Correo Electrónico Seguro con PGP y S/MIME

Presentado por:
Alberto Sesma Bailador
22 de junio de 2000

Índice

- Introducción a S/MIME y PGP
- Certificados PGP
- Algoritmos
- Comparativas
- Aplicaciones
- Links

S/MIME (i)

- Secure Multipurpose Internet Mail Extensions nace en 1995 como una iniciativa de RSA Security y varios fabricantes de software
- Objetivos:
  - Autenticación
  - Privacidad
  - Integridad de datos
  - Interoperabilidad total entre aplicaciones
- Basado en los Public Key Cryptography Standards (PKCS)
- En desarrollo el estándar S/MIME v2 y v3

S/MIME (ii)

- RSA Security proporciona el sello S/MIME-Enabled a los fabricantes de software
- S/MIME no es una marca registrada, S/MIME-Enabled sí lo es
- El sello se obtiene mediante pruebas online: certificación, firmado, encriptación, verificación y desencriptación de mensajes recibidos.
- Las pruebas se realizan contra una implementación de referencia: *Worldtalk's WorldSecure Client*
- Los certificados siguen el estándar X.509

Pretty Good Privacy (i)

- Objetivos: los mismos que S/MIME
- Primera versión de Phil R. Zimmermann en 1991
- Versiones posteriores de MIT, ViaCrypt y PGP Inc.
- Últimas versiones de Network Associates Inc. (NAI).
- Larga historia de problema legales.
- Versiones freeware sin RSA y versiones comerciales con aplicaciones extra
- Código fuente bajo licencia GPL

Pretty Good Privacy (ii)

- PGP es marca registrada de NAI
- PGP acepta certificados X.509 y certificados PGP
- Estándar OpenPGP v1 en desarrollo

Certificados PGP (i)

- Incluyen, como mínimo:
  - Versión de PGP
  - Clave pública + algoritmo (RSA, DH, DSA)
  - Información del usuario
  - Firma(s)
  - Periodo de validez
  - Algoritmo simétrico preferido: CAST, IDEA, 3DES
- Las claves públicas pueden ser firmadas por todas las personas que se desee.
- Se pueden añadir nuevos campos y firmarlos aparte
- Cualquiera puede validar el par clave pública/poseedor

Certificados PGP (ii)

- Cualquiera puede crear su propio certificado PGP, sin necesidad de una CA
- Cualquiera puede revocar su propio certificado
- No existe manera de revocar un clave ‘perdida’
- Keyservers: wwwkeys.es.pgp.net
- “Fiestas de firmado”

Algoritmos S/MIME

- Clave pública: RSA, **DH**
- Clave simétrica: DES, **3DES** y **RC-2**
- Firma: RSA, **DSS** (Digital Signature Standard)
- Hash: **SHA-1,** MD5*
- Las claves de RC-2 son de longitud variable pero el estándar obliga a 40 bits
- Claves públicas hasta 1024 bits

Algoritmos PGP (i)

- Clave pública: RSA (excepto versiones freeware), **ElGamal**
- Clave simétrica: IDEA*, CAST-128, **3DES**, AES
- Firma: RSA, **DSS**
- Hash: MD5*,**SHA-1,** RIPEMD-160
- Compresión: Lempel-Zip
- Claves simétricas de 128 bits. Públicas hasta 4096 bits.

Algoritmos PGP (ii)

- NIST declaró a DES el sistema de encriptación oficial en 1977
- En Enero 1997 publicó la iniciativa de encontrar una algoritmo para reemplazar a DES. Cuando lo encuentren lo llamarán AES (Advanced Encription System)
- En el 2001 se elegirá uno de entre: MARS, Serpent, RC6, Rijndael, **Twofish**
- OpenPGP ya ha reservado tres identificadores para claves de 128, 192 y 256 bits

S/MIME vs PGP (i)

	OpenPGP	S/MIME
Clave simétrica	3DES(CFB)	3DES (CBC) & RC2/40
Clave pública	ElGamal (4096)	Diffie-Hellman (1024)
Firma	DSS	DSS
Hash	SHA-1	SHA-1

S/MIME vs PGP (ii)

- Debido a la complejidad del estándar, el sello S/MIME-Enabled no garantiza la interoperabilidad de las aplicaciones
- El estándar S/MIME fija la longitud máxima de claves públicas en 1024 bits. OpenPGP habla de 4096 bits
- Puerta abierta a *key scrow* en S/MIME v3
- *Additional Decryption Key* en PGP
- La difusión del código PGP evita sospechas (*backdoors, key* scrow) y permite la exportación a múltiples plataformas

S/MIME vs PGP (iii)

- PGP almacena la(s) clave(s) privada(s) encriptada(s) con una *'phrase password'.* El estándar S/MIME no dice nada al respecto
- Es imposible invalidar un certificado PGP si se pierde, o no se puede acceder, a la clave privada
- Los certificados X.509 parecen tener más credibilidad que los PGP, pero éstos son más flexibles
- Algunas versiones de PGP para Windows dependen de CryptoAPI

Aplicaciones S/MIME-Enabled

- Baltimore Technologies' MailSecure
- Entrust
- Microsoft Outlook y Outlook Express
- Netscape Communicator
- OpenSoft ExpressMail
- SSE TrustedMIME
- VeriSign Digital ID
- WorldTalk

Aplicaciones PGP

- PGPv6.02
- Eudora 3.x y 4.x
- Outlook Express, 97, 98 y 2000
- Pegasus Mail
- Lotus Notes
- “Netscape Communicator 3.x 4.x”
- GNU Privacy Guard (GPG)

Links

- PGP
  - www.pgpi.org
  - www.rediris.es/pgp
  - www.scramdisk.clara.net/pgpfaq.html
- S/MIME
  - www.rsasecurity/standards/smime
- Estandarización
  - www.imc.org
  - www.ietf.org
- Certificados gratuitos
  - www.truscenter.de
  - www.thawte.com