



Http vsHttps

http: Hyper Text Transfer Protocol, protocolo para transmisión de información en plano, sin cifrado. Su puerto por defecto es el número 80.

https: Hyper Text Transfer Protocol **Secure**, protocolo para transmisión información cifrada mediante SSL o TLS. Su puerto por defecto es el numero 443.



SSL (Secure Sockets Layer)

Es un protocolo que proporciona privacidad e integridad entre dos aplicaciones. El sistema SSL es independiente del protocolo utilizado; esto significa que puede asegurar transacciones realizadas en la Web a través del protocolo HTTP y también conexiones a través de los protocolos FTP, POP e IMAP. SSL actúa como una capa adicional que permite garantizar la seguridad de los datos y que se ubica entre la capa de la aplicación y la capa de transporte (por ejemplo, el protocolo TCP)

Originado en Netscape su Version 3.0 data de **1996**, definida en la **RFC-6101** por la Internet Engineering Task Force (IETF).



SSL (Secure Sockets Layer)

Los datos que circulan en un sentido y otro entre el cliente y el servidor se cifran mediante un algoritmo simétrico como DES o RC4. Un algoritmo de clave pública -generalmente RSA- se utiliza para el intercambio de las claves de cifrado y para las firmas digitales. El algoritmo utiliza la clave pública en el certificado digital del servidor. Con el certificado digital del servidor, el cliente también puede verificar la identidad del servidor. Las versiones 1 y 2 del protocolo SSL sólo proporcionan autenticación de servidor. La versión 3 agrega la autenticación del cliente, utilizando los certificados digitales de cliente y de servidor.



SSL (Secure Sockets Layer)

Fases

1. Establecimiento de la conexión y negociación de los algoritmos criptográficos que van a usarse en la comunicación, a partir del conjunto de algoritmos soportados por cada uno de los interlocutores.
2. Intercambio de claves, empleando algún mecanismo de clave pública y autentificación de los interlocutores a partir de sus certificados digitales.
3. Cifrado simétrico de tráfico.



TLS (Transport Layer Security)

TLS (Transport Layer Security) es una evolución del protocolo SSL (**Secure Sockets Layer**), es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor.





