Implementando una Autoridad de Sellado de Tiempo con herramientas Open Source

Javier Díaz, Alejandro Sabolansky y Paula Venosa

LINTI - Facultad de Informática - Universidad Nacional de La Plata,
La Plata, B1900ASD, ARGENTINA
{javierd,asabolansky,pvenosa}@linti.unlp.edu.ar
http://www.linti.unlp.edu.ar

Resumen El tiempo es una magnitud que afecta a todas las actividades humanas y es un componente esencial en todos los procesos, donde registrar el momento exacto en que se suceden los acontecimientos es fundamental. Una aplicación que utiliza firma digital sobre una infraestructura PKI exige que la medida de tiempo usada sea precisa y acordada[1][2].
El sellado de tiempo (Time stamping) es un mecanismo que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo[3].
El presente artículo describe el trabajo realizado para implementar un servicio de sellado de tiempo utilizando herramientas open source, que cuenta con mecanismos de seguridad y monitoreo. Se detallan las componentes del servicio, los requisitos para implementarlo, las decisiones de la implementación propiamente dicha y lo aprendido en base a dicha experiencia.

1. Motivación

Al momento de visualizar un documento digital surgen dos interrogantes:

- ¿Quién es el autor de documento? ¿Quién autorizó su publicación?
- ¿Cuándo fue creado o modificado por última vez dicho documento?

En ambos casos la pregunta es sobre un documento específico y no otro. Una respuesta al primer planteo permite conocer quién y qué: Quién aprobó exactamente qué en dicho documento. La segunda de las preguntas planteadas permite saber cuándo y qué: Desde cuándo el contenido de ese documento existe.

Las preguntas presentadas ameritan analizar diferentes variantes. Una alternativa para responder la primer cuestión es la firma digital, mientras que una alternativa para responder el otro interrogante es el servicio de sellado digital de tiempo. En este marco, debe haber un procedimiento con el cuál un autor de un documento pueda firmar un conjunto de bytes que actúan como firma. Por otra parte, debe haber un mecanismo de verificación mediante el cual cualquier usuario puede chequear un documento y la firma adjunta para que, con garantía razonable, se pueda asegurar que la misma responde a las preguntas quién y qué, o cuándo y qué.

La firma digital es un mecanismo orientado a garantizar la identidad del emisor de la información, la integridad y confiabilidad de la información y el no repudio tanto del emisor como del receptor[4]. Esta es la forma que garantiza conocer quién ha hecho qué. Pero hay un parámetro importante que la firma digital no abarca; es el instante de tiempo en que ha sucedido ese determinado suceso. Esta falencia es la que genera el surgimiento de los mecanismos de sellado digital de tiempo.

Numerosos son los trabajos que se han realizado en relación a los aspectos conceptuales del sellado de tiempo[5][6], así como a los mecanismos existentes para implementarlos[7][8]. Algunas experiencias que se han publicado se centran en describir la implementación del servidor TSA y el cliente que genera los requerimientos[9][10][11]. Nuestro artículo presenta una visión integral de la implementación del servicio, desde los requerimientos normativos y técnicos, pasando por los criterios usados para la selección de los componentes, hasta la implementación propiamente dicha con herramientas open source; incluyendo también la integración con los servicios PKI y NTP, el desarrollo del frontend para el usuario final y las herramientas instaladas y puestas a punto para monitorear el servicio.

2. Introducción

La implementación de un servicio de sellado de tiempo fue el objetivo del trabajo de fin de carrera de la Licenciatura en Informática de la Facultad de Informática de la Universidad Nacional de La Plata[12], realizado por el actual egresado Alejandro Sabolansky, durante el transcurso del año 2010.

Las premisas para la implementación de la infraestructura de sellado de tiempo fueron utilizar software libre, teniendo en cuenta el cumplimiento de los estándares tecnológicos existentes, así como los requisitos necesarios para brindar un servicio 7x24.

