TESIS TSA

AUTORIDAD DE SELLADO DIGITAL DE TIEMPO

Utilizando Software Libre para un servicio de Sellado Digital de Tiempo

AUTOR: Alejandro Javier Sabolansky
DIRECTOR: Lic. Francisco Javier Díaz
CODIRECTOR: Lic. Paula Venosa
CARRERA: Licenciatura en Informática

FECHA: 10 de noviembre de 2010

Planteo inicial

Una organización requiere garantizar la fecha exacta de emisión de sus documentos electrónicos.

Motivación

- Con la firma digital se garantiza autenticidad del autor y no repudio en la emisión de los documentos electrónicos. Sin embargo, no brinda seguridad sobre el instante específico en el que el mismo fue emitido.

- El sellado de tiempo surge como un mecanismo para suplir esta carencia y permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

Interrogantes

- ¿Quién es el autor de este documento?
  ¿Quién autorizó su publicación? → **FIRMA DIGITAL**

- ¿Cuándo fue creado o modificado por última vez dicho documento? → **SELLADO DIGITAL DE TIEMPO**

Objetivo del trabajo

Implementación de una infraestructura de sellado de tiempo utilizando software libre cumpliendo con los estándares tecnológicos existentes.

Preguntas a responder

Si hablamos de sellado digital de tiempo, podrían surgir las siguientes preguntas:

- ¿En qué consiste el sellado digital de tiempo?
- ¿Cómo se implementa un servicio de sellado digital de tiempo utilizando software libre?
- ¿Funciona el servicio de sellado digital de tiempo implementado?
- ¿Es seguro el servicio de sellado digital de tiempo implementado?

¿En qué consiste el sellado digital de tiempo?

Firma digital

Esquema que permite garantizar la autenticidad de un mensaje o documento. Se implementa a través de una Infraestructura de Clave Pública (PKI).

Componentes:

- Usuario subscriptor.
- Autoridad de certificación (CA).
- Autoridad de registración (RA).
- Repositorios.

Certificados digitales

- Documento emitido por una Autoridad de Certificación que garantiza la vinculación entre el sujeto y la clave pública.

- Definido en el estándar X.509.

- La versión 3 soporta extensiones que permiten introducir nuevas capacidades entre las que se encuentra el **sellado digital de tiempo**.

Sellado de Tiempo - Definición

El sellado de tiempo es un método que permite:

- Probar que un conjunto de datos existió antes de un momento dado.
- Garantizar que ninguno de estos datos ha sido modificado desde ese momento.

Características:

- El dato a sellar no requiere ser enviado.
- Se genera un valor de hash o resumen que se corresponde en forma unívoca con el mismo.

