Certificados en Windows

Jorge Chávez Saab

1 Introducción

Una de las principales aplicaciones de la criptografía de llave pública es la de *firmas digitales*, esquema en el cual un emisor puede añadir una firma a un mensaje para que el que lo lea pueda cerciorarse de que el mensaje está íntegro y fue escrito por quien se presume. En este esquema se utiliza un par de llaves distintas para diferenciar entre el emisor (*llave privada*) y el receptor (*llave pública*) del mensaje: cualquiera que posea la llave pública puede verificar que la firma sea válida, y esta llave normalmente se distribuye libremente al público, mientras que solo el que posea la llave privada tiene la habilidad de generar la firma de un mensaje.

Un esquema de firmas digitales garantiza al receptor que, si la firma es válida para la llave pública con la que se verificó, entonces el mensaje fue escrito por el dueño de la llave privada correspondiente. Sin embargo, los pares de llaves pueden generarse fácilmente y con gran frecuencia, por lo que para estar seguros de la identidad física del emisor (el nombre de la organización o persona) necesitamos garantía por parte de un tercero de que esta llave privada corresponde a dicha identidad. Por lo tanto, una *infraestructura de llave pública* consiste en los protocolos de firma y verificación acompañados de una estructura para las llamadas *autoridades certificadoras* (AC). Una AC es la encargada de verificar la identidad detrás de una llave, y una vez que lo hace emite un documento llamado *certificado* donde indica la llave pública, la identidad correspondiente y otros datos relevantes, y lo firma usando su propia llave (se asume que cualquiera puede verificar la firma de una AC, pues su llave pública es de conocimiento común). Así, las firmas digitales suelen ir acompañadas de un certificado que (asumiendo que se confía en la AC) demuestra la identidad del que firmó.

2 Organización de certificados en Windows

El sistema Windows depende fuertemente en el uso de certificados para verificar la identidad de clientes y servidores. Para esto se usa el estándar X.509, que especifica el formato y los campos que debe incluir un certificado. El sistema Windows guarda estos certificados en dos direcciones del disco llamadas *tiendas de certificados*:

- **Tienda de sistema:** contiene los certificados necesarios para los procesos esenciales del sistema operativo. Si la máquina funciona como servidor, también incluye los certificados que necesitará para identificarse ante sus clientes.

- **Tienda de usuario:** contiene los certificados específicos para el usuario, como aquellos requeridos por aplicaciones cliente que éste haya instalado.

Cabe mencionar que muchos certificados son emitidos por ACs menores que no son lo suficientemente reconocidas para ser aceptadas universalmente. En este caso los certificados que emite la AC van acompañados de un certificado que emite una AC superior a la AC menor para indicar que ésta es de confianza. Esta *cadena de autorización* se puede repetir múltiples veces hasta llegar a una AC llamada la *autoridad certificadora raíz*, la cual es tan conocida que se puede confiar ciegamente en ella. Esto nos lleva a que ambas tiendas de certificados contengan dos subtiendas especiales:

- **Certificados de autoridades raíz:** son certificados emitidos por una AC que se presume es lo suficientemente conocida para confiar ciegamente en ella. Se requieren permisos de administrador para agregar certificados aquí, ya que esto puede conllevar un gran riesgo.
- **Certificados personales:** son certificados típicamente usados por el usuario en los que no se confía a menos que se encuentre una cadena de autorización que llegue hasta un certificado de autoridad raíz.

A demás de certificados, las tiendas de Windows también pueden contener dos tipos de listas llamadas *listas de certificados de confianza* (CTL) y *listas de certificados revocados*. La primera se utiliza para confiar en certificados personales aun si no se encuentra una cadena de confianza a una AC raíz, y la segunda se utiliza para listar certificados en los que no se debe confiar aun si la tienen debido a que tuvieron que ser revocados por alguna emergencia (por ejemplo, si la llave privada del emisor fue comprometida).

