ENTRUST EU S.L.

Declaración de Prácticas de la Autoridad Cualificada de Sellado de Tiempo de tipo eIDAS

Versión: 1.1

1 de diciembre de 2023

Historial de cambios

Issue	Date	Changes in this Revision
1.0	1 de septiembre de 2022	Versión inicial
1.1	1 de diciembre de 2023	Actualizar referencia a la política de seguridad

Contenido

Introducción

Esta Declaración de Prácticas de la Autoridad de Sellado de Tiempo (TPS) se aplica a los Servicios Cualificados de Sellado de Tiempo eIDAS de Entrust EU S.L. ("Entrust").

Los Sellos de Tiempo cualificados cumplen con los requisitos establecidos por el “Reglamento (UE) No. 910/2014” del Parlamento Europeo (eIDAS a lo largo de este documento).

Los términos y condiciones del Servicio Cualificado de Sellado de Tiempo de eIDAS están determinados por la Declaración de Prácticas de Certificación (CPS) de Entrust para Certificados Cualificados.

Este documento establece solo prácticas adicionales específicas de Sellado de Tiempo; en particular, las instalaciones, los controles de gestión y operativos, las medidas de seguridad, los procesos y los procedimientos que se han implementado para satisfacer los requisitos de eIDAS y otros estándares internacionales relevantes para las Autoridades de Sellado de Tiempo. Un organismo independiente de evaluación de la conformidad verifica periódicamente la eficacia de estos procedimientos.

Este documento está estructurado de acuerdo con ETSI EN 319 421 "Política y Requisitos de Seguridad para Proveedores de Servicios de Confianza que emiten Sellos de Tiempo".

1. Ámbito

Este documento especifica los requisitos de política y seguridad relacionados con la operación y las prácticas de gestión de la Autoridad Cualificada de Sellado de Tiempo de Entrust que emite Sellos de Tiempo. Dichos Sellos de Tiempo pueden utilizarse como soporte de firmas digitales o para cualquier aplicación que requiera probar que un dato existía antes de un tiempo determinado.

El presente documento puede ser utilizado por organismos independientes como base para confirmar que se puede confiar en Entrust para emitir Sellos de Tiempo Cualificados de acuerdo con eIDAS.

Este y otros documentos relacionados con Entrust a los que se hace referencia en este documento están disponibles en línea en https://entrust.net/cps.

2. Referencias

A los efectos de este documento, se aplican los estándares a los que se hace referencia en la DPC de Entrust para Certificados Cualificados y los siguientes:

- ETSI EN 319 401: Requisitos Generales de Política Para Proveedores de Servicios de Confianza
- ETSI EN 319 421: Política y Requisitos de Seguridad Para Proveedores de Servicios de Confianza Que Emiten Sellos de Tiempo
- ETSI EN 319 422: Protocolo de Sellado de Tiempo y Perfiles de Token de Sellado de Tiempo
- RFC 3161: Protocolo de Marca de Tiempo (TSP) de Infraestructura de Clave Pública X.509 de Internet
- RFC 1305: Protocolo de Tiempo de Red

3. Definiciones y acrónimos

3.1 Definiciones

A los efectos de este documento, se aplican los términos y definiciones que se dan en la CPS de Entrust para Certificados Cualificados y los siguientes:

Tiempo Universal Coordinado (UTC): escala de tiempo basada en el segundo como se define en la Recomendación UIT-R TF.460-6

Parte que confía: destinatario de un Sello de Tiempo que confía en ese Sello de Tiempo

Suscriptor: persona física o jurídