

# Servicio de Sellado de documentos vía correo-e

Francisco Jesús Monserrat Coll  
<francisco.monserrat@rediris.es>

# Índice

- ¿Qué es un sellado de tiempos (ST)?
- El Servicio de S.T. por correo-e
- Implementación del sellado. Ejemplos
- Mejoras futuras.



# Sellados de Tiempos

RFC 3161: Internet X.509 PKI Time-Stamp Protocol (TSP)

Un servicio que certifica que un determinado dato existía en un instante determinado de tiempo.

Básicamente un registrador electrónico:

- Se le presenta información.
- Queda “Registrada” .
- Es posible a posteriori comprobar las entradas en el registro.



# El servicio de sellado de RedIRIS

**OBJETIVO:** Implementar un servicio de sellado de ficheros que pueda ser usado fácilmente por un usuario habitual.

- Difundir el uso de la firma digital.
- Ver la forma de compatibilizar los sistemas de firma electrónica existentes.

## Servicio de Sellado de tiempos vía correo-e

- El correo-e es la herramienta más utilizada para el intercambio de información en entornos heterogéneos.
- Algunos usos dentro de la comunidad académica:
  - Presentaciones de ponencias y/o artículos en congresos técnicos.
  - Entrega de prácticas por parte de alumnos/ evaluación continua.
  - ....
  - En General como prueba de existencia de un fichero con un contenido determinado en un instante de tiempo



## RFC 3161 y servicios similares

- Pensado para su uso dentro de jerarquías de certificación X509.
- Estructura cliente/servidor.
- Diversas limitaciones legales (Patentes y Copyright) sobre este tipo de servicios.
- Escasas implementaciones de código abierto.
- Destinadas sobre todo a un uso comercial.
- Procedimientos de verificación externos complejos.



# Requisitos de un sistema de tiempos

¿Qué hace falta realmente ? : Para el registro:

- Emplear una fuente fiable de Tiempos.
- Registrar de forma única cada documento presentado.
- Entregar al usuario un “resguardo” del registro fiable.

Para la comprobación:

- Poder comprobar si efectivamente determinada información fue registrada y la fecha.

Y siempre: Confiar en el registrador ;-).



## Terceras partes de Confianza

Entidad en la que confían los demás integrantes de una transacción.

- Gobierno (ej. carnet de identidad, títulos).
- Bancos
- Notarios

Autoridades de Certificación. ¿Qué nivel de confianza puede tener un sistema gratuito ?:





# Características del sistema

- Interface de registro vía correo electrónico.
- Confirmación vía correo-e firmados (S/MIME y PGP/MIME).
- Consulta de la información vía HTTP.

Uso en entornos no comerciales.



# Fuente Fiable de Tiempos

Fácil de obtener.

- Proporcionada a partir de la hora del sistema.
- Sincronización del equipo donde se realiza el sellado vía NTP (RFC-1305)
- Disponible fácilmente,  
<http://www.rediris.es/gt/iris-ntp>
- Precisión a los mili segundos.



# Registro de los documentos

Almacenar:

- huella digital (hash) MD5 de los documentos
- Fecha precisión de segundos.
- Código de la entrada.
- Valor de verificación



# Huella digital

Funciones Hash: función matemática que genera un valor o resumen reducido de una información más grande.

Características:

- Cualquier modificación por pequeña que sea genera un valor MD5 completamente distinto.
- No se puede calcular a partir del resumen MD5 la información original que tenía el fichero
- No es posible calcular a priori que valor MD5 va a tener un fichero sin hacer el calculo



# Valor de Verificación

¿Qué pasa si alguien manipula la B.D. ?

- Las entradas se almacenan firmadas (GnuPG) y sin firmar.
- Es posible comprobar si una entrada ha sido modificada (fallaría la comprobación).



## Resguardo de sellado

Por cada correo recibido el servicio de sellado genera un correo:

- firmado con S/MIME
- firmado con PGP/MIME

Con la información e instrucciones necesarias para proceder a su verificación.



## ¿Qué se registra?

- Todos los anexos que contenga el mensaje, asignándoles un código distinto a cada uno.
- El mensaje de correo-e, excluyendo las cabeceras susceptibles de ser modificadas por los equipos intermedios.