Este servicio es esencial para ser integrado con sistemas de firma digital, en los cuales es fundamental tener certeza del momento cierto en que se realiza cada operación. La idea inicial era integrarlo con PKIUNLPGrid[13], la autoridad de certificación de la UNLP que emite certificados para e-ciencia, para lo cual se realizaron los análisis pertinentes, como parte del trabajo de investigación aquí presentado.

3. Componentes del servicio

El servicio de Time Stamping se sustenta en los mecanismos de firma digital y generalmente es un servicio adicional que prestan las autoridades de certificación. A grandes rasgos, existe una tercera parte de confianza, que es aceptada tanto por el emisor como por el receptor, que es la que da fe de la fecha y hora de una transacción. Es decir, añade el dato "tiempo" a la transacción o al documento, por el cual las partes aceptan la validez temporal que se asocia a ese dato determinado.

3.1. Entidades intervinientes

La normativa existente: RFC 3161[14], ISO 18014[15][16][17], X.995[18] relacionada con el sellado digital de tiempo, distingue las siguientes entidades principales:

- Solicitante: Es la entidad que posee documentos, información o, en general, cualquier tipo de datos electrónicos a los que quiere incluir un sello de tiempo que garantice que fueron creados previo a la solicitud del sello.
- Verificador: Es la entidad que quiere comprobar que los datos sellados que ha recibido contienen un sello de tiempo válido. Incluso podría ser la misma entidad que utilizó el servicio de sellado de tiempo, para comprobar que el sello generado es válido y correcto.
- Autoridad de sellado de tiempo: La autoridad de sellado de tiempo, TSA (Time Stamping Authority, por sus siglas en inglés) es el proveedor del servicio. Su finalidad es la de comprobar la existencia de los datos a sellar y generar el sello de tiempo que irá unido a esos datos. De esta forma, la TSA asegura que esos datos existían en un determinado instante de tiempo y garantiza que el parámetro de tiempo de ese sello es correcto.

3.2. Fases de sellado de tiempo

En el sellado de tiempo se diferencian dos procedimientos principales:

- Creación de sellado de tiempo: En primer término, el solicitante genera un hash (función o método para generar claves que representen de manera unívoca a un dato) de la información que quiere sellar. Este hash es enviado a la autoridad de sellado de tiempo, la cual anexa el sello de tiempo tiempo al hash y vuelve a calcular el resumen considerando ahora el nuevo dato generado. Este hash es firmado digitalmente con la clave privada de la TSA. Por último el hash firmado junto con el sello de tiempo son enviados al solicitante del sellado de tiempo.
- Verificación del sellado de tiempo: Cualquier entidad que confíe en el emisor del sello de tiempo puede verificar que el documento no fue creado después de la fecha que indica el sello. Para probar esto, se calcula el hash de la información original, se concatena a este hash el sello de tiempo recibido y se vuelve a calcular una nueva función de hash. En este punto, resta validar la firma digital de la TSA. Se debe verificar que el hash recibido fue firmado con la clave privada. Para ello, se aplica la clave pública de la TSA a dicho dato, y se comparan ambos hashes. Esta comprobación permite probar que el sello de tiempo y el mensaje no fueron alterados y que efectivamente fue emitido por la autoridad de sellado.

4. Requisitos para implementar la TSA

Para implementar la infraestructura sobre la cual se va a montar la autoridad de sellado de tiempo es necesario analizar las distintas alternativas para cada uno de los componentes.

Primero se debe contextualizar el servicio de sellado de tiempo dentro de un servicio de certificación de firma digital. Luego, es necesario definir la política de sellado digital de tiempo[19] adecuándose a lo especificado en la política de la autoridad de certificación, siguiendo las recomendaciones de las normativas existentes[20].

Una vez definida la política se debe definir la fuente confiable de tiempo que va a ser consultada por la TSA para sellar los requerimientos, teniendo como una opción probable el protocolo NTP (protocolo estándar muy aceptado), utilizando como fuente de referencia un reloj Stratum 0 tipo GPS.