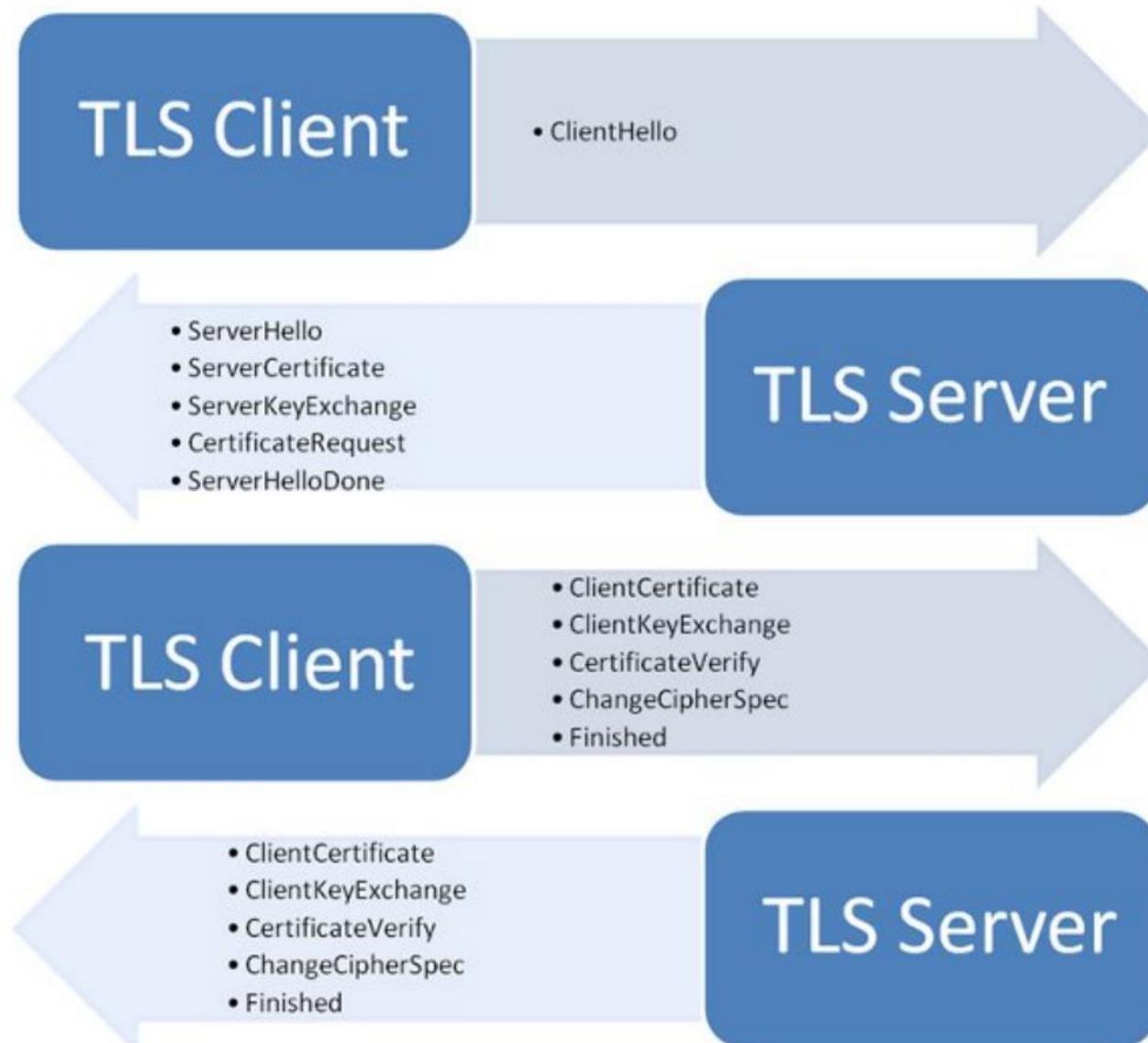
TLS (Transport Layer Security)

Características adicionales

- Incompatible con SSL v3.0
- Uso de funciones MAC en lugar de funciones MDC únicamente
- Numeración secuencial de todos los campos que componen la comunicación, e incorporación de esta información al cálculo de los MAC.
- Protección frente a ataques que intentan forzar el empleo de versiones antiguas —menos seguras— del protocolo o cifrados más débiles.
- El mensaje que finaliza la fase de establecimiento de la conexión incorpora una firma (hash) de todos los datos intercambiados por ambos interlocutores.



TLS (Transport Layer Security)





TLS (Transport Layer Security)

Algoritmos utilizados

- Cifrado Asimetrico: RSA, Diffie-Hellman(DHE), Curva Elíptica (ECDHE), DSA (Digital Signature Algorithm).
- Cifrado Simetrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard)
- Funciones de Hash: MD5 o de la familia SHA .



TLS (Transport Layer Security)

RFC 2246 (1999) - The TLS Protocol Version 1.0

Primer versión del protocolo

RFC 4346 (2006) - The TLS Protocol Version 1.1

Se destacan mejoras en el manejo del padding y protecciones a ataques por CBC usando IV explícitos

RFC 5246 (2008) / RFC 6176 (2011) - The TLS Protocol Version 1.2

Incorporación de SHA-256 para función de PRF(pseudo-aleatoria) y cierre de mensajes, SHA-1 para firma digital, entre otros.

RFC 8446 (2018) - The TLS Protocol Version 1.3

Remoción de cifrados obsoletos, optimización del protocolo (handshaking con Zero Round-Trip Time, etc)



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 alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.



Firma Digital

Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.



Firma digital - Propiedades

- Va ligada indisolublemente al mensaje. Una firma digital válida para un documento no puede ser válida para otro distinto.
- Solo puede ser generada por su legítimo titular. Al igual que cada persona tiene una forma diferente de escribir, y que la escritura de dos personas diferentes puede ser distinguida mediante análisis caligráficos, una firma digital sólo puede ser construida por la persona o personas a quienes legalmente corresponde.
- Es públicamente verificable. Cualquiera puede comprobar su autenticidad en cualquier momento, de forma sencilla.

