GLOSARIO SOBRE FIRMA DIGITAL
Terminología de uso frecuente

Infraestructura de Firma Digital

Se define Infraestructura de Firma Digital o Infraestructura de Claves Públicas como el conjunto de normas jurídicas, hardware, software, bases de datos, redes, estándares tecnológicos, personal calificado y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones), mediante el uso de certificados digitales como herramienta, se identifiquen entre sí de manera segura al realizar transacciones en redes, especialmente Internet, permitiendo además dotar de autoría e integridad a los documentos digitales.

Autoridad Certificante (AC)

Toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el Ente Licenciante.
Pueden ser por ejemplo:
- El estado respecto de sus agentes públicos.
- Empresas respecto de sus empleados.
- Colegios profesionales respecto de los matriculados.
- Bancos respecto de sus clientes, etc.

Autoridad de Registro (AR)

Efectúan las funciones de validación de identidad y de otros datos de los solicitantes y suscriptores de certificados, registrando las presentaciones y trámites que les sean formulados por éstos.
Los organismos públicos que han sido habilitados para operar como AR del Certificador, incluyendo su domicilio, datos de contacto y si operan bajo modalidad de Puesto Móvil, se encuentran disponibles en su sitio web https://pki.jgm.gob.ar/app
Colegio de Escribanos de la Provincia de Buenos Aires se ha constituido como Autoridad de Registro de la Oficina Nacional de Tecnologías de la Información (ONTI) dependiente del Ministerio de Modernización de la Nación.

Certificado digital

Se entiende por Certificado digital al documento digital firmado digitalmente por un Certificador, que vincula los datos de verificación de firma a su titular.
Los certificados de firma digital deben ser emitidos por un Certificador Licenciado cuya licencia esté certificada por el Ente Licenciante.

Firma Digital

Es el resultado de aplicarle a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante (clave privada), encontrándose ésta bajo su absoluto control.
Debe ser susceptible de verificación por terceras partes, de manera tal que dicha verificación permita simultáneamente identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Firma Digital, Propiedades

- Autenticidad: Poder atribuir el documento únicamente a su autor de forma fidedigna, de manera de poder identificarlo.
- Integridad: Estar vinculada a los datos del documento digital, poniendo en evidencia su alteración luego de que fue firmado.
- Exclusividad: Garantizar que la firma se encuentre bajo el absoluto y exclusivo control del firmante.
- No repudio: Garantizar que el emisor no pueda negar o repudiar su autoría o existencia; ser susceptible de verificación ante terceros.
- Validez: Haber sido producida con un certificado emitido por un Certificador Licenciado.

Firma Electrónica

Se entiende por Firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para ser considerada una firma digital.

Token

Dispositivo criptográfico capaz de generar y almacenar tanto claves privadas como certificados digitales. Contiene un software interno que permite generar el par de claves (pública y privada) de manera que la clave privada nunca abandona el dispositivo.

Consideraciones de seguridad

- La clave privada es generada, almacenada y utilizada en el token.
- Se debe proteger la clave privada, para esto se pueden utilizar contraseñas.
- La Autoridad Certificante NO posee copia de la clave privada, por lo tanto no puede restaurarla si se pierde.
- El certificador NO interviene en las comunicaciones entre las partes.
- No es necesario un certificado por cada documento a firmar digitalmente.
- La firma digital no se puede imprimir.

Hash

Es un procedimiento matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud. Existen distintos tipos de algoritmos para generar los hash.

Cifrado

Procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave privada) para transformar un mensaje de manera que sea incomprensible para toda persona que no cuente con la clave secreta (clave pública) del algoritmo. Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica), distintas (criptografía asimétrica) o de ambos tipos (criptografía híbrida)

Suscriptor de certificados

Las personas físicas que desempeñen funciones en entes públicos estatales.
Las personas físicas o jurídicas que realicen trámites con el Estado, cuando existe una aplicación que requiera una firma digital

Terceros Usuarios
Toda persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

CRL
Lista de certificados revocados. Es generada por el Certificador Licenciado y contiene todos los certificados revocados. Es consultada en línea por los softwares utilizados para la verificación de documentos firmados digitalmente.

Marco Normativo
- Ley N° 25.506 de Firma Digital
- Decreto N° 2.628/02: Reglamenta la ley de firma digital.
- Decreto N° 409/05: Designa a la Subsecretaría de la Gestión Pública como Autoridad de Aplicación de la Ley N° 25.506 y le asigna las funciones de ente licenciante.
- Decisión Administrativa JGM N° 927/14: Establece el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten. Establece una Política Única de Certificación común a todos los Certificadores Licenciados. Los certificados emitidos por los Certificadores Licenciados son interoperables.