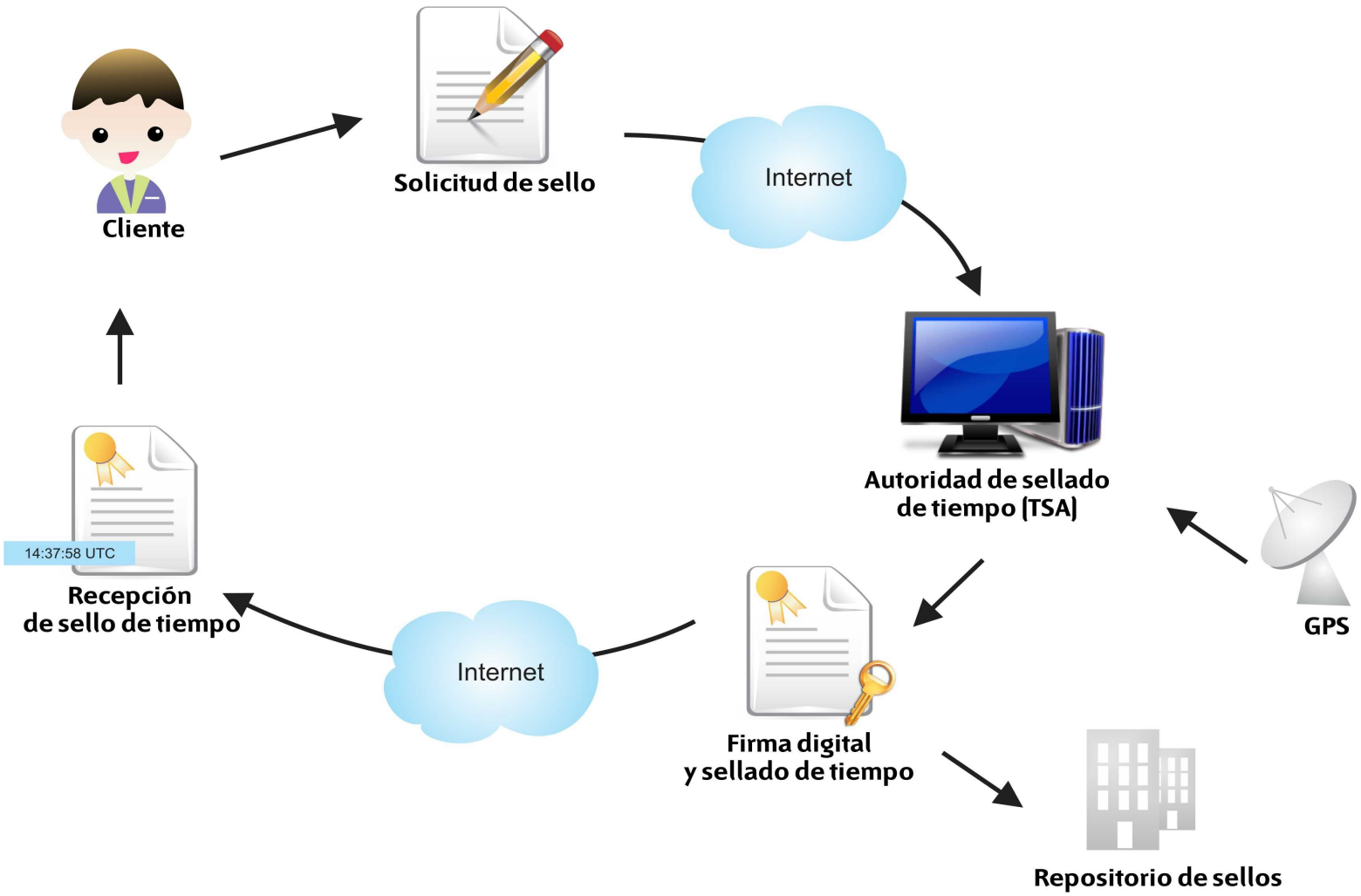
Sellado de Tiempo - Estándares involucrados

El sellado de tiempo digital está definido en los siguientes estándares creados por diferentes organizaciones:

