File Based Protocol, Socket Based Protocol o Protocol vía HTTP.

4.3 Firma Digital

La Firma digital es una herramienta tecnológica que permite garantizar la integridad, inalterabilidad y autenticidad de los documentos enviados por medios electrónicos, así como también permite verificar su autoría.

Es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente. La creación y verificación de firmas digitales se realiza mediante procedimientos técnicos, y supone la existencia de normas que respaldan su valor legal.

Funciona utilizando complejos procedimientos matemáticos que relacionan el documento firmado con información propia del firmante, el mismo, mediante una función matemática, genera una huella digital del mensaje, la cual se cifra con la clave privada del firmante. Permite establecer en documentos digitales, características que eran propias de los documentos en forma física o papel brindándonos las siguientes propiedades importantes:

- *Autoría*: implica poder atribuir de forma que no admite duda, que el mensaje electrónico recibido es de una determinada persona, autora del mensaje.
- *Integridad*: implica la certeza de que el mensaje recibido por el receptor es exactamente el mismo mensaje enviado por el emisor, sin que haya sufrido alteración alguna durante el proceso de transmisión.
- *No repudio*: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado.

---

25 e-Ping -, http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-deinteroperabilidade

26 Mercosur Digital - http://www.mercosurdigital.org

27 Plataforma de Sellado de Tiempo Ts@ - http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=tsa

Con la implementación de firma digital, ya no es necesario desplazarse desde un lugar de trabajo o la casa para realizar trámites que muchas veces requieren largas esperas, puesto que no se requiere desde ahora de la presencia física de las partes para la suscripción de acuerdos. Se abre paso a una multitud de nuevas formas de contratación de trámites públicos y privados que pueden realizarse digitalmente con mayor seguridad. Gráficamente se ilustra el proceso en la Figura1.

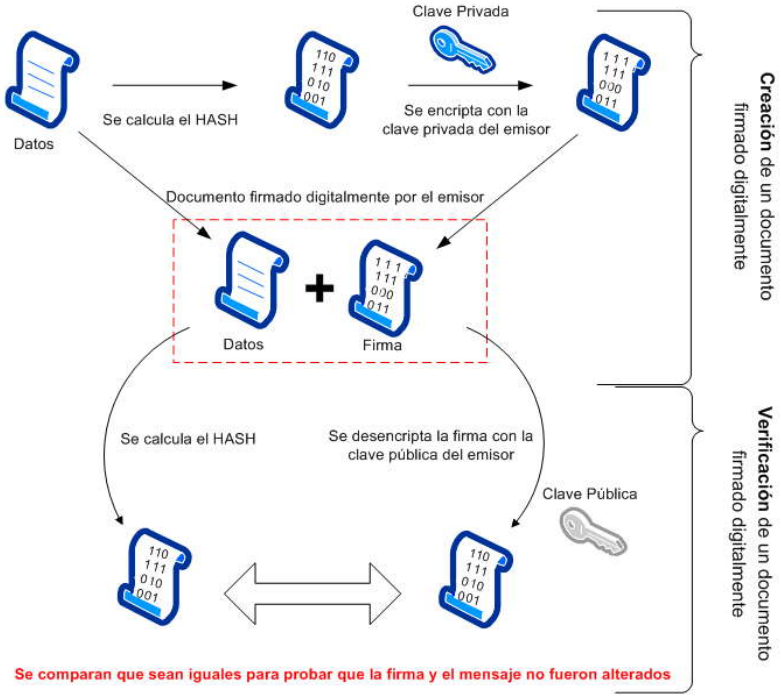


Figura 1: Proceso de Firmado y verificación

4.4 Time-Stamping y su relación con Firma Digital

Cuando se utiliza firmado con Time-Stamping se unen dos procedimientos que coexisten por separado, el procedimiento de firmado digital y el de Time-Stamping. Lo primero que se hace es firmar el documento luego, se adiciona un Time-Stamp dejando constancia del momento en que se firmó el documento. En este caso, para el proceso de Time-Stamping se tiene como entrada los datos de un documento con una firma digital asociada, emitida por una entidad de confianza. Considerando al documento firmado como cualquier conjunto de datos electrónicos, se trabaja con las pautas del procedimiento explicado anteriormente de Time-Stamping.