Para evitar el registro de correos con Virus y SPAM, el contenido de los mensajes es filtrado previamente, <http://www.rediris.es/mail/resaca>



## Firmado de los mensajes

Para asegurar la autoría de la firma los mensajes están firmados empleando SMIME y PGP/MIME, simultáneamente:

- SMIME: Para instituciones que estén dentro de la jerarquía de certificación de RedIRIS  
<http://www.rediris.es/cert/servicios/pca>
- PGP/MIME: Como medio de verificación alternativo o para usuarios que empleen este sistema, <http://www.rediris.es/pgp>

Para realizar el firmado se emplea una estructura MIME compatible con los diversos clientes de correo-e.





# Estructura MIME

- Compatibilidad con los clientes actuales de correo.
- Ambas firmas independientes una de la otra
- Posibilidad de verificación desde línea de comandos/scripts



## Multipart/signed

### Multipart/signed

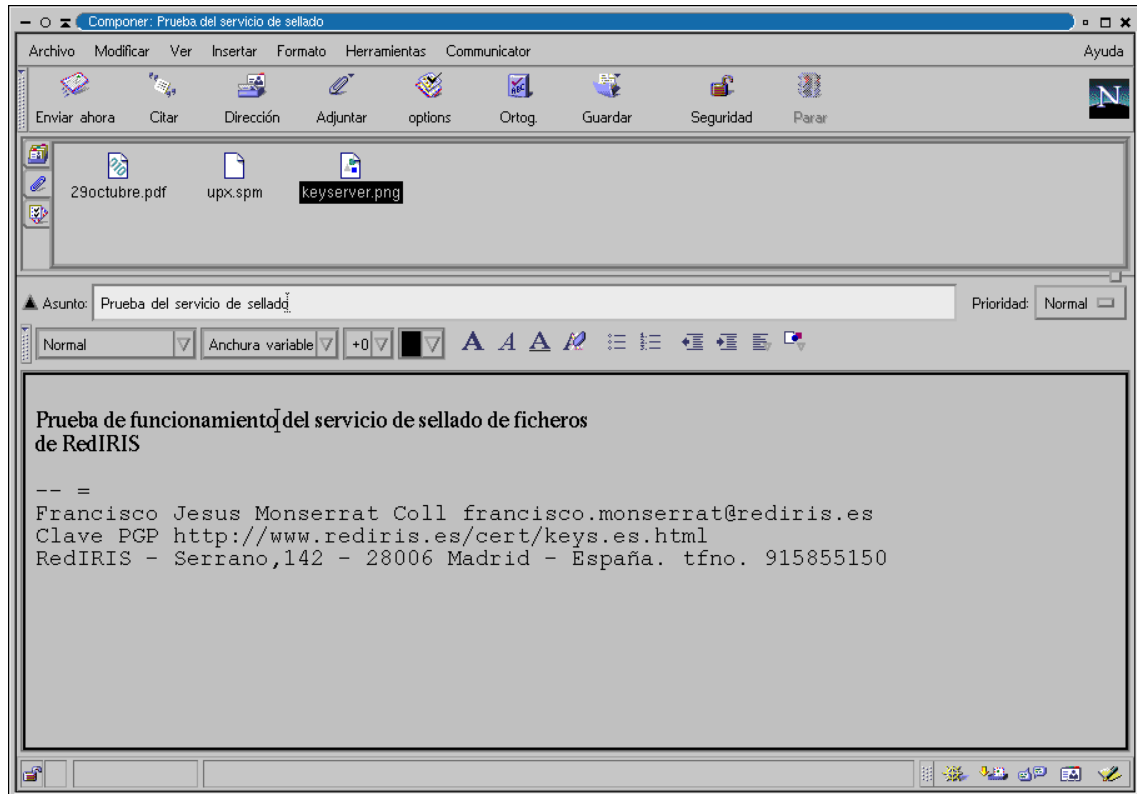
text/plain

Informacion enviada  
por el servicio de sellado

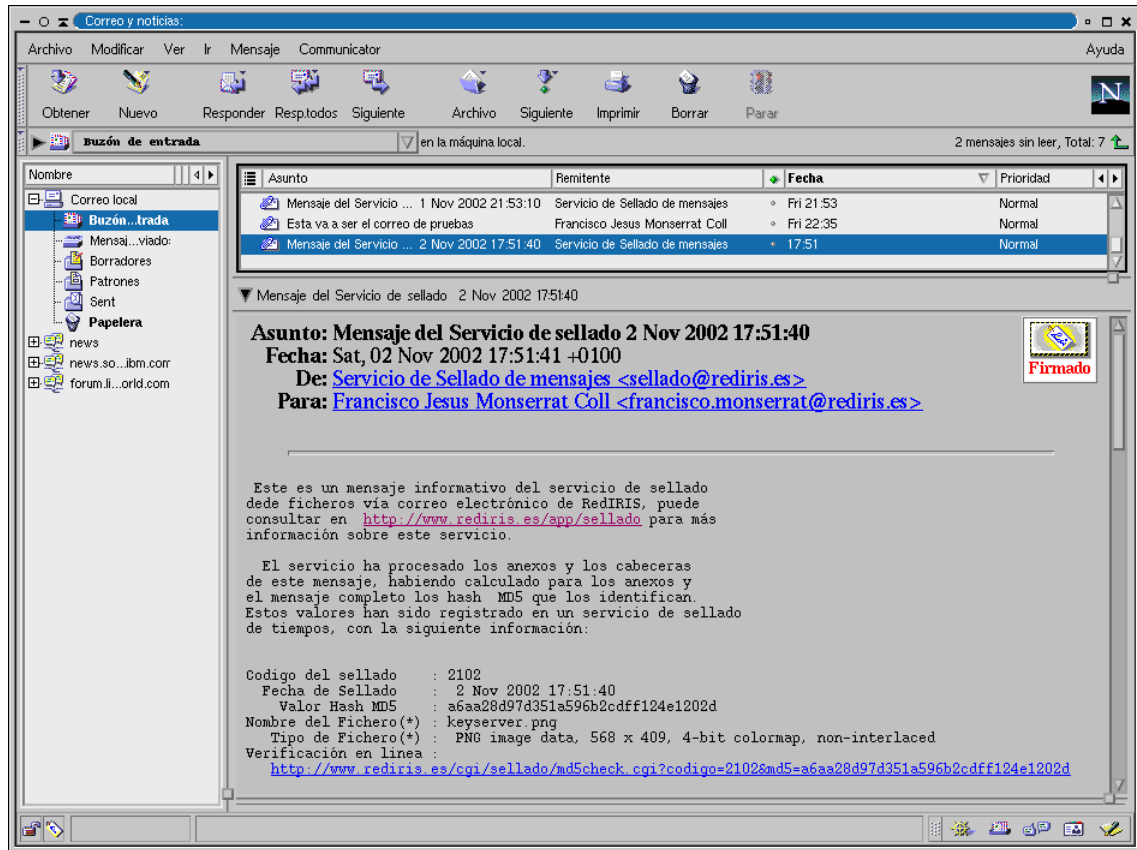
application/pgp-signature  
(firma GnuPG)

application/x-pkcs7-signature  
(firma smime)

