Servicio de Sellado de documentos vía correo-e

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

Jornadas Científicas de Usuarios de RedIRIS 2002 Valencia.
28 Nov 2002

Índice

- ¿Qué es el servicio de seguridad de RedIRIS ?
- ¿Qué es todo esto de la criptografía ?
- El servicio de Sellado de tiempo
- Ejemplo
- Mejoras y vías futuras.

Seguridad en RedIRIS: IRIS-CERT

- Establecido formalmente en 1995
- Finalidad: Solución de problemas de seguridad en las organizaciones afiadas.
- Nunca una finalidad "policial"
- Desarrollo de proyectos de específicos en el área de Seguridad

IRIS-CERT II

Apoyo a los proyectos de firma digital y confidencialidad.

- Soporte a la problemática de los incidentes de seguridad.
- ¿ Como verificar el origen de un mensaje ?
- ¿ Como enviar un mensaje de forma confidencial.

Experiencias iniciales con PGP:

- Servidor de claves
- Información a los usuarios finales

IRIS-PCA

Experiencias desde 1997 con certificaciones jerárquicas (X509).

- autoridad de Certificación de RedIRIS.
- Firmado a instituciones y organismos afiliados a RedIRIS
- Gestión de los certificados de usuario por parte de las instituciones

OBJETIVO: Fomentar el uso de sistemas de criptográficos entre los usuarios de la Red Académica.

Usos de la criptografía

Integridad : Poder comprobar que una determinada información no ha sido modificada.

Confidencialidad : Ocultar la información de forma que solamente el receptor del mensaje pueda leer la información contenida en este.

Autenticación : Poder establecer que determinado persona es quien dice ser.

No repudio : Derivada de la autenticación, no poder negar la autoría de determinada información.

Historia de la criptografía

- La criptografía es una ciencia muy antigua, estudio de la escritura secreta.
- Cifrado/codificado, consiste en la conversión de un texto entendible en algo inteligible para protegerlo. La información puede volver a ser entendible mediante la operación inversa "descifrado"
- Julio Cesar, empleaba un cifrado por sustitución para el envío de información a Roma durante la campaña de las Galias
- Durante la II Guerra Mundial los alemanes desarrollaron "Enigma" una máquina de substitución para el envío de la información cifrada.
- La criptografía moderna se basa en transformaciones matemáticas, para lo cual los ordenadores han permitido una automatización completa

Ejemplo de Cifrado por sustitución

- Los cifrados de sustitución son los más antiguos empleados
- Cada letra del alfabeto se le asigna otra distinta, en función de un valor conocido solamente por el emisor y el receptor.

A	B	C	D	E	F	G	H	I	..
N	O	P	Q	R	S	T	U	V	...

Texto encriptado: ubyn dhr gny

Texto en claro: hola ??? ???

Tipos de Cifrado I

simétrico : Una clave se emplea para cifrar y descifrar

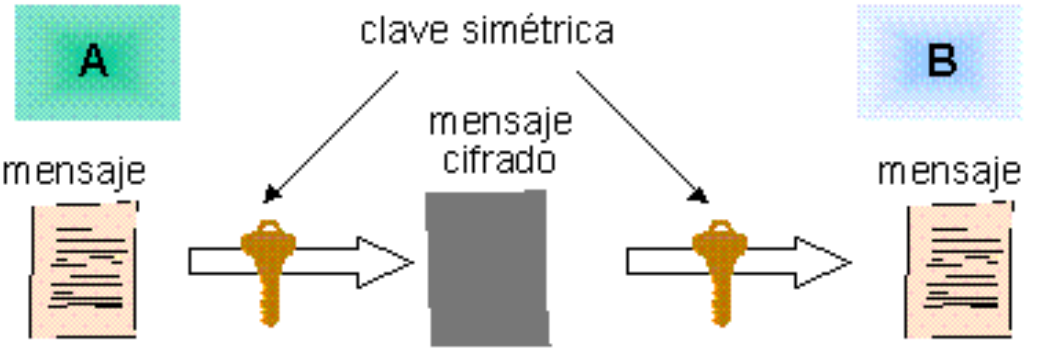
- Ventajas
  - Rápido
  - Facilidad de compartición entre varias partes
- Desventajas
  - Hay que mantener las claves secretas
  - Hace falta un método "fuera de banda" para cambiar la clave.

Algunos algoritmos

- DES (56 bits), 3DES.
- IDEA (128 bits).
- AES (256 bits).

Tipos de cifrado II

Ejemplo de cifrado simétrico



Tipos de cifrado III

asimétrico

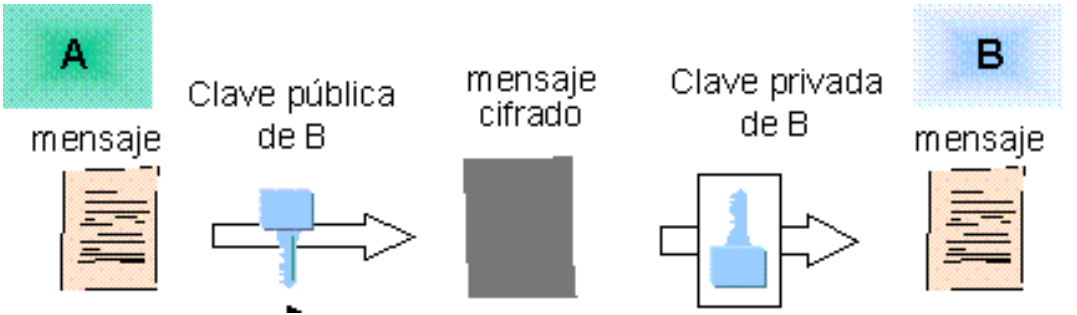
- dos claves para cifrar y descifrar.
- Lo cifrado con una clave solo puede ser descifrado por la otra.
- Una clave es pública ,cualquiera puede tenerla y otra es privada (solo la tiene el usuario).
- Ventajas
  - No se necesita un canal seguro para enviar la clave
  - Posibilidad de encriptar y firmar
- Desventajas
  - Muy lento

Algoritmos utilizados

- RSA
- Diffie-Hellman

Tipos de Cifrado III

Ejemplo de cifrado asimétrico



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

Algunos algoritmos:

- MD5
- SHA-1

Usos de la criptografía I

Confidencialidad :

- Solución 1 : Emplear con clave simétrica
- Solución 2 : Con clave asimétrica

1. Generamos una clave simétrica al azar.
2. Encriptamos el documento con esta clave aleatoria.
3. Encriptamos la clave aleatoria con la clave publica del destinatario
4. Enviamos ambos datos al destinatario

Usos de la criptografía II

Autenticación y No Repudio

Solución:

- Mediante claves asimétricas, cualquier documento cifrado por la clave privada es posible desencriptarlo con la publica y por lo tanto comprobar su autenticidad.
- Ya que solo el dueño de la clave privada ha podido cifrar el documento , no se puede repudiar.

Integridad

Solución: Mediante huellas digitales

- Si un documento ha sido modificado su huella digital cambiara.
- Firma de la huella .

Certificación digital

- Emplea de criptografía asimétrica
- Parte publica = clave publica + firma por un emisor válido
- Se confía la "firma del emisor".

Usos:

Credencial Digital : Sabemos que la clave pertenece a quien dice ser porque esta firmada por una autoridad reconocida.

Terceras partes de Confianza

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

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

Problema: ¿En quien se debe confiar ?.

- Confianza jerarquizada
- Confianza Distribuida

Confianza distribuida: PGP

- Los usuarios deciden en que "firmantes" confían.
- Los usuarios son a su vez las autoridades de certificación.
- Cualquier usuario puede firmar una claves.

Problema: ¿ Como se verifica la identidad del poseedor de una clave ?

- Reuniones de Firma de claves

Confianza centralizada: X509

1. Existe una clave principal, en la que se confía
2. Esta clave central firma otras claves "secundarias"
3. El árbol se repite hasta llegar a los nodos (usuarios finales y servidores).
4. Es posible verificar a partir de un certificado, la firma del certificado padre y ver si se llega al certificado raíz.

Ejemplos de uso X509

Gran parte de los servicios que se emplean actualmente.

- Acceso seguro a los servidores WWW
- Servicios ofrecidos por las Universidades , carnet inteligente.
- Certificados de la FNMT, declaración de la renta.

Problemas: Interacción entre diversas autoridades de certificación.

Sellados de Tiempos

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.
  - Certificación de autoría de documentos.
  - ....
  - En General como prueba de existencia de un fichero con un contenido determinado en un instante de tiempo

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 ;-).

Características:

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

Uso en entornos no comerciales. Servicio

complementario, no sustitutivo a otros mecanismos de registro.

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

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.

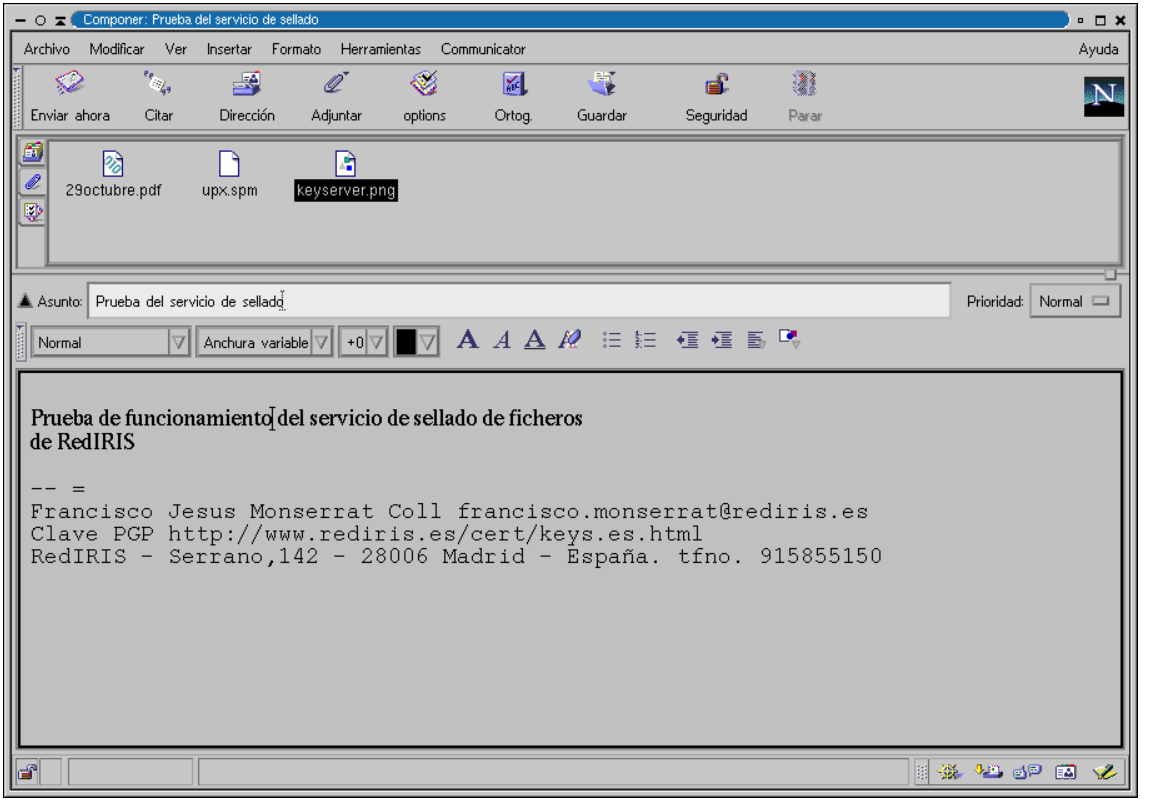
¿Qué se registra?

- Todos los anexos que contenga el mensaje, asignándoles un código distinto a cada uno.

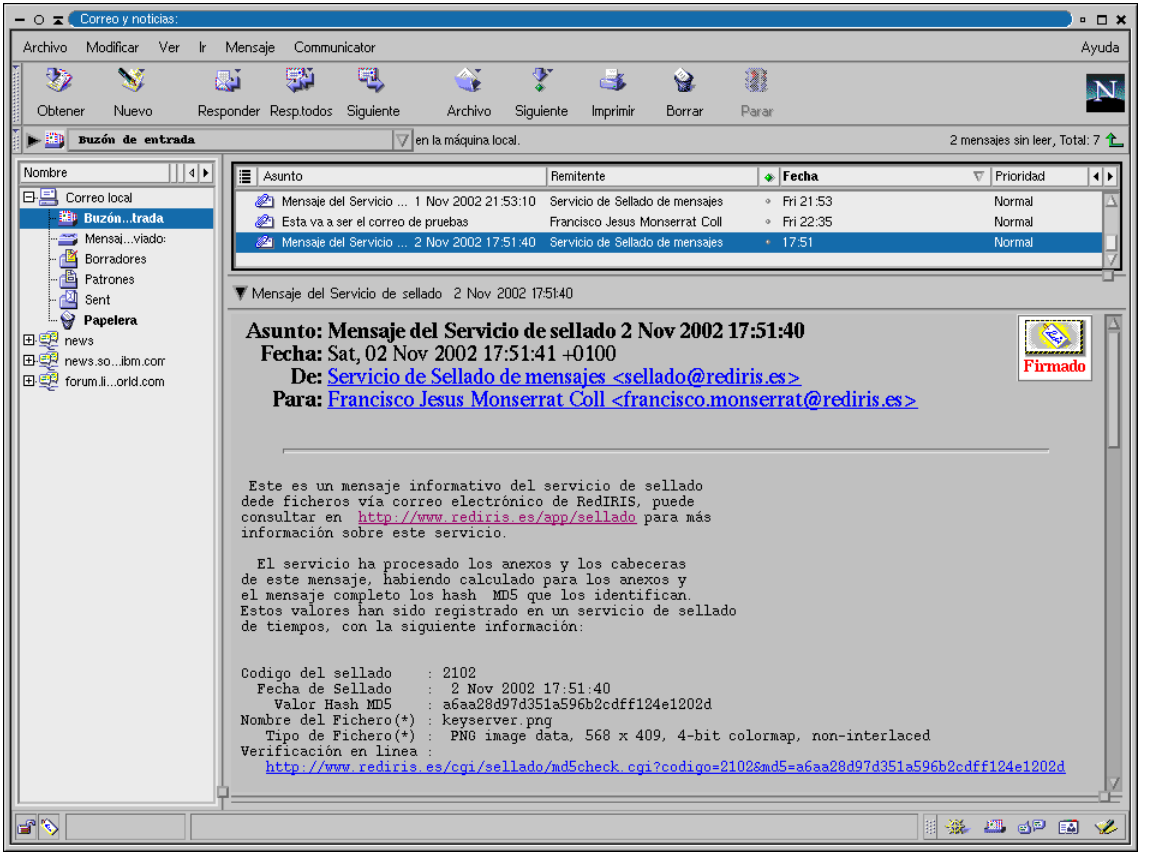
- El mensaje de correo-e, excluyendo las cabeceras susceptibles de ser modificadas por los equipos intermedios.