Como conclusión podemos decir que para aplicar Time-Stamping no importa si los datos vienen firmados o no. En el primer caso, al final del proceso los datos tienen una firma más un Time-Stamp y en el segundo, los datos sólo tienen el Time-Stamp

La principal ventaja de unir el proceso de Firma Digital con Time-Stamping radica en agregar más seguridad a las transacciones digitales. No sólo se cuenta con las propiedades de Integridad, Autenticación y No Repudio dadas por una firma digital, sino que además se puede determinar fehacientemente el momento que se creó la misma. Como se mencionó anteriormente, esto juega un rol importante en las transacciones donde se manipula información que tiene una validez que depende del tiempo, como por ejemplo, concursos de precios, voto electrónico, movimiento de expedientes, etc.

La Figura 2 ilustra el proceso completo en donde, a partir de los datos firmados se le inserta un Time-Stamp provisto por la TSA.

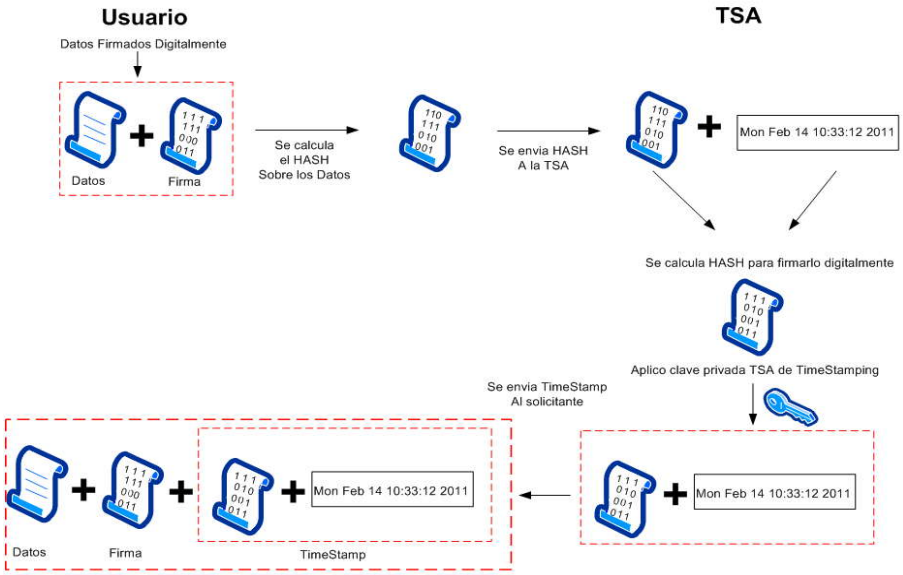


Figura 2: Proceso de Firmado con Time-Stamping

5 Propuesta Tecnológica

5.1 Tecnología para la obtención de fecha/hora

Dentro de las opciones posibles a implementar se tomaron como base los criterios de Confiabilidad, Accesibilidad, Disponibilidad y Redundancia para determinar qué

opción era la más viable. Se seleccionó NTP (Network Time Protocol) como la tecnología para la selección de fecha y hora porque dado que es un proyecto académico, el mayor limitante en la implementación de la solución óptima son los costos en la adquisición de hardware específico. NTP presenta sencillez, alta confiabilidad y disponibilidad por tratarse en un entorno de red local. Por ello, si bien se analizaron, fueron descartadas implementaciones tales como un reloj atómico, uno controlado por satélite o la instalación y configuración de una clock card en un servidor.

En base al hardware que se dispone en el gobierno provincial, la infraestructura de red local, la infraestructura de red existente en la Red Provincial de Datos, la normativa legal respecto a su uso y los criterios anteriormente detallados, se analizó el escenario que brindara una solución viable para este ambiente de investigación.

Específicamente, para su configuración se trabajó con SuSE[28] versión 11.3 como sistema operativo, siendo SuSE la distribución de Linux oficial en los servidores de la Provincia. Su fuente de actualización horaria se basa en una primaria, un servidor público stratum nivel 1 (http://tic.ntp.telstra.net) y una secundaria, un servidor interno stratum 2 perteneciente a la Red de Servidores de la Provincia.

5.2 Implementación para Time-Stamping

En la implementación propuesta como solución tecnológica contamos con dos agentes que interactúan, los usuarios y la TSA. Los usuarios, son todas aquellas personas que solicitan un sello de tiempo para un determinado fin, los mismos son peticiones http o https a un puerto determinado de la TSA.