Posteriormente, es preciso definir la Autoridad de Sellado de Tiempo, implementando una solución que cumpla con lo especificado en las política definida. Es una buena práctica definir servidores redundantes de almacenamiento, donde se resguardarán los sellos de tiempo emitidos para su posterior consulta y servidores replicados para poder recibir las solicitudes de los sellos de tiempo.

5. Selección de componentes

5.1. Criterios de selección de componentes

Los componentes que comprenden la puesta en funcionamiento del servicio de sellado digital de tiempo incluyen principalmente el producto de implementación de la RFC 3161, el sistema operativo y el servidor de base de datos para dar soporte de almacenamiento a la información generada en el servicio.

Para cada uno de los componentes mencionados para implementar el servicio, fue preciso analizar las ventajas y las desventajas de las distintas alternativas disponibles teniendo como precondición esencial el requisito de utilizar software libre para toda la solución así como los siguientes criterios:adecuación a la normativa existente relativa a los servicios de sellado digital de tiempo, licencia del software utilizado, comunidad que utiliza los potenciales productos o tecnologías y documentación existente y facilidad de acceso a la misma.

5.2. Implementación de la RFC 3161

Con respecto a la selección del producto que implementa el protocolo desarrollado en la RFC 3161, se analizaron tres alternativas distintas.

Openevidence[21]: Financiado por la comunidad europea, este es un framework de código abierto para la certificación, sellado temporal y archivo de datos que brinda tecnología para la creación de evidencias, validación y protección a largo plazo de documentos electrónicos. La funcionalidad es provista a través de dos módulos: el módulo de Apache (que las peticiones HTTP o HTTPS al protocolo basado en sockets y las respuestas del protocolo basado en sockets a HTTP o HTTPS) y un demonio de UNIX (que implementa las funcionalidades principales del servicio).

OpenTSA[22]: Esta aplicación, que implementa una autoridad de sellado de tiempo sin costo alguno y de código abierto provee: integración con OpenSSL

(creación de peticiones de sellado de tiempo, generación de respuestas y la verificación de las mismas; implementadas como una extensión para la última versión estable de OpenSSL), módulo de Apache (que funciona como un servidor que cumple con lo especificado en la RFC 3161 y utiliza tanto HTTP como HTTPS como protocolos de transporte) 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 y funcionalidad para verificar las respuestas recibidas)

Otra posible alternativa para implementar un servicio de sellado digital de tiempo es desarrollar una solución propia, para lo cual existen librerías públicas que implementan el protocolo en diversos lenguajes[23][24].

Una vez analizadas las diferentes posibilidades se debía elegir el producto a utilizar. Openevidence fue descartado porque el proyecto que lo implementó fue dado de baja en el año 2004, dejando como legado escasa documentación que hace casi imposible la puesta en funcionamiento del mismo. Por otro lado la alternativa de desarrollar una solución propia se desviaba del objetivo planteado, dado que el desafío no era construir algo desde cero sino integrar distintos productos seleccionados y establecer una configuración adecuada, para montar un servicio de sellado de tiempo eficiente y confiable. Por las razones aquí expresadas, OpenTSA fue el producto elegido.

5.3. Sistema operativo de base

Al momento de seleccionar el sistema operativo, la premisa planteada de utilizar software libre, redujo el espectro de productos a seleccionar.Por lo tanto todos los sistemas pertenecientes a la empresa Microsoft, varios sistemas UNIX propietarios como AIX de IBM y Solaris de Sun Microsystems, adquirida recientemente por Oracle, y algunas distribuciones Linux como SuSE Enterprise, quedaron descartadas.

Teniendo en cuenta la experiencia personal, la facilidad de uso, la gran comunidad que lo soporta y la documentación existente, la balanza se terminó inclinando hacia el lado de Debian GNU/Linux[25], por lo cual ese fue el sistema operativo de base elegido.

