Declaración de Prácticas y Políticas del Servicio Cualificado de Sellado de Tiempo

Servicios de Confianza

Evicertia
Abril de 2022

Público

Índice

1 Introducción

1.1 Presentación

Evicertia, S.L. (Evicertia) es un Prestador de Servicios de Cualificación (PSC) que presta “Servicios Cualificados de Sellado de Tiempo” de acuerdo a lo indicado en la Sección 7 del REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

1.2 Nombre del documento e identificación

Este documento es la “Declaración de Prácticas y Políticas del Servicio Cualificado de Sellado de Tiempo” de Evicertia en los sucesivo “DPPSCST”.

Este documento debe ser leído a la par que la Declaración de Prácticas (en lo sucesivo DPC) de Evicertia, a la cual está subordinada. A lo largo de la presente DPPSCST se hace referencia a apartados de dicha DPC que sirven para completar el presente documento.

1.3 Participantes en los servicios de certificación

Revisar este apartado en la DPC de Evicertia.

1.4 Uso del servicio de sellado de tiempo

1.4.1 Usos permitidos

El servicio de sellado de tiempo expide sellos de tiempo con el fin de probar que una serie de datos han existido y no han sido alterados a partir de un instante específico en el tiempo. Su uso se limita a las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios.

1.4.2 Límites y prohibiciones de uso

El servicio de sellado de tiempo no se utilizará para fines distintos de los especificados en el presente documento. Del mismo modo, el servicio deberá emplearse únicamente de acuerdo con la regulación aplicable.

1.5 Administración de la política

1.5.1 Organización que administra el documento

Los datos de la sociedad son los siguiente:

- Evicertia, S.L. (Evicertia)
- NIF: ESB86021839

- Registro Mercantil de Madrid Tomo: 28127, Libro: 0, Folio 11, Sección 8, Hoja M-506734, Inscripción 1.

1.5.2 Datos de contacto de la organización

Los datos de contacto de Evicertia, S.L., son los siguientes:

- Web: https://www.evicertia.com
- Email: info@evicertia.com
- Teléfono: +34914237080
- Fax: +34911410144
- Domicilio postal: c/ Lagasca, 95. 28006, Madrid

1.5.3 Procedimientos de gestión del documento

El sistema documental y de organización de Evicertia garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

2 Control de versiones

Ver.	Fecha	Observaciones
1.0	20/09/2019	Se aprueba la primera versión de este documento.
1.1	29/11/2019	Adecuación con informe preliminar de la auditoría.
1.2	12/05/2021	• Cambio del nombre del documento a "Declaración de Prácticas y Políticas del Servicio Cualificado de Sellado de Tiempo". • Con el cambio de nombre, se cambian todas las referencias de DPC a DPPSCST en el propio documento. • En el apartado 2.2 se añade referencia de subordinación del presente documento a la DPC de Evicertia. • Actualizaciones menores de formato y fechas de la portada • Se modifican varios apartados del documento para indicar que la información que contenían está en la DPC de Evicertia (2.3, 4.4, 7, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 10, y 11). • Se hace un pequeño cambio en el apartado 4.2 para indicar que son dos claves públicas de certificados. • Se añade en el apartado "6.3 Formato de la respuesta" información sobre la extensión *id-etsi-tsts-EuQCompliance*.
1.3	04/04/2022	• Se adecua la plantilla del documento y los logos. • Pequeñas correcciones gramaticales o lingüísticas en el documento.

3 Publicación y preservación

3.1 Depósito

Evicertia custodia de manera segura todos los sellos de tiempo generados como mínimo durante 15 años. Asimismo, dispone de un Depósito, en el que se publican las informaciones relativas al servicio de expedición de sellos de tiempo electrónicos cualificados. El depósito de publicación se puede consultar en https://www.evicertia.com/.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de Evicertia, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo de acuerdo con los plazos y procedimientos establecidos con respecto de la continuidad del negocio.

3.2 Publicación de información del prestador de servicios de certificación

Evicertia publicará las siguientes informaciones, en su depósito:

- La Declaración de Prácticas de Certificación de Evicertia.
- El texto de divulgación, en lo sucesivo "TD" del servicio de sellado de tiempo.
- Las claves públicas de los certificados de sello de tiempo electrónico.

3.3 Frecuencia de publicación

La información del PSC, incluyendo el TD, la DPC y esta DPPSCSTC , se publica en cuanto se encuentra disponible.

Los cambios en la DPPSCSTC se rigen por lo establecido en el procedimiento de gestión de este documento y de acuerdo a la normativa de aplicación.

3.4 Control de acceso

Revisar este apartado en la DPC de Evicertia.

