Sintaxis:

openssl <comando> [opciones]

openssl genrsa [opciones] [tamaño]

Genera una nueva clave RSA del tamaño especificado como argumento.

-aes128, -aes192, -aes256
: Usa cifrado AES para la clave privada

-des, -des3
: Cifra la clave privada con DES o Triple-DES respectivamente.

-out <fichero>
: Almacena la clave en el fichero especificado como argumento

openssl dgst [opciones]

*Calcula el resumen (*digest*) de un mensaje leído desde la entrada estándar, y muestra dicho resumen en la salida estándar.*

-md5, -md4, -md2
: Utiliza los algoritmos md5, md4 y md2 respectivamente

-sha1, -sha
: Utiliza los algoritmos SHA1 o SHA, respectivamente

-mdc2
: Utiliza el algoritmo MDC2

-ripemd160
: Utiliza el algoritmo RIPEMD160

-binary
: La salida se origina en crudo (en binario)

openssl enc [opciones]

Cifra/descifra un mensaje leído desde la entrada estándar y lo devuelve codificado a la salida estándar. Cifra/descifra utilizando un criptosistema simétrico.

-e, -d
: Cifra o descifra, respectivamente.

-a, -base64
: Muestra la salida en formato BASE64

-bufsize <n>
: Fija el tamaño del búfer a "n" bytes.

-k <clave>
: Usa el argumento dado como la clave de cifrado.

-k<fichero>
: La clave es la primera línea del fichero dado.

-aes128, -aes192, -aes256
: Utiliza el algoritmo de cifrado AES, de 128, 192 o 256 bits respectivamente.

-des, -des3
: Utiliza el algoritmo DES o TripleDES, respectivamente.

-blowfish
: Utiliza el algoritmo de cifrado Blowfish.

-rc2, -rc4
: Utiliza el algoritmo de cifrado RC2, o RC4 respectivamente

openssl req [opciones]

Genera una petición de certificado (o un certificado autofirmado).

-inform <format>, -outform <format>
: El fichero de entrada o el de salida se encuentran en el formato *format*, que puede ser PEM o DER.

-key <fichero>
: Lee la clave privada del fichero dado como argumento

-new
: Indica que estamos realizando una petición nueva.

-x509
: Crea una estructura X.509 en lugar de una petición

-days <dias>
: Especifica el número de días que un certificado creado con -x509 es válido.

-noout
: Muestra una salida resumida, en lugar de un bloque PEM

-text
: Muestra la salida en texto plano

-[digest]
: Usa el algoritmo *digest* para hacer el resumen de la petición/certificado. Vea el comando dgst para una lista más exhaustiva de los algoritmos.

openssl ca [opciones]

Gestiona una CA definida en el fichero de configuración de OpenSSL (openssl.cnf). Por defecto firma una CSR (petición de certificado).

-days <dias>
: Número de días para los cuales la firma será válida.

-md <digest>
: Algoritmo que se usará para el resumen del certificado firmado (Vea el comando dgst)

-policy <política>
: Política que se aplicará para firmar el certificado (debe estar definida en openssl.cnf)

-keyfile <fichero>
: En el fichero dado como argumento se encuentra la clave privada de la CA, que se utilizará para firmar.

-cert <fichero>
: En el fichero dado como argumento se encuentra el certificado autofirmado de la CA (o firmado por otra CA)

-status <numerodeserie>
: Dado el número de serie de un certificado, comprueba su estado en la base de datos de la CA

-updatedb
: Actualiza la base de datos de la CA con los certificados revocados.

-in <fichero>
: El CSR para firmar se encuentra en el fichero dado como argumento

-out <fichero>
: El certificado firmado se almacenará en el fichero dado.

-revoke <fichero>
: Revoca el certificado dado en el fichero especificado.

-gencrl
: Genera una CRL de la CA, con los certificados revocados.

-verbose
: Muestra más información en la pantalla.

-batch
: No hace preguntas, asume valores por defecto.

openssl rand [opciones] <bytes>

Genera una secuencia seudoaleatoria de tantos bytes como se especifiquen como argumento, y la muestra en pantalla.

-out <fichero>
: Guarda la secuencia en el fichero dado como argumento

-base64
: Muestra la secuencia en formato BASE64.

grupo de programadores y usuarios de linux

Taller de Criptografía Aplicada
Julio 2004

Gestión de Certificados con OpenSSL

(chuletilla)

Andrés J. Díaz <ajdiaz@gpul.org>