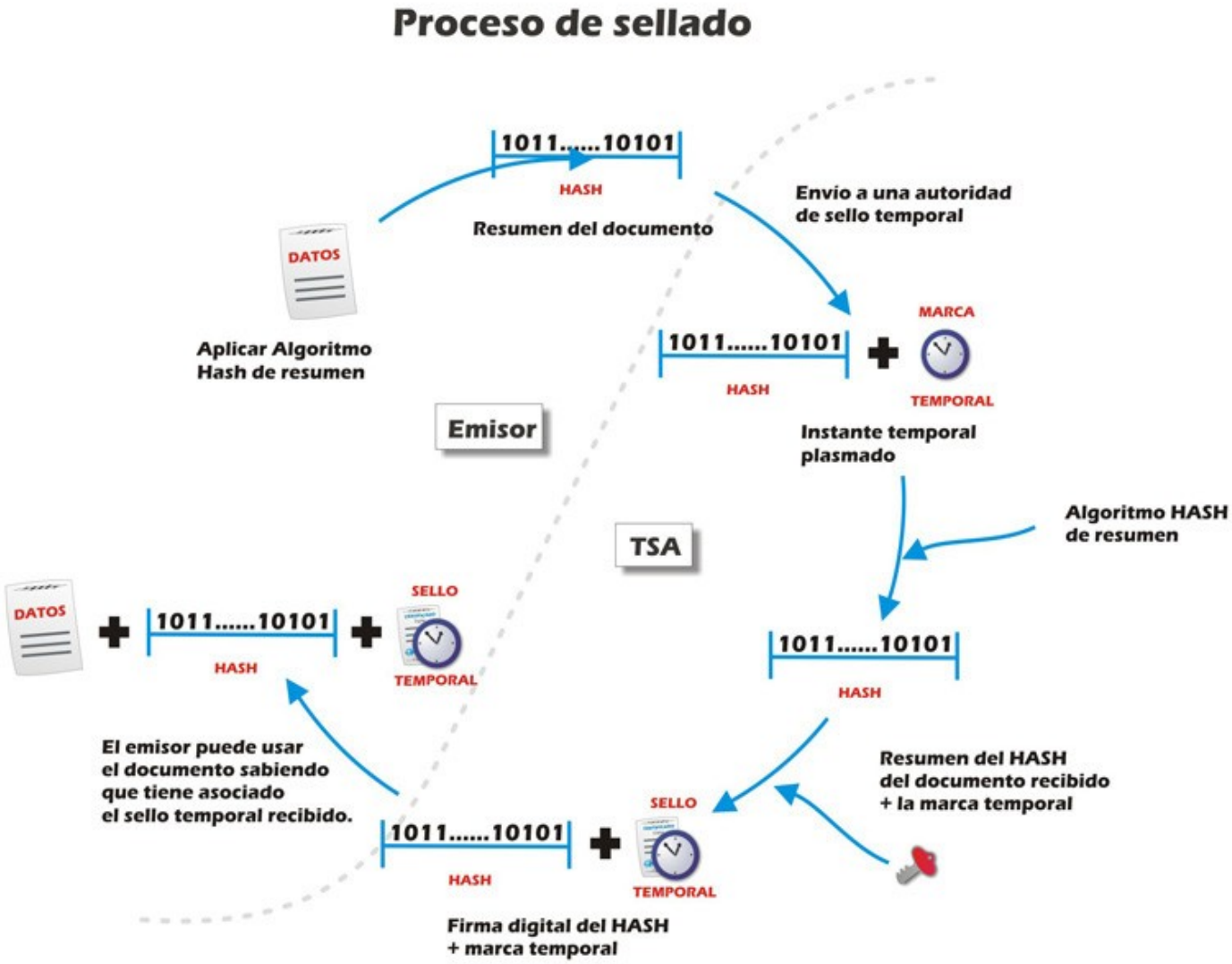
- RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- ISO/IEC 18014. Time stamping services.
- ETSI TS 101 861 – Time stamping profile.
- ETSI TS 102 023 – RFC 3628. Requirements for Time-Stamping Authorities.