5.4. Servidor de base de datos

La decisión de utilizar el producto OpenTSA como servicio de Servicio de sellado de tiempo, restringe los motores de base de datos a utilizar, dado que de acuerdo a la documentación, el producto soporta tres motores de base de datos distintos: MySQL, PostgreSQL y Firebird. MySQL fue descartado debido a las diversas licencias existentes y a la aparición de Oracle como propietario de dicho producto.

Para decidir entre las otras dos alternativas, Firebird y PostgreSQL, se tuvo en cuenta que al momento de armar un infraestructura para soportar un servicio que requiere estar disponible 7X24, con una potencial gran cantidad de usuarios concurrentes accediendo al servicio, hay varias características deseables en un motor de base de datos: la replicación y el clustering tanto para balanceo de

carga como para tolerancia a fallos. Estas características no están disponibles en Firebird mientras que PostgreSQL las ofrece como una de sus características distintivas. Además, PostgreSQL cuenta con una gran cantidad de documentación en línea, foros, listas de correo, canales de chat, libros y una gran comunidad que contribuye a diario en el proyecto. Por lo detallado en los párrafos anteriores, se eligió PostgreSQL como Servidor de Base de Datos.

6. Principales decisiones de implementación

En los comienzos de la implementación se planteó la integración de este nuevo servicio de sellado de tiempo con la infraestructura PKI para e-ciencia "PKIUNLPGrid" que se encuentra disponible en la UNLP.

Para ello se realizó un análisis de factibilidad que incluyó tanto el estudio de la Política de Certificación (CP) y la Declaración de Prácticas de Certificación (CPS), como un análisis de compatibilidad entre los certificados emitidos por UNLP PKIGrid y las necesidades del producto OpenTSA.

Dado que la CA de UNLP PKIGrid emite certificados para actividades de e-ciencia realizadas dentro del ámbito de la UNLP, tanto para personas como para servidores y servicios, los certificados para una Autoridad de Sellado de Tiempo que preste soporte para los servicios de e-ciencia se enmarcan dentro de lo prescripto por la CA de UNLP PKIGrid. Por la tanto, a nivel normativo, los certificados necesarios para el servicio de sellado de tiempo podrían ser emitidos por el servicio de firma digital existente en la UNLP.

Luego de ello se analizaron los diversos perfiles de certificados emitidos por UNLP PKIGrid, y se concluyó que los certificados no podían usarse porque los valores en los campos Key Usage y Extended Kay Usage no coincidían con lo requerido para una TSA. A raíz de ello se requería instalar una nueva CA que se adecuara especialmente a las necesidades de nuestro servicio de sellado de tiempo

En cuanto al protocolo de transporte y el mecanismo de sellado de tiempo, la norma ETSI TS 101 861 obliga a disponer de un protocolo en línea para la Autoridad de Sellado de Tiempo, por lo cual utilizar el protocolo de sellado vía HTTP a través del servicio implementado por OpenTSA resulta apropiado conforme a esta normativa.

A fin de contar con una fuente confiable de tiempo en el servicio, se decidió utilizar el protocolo NTP para mantener sincronizada la hora de los servidores involucrados en la arquitectura de la Autoridad de Sellado de Tiempo.

7. Implementación del servicio

Las tareas de implementación de un servicio de sellado de tiempo involucra:

- Instalación de una Autoridad de Certificación.
- Instalación y optimización de un servicio de NTP.
- Compilación de librerías de SSL para el sellado de tiempo.

- Integración de Apache con OpenTSA.
- Desarrollo de un frontend web.