3 Manejo de certificados

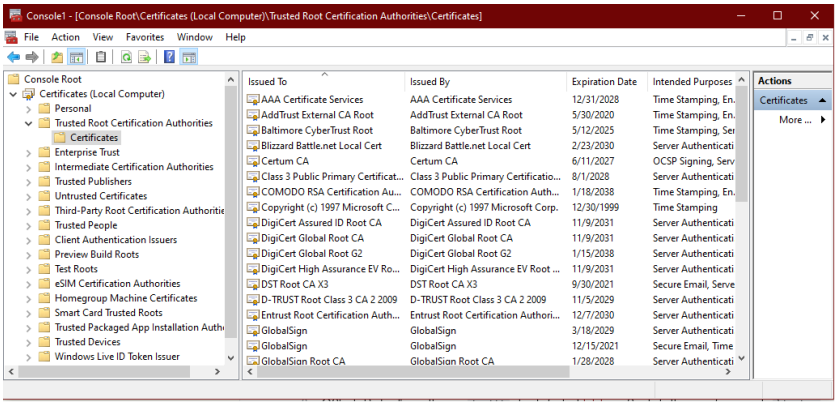

Figure 1: Visualización de certificados a través del Microsoft Management Console

Para visualizar los certificados instalados presionamos `Windows+R` y escribimos `mmr` para abrir el *Microsoft Management Console*. En esta pantalla presionamos `Archivo -> Añadir snap-in` y seleccionamos `Certificados` para añadir este rubro a la consola. El sistema nos preguntará si deseamos ver los certificados de usuario o de sistema (si tenemos derechos de administrador), y posteriormente podremos navegar la tienda de certificados (ver figura 1).

Desde aquí podemos eliminar certificados directamente, pero para añadir nuevos certificados es necesario usar la aplicación `certmgr.exe` que viene con la instalación de Visual Studio (disponible aquí). Una vez instalado abrimos el *command prompt* (presionando `Windows+R` y tecleando `cmd`) y escribimos el comando. Su uso es:

```
    certmgr [/add | /del | /put] [opciones]
[/s[/r ubicacionRegistro]] [tiendaFuente]
[/s[/r ubicacionRegistro]] [tiendaObjetivo]
```

el cual disecamos a continuación:

- El primer corchete se refiere a la acción a tomar: `/add` añade un certificado a una tienda, `/del` lo borra de una tienda y `/put` guarda un certificado en un archivo para ser exportado.
- El segundo corchete se refiere a distintas opciones. Por ejemplo, cuando se especifica una tienda y no un certificado como fuente, la opción `/all` puede usarse para tomar la misma acción con todos los certificados de la tienda. Además debemos especificar `/c`, `/ctl` o `/crl` según sea el caso si queremos manejar certificados, CTLs o CRLs.
- La segunda línea se refiere a la fuente. Si se trata de un solo nombre entonces la fuente se considera un archivo en el directorio de trabajo. Si se precede con la opción `/s` entonces la fuente será una tienda con ese nombre. Seguido de la opción `/s` puede usarse `/r ubicacionRegistro` para especificar la ubicación de la tienda: *ubicacionRegistro* debe de tener el valor ya sea `currentUser` (tienda de usario) o `localMachine` (tienda de sistema).
- La tercera línea se refiere al objetivo, con la misma sintaxis que la fuente. Al usar la opción `/del` no se requiere esta línea.

Ejemplos:

```
certmgr /add /c miCertificado /s /r localMachine miTienda
```

Agrega el certificado en el archivo *miCertificado* a la tienda de sistema *miTienda* (habrá que confiar muy bien en el).

```
certmgr /del /all /c /s /r currentUser miTienda
```

Elimina todos los certificados en la tienda de usuario *miTienda*

```
certmgr /put /all /c /s /r currentUser miTienda nuevoArchivo
```

Exporta todos los certificados en *miTienda* a *nuevoArchivo*