Sellado de Tiempo - Componentes

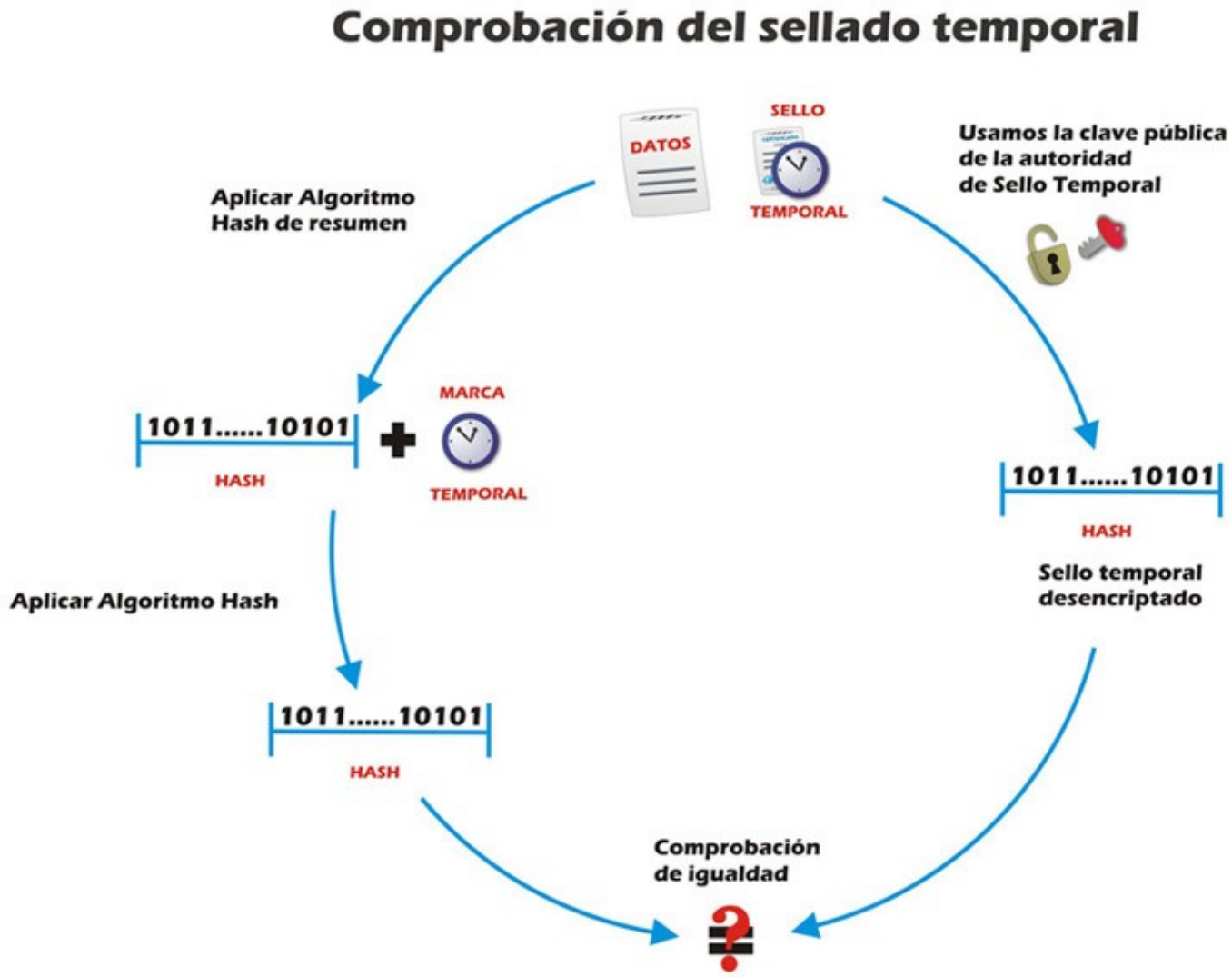
Componentes



Sellado de Tiempo – Fases (I)



Sellado de Tiempo – Fases (II)



Sellado de Tiempo - Roles

- Autoridad de sellado de tiempo
- Solicitante
- Fuente de tiempo confiable
- Verificador

Sellado de Tiempo – Aplicaciones

- Comercio electrónico.
- Protección de la propiedad intelectual.
- Firma de documentos y contratos.
- Cierre de libros financieros.
- Declaraciones de testamentos.
- Licitaciones o concursos públicos.
- Transacciones bursátiles.

¿Cómo se implementa un servicio de sellado digital de tiempo utilizando software libre?

Implementación – Componentes

- Sistema operativo → **GNU/Linux Debian Lenny**
- Servidor de base de datos → **PostgreSQL + Pgpool-II**
- Servicio de sellado de tiempo → **OpenTSA**
- Servidor web → **Apache Web Server**
- Servidor de NTP → **NTP daemon for Debian**
- Autoridad de Certificación → **OpenCA**

Implementación – Decisiones

- Criterios de selección de componentes
- Integración con PKIGrid UNLP → **Incompatibilidad**
- Selección del protocolo de transporte → **HTTP**
- Sincronización de relojes → **NTP**
- Precisión de relojes → **500 milisegundos**
- Algoritmos de cifrado
  - Hashing → **SHA-1**
  - Firma → **SHA-1 + RSA 2048 bits**

