AUTORIDADES CERTIFICADORAS (CA).

Una autoridad certificadora es una organización fiable cuya función es únicamente expedir certificados de identidad y mantener la información de su estado. Las labores de un CA son:

- Admisión de solicitudes. Un usuario rellena un formulario y lo envía a la CA solicitando un certificado. La generación de las claves pública y privada son responsabilidad del usuario o de un sistema asociado a la CA.
- Autentificación del usuario. Antes de firmar la información proporcionada por el usuario la CA debe verificar su identidad.
- Generación de certificados. Después de recibir una solicitud y validar los datos la CA genera el certificado correspondiente y lo firma con su clave privada.
- Distribución de certificados. La autoridad certificadora puede proporcionar un servicio de distribución de certificados.
- Anulación de certificados. La CA debe mantener información sobre una anulación durante todo el tiempo de validez del certificado original.
- Almacenes de datos. Almacenar en una base de datos los certificados y la información de las anulaciones.
- Generación de documentación. En ella se explica los procedimientos y las prácticas y políticas de certificación de la CA.

Autoridades de Certificación

ACE

La Agencia de Certificación Electrónica (ACE) es una autoridad de certificación en la que participan el grupo Telefónica (40%), CECA, SERMEPA y Sistema 4B (20% cada uno) tiene como objetivo principal la emisión de certificados para utilizar con el protocolo de pago electrónico SET definido por VISA y MasterCard.

FESTE

Es la autoridad de certificación de la Fundación para el Estudio de la Seguridad de las Telecomunicaciones, entidad en la que participan, entre otros, los notarios y corredores de comercio.

SISCER (Sistema de Certificación) es una autoridad que desde 1997 presta servicios de certificación a varios bancos y cajas de ahorro. SISCER pertenece a Intercomputer S.A., empresa miembro de la Fundación FESTE, y quedará integrada en la autoridad de certificación FESTE.

IPS

IPS Seguridad es una división de Internet Publishing Services, empresa española dedicada a las tecnologías relacionadas con Internet desde 1995, con oficinas en Madrid y Barcelona. IPS Seguridad ofrece certificados para servidores y para usuarios. La obtención de un certificado de servidor requiere entrega física de documentación a IPS Seguridad y tienen un plazo de validez de un año.

CERES

CERES (Certificación Pública de Transacciones Electrónicas) es una autoridad de certificación pública desarrollada por la Fábrica Nacional de Moneda y Timbre (FNMT). Además de la FNMT, colabora en CERES el Ministerio de Administraciones Públicas, que participa en los grupos de trabajo técnico y jurídico encargados de desarrollar la infraestructura técnica y el soporte legal a las operaciones de la autoridad de certificación. Mediante CERES, la FNMT, cuyo papel tradicional ha sido garantizar la seguridad de documentos físicos, extiende su ámbito de actuación a los documentos y transacciones electrónicas realizadas entre ciudadanos o empresas y las administraciones públicas. El objetivo principal de CERES es garantizar a ciudadanos y administraciones la identidad de ambos partícipes en una comunicación, así como la confidencialidad e integridad del mensaje enviado.

CERES tiene dos características básicas:

- La información privada del usuario se encuentra almacenada en una tarjeta inteligente (el equivalente a un documento de identidad electrónico) protegida por un número de identificación personal, similar a la clave de una tarjeta de crédito.
- El sistema es completamente transparente al usuario, es decir, no es necesario conocer ninguna técnica criptográfica para realizar o verificar una firma electrónica o cifrar o descifrar un mensaje.

Los servicios que prestará CERES se dividen en cinco grupos:

- Servicios de certificación de claves.
- Servicios de registro de usuarios.
- Servicios de publicación de certificados, listas de revocación y políticas de actuación.
- Servicios de certificación de documentos. Garantizan la integridad de los contenidos y la fecha de comunicación, proporcionando al usuario
- Destino u origen la constancia de haber enviado o recibido el mensaje respectivamente.
- Servicios de recuperación de claves.

Otras autoridades de certificación

Además de las citadas en las secciones anteriores, existen varias autoridades de certificación más que prestan servicios en España, por ejemplo la autoridad de Banesto, una de las primeras en funcionar en España, o VeriSign, una de las empresas líderes a nivel internacional y muy utilizada en España.