

Listas de Revocación de Certificados (CRLs)

Los certificados tienen un periodo de validez que va de unos meses a unos pocos años, información que se encuentra integrada en el propio certificado. Durante el tiempo que el certificado es válido la entidad certificadora que lo generó mantiene información sobre el estado de ese certificado, en el caso de ANF AC el periodo durante el cual se mantiene la información es de 15 años después de que expire el periodo de vigencia del certificado.

La información más importante que guarda es el *estado de revocación*, que indica que el periodo de validez del certificado ha terminado antes de tiempo y el sistema que lo emplee no debe confiar en él. Las razones de anulación de un certificado son varias: la clave privada del sujeto se ha visto comprometida, la clave privada de la CA se ha visto comprometida o se ha producido un cambio en la afiliación del sujeto (por ejemplo cuando un empleado abandona una empresa).

Las *listas de revocación de certificados* (*Certification Revocation Lists* o CRL) son un mecanismo mediante el cual la CA publica y distribuye información a cerca de los certificados anulados a las aplicaciones que los emplean. Una CRL es una estructura de datos firmada por la CA que contiene su fecha y hora de publicación, el nombre de la entidad certificadora y los números de serie de los certificados anulados antes de su fecha de caducidad.

Verificación del certificado CRL. Las Listas de Revocación de Certificados (CRL's) deben de ser verificadas tras su descarga. ANF AC facilita gratuitamente dispositivos de verificación al efecto.