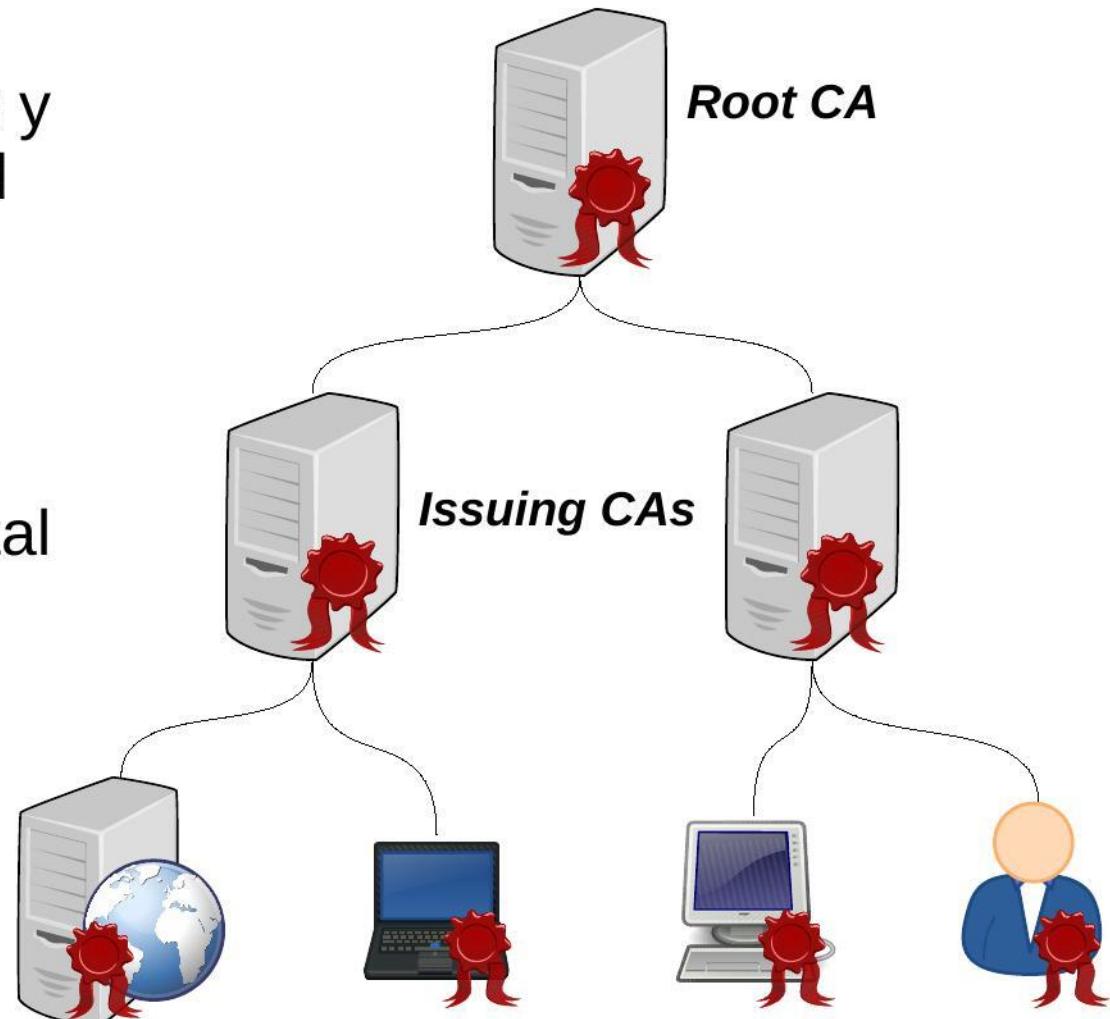


Modelos de Infraestructura de Seguridad



PKI – Infraestructura de Clave Pública

Es una combinación de hardware, software, políticas y procedimientos de seguridad que define un entorno de confianza **centralizado** y provee garantías para operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas





Certificados Digitales

Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular

Es esencialmente una clave pública, un identificador e información accesoria; firmados digitalmente por una autoridad de certificación, y su utilidad es demostrar que una clave pública pertenece a un usuario concreto.