# Ejemplo: Composición de un mensaje



# Ejemplo: Recepción del mensaje



Correo y noticias: Archivo Modificar Ver Ir Mensaje Comunicador Ayuda


Obtener Nuevo Responder Resp.todos Siguiente Archivo Siguiente Imprimir Borrar Parar

Buzón de entrada en la máquina local. 2 mensajes sin leer, Total: 7

Asunto	Remitente	Fecha	Prioridad
Mensaje del Servicio ...	Servicio de Sellado de mensajes	Fri 21:53	Normal
Esta va a ser el correo de pruebas	Francisco Jesus Monserrat Coll	Fri 22:35	Normal
Mensaje del Servicio ...	Servicio de Sellado de mensajes	17:51	Normal

Mensaje del Servicio de sellado 2 Nov 2002 17:51:40

**Asunto:** Mensaje del Servicio de sellado 2 Nov 2002 17:51:40  
**Fecha:** Sat, 02 Nov 2002 17:51:41 +0100  
**De:** [Servicio de Sellado de mensajes <sellado@rediris.es>](mailto:sellado@rediris.es)  
**Para:** [Francisco Jesus Monserrat Coll <francisco.monserrat@rediris.es>](mailto:francisco.monserrat@rediris.es)



Este es un mensaje informativo del servicio de sellado de ficheros via correo electrónico de RedIRIS, puede consultar en <http://www.rediris.es/app/sellado> para más información sobre este servicio.

