Seguridad en Redes
Practica 2.3

David Antuña Rodríguez
Javier Carrión García

1 OpenSSL

1.1 Creación de una CA

Si intentamos utilizar otros directorios dará error a no ser que se modifique el fichero de configuración, concretamente los datos de la sección [CA_default].

La clave privada se ha almacenado en *demoCA/private/cakey.pem* y el certificado en *demoCA/cacert.pem*. Como hemos empleado la opción -new la clave generada es de tipo RSA y su tamaño viene especificado en el fichero de configuracion, valor de default_bits en la sección [req], por defecto son 2048 bits.

Los ficheros de este apartado están en la carpeta *ca*,

1.2 Creación de solicitudes de firma de certificado

El algoritmo por defecto se encuentra en la variable default_md del fichero de configuración, en nuestro caso hemos empleado la opción -new que crea una clave rsa nueva y la ha almacenado en userkey1.pem y userkey2.pem, también podriamos haber utilizado una que tuvieramos previamente con la opción -key.

El certificado contiene los datos que identifican al usuario solicitante, incluida su clave pública. Puede verse en los ficheros de la carpeta *csr*

1.3 Consulta y manipulación de certificados

La información de los certificados se puede ver en los ficheros de la carpeta *certs*. Los certificados usan la version 3.

En un certificado van todos los datos del poseedor del certificado, Subject, junto con la validez del mismo.

Si se quiere comprobar si el poseedor es una CA basta con ver el common name del Subject, x509 también añade un campo Basic Constraints en los certificados que no son de CA con el valor CA:FALSE.

1.4 Revocación de certificados

La crl está en la carpeta *revocacion*.

Hay un certificado revocado con serial number 02, corresponde a usercert2, lo ha revocado la CA que es quien ha creado el crl, campo Issuer. El CRL es válido porque la CA lo ha firmado.

2 GnuPG

2.1 Firma de claves (Web of trust)

En los check-trust y validity aparecen claves 2 extra, con nivel ultimate, que corresponden a las dos que generamos en la práctica anterior. Tambien está en el anillo la clave pública que subiste el otro día, tiene confianza desconocida.

Todos los ficheros están en la carpeta *trust*.

C será valida porque aunque desconocemos la validez de C sí conocemos la de B, y nos fiamos de ella, y la clave C ha sido firmada por B.
Ficheros *checktrustdb.txt* y *validity.txt*.

En el segundo caso C no será válida porque B es dudosa y para validar una clave con firmas dudosas son necesarias al menos 3, también debe cumplir que el camino que lleva hasta nuestra firma es menor de 5, como hemos firmado B con la clave A esto se cumple pero estas condiciones no son excluyentes.
Ficheros *checktrustdb2.txt* y *validity2.txt*.

Ahora C vuelve a ser válida porque como hemos explicado antes ha sido firmada por 3 claves dudosas (B, D y E) y además el camino a nuestra clave es menor de 5.
Ficheros *checktrustdb3.txt* y *validity3.txt*.