Certificados Digitales

El estándar X.509 solo define la sintaxis de los certificados, por lo que no esta atado a ningún algoritmo en particular, y contempla los siguientes campos:

- Versión.
- Numero de serie.
- Identificador del algoritmo empleado para la firma digital.
- Nombre del certificador.
- Periodo de validez.
- Nombre del sujeto.
- Clave pública del sujeto.
- Identificador único del certificador.
- Identificador unico del sujeto.
- Extensiones.
- Firma digital de todo lo anterior generada por el certificador.



Certificados Digitales de revocación

Cuando una clave pública pierde su validez —por destrucción o robo de la clave privada correspondiente, por ejemplo—, es necesario anularla. Para ello se emplean los denominados certificados de revocación que no son más que un mensaje que identifica a la clave pública que se desea anular, firmada por la clave privada correspondiente.



PKI – Infraestructura de Clave Pública

Componentes:

- **Autoridad de Certificación** (CA, Certificate Authority): Emite y revoca certificados, vinculando las claves públicas con la identidad del propietario.
- **Autoridad de Registro** (RA, Registration Authority): Verifica la relación de los certificados y la identidad de sus titulares.
- **Autoridad de Validación** (VA, Validation Authority): Es la encargada de comprobar la validez de los certificados digitales.
- **Autoridad de Sellado de Tiempo** (TSA, TimeStamp Authority): Es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.
- **Los repositorios**: Almacenan información relativa a la PKI, como certificados y listas de revocación (CRL, Certificate Revocation List).
- **Los usuarios y entidades finales** que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública.

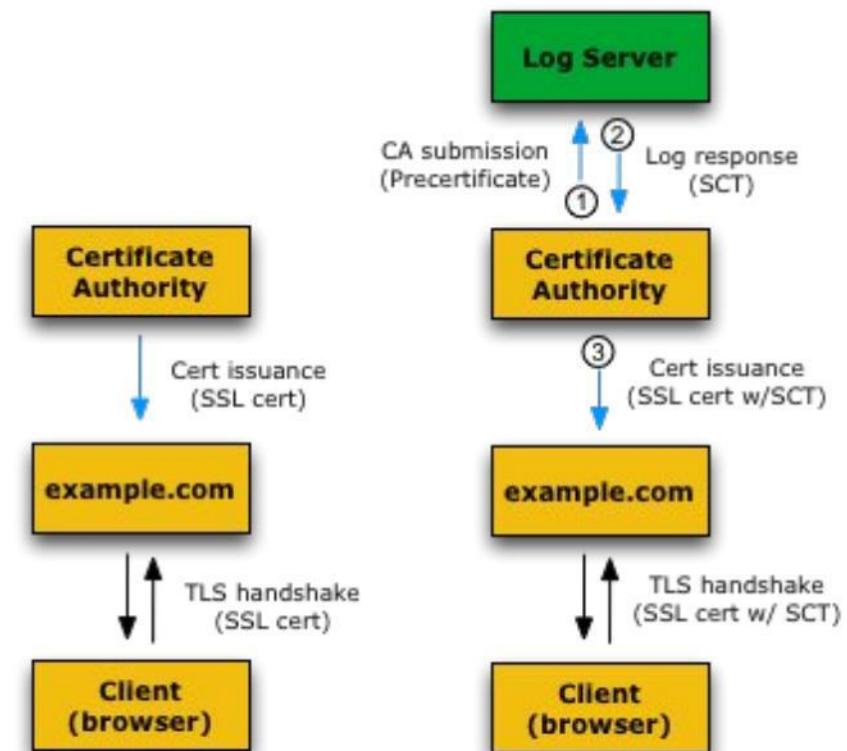


Certificate Transparency



Current TLS/SSL System

TLS/SSL System with Certificate Transparency (X.509v3 Extension)