El servicio ha procesado los anexos y los cabeceras de este mensaje, habiendo calculado para los anexos y el mensaje completo los hash MD5 que los identifican. Estos valores han sido registrado en un servicio de sellado de tiempos, con la siguiente información:

```

Codigo del sellado      : 2102
Fecha de Sellado       : 2 Nov 2002 17:51:40
Valor Hash MD5         : a6aa28d97d351a596b2cdf124e1202d
Nombre del Fichero(*)  : keyserver.png
Tipo de Fichero(*)     : PNG image data, 568 x 409, 4-bit colormap, non-interlaced
Verificación en línea  :
http://www.rediris.es/cgi/sellado/md5check.cgi?codigo=2102&md5=a6aa28d97d351a596b2cdf124e1202d

```



[pgp-server](#) [pkcs](#) [plantillas](#) [projectos](#) [psycoc](#) [taro](#) [recordar](#) [reuniones](#) [spanish](#)  
[temp](#) [templates](#)  
[inbox](#) [cert](#) [abuse](#) [vulnwatch](#) [first](#) [wizard](#) [abuse](#) [news](#) [rootiris](#) [web](#) [bridge](#)  
[linux-ipsec](#) [security-modules](#) [cygnus](#) [opendos](#) [s-x86](#) [sunmanagers](#) [cisco-nsp](#)  
[nanog](#) [bugtraq](#) [intrusions](#) [nsp-security](#) [security-basic](#) [vuln-bugtraq](#) [openssl](#)

inbox+ 899 msgs (1-90) **New** **Flist** **Inc** **Commit** **Sort...** **Search...** **More...**  
 886 C 30/10 12:56+01 "Angel L. Mateo" [Fwd: Chiste]  
 887 30/10 13:02+01 "Javier Cao Avell" Mira a ver si le cabe esto a  
 888 30/10 13:34+01 "Javier Cao Avell" Lo de la CARM y varias cosas  
 889 C 30/10 20:54+02 "Dimitris Lioupis" Embedded Grid (e-Grid) BOF p  
 890 01/11 15:15+05 letsriiide4287o37 Attention DVD lovers: This p  
 891 R 01/11 20:33+01 jesus.ibanez@tecn Call For Papers: 2003 Int'l  
 892 01/11 20:57+01 Servicio de Sella Mensaje del Servicio de sella  
 893 01/11 21:21+01 "HMR Noticias" HMRSYS Noticias\* UN PAIS QUE  
 894 01/11 21:21+01 Servicio de Sella Mensaje del Servicio de sella  
 895 - 01/11 21:25+01 jesus.ibanez@tecn Re: Call For Papers: 2003 Int  
 896 01/11 21:47+01 Servicio de Sella Mensaje del Servicio de sella  
 897 01/11 22:35+01 To:paco Esta va a ser el correo de p  
 898 01/11 21:50+01 Mail Delivery Sys Undelivered Mail Returned to  
 899 01/11 21:51+01 Servicio de Sella Mensaje del Servicio de sella  
 900+ 01/11 21:53+01 Servicio de Sella Mensaje del Servicio de sella

inbox:900  
[rwa](#) [Comp](#) [Prev](#) [Next](#) [Delete](#) [Move](#) [Link](#) [IRIS-CERT](#) [Reply...](#) [More...](#)  
 U  
 EXMH R  
 L