Luego un aplicativo específico con soporte para Time-Stamping correctamente configurado hace esta tarea transparente para el usuario. La TSA es la encargada de dar respuestas a la peticiones, devolverlas firmadas y almacenarlas en algún esquema de base de datos.

El funcionamiento de la implementación es cliente-servidor, detallando en esta sección la solución propuesta para una entidad emisora de sellos de tiempo, que se basa en las librerías OpenTSA[29].

OpenTSA permite desarrollar un servidor estable, seguro, de código abierto para una autoridad de sellado de tiempo de acuerdo a los estándares y directivas expuesta en la RFC 3161.

La Figura 3 ilustra el proceso detallado anteriormente.

28 OpenSuSE - http://suse.org/
29 Librerías OpenTSA - http://www.opentsa.org/#download

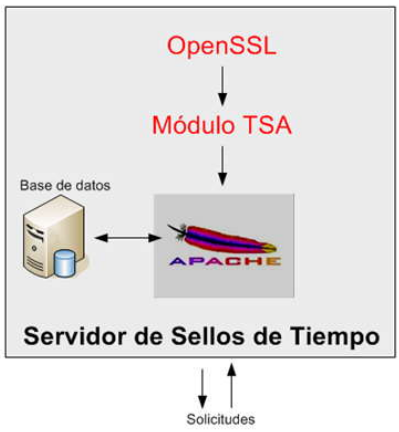


Figura 3: Esquema de funcionamiento de una TSA con OpenTSA

Cuando alguien recibe un sello de tiempo se debe verificar fehacientemente que se trata de un sello válido de la TSA configurada como entidad de confianza y ésto simplemente se realiza con la implementación de certificados digitales.

La Figura 4 ilustra el esquema donde un usuario solicita sellos de tiempos a una TSA de confianza.

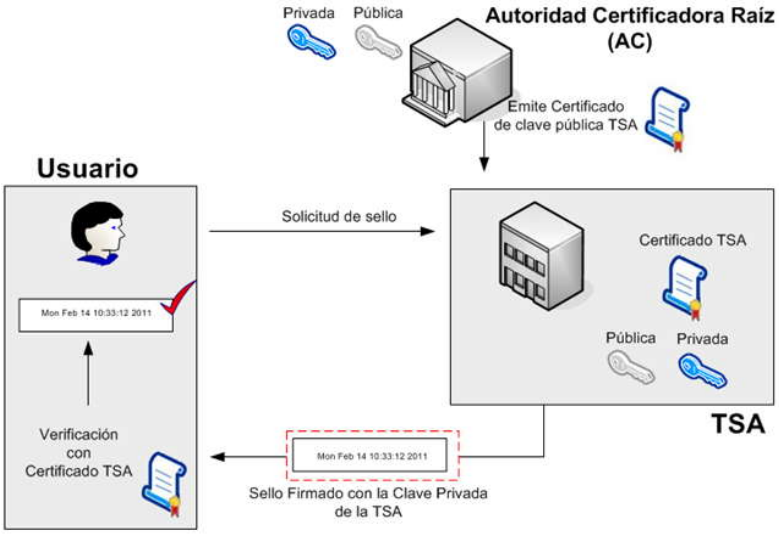


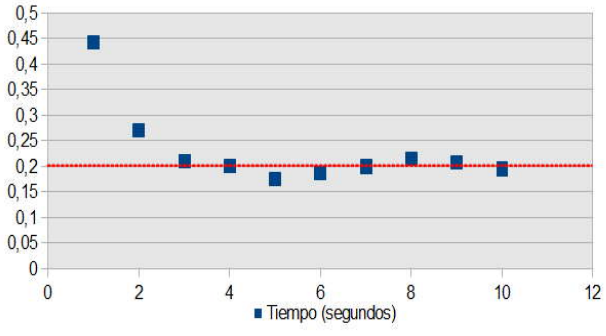
Figura 4: Esquema de funcionamiento de una TSA con OpenTSA

6 Pruebas y análisis

Para verificar el funcionamiento y rendimiento del servidor TSA se realizaron pruebas las cuales contemplaban integrarlo a la Red provincial de Datos de la Provincia de Santa Fe. Para considerar un mayor abanico de escenarios se seleccionaron diferentes medios físicos de conexión (VPN, Fibra Óptica, enlaces MPLS) y cinco localidades distantes geográficamente en la Provincia de Santa Fe (Rosario, Reconquista, Rafaela, Tostado y Santa Fe).

