Mecanismos de verificación de validez de un certificado dentro de una PKI

Una vez definidos los métodos de revocación de certificados dentro de una PKI, es muy importante disponer de mecanismos por parte de la misma para que los servicios asociados a su uso puedan discriminar de manera fiable la validez de los certificados en cada momento.

Disponer de toda una infraestructura que permite distribuir la confianza y que está tan extendida en el uso final de aplicaciones y usuarios (p.ej.: navegadores y SSL, servicios Web, etc.), pero no utilizar servicios de **actualización del estado actual** de la misma, no parece un marco de trabajo adecuado, sin embargo, en muchos entornos se configuran las cosas correctamente de manera inicial pero no se contempla el ciclo de vida de la misma.

Se definen dos estados de revocación dentro del estándar X.509:

- Revocado: Implica revocación irreversible
- "Hold" (sostenido): Es una revocación temporal que puede ser revertida

Se definen también en el estándar los diferentes motivos posibles para la revocación.

En este sentido, en el mundo de las PKI que utilizan certificados basados en el estándar X.509, se definen dos mecanismos estandarizados de consulta de validez de certificados:

- **Listas de revocación de certificados**: Llamadas CRLs (por sus siglas en inglés), se trata de certificados especiales emitidos periódicamente por la Autoridad de Certificación (AC), en la que el contenido que se certifica es la lista de certificados no válidos por revocación (y la fecha de la misma) que "cuelgan" de dicha AC, es decir, certificados que, todavía en el espacio de validez temporal, no deben ser confiados más para su uso. La certificación se realiza mediante la firma digital de dicha lista por parte de la AC. La AC dispone de un periodo concreto de publicación de las CRLs (por ejemplo, diaria), y además, habitualmente implementa la publicación mediante mecanismos Web, para que las aplicaciones cliente puedan consultarlas previamente al uso de los certificados. Se establece también un formato de fichero estandarizado para las CRLs.
- **OCSP** (Online Certificate Status Protocol): Se trata de un protocolo de Internet estandarizado (RFC 6960) para su implementación en servidores por parte de los Proveedores de Servicios de Certificación. A esos servidores se les denomina OCSP-Responders. El protocolo tiene las siguientes características:
  - Se implementa para mejorar aspectos negativos de las CRLs
    - Las CRLs no dan la información puntual, ya que dependen del periodo en el que se publican
    - Las CRLs contienen TODOS los certificados revocados por una AC. Hay que procesar esos datos en el cliente cada vez que se consulta
  - OCSP permite la consulta por parte de un cliente de la validez de un certificado concreto (mediante su Serial Number)
  - La respuesta puede ser: "good", "revoked" o "unknown"
  - Se suele añadir seguridad a esta nueva comunicación (implica una nueva relación de confianza:
    - La respuesta está firmada
    - Suele incluir un sellado de tiempo confiable en la misma
    - Se suele realizar por un canal SSL/TLS

Un punto negativo de todo esto es que, lo que se contemplaba como un **marco autocontenido** de autenticación (disponiendo del certificado del otro extremo por delante, no se necesita nada más para establecer la comunicación), ya deja de serlo, ya que requiere que un servicio externo esté

disponible de manera continua para que todas las verificaciones puedan realizarse de manera absolutamente segura.

Fuentes: Wikipedia, Microsoft.com