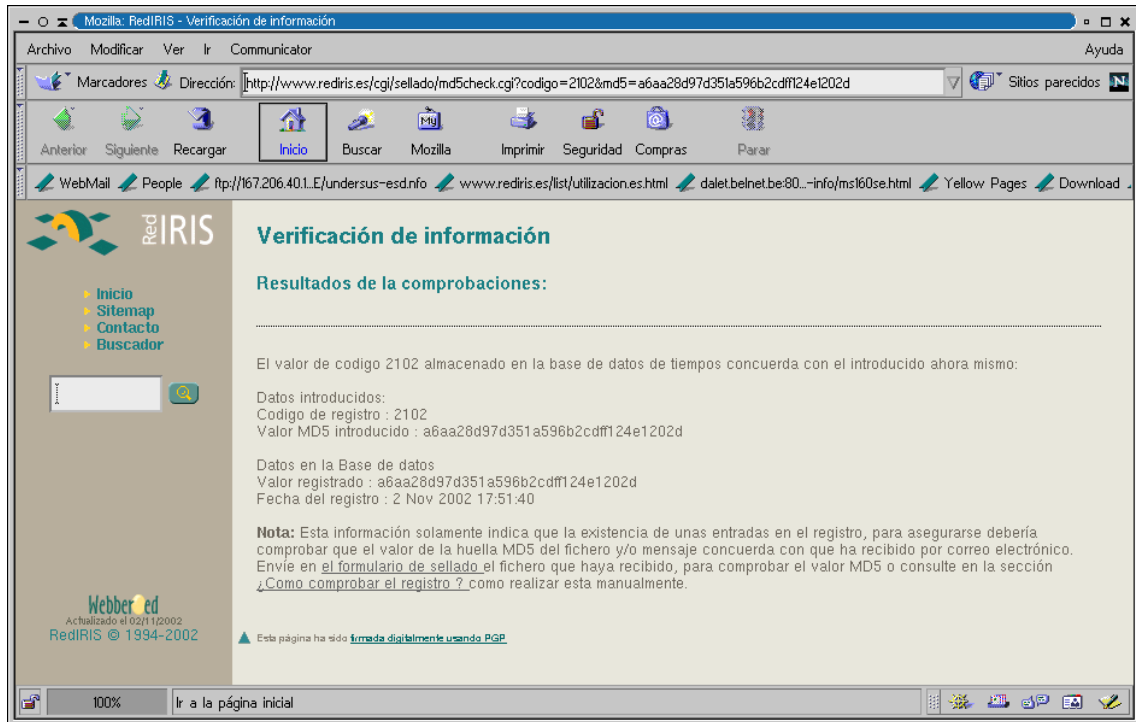
Subject: Mensaje del Servicio de sellado 1 Nov 2002 21:53:10  
 From: Servicio de Sellado de mensajes <sellado@rediris.es>  
 Date: Fri, 01 Nov 2002 21:53:10 +0100  
 To: Francisco Jesus Monserrat Coll <francisco.monserrat@rediris.es>

(multipart/signed)  
 #1. (multipart/signed)  
 Warning: using insecure memory!  
 please see <http://www.gnupg.org/faq.html> for more information  
 Signature made Fri Nov 1 21:53:10 2002 CET using RSA key ID 0D1EE81F  
 Good signature from "RedIRIS TimeStamping Authority Test Version  
 <tsa@rediris.es>"

(text/plain)  
 Este es un mensaje informativo del servicio de sellado  
 dede ficheros via correo electrónico de RedIRIS, puede  
 consultar en <http://www.rediris.es/app/sellado> para más  
 información sobre este servicio.



# Ejemplo: Comprobación mensaje




Mozilla: RedIRIS - Verificación de información

Archivo Modificar Ver Ir Comunicador Ayuda

Marcadores Dirección: <http://www.rediris.es/cgi/sellado/md5check.cgi?codigo=2102&md5=a6aa28d97d351a596b2cdf124e1202d> Sitios parecidos

Anterior Siguiente Recargar Inicio Buscar Mozilla Imprimir Seguridad Compras Parar

WebMail People ftp://167.206.40.1.E/undersus-esd.info www.rediris.es/list/utilizacion.es.html daletbelnet.be:80...-info/ms160se.html Yellow Pages Download

 Red IRIS

- Inicio
- Sitemap
- Contacto
- Buscador

Buscar

## Verificación de información

### Resultados de la comprobaciones:

El valor de codigo 2102 almacenado en la base de datos de tiempos concuerda con el introducido ahora mismo:

Datos introducidos:  
Codigo de registro : 2102  
Valor MD5 introducido : a6aa28d97d351a596b2cdf124e1202d

Datos en la Base de datos  
Valor registrado : a6aa28d97d351a596b2cdf124e1202d  
Fecha del registro : 2 Nov 2002 17:51:40

**Nota:** Esta información solamente indica que la existencia de unas entradas en el registro, para asegurarse debería comprobar que el valor de la huella MD5 del fichero y/o mensaje concuerda con que ha recibido por correo electrónico. Envíe en el [formulario de sellado el fichero](#) que haya recibido, para comprobar el valor MD5 o consulte en la sección [¿Como comprobar el registro ?](#) como realizar esta manualmente.

▲ Esta página ha sido [firmada digitalmente usando PGP](#)

100% Ir a la página inicial



# Vías Futuras

- Empleo directamente de una fuente de tiempo.
- Empleo de un sellado de tiempos compatible RFC 3161.
- Procesamiento de mensajes encriptados/firmados.
- Control de Acceso al servicio.
- Clientes específicos de acceso al servicio de sellado.



# ¿¿ Preguntas ??

Información:

- <http://www.rediris.es/app/sellado>
- sellado: [sellado@rediris.es](mailto:sellado@rediris.es)
- correo-e: [sellado-admin@rediris.es](mailto:sellado-admin@rediris.es)

