TIPOS DE CERTIFICADOS

Dependiendo del uso que se vaya a dar al certificado y de qué persona o entidad lo solicita, las Autoridades Certificadoras han dividido los certificados en varios tipos. Del tipo de certificado a emitir van a depender las medidas de comprobación de los datos y el precio del mismo.

Los **certificados, según las comprobaciones de los datos que se realizan**, se dividen en cuatro clases:

- **Certificados de Clase 1**: corresponde a los certificados más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.
- **Certificados de Clase 2**: en los que la Autoridad Certificadora comprueba además el DNI o permiso de conducir, el número de la Seguridad Social y la fecha de nacimiento.

- **Certificados de Clase 3**: en la que se añaden a las comprobaciones de la Clase 2 la verificación de crédito de la persona o empresa mediante un servicio del tipo Equifax o Duns&Bradstreet.

- **Certificados de Clase 4**: que a todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización (todavía no formalizados los requerimientos; está en estudio).

Desde el punto de vista de la finalidad, los certificados electrónicos se dividen en:

1. **Certificados SSL para cliente**: usados para identificar y autentificar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden normalmente a una persona física, bien un particular, bien un empleado de una empresa.

2. **Certificados SSL para servidor**: usados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor. La presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL.

3. **Certificados S/MIME** : usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona Autentificación, Integridad y No Repudio. También se puede cifrar el mensaje con la clave pública del destinatario, lo que proporciona Confidencialidad al envío.

4. **Certificados para la firma de código**: usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red (Java, JavaScript, CGI, etc). Cuando un código de éste tipo puede resultar peligroso para el sistema del usuario, el navegador lanza un aviso de alerta, en el que figurará si existe certificado que avale al código, con lo que el usuario puede elegir si confía en el autor, dejando que se ejecute el código, o si por el contrario no confía en él, con lo que el código será rechazado.

5. **Certificados para AC**: que identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera, accediendo al certificado de la AC y comprobando que ésta es de confianza.

   Toda persona o entidad que desee obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo (ambas están relacionadas). A mayor nivel de comprobación de datos (clase mayor), más costará el certificado.