La prueba consistió, desde cada una de las localidades, realizar 10 peticiones de sellos de tiempo y de este modo, se pudo analizar los tiempos de respuesta por cada petición.

Dependencia: Educación Reconquista

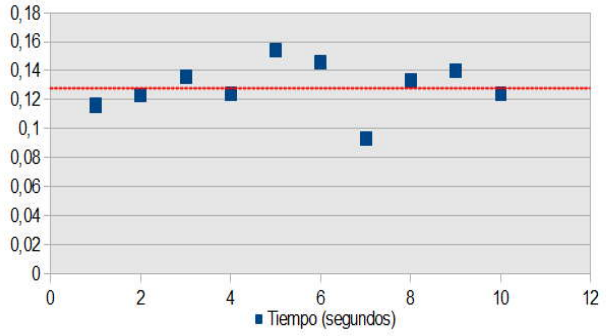


Medición Número	Tiempo
1	0,441699
2	0,270709
3	0,210780
4	0,199957
5	0,175141
6	0,187140
7	0,199442
8	0,214999
9	0,207119
10	0,194828

AVG: 0,226181 (segundos)

Figura 5: Medición de tiempos de Respuesta-Reconquista

Dependencia: API Rafaela



Medición Número	Tiempo
1	0,116075
2	0,122942
3	0,135666
4	0,123667
5	0,153938
6	0,145454
7	0,093081
8	0,133286
9	0,139709
10	0,124213

AVG: 0,128803 (segundos)

Figura 6: Medición de tiempos de Respuesta-Rafaela

Como se observa en las Figuras 5 y 6, los tiempos de respuesta del servidor están en el orden de milisegundos, con valores alrededor de la media. Estos valores relativamente bajos, representan un buen resultado para incluir la TSA en un proceso de firmado digital futuro, dado que no influye la distancia geográfica o medio físico de conectividad que nos generen demoras y degraden la calidad del proceso de TimeStamping.

Como última instancia, en la Figura 7 se muestra la estructura del sello de tiempo emitido por TSA para poder verificar que los campos cumplen con un sello de tiempo definido por el estándar.

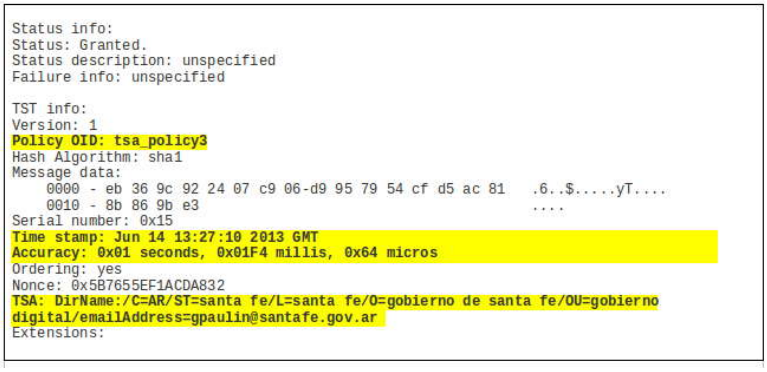


Figura 7: Estructura de un sello de Tiempo emitido por OPENTSA

7 Conclusiones

El Poder Ejecutivo Provincial ha avanzado en el desarrollo de propuestas innovadoras que permitan agilizar y aportar eficiencia y eficacia a los procesos del Estado para llegar, en última instancia, a su principal beneficiario que es el ciudadano. En este marco, se han impulsado actividades de gobierno electrónico que comprenden también la administración electrónica dentro de la organización y es en este escenario, que la firma digital cobra protagonismo.

En la medida que se ha avanzado con aplicaciones sobre firma digital, se ha detectado necesidades relativas al establecimiento de fecha y hora cierta en las transacciones digitales, con o sin firma digital.

Es por ello, que en una primera instancia se analizaron y evaluaron alternativas para la obtención de fecha y hora confiable y todas las consideraciones necesarias para la puesta en funcionamiento de una Autoridad de Time-Stamping (TSA). En una segunda etapa, presenta también como integrar esta tecnología de Time-Stamping con firma digital.