- Existing TLS/SSL system
- Supplemental CT components
- ← One-time operations
- ↔ Synchronous operations
- ① Order of operation

CT Logs: Certificate Transparency logs

SCT: Signed Certificate Timestamp

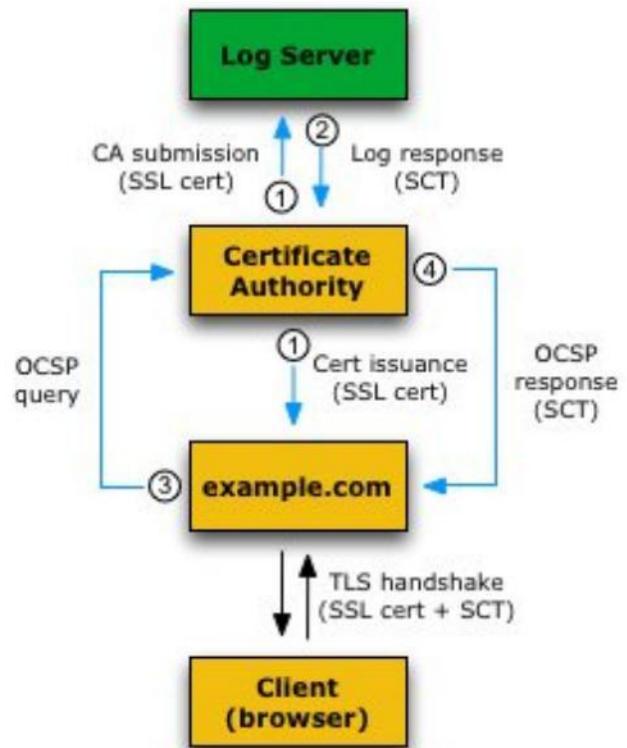


Online Certificate Status Protocol

OCSP: es un método para determinar el estado de vigencia de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados).

<https://tools.ietf.org/html/rfc6960>

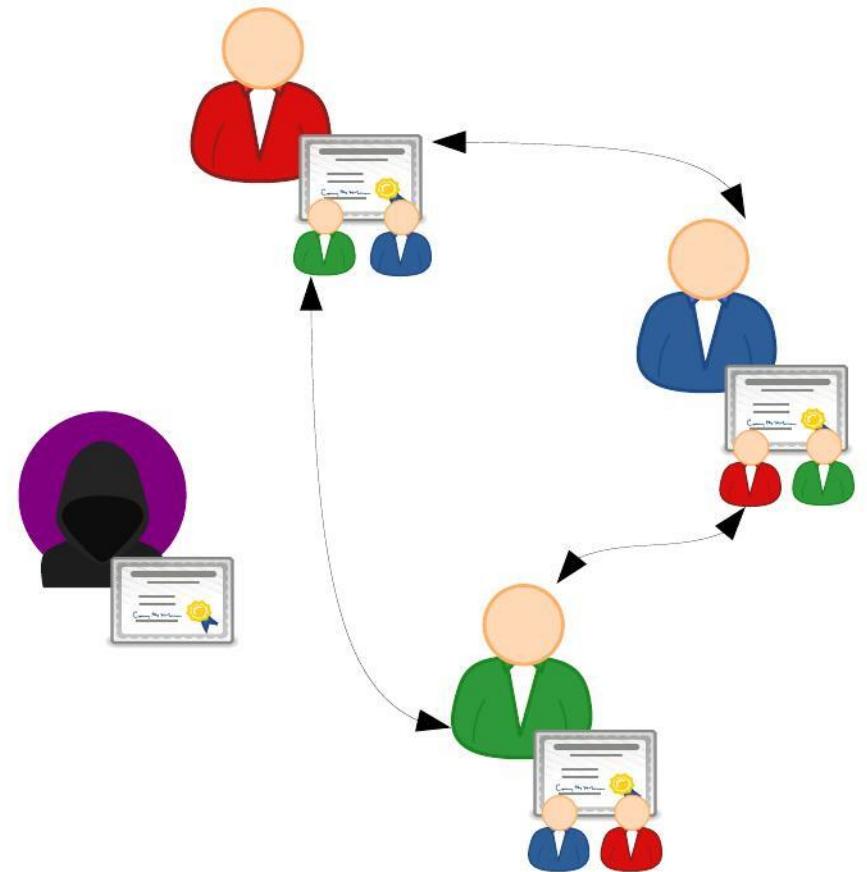
**TLS/SSL System with
Certificate Transparency
(OCSP Stapling)**