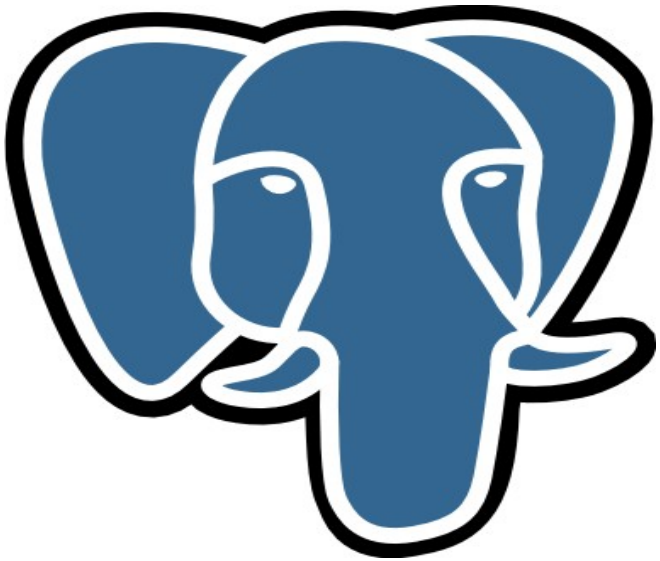
Implementación - OpenCA

- Instalación.
- Adaptación de roles.
- Emisión de certificados para el servicio de sellado de tiempo y para el frontend web implementado.

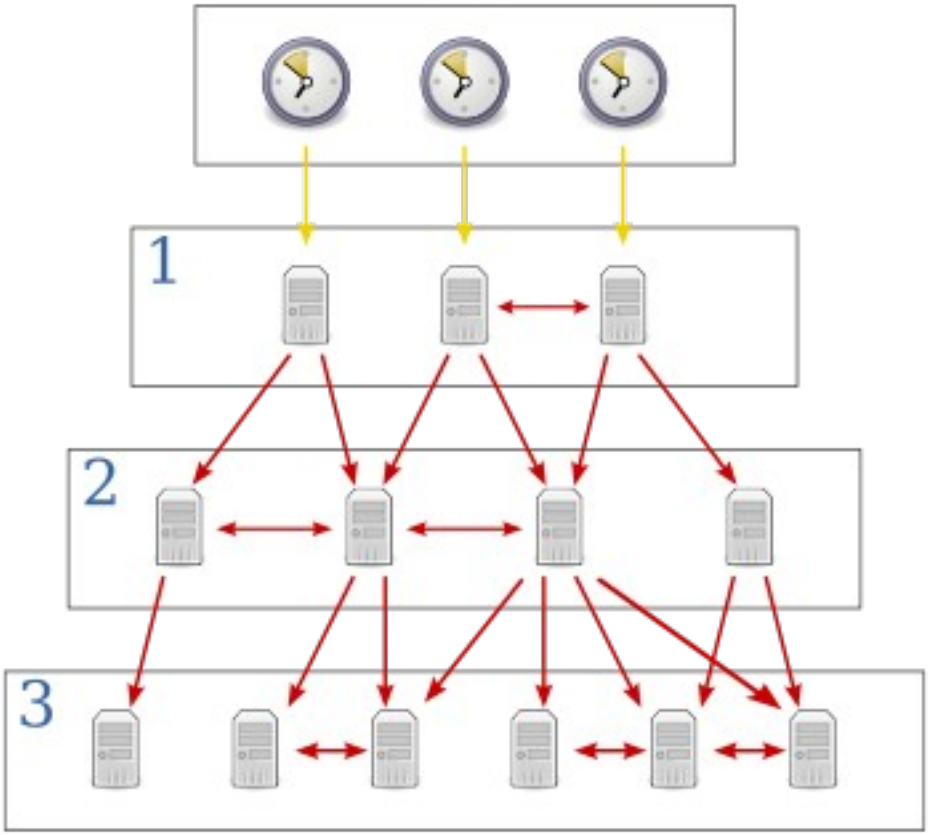
PKIGrid CA

Implementación - PostgreSQL

- **Instalación de PostgreSQL.**
- **Instalación de Pgpool-II.**
  - Alta disponibilidad.
  - Replicación de información.



Implementación - NTP



- Reloj GPS del IAR (Conicet – UNLP).
- Servidor NTP de UNLP.
- Servidores alcanzables por Internet comercial.
- Servidores alcanzables por Internet 2.