4 Identificación y autenticación

4.1 Registro inicial

4.1.1 Tipos de nombres

Los certificados electrónicos utilizados en el servicio de expedición de sellos de tiempo electrónicos cualificados, en adelante "Certificado/s de TSU", contienen un nombre distintivo (*DN* o *distinguished name*) conforme al estándar X.501 en el campo *Subject*, incluyendo un componente *Common Name* (*CN*=).

Los certificados de TSU son emitidos por Uanataca, S.A., en adelante "UANATACA", son certificados electrónicos de acuerdo con el artículo 38 y el Anexo III del REGLAMENTO (UE) No 910/2014 DEL

PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por las normativas técnicas identificadas con las referencias ETSI EN 319 412-3, ETSI EN 319 421 y ETSI EN 319 422.

4.1.2 Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

4.1.3 Empleo de anónimos y seudónimos

N/A

4.1.4 Interpretación de formatos de nombres

Evicertia cumple con los requisitos del estándar X500.

4.1.5 Unicidad de los nombres

El nombre distintivo de los certificados de TSU serán únicos.

4.2 Validación inicial de la identidad

N/A

4.3 Identificación y autenticación de solicitudes de renovación

N/A

4.4 Identificación y autenticación de la solicitud de revocación, suspensión o reactivación

N/A

5 Requisitos operacionales

5.1 Solicitud de emisión de sello de tiempo

5.1.1 Legitimación para solicitar el servicio de sellado de tiempo

El solicitante o usuario del servicio de sellado de tiempo puede usar su propio aplicativo o software a través del protocolo definido en el RFC 3161 y conforme a la ETSI 319 422, todo ello conectándose a una dirección web, y control de acceso basado en credenciales, certificado de cliente sobre HTTPS o restricción de la dirección IP.

Una vez que la solicitud ha sido aceptada y registrada y se han llevado a cabo las comprobaciones adecuadas, se genera la marca de tiempo y la envía al solicitante.

5.1.2 Procedimiento de alta y responsabilidades

Evicertia recibe solicitudes para el servicio de sellado de tiempo, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se realizan mediante protocolo HTTPS y formato ASN1 conforme al RFC3161,

5.2 Formato de la solicitud

Las solicitudes de sellos tienen que ser de acuerdo a la sintaxis de la especificación “RFC 3161 Time Stamp Protocol (TSP)”, siguiendo el formato especificado en el apartado 2.4.1 Request Format. Los algoritmos admitidos serán SHA-256, SHA-384 y SHA-512.

Las URL del servicio de sellado de tiempo será, en función del servicio, una de las siguientes, teniendo en cuenta que las peticiones solo se podrán hacer tanto por HTTPS.

- https://tsa.evicertia.com/evitsa/qe1

El formato de envío de las solicitudes será mediante petición HTTP POST. El contenido de la solicitud será en ASN.1 codificado en DER, y debe contener las siguientes cabeceras:

- Content type: `application/timestamp-query`
- Content-length: `required`

5.3 Formato de la respuesta

El formato de las respuestas será vía HTTPS. El formato del contenido de la respuesta será en ASN.1, codificado en DER, y contendrá la siguiente cabecera.

- Content type: `application/timestamp-reply`

La respuesta es acorde a la RFC 3161 apartado 2.4.2, en particular el contenido del token `TSTInfo` contendrá los siguientes campos:

- TSA: <DN del certificado de la TSA>
- Time stamp: <la fecha del sellado>
- Policy OID: 0.4.0.2023.1.1
- Ordering: no
- Hash Algorithm: sha256 (el algoritmo lo especifica la petición)
- Serial number: <número de serie del certificado>
- Accuracy: 0x01 seconds, unspecified millis, unspecified micross
- Nonce: unspecified.
- Extensions: *qcStatements (esi4-qtstStatement-1 identified by id-etsi-tsts-EuQCompliance).*

Durante el proceso, Evicertia:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Indica la fecha y la hora en que se expidió un sello de tiempo.

5.4 Entrega y aceptación del certificado

La entrega y aceptación de los Certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de UANATACA, todo ello disponible en la página web: https://www.uanataca.com.

5.5 Uso del par de claves y del certificado

El Certificado de TSU utiliza exclusivamente el servicio de expedición de sellos de tiempo electrónicos cualificados.

5.6 Modificación de certificados

N/A

5.7 Revocación, suspensión o reactivación de certificados

Los procedimientos de revocación, suspensión y reactivación de los Certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de UANATACA, todo ello disponible en la página web: https://www.uanataca.com.

- La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.
- La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible.
- La reactivación de un certificado supone su paso de estado suspendido a estado activo.