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

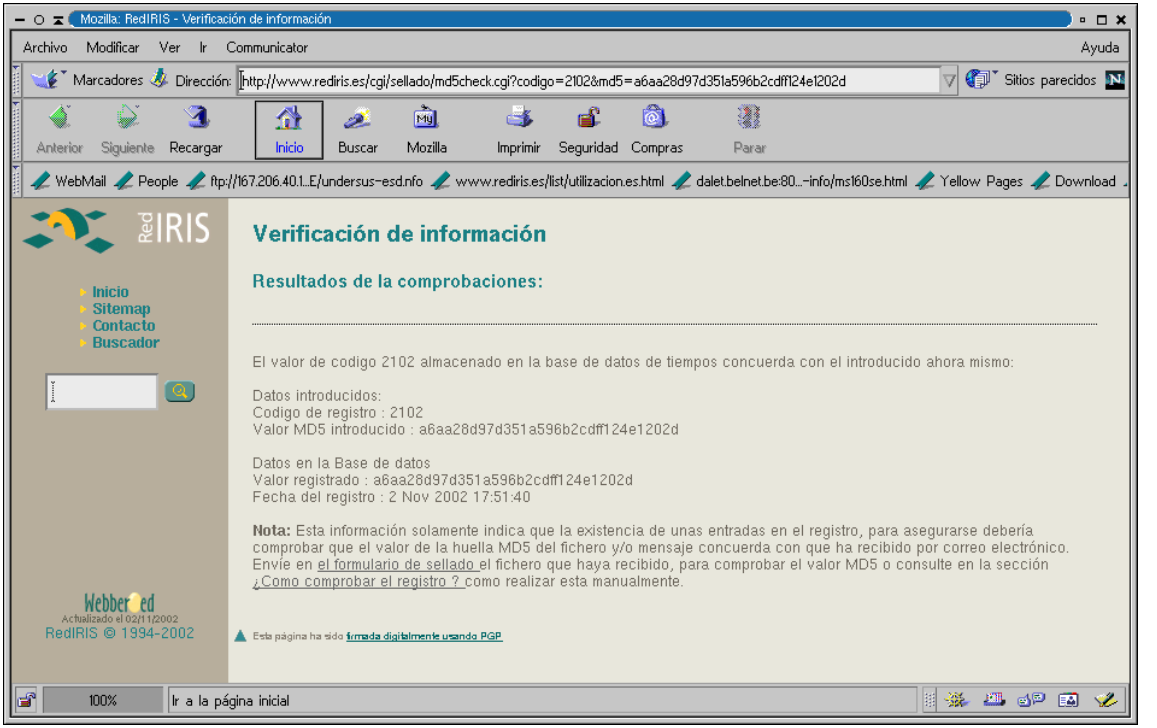
Ejemplo: Composición de un mensaje



Ejemplo: Recepción del mensaje



Ejemplo: Comprobación mensaje



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.

Referencias

- Seguridad http://www.rediris.es/cert Grupo de Seguridad de RedIRIS, procedimientos de actuación, estadísticas, etc.

- PGP
  - Lista de correo sobre uso del PGP: MAIL-PGP@listserv.rediris.es
  - Información Sobre PGP http://www.rediris.es/pgp
  - Servidor de claves PGP, http://www.rediris.es/keyserver

Referencias II

- IRIS-PCA
  - Información sobre IRIS-PCA, http://www.rediris.es/cert/proyectos/iris-pca
  - EuroPKI, http://www.europki.org

¿¿ Preguntas ??

Información:

- http://www.rediris.es/app/sellado
- sellado: sellado@rediris.es
- correo-e: sellado-admin@rediris.es