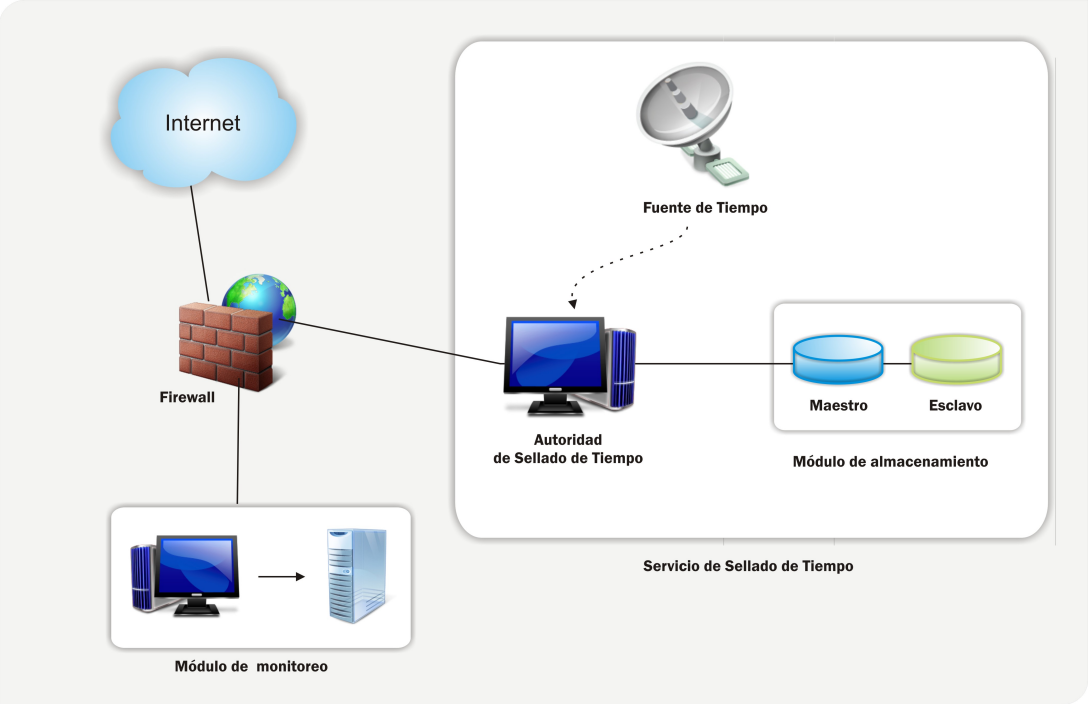

Figura 1. Arquitectura del servicio de sellado de tiempo

7.1. Instalación de una autoridad de Certificación utilizando OpenCA

Ante la necesidad de emitir certificados digitales para los diversos componentes de la Autoridad de Sellado de Tiempo, se ha decidido instalar el producto OpenCA[26]. La configuración de este producto tuvo en cuenta el análisis de las extensiones X.509 que soportan el sellado digital de tiempo.

7.2. Instalación de PostgreSQL

Para poder almacenar los sellos de tiempo emitidos, se ha elegido PostgreSQL como motor de base de datos, debido al soporte de replicación y alta disponibilidad. Para cumplir con este objetivo, se han instalado, configurado y optimizado dos instancias del producto, junto con el producto PGPPool-II, el cuál brinda tanto replicación como tolerancia a fallos.

7.3. Configuración de NTP

Se ha configurado un servidor de tiempo utilizando el paquete NTP provisto en la distribución del sistema operativo Debian. Para la sincronización de la hora del servidor de tiempo configurado se utilizan diversas fuentes, tanto pertenecientes a la infraestructura de la UNLP, como relojes disponibles en Internet e Internet 2. De esta forma, se proporciona un mecanismo de sincronización de alta disponibilidad y tolerancia a fallos de conectividad.

7.4. Integración de OpenTSA con Apache

Para poder hacer uso de OpenTSA, es necesario integrarlo a Apache, de forma tal que las peticiones a la TSA lleguen mediante el protocolo HTTP. Para ello, fue necesario compilar OpenTSA, indicándole la versión de OpenSSL a utilizar y los diversos motores de base de datos que debía soportar, entre ellos PostgreSQL, que resultó el elegido.