Anillo o Circulo de confianza

Es un modelo de confianza **distribuido** que provee garantías para operaciones criptográficas como el cifrado, la firma o el no repudio de transacciones electrónicas basado en la cantidad de firmas de actores de confianza que posea una clave publica.





Anillo o Circulo de confianza

El concepto original es un aporte de Phil Zimmermann, documentado en el manual de PGP Version 2.0 (1992)

Con el paso del tiempo, usted acumulará claves de otras personas que podría querer designar como introductores de confianza. Todos los demás elegirán sus propios introductores de confianza. Y todos gradualmente acumularán y distribuirán junto con su clave una colección de firmas certificadas por otras personas, en la expectativa de que quien quiera que la reciba confiará por lo menos en una o dos de las firmas. Esto llevará a la aparición (espontánea) de un anillo de confianza descentralizado y resistente a los fallos para todas las claves públicas.



Situación en La República Argentina



Ley de Firma Digital - República Argentina

Ley 25.506

Consideraciones generales. Certificados digitales.

Certificador licenciado. Titular de un certificado digital.

Organización institucional. Autoridad de aplicación.

Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad.

Sanciones. Disposiciones Complementarias.

Sancionada: Noviembre 14 de 2001.

Promulgada de Hecho: Diciembre 11 de 2001.



El proyecto de Firma Digital tiene por objetivo lograr la implementación de esta herramienta tecnológica en los sistemas administrativos y de gestión de los distintos organismos que conforman la Administración Pública, con el fin de que el accionar de éstos resulte más eficiente.

Con este propósito, el equipo de Firma Digital de la ONTI lleva adelante las siguientes tareas: generar un marco tecnológico, legal y procedimental adecuado que conforme la **Infraestructura de Firma Digital Nacional (IFDN)**, con el fin de poder utilizar esta tecnología en forma segura; capacitar/instruir a los distintos actores que conforman la IFDN; proveer de certificados a los organismos del sector público en forma gratuita.



ACAP

Autoridad Certificante de la Administración Pública.
<https://pki.jgm.gov.ar/app>



AC Raíz

Autoridad Certificante Raíz de la República Argentina.
[https://www.acraiz.gob.ar/](http://www.acraiz.gob.ar/)



AC Mail

Autoridad Certificante para correo electrónico.
<http://ca.sgp.gov.ar/eMail/>



La **Infraestructura de Firma Digital de la República Argentina (IFDRA)** está conformada por un conjunto de componentes que interactúan entre sí, permitiendo la emisión de certificados digitales para verificar firmas digitales en condiciones seguras, tanto desde el punto de vista técnico como legal.

La **Secretaría de Gabinete y Coordinación Administrativa actúa como Ente Licenciatante** otorgando, denegando o revocando las licencias de los certificadores licenciados y supervisando su accionar.

En este sentido, los certificadores licenciados son entidades públicas o privadas que se encuentran habilitados por el Ente Licenciatante para emitir certificados digitales, en el marco de la Ley **25.506 de Firma Digital**.



Certificadores Licenciados

- **AFIP** – Administración Federal de Ingresos Pùblicos. -
<http://www.afip.gov.ar/firmaDigital/>
- **ANSES** – Administración Nacional de la Seguridad Social.
- <http://www.anses.gob.ar/firmadigital/index.html>
- **ONTI** – Oficina Nacional de Tecnologías de Información. -
<https://pki.jgm.gov.ar/app/>
- **ENCODE S.A.** -
<http://www.encode.com.ar/pages/firma.html>