5.7.1 Causas de revocación de certificados

Evicertia procederá a la revocación de los Certificados de TSU cuando concurra alguna de las siguientes causas:

1. Circunstancias que afectan a la información contenida en el certificado:
    a. Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
    b. Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
2. Circunstancias que afectan a la seguridad de la clave o del certificado:
    a. Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
    b. Infracción, por Evicertia, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación de Sellado de Tiempo.
    c. Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
    d. Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
3. Otras circunstancias:

a. La terminación del servicio de certificación de Evicertia.
b. El uso del certificado que sea dañino y continuado para Evicertia. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
    i. La naturaleza y el número de quejas recibidas.
    ii. La identidad de las entidades que presentan las quejas.
    iii. La legislación relevante vigente en cada momento.
    iv. La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

5.7.2 Causas de suspensión de un certificado

Los Certificados de TSU pueden ser suspendidos si se sospecha el compromiso de una clave, hasta que este sea confirmado. En este caso, Evicertia tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

5.7.3 Causas de reactivación de un certificado

Los Certificados de TSU pueden ser reactivados.

5.7.4 Quién puede solicitar la revocación, suspensión o reactivación

La revocación, suspensión o reactivación será solicitada por Evicertia.

5.7.5 Procedimientos de solicitud de revocación, suspensión o reactivación

El Procedimiento de solicitud de la revocación, suspensión y/o reactivación de los certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de UANATACA, todo ello disponible en la página web: https://www.uanataca.com.

5.7.6 Plazo temporal de solicitud y procesamiento de la revocación, suspensión o reactivación

El plazo temporal de la solicitud y del procesamiento de la misma para la revocación, suspensión y/o reactivación de los certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de UANATACA, todo ello disponible en la página web: https://www.uanataca.com.

5.7.7 Obligación de consulta de información de revocación o suspensión de certificados

Los terceros deben comprobar el estado de los sellos de tiempo electrónicos cualificados en los cuales desean confiar, para ello deberán consultar el estado del Certificado de TSU. Un método por el cual se puede verificar el estado de los certificados de TSU es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de UANATACA, responsable de la emisión de los mismos.

Las Listas de Revocación de Certificados o LRC se publican en la página web de UANATACA, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl

- http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

5.7.8 Frecuencia de emisión de listas de revocación de certificados (LRCs)

UANATACA, entidad de certificación emisora de los certificados de TSU, emite una LRC al menos cada 24 horas.

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

5.7.9 Plazo máximo de publicación de LRCs

Las LRCs se publican en https://www.uanataca.com y en las direcciones web indicadas, en un periodo inmediato razonable tras su generación, que en ningún caso supera unos pocos minutos.

5.7.10 Disponibilidad de servicios de comprobación en línea de estado de certificados

De forma alternativa, los terceros que confían en los sellos de tiempo electrónicos cualificados podrán consultar el Depósito de certificados de UANATACA, que se encuentra disponible las 24 horas de los 7 días de la semana en el web:

- https://www.uanataca.com/public/pki/crtlist

Para comprobar la última LRC emitida en cada CA se debe descargar:

- Autoridad de Certificación Raíz (UANATACA ROOT 2016):
  - http://crl1.uanataca.com/public/pki/crl/arl_Evicertia.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_Evicertia.crl
- Autoridad de Certificación Intermedia 2 (UANATACA CA2 2016):
  - http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

5.7.11 Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los Certificados de TSU antes de confiar en los sellos de tiempo electrónicos cualificados.

5.7.12 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de los Certificados de TSU de Evicertia es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de Evicertia, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

5.8 Finalización de la suscripción

N/A

5.9 Depósito y recuperación de claves

5.9.1 Política y prácticas de depósito y recuperación de claves

N/A

5.9.2 Política y prácticas de encapsulado y recuperación de claves de sesión

N/A

6 Controles de seguridad física, de gestión y de operaciones

Revisar este apartado en la DPC de Evicertia.

7 Controles de seguridad técnica

Evicertia emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

7.1 Generación e instalación del par de claves

7.1.1 Generación del par de claves

El par de claves del Certificado de TSU son generadas por el Prestador de Servicios de Confianza UANATACA, de acuerdo con su Declaración de Prácticas de Certificación y su texto de divulgación, encontrándose disponibles en la página web: www.uanataca.com.

Asimismo, se han seguido los procedimientos de ceremonia de claves de Evicertia, dentro del perímetro de alta seguridad destinado a esta tarea. Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por Evicertia.

Para la generación de la clave del certificado de TSU se utilizan dispositivos con las certificaciones *FIPS 140-2 level 3* y *Common Criteria EAL4+*.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

Certificados de la Unidad de Sello de	2.048 bits	Hasta 8 años

tiempo		

7.1.2 Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al prestador de servicios electrónicos de confianza es *PKCS#10*, otra prueba criptográfica equivalente o cualquier otro método aprobado por Evicertia.