Con respecto a la obtención de fecha y hora confiable, se trabajó una propuesta basada en la utilización del protocolo NTP, la cual no requiere infraestructura hardware y permitió alcanzar una alta precisión horaria sincronizando con servidores oficiales. Como principal ventaja se tiene que este servicio es fácilmente configurable

e integrable con el servidor existente, aportando atributos de calidad, tales como confiabilidad, accesibilidad, disponibilidad y redundancia. Pero, el aporte central de esta tesis es que la misma permite mostrar una forma para generar sellos de tiempo a través de una TSA, en el marco de las políticas y normativas del Gobierno Provincial.

Al respecto y dado que la Provincia adhirió a la ley de software libre, la propuesta se centró en la búsqueda de proyectos y herramientas OpenSource para implementar una TSA.

Se estudiaron en detalle las librerías OpenTSA que implementa una autoridad de sellado de tiempo código abierto con integración con OpenSSL, OpenSSL que permite la creación de peticiones de sellado de tiempo, generación de respuestas y la verificación, el módulo TSA para el servidor Apache permitiendo crear un servidor que cumple con lo especificado en la RFC 3161 y utiliza tanto HTTP como HTTPS y el cliente de sellado de tiempo que provee comandos para la creación y envío de requerimientos de sellado de tiempo sobre HTTP o HTTPS.

De este modo, se propone una infraestructura que respeta el marco normativo existente en la Provincia de Santa Fe y que permite una puesta en producción a mediano plazo y de bajo costo.

Como anexo a este trabajo principal, se desarrolló un prototipo de aplicativo básico donde se utilizan los sellos generados por la TSA y se los integra a la firma, mostrando de este modo, cómo ambas tecnologías se complementan para aportar mayores niveles de seguridad a las transacciones electrónicas.

Apéndice

Implementación para Time-Stamping

El funcionamiento de la implementación es cliente-servidor, detallando en esta sección la solución propuesta para una entidad emisora de sellos de tiempo, que se basa en las librerías OpenTSA.

Se utilizó un servidor con las siguientes características, suponiendo cumplidas las expectativas de rendimiento:

- Procesador Intel Core 2 Duo E7500.
- Disco rígido: 250 Gb.
- Memoria RAM: 2GB DDR 3.
- Placa de Red Ethernet 10/100/1000.

Dado que OpenTSA son librerías opensource y se requería compilarlas para sistema operativo Linux, se implementó en Debian 6.0.4 (stable) dado que Debian es estándar en la provincia desde que se adhirió a la Ley de Software Libre (marzo 2012).

Los necesarios paquetes requeridos por OpenTSA:

- Servidor Web Apache no había opción de seleccionar otro diferente dado que las librerías compilan un módulo para este servidor específico.
- MySQL

Dado que OpenTSA son librerías opensource y se requería compilarlas para sistema operativo Linux, se implementó en Debian 6.0.4 (stable) dado que Debian es estándar en la provincia desde que se adhirió a la Ley de Software Libre (marzo 2012).

Cumplidos lo requerimientos en el sistema que solicita OpenTSA, se procedió a la compilación, cuyo resultado es el módulo mod tsa.so que funcionará con Apache para la solicitud vía http de sellos de tiempo.
En detalle:

1. make OPENSSL=/usr/local/ssl TS MYSQL=1
2. make install

Una vez compilado e instalado el modulo time-stamping para Apache, quedan las dos últimas etapas de configuraciones.

La creación y configuración de la base de datos, que almacenara los token que se generen y envien, se hizo a través del gestor de MySQL, el paquete OpenTSA ya trae el script de SQL para generar la tabla, solo restó crear la base de datos con los comandos de SQL:

1. mysql –u root -p
2. create database tesis tsa;

Antes de configurar OpenSSL, se necesita definir las claves y posteriormente certificados para que la TSA firme los token de tiempo. Dado que no se dispone una Autoridad de Certificación que avale la TSA para la emisión de token, y no es objeto de estudio del presente trabajo, se creó una propia CA en el servidor TSA.