7.5. Frontend Web

Un componente fundamental en la puesta en funcionamiento de una Autoridad de Sellado de Tiempo, es la creación de una interfaz web que permita la interacción entre el usuario y la aplicación. Para ello se ha diseñado una sencilla aplicación que puede ser utilizada por dos perfiles de usuario, el usuario que interactúa con el servicio y el operador que tiene como misión monitorear el correcto funcionamiento del mismo. La interfaz pública tiene la siguientes funcionalidades:

- Listar tokens emitidos: Mediante esta opción es posible listar los tokens emitidos, visualizando algunos campos importantes que comprenden el sello de tiempo: el número de serie del token emitido, la fecha en formato UTC que indica el momento que el dato fue sellado, el hash del dato enviado y finalmente el algoritmo de resumen utilizado para realizar el hash.
- Validar tokens: Con esta función un usuario que posea un sello de tiempo emitido por esta Autoridad de Sellado de Tiempo, puede verificar la validez del sello. Para ello, el usuario debe subir al servidor el sello de tiempo, en un archivo con extensión .tsr y aguardar por la respuesta del servidor.
- Obtener certificados: Todas las Entidades Certificadoras entre las que podemos enmarcar a las autoridades de sellado de tiempo, deben ofrecer para su descarga los certificados digitales utilizados para la firma de los sellos de tiempo. Esta funcionalidad es proporcionada desde la opción Certificados.

Para la creación de esta interfaz web se han utilizado diversas herramientas y tecnologías para facilitar el desarrollo actual y una posterior ampliación de la funcionalidad del mismo: Perl, Ajax, PHP, CSS, entre otras.

8. Garantizando la seguridad del servicio

En un servicio que debe estar disponible 7X24, es necesario contar con un conjunto de herramientas que permitan monitorear el servicio en forma constante, de manera tal que cualquier anomalía en alguno de los componentes de la arquitectura, pueda ser detectada y subsanada en forma inmediata.

Teniendo en cuenta la experiencia personal adquirida en el campo de monitoreo de redes y servicios, se seleccionaron las herramientas más adecuadas y más aceptadas por la comunidad, y se configuraron y optimizaron las mismas con el objetivo de contar con la información necesaria para el análisis de comportamiento y monitoreo de disponibilidad de todos los componentes desarrollados.

Las herramientas instaladas y configuradas para el monitoreo fueron: MRTG[27], Nagios[28] y PNP for Nagios[29]

9. Conclusiones

Fue posible la puesta en funcionamiento del servicio, teniendo en cuenta los requerimientos de seguridad y monitoreo utilizando herramientas software libre.

A partir de esta experiencia, se pueden destacar los siguientes aspectos relevantes en relación a la implementación del servicio:

- Resulta imprescindible la implementación del servicio de sellado digital de tiempo debido a que la firma digital no garantiza el instante de tiempo en que se ha realizado la firma.
- Al momento de implementar una Autoridad de Sellado de Tiempo, la misma debe enmarcarse en la normativa vigente tanto para la definición de las políticas y procedimientos como para la implementación del servicio en sí mismo.
- El servicio puede ser implementado en su totalidad con componentes open source aprovechando las ventajas que otorga este paradigma. Las herramientas utilizadas, son desarrollos sustentados por una gran comunidad de usuarios y programadores alrededor del mundo, lo que convierte a estos productos en software estable y confiable.
- Es necesario actualizar constantemente el servicio implementado de acuerdo al estado del arte de los algoritmos criptográficos y demás componentes involucrados en la solución.

Por otra parte, este trabajo genera un aporte en la formación académica universitaria. Los tópicos desarrollados en este trabajo pueden ser incorporados como material de estudio en la cátedra de Seguridad y Privacidad en Redes, en la cual desempeñan su actividad docente los autores de este trabajo, tanto en las carreras de grado como en la Maestría en Redes de Datos.