Implementación - OpenSSL

- Al comienzo de este trabajo, OpenSSL no contaba con soporte para el sellado de tiempo. Era necesario implementar un parche previo a la compilación del producto.

- Desde la versión 1.0.0, liberada en marzo de este año, OpenSSL soporta las extensiones de sellado de tiempo en forma nativa.

Implementación - OpenTSA

- Desarrollo Open Source compatible con la RFC 3161.
- Integración con OpenSSL.
- Módulo para Apache.
- Cliente de sellado de tiempo.

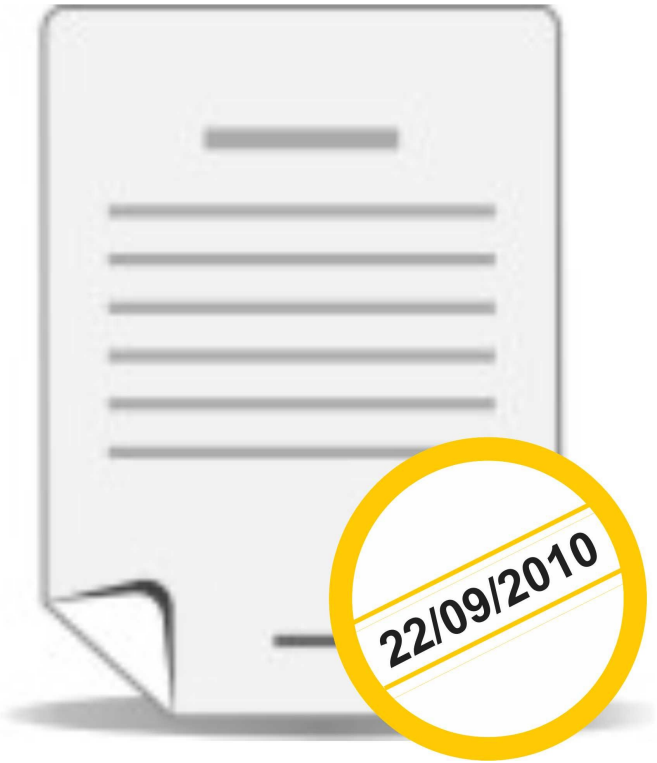
Implementación – Interfaz Web

El servicio web implementado cuenta con dos interfaces:

- **Frontend público**
  - Listar sellos emitidos.
  - Validar sellos.
  - Obtener certificados.
- **Interfaz de monitoreo**

Se implementó un módulo en Perl para hacer uso de las operaciones provistas por OpenSSL.

¿Funciona el servicio de sellado digital de tiempo implementado?



Pruebas de funcionamiento

- **Demo 1:** Sellado de tiempo del documento del informe de la tesis.
- **Demo 2:** Navegación de la interfaz web pública.
- **Demo 3:** Verificación de sellos de tiempo mediante la interfaz web y mediante la línea de comandos.

¿Es seguro el servicio de sellado digital de tiempo implementado?

Seguridad del servicio

- **Alternativas de acceso**
  - HTTP
  - HTTPS
- **Monitoreo de componentes**
  - Nagios
  - MRTG
  - PNP4Nagios

Nagios®

MRTG
MULTI ROUTER TRAFFIC GRAPHER

- **Demo 4:** Navegación de la interfaz de monitoreo.

Conclusiones

•Es imprescindible implementar el servicio de sellado de tiempo debido a que la firma no garantiza el instante de tiempo en que se ha realizado la misma.

•Es necesario enmarcarse en la normativa vigente tanto para la definición de los procedimientos como para la implementación de la solución.

•El servicio puede ser implementado en su totalidad utilizando software libre en todos sus componentes.

Trabajos futuros

- Definición formal de la Política de Certificación y de la Declaración de Prácticas de Certificación de la Autoridad de Sellado de Tiempo.
- Análisis de factibilidad para adaptar PKIGrid CA UNLP para la emisión de los certificados digitales necesarios para el servicio de sellado de tiempo implementado.
- Implementación de aplicaciones, prototipos o agregados a soluciones existentes que hagan uso del servicio.

¿Preguntas?

¡Gracias !