1. Creación de un par de clave pública y privada de la CA.

   debian#openssl req -x509 -newkey rsa:2048 -keyout cakey.pem -days 650 -sha256 –out cacert.pem

   Detalles de los parámetros solicitados:
   a. Phrase: gobierno digital
   b. Country Name: AR
   c. State or Province Name: santa fe
   d. Locality: santa fe
   e. Organization Name: gobierno de santa fe
   f. Organizational Unit Name: secretaria de tecnologia para la gestion
   g. Common Name: Guillermo Paulin
   h. Email Address: gpaulin@santafe.gov.ar

La clave privada de la CA es cakey.pem, la clave pública cacert.pem y las mismas tendrán un periodo de validez de 3650 días, es decir, 10 años.

2. Creación de un par de clave pública y privada de la TSA (tsspub.pem y tsskey.pem).

   debian#openssl req -newkey rsa:2048 -keyout tsakey.pem -sha256 -out tsaCSR.pem

   Detalles de los parámetros solicitados:
   a. Phrase: tsasantafe
   b. Country Name: AR
   c. State or Province Name: santa fe
   d. Locality: santa fe
   e. Organization Name: gobierno de santa fe
   f. Organizational Unit Name: gobierno digital
   g. Common Name:
   h. Email Address: gpaulin@santafe.gov.ar

   La clave privada de la TSA será tsakey.pem y la clave pública tsaCSR.pem. Si bien ya se dispone de un conjunto de claves y podemos utilizarlas, éstas no tienen validez legal si no estan avaladas por una AC.
   .

3. AC Raíz emite certificado de clave pública TSA.

   debian#openssl -x509 -CA cacert.pem cakey.pem tsakey.pem -req -in tsaCSR.pem -days 365 -sha1 -CAcreateserial -out tsaCRT.pem -extfile openssl.cnf

   La nueva clave pública de la TSA ser_a tsaCRT.pem con un periodo de validez de 365, es decir, un año. A partir de éste momento se puede utilizar la clave privada en la TSA dado que está avalada por una AC de confianza.

   Gráficamete el paso nro 3 lo podemos observar en la siguiente imagen:

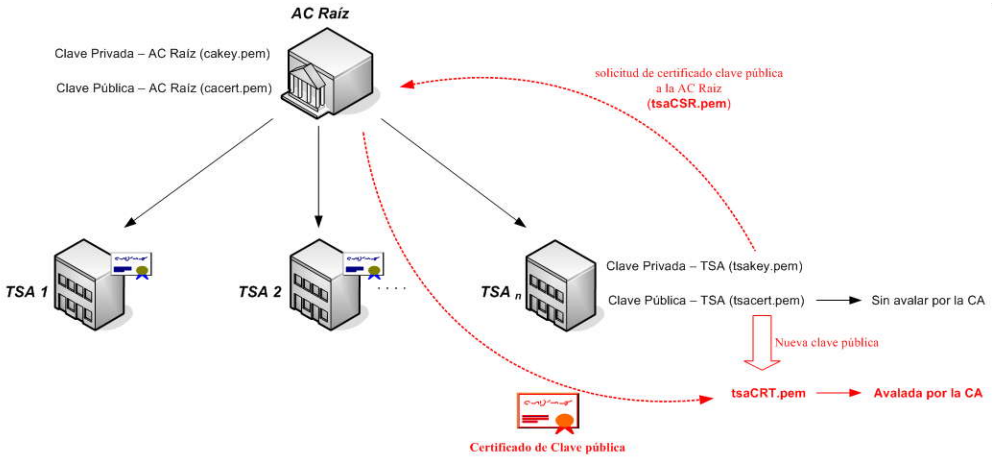


Figura 8: Proceso de generación de certificados

Seguidamente para que se genere los sellos de tiempo se deben agregar las rutas de los certificados y algunos parámetros en el archivo de configuración del openssl denominado openssl.cnf ubicado en el directorio /etc/ssl.

Para funcione Time-Stamping se edita el siguiente tag:
[usr cert]
extendedKeyUsage = critical, timestamping
En cuanto a los certificados creados los siguientes tags:
[CA default]
[tsa config1]

Concluida la etapa de configuración de los paquetes dependientes del módulo tsa, resta configurar el tsa.conf ubicado en el directorio /etc/apache2/mods-enables/

La configuración de los parámetros de la base de datos creada:
TSAMySQLHost localhost
TSAMySQLPort 3306
TSAMySQLUser [usuario de acceso a la base de datos]
TSAMySQLDatabase [base de datos creada]
TSAMySQLUnixSocket [ruta del .pid del proceso MySQL]