7.1.3 Distribución de la clave pública del prestador de servicios de certificación

Las claves de Evicertia son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las Autoridades de Certificación Raíz y Subordinadas estarán a disposición de los usuarios en la página web de Evicertia.

7.1.4 Tamaños de claves

La longitud de las claves de los Certificados de TSU es de 2048 bits.

7.1.5 Generación de parámetros de clave pública

La clave pública de los certificados de TSU está codificada de acuerdo con RFC 5280.

7.1.6 Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096 bits
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

7.1.7 Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en el apartado "Generación del par de claves".

7.2 Protección de la clave privada

Revisar este apartado en la DPC de Evicertia.

7.3 Controles de seguridad informática

Revisar este apartado en la DPC de Evicertia.

7.4 Controles técnicos del ciclo de vida

Revisar este apartado en la DPC de Evicertia.

7.5 Controles de seguridad de red

Revisar este apartado en la DPC de Evicertia.

7.6 Controles de ingeniería de módulos criptográficos

Revisar este apartado en la DPC de Evicertia.

7.7 Fuentes de Tiempo

Revisar este apartado en la DPC de Evicertia.

Adicionalmente a lo indicado en la DPC de Evicertia, la exactitud del servicio de Sellado Cualificado de tiempo de EVICERTIA es de **1 segundo** respecto a UTC (*Universal Time Coordinated*).

8 Perfil del certificado de TSU

El perfil de certificado de TSU para la prestación del servicio de sellado de tiempo siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de UANATACA, todo ello disponible en la página web: www.uanataca.com.

8.1 Perfil de certificado

Los certificados de TSU cumplen con el estándar X.509 versión 3, el RFC 3739 y la norma EN 319 422.

8.1.1 Número de versión

Los certificados son X.509 Versión 3.

8.1.2 Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la página web de UANATACA (https://www.uanataca.com).

De esta forma se permite mantener unas versiones más estables de la Declaración de Prácticas de Certificación y desligarlos de los frecuentes ajustes en los perfiles.

8.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

8.1.4 Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

8.1.5 Restricción de los nombres

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos.

8.1.6 Identificador de objeto (OID) de los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos.

8.2 Perfil de la lista de revocación de certificados

El Procedimiento de revocación, suspensión y/o reactivación de los certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de UANATACA, todo ello disponible en la página web: www.uanataca.com.

8.2.1 Número de versión

Las CRL emitidas por UANATACA son de la versión 2.

8.2.2 Perfil de OCSP

Según el estándar IETF RFC 6960.

9 Auditoría de conformidad

Revisar este apartado en la DPC de Evicertia.

10 Requisitos comerciales y legales

Revisar este apartado en la DPC de Evicertia.

11 Anexo I - Acrónimos

A continuación se muestran los acrónimos utilizados en la presente Declaración de Prácticas de Certificación.

- AC: Autoridad de Certificación
- CA: Certification Authority. Autoridad de Certificación
- RA: Autoridad de Registro
- CN: Common Name
- CP: Certificate Policy
- CPD: Centro de Procesamiento de Datos
- CPS: Certification Practice Statement. Declaración de Prácticas de Certificación
- CRL: Certificate Revocation List. Lista de certificados revocados
- CSR: Certificate Signing Request. Petición de firma de certificado
- DES: Data Encryption Standard. Estándar de cifrado de datos
- DN: Distinguished Name. Nombre distintivo dentro del certificado digital
- DPC: Declaración de Prácticas de Certificación
- DSA: Digital Signature Algorithm. Estándar de algoritmo de firma

- DCCF: Dispositivo Cualificado de Creación de Firma
- ETSI: European Telecommunications Standards Institute o Instituto Europeo de Normas de Telecomunicaciones
- QSCD: Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma
- FIPS: Federal Information Processing Standard Publication
- ISO: International Organization for Standardization. Organismo Internacional de Estandarización
- LRC: Listas de Revocación de Certificados
- LDAP: Lightweight Directory Access Protocol. Protocolo de acceso a directorios
- NTP: Network Time Protocol
- OCSP: On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
- OID: Object Identifier. Identificador de objeto
- PA: Policy Authority. Autoridad de Políticas
- PC: Política de Certificación
- PDS: Texto de divulgación
- PIN: Personal Identification Number. Número de identificación personal
- PKCS: Public-Key Cryptography Standards
- PKI: Public Key Infrastructure. Infraestructura de clave pública
- PSC: Prestador de Servicios Electrónicos de Certificación / Confianza
- RSA: Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
- SHA: Secure Hash Algorithm. Algoritmo seguro de Hash
- SSL: Secure Sockets Layer
- TCP/IP: Transmission Control. Protocol/Internet Protocol
- TSA: Autoridad de Sellado de Tiempo
- TSU: Unidad de Sellado de Tiempo