Referencias

1. `http://physics.nist.gov/GenInt/Time/world.html`. Escalas de tiempo.

2. http://www.nist.gov/physlab/div847/faq.cfm. FAQ de tiempo y frecuencias elaborado por el NIST.
3. J. Diaz, L. Molinari, A. Sabolansky, P. Venosa. Importancia de contar con un servicio de sellado digital de tiempo en una PKI. XII Workshop de Investigadores en Ciencias de la Computación (2010). ISBN 978-950-34-0652-6.
4. Bruce Schneier. *Applied Cryptography*. John Wiley and Sons, 1996.
5. Ahto Buldas, Helger Lipmaa. Digital Signature, timestamping and corresponding infraestructure. January 6, 1998.
6. J.Quisquater , H.Massias, B.Preneel, B. Van Rompay. TIMESEC Digital Timestamping and the Evaluation of Security Primitives. Université Catholique de Louvain. December 1999.
7. Dominic Béchaz, Hans Weibel. IEEE 1588 Implementation and Performance of Time Stamping Techniques. Zurich University of Applied Sciences.
8. Stuart Haber, W. Scott Stornetta. How to Time-Stamp a Digital Document.
9. Chung-Huang Yang, Chih-Ching Yeh, Li-Ling Hsu3. On the Design and Implementation of a Secure Time-Stamping Service. The 2004 Symposium on Cryptography and Information Security Sendai, Japan, Jan.27-30, 2004.
10. Aleksej Jerman Blažič, M.Sc., Borka Džonova Jerman, Prof, Ph.D. APPROACH FOR PRESERVATION THE AUTHENTICITY OF DIGITAL OBJECTS – THE EKEEPER SERVICE. Institute Jamova 39 Ljubljana, Slovenia.
11. A. Cilardo, A. Mazzeo, L. Romano, G. P. Saggese, G. Cattaneo. Providing Interoperable Time Stamping Services.
12. http://www.unlp.edu.ar. Portal de UNLP.
13. http://www.pkigrid.unlp.edu.ar. Sitio del proyecto PKIGrid UNLP.
14. C. Adams, P. Cain, D. Pinkas, and R. Zuccherato. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). RFC 3161 (Proposed Standard), August 2001. Updated by RFC 5816.
15. ISO/IEC JTC 1/SC 27, Time stamping services - Part 1: Framework, ISO ISO-18014-1, August 2008.
16. ISO/IEC JTC 1/SC 27, Time stamping services - Part 2: Mechanisms producing independent tokens, ISO ISO-18014-2, December 2009.
17. ISO/IEC JTC 1/SC 27, Time stamping services - Part 3: Mechanisms producing linked tokens, ISO ISO-18014-3, December 2009.
18. ANSI X9.95-2005, Trusted Time Stamp Management and Security, 2005, URL: http://x9.org/.
19. D. Pinkas, N. Pope, and J. Ross. Policy Requirements for Time-Stamping Authorities (TSAs). RFC 3628 (Informational), November 2003.
20. ETSI Technical Specification TS 101 861 V1.2.1. (2001-11). Time stamping profile. Note: copies of ETSI TS 101 861 can be freely downloaded from the ETSI web site www.etsi.org.
21. http://www.openevidence.org. Sitio de OpenEvidence.
22. http://www.opentsa.org. Sitio de OpenTSA.
23. http://www.bouncycastle.org. Sitio de OpenTSA.
24. http://www.digistamp.com/toolkitDoc/MSToolKit.htm. Sitio de Digistamp.
25. http://www.debian.org. Sitio Oficial de Debian.
26. http://www.openca.org. Sitio Oficial de OpenCA.
27. Tobias Oetiker and Traffic Grapher. Mrtg – the multi router.
28. http://www.nagios.org. Sitio Oficial de Nagios.
29. http://docs.pnp4nagios.org. Sitio Oficial de PNP4Nagios.