El último ítem que resta configurar es los certificados de la TSA:
TSACertificate [ruta del certificado emitido por la CA]
TSAkey [ruta de la clave privada]

Bibliografía

1. Talens-Oliag Sergio. “Introducción a los Certificados Digitales”. http://www.uv.es/sto/articulos/BEI-2003-11/certificados digitales.html
2. C. Adams and S. Lloyd, (1999), “Understanding Public-Key Infrastructure”, Macmillan Technical Publishing.
3. T. Nishikawa, S. Matsuoka, (2008), “Time-Stamping Authority Grid”, IEEE, vol. 7, p. 98 - 105.
4. Ros Anderson, (2000), “Two remarks on Public keys Cryptology”. http://www.citeulike.org/user/zooko/article/2363607
5. R. Miskinis, D. Smirnov, E. Urba, A. Burokas, (2010), “Digital time stamping system based on open source technologies”, IEEE, vol. 57, p. 721 - 727.
6. R.Gatautis, M. Romeris, P. Laud, R. Satkauskas, (2008), “Enhancing e-Government Services through Digital Time Stamping:Time Stamping System Specifications”, IEEE, vol. 57, p. 204 - 210.
7. Adams, C. Cain, P. Pinkas, D. and Zuccherato, R., (2001), “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”, IETF RFC 3161.
8. Policy requirements for time-stamping authorities. (2003). European Telecommunications Standards Institute Technical Specification 102 023 (ETSI TS 102 023), v.1.2.1.
9. Williams Stallings, (2004), “Comunicaciones y Redes de Computadores”, Prentice Hall.
10. Pablo A. Anselmo, (2007), “Criptosistemas Simétricos y Asimétricos”, Revista Nex IT nro 35, páginas 50-55. http://www.nexweb.com.ar
11. IETF RFC 1829, (1995), “The ESP DES-CBC Transform".
12. IETF RFC 1851, (1995), “The ESP Triple DES Transform".
13. IETF RFC 3394, (2002), “Advanced Encryption Standard (AES) Key Wrap Algorithm”.
14. G. C. Sackett, (2002),”Manual de Routers Cisco”, McGraw-Hill.
15. W Die, ME Hellman, (1976), ”New Directions in Cryptography'", IEEE Transactions on information theory v 22 no 6, pp 644-654.
16. IETF RFC 2313, (1998),”PKCS #1: RSA Encryption Version 1.5”.
17. IETF RFC 1321, (1992),”The MD5 Message-Digest Algorithm”.
18. FIPS Publication 180-1, (1995), “Secure Hash Standard”.
19. Autoridad Privada Argentina de Certificación Digital, Certificado Digital. http://www.certificadodigital.com.ar/download/GUsuario.pdf
20. Ministerio de Ciencia y Tecnología (MICIT) Republica de Costa Rica, (2007), “Política de sellado de tiempo del Sistema nacional de certificación digital”
21. Husos Horarios http://www.worldtimezone.com/index_es.php
22. Postigo Linares, (2010), Coordinated Universal Time, “Desarrollo de la hora Nacional'".
23. Arias, Elisa Felicita, "Informe acerca de la problematica de la hora oficial y legal de Argentina'". http://www.prmarg.org/upload/Informe-Problematica-Hora-Oficial.pdf
24. Housley. R., (2004), “Cryptographic Message Syntax", IETF RFC 3852.
25. Bruera, Horacio, “Criterios jurisprudenciales en materia de firma digital”,

http://www.carranzatorres.com.ar/index.php?option=com_content&view=article&id=437:criterios-jurisprudenciales-en-materia-de-firma-digital&catid=96:guardar&Itemid=166

26. España, Boquera Maria, (2003), "Servicios avanzados de Telecomunicación", Diaz de Santos.
27. Dibowitz, Phil, "X509 and SSL", http://www.phildev.net/ssl/ssl_talk_uuasc.pdf
28. Espinoza, Carlos, "Seguridad Informática y Criptografía. Certificados Digitales y Estándar PKCS" http://es.scribd.com/doc/4680046/Seguridad-Informatica-y-Criptografia-Certificados-Digitales-y-Estandar-PKCS
29. Reyes, Alfredo Alejandro, "La Firma electrónica", http://www.razonypalabra.org.mx/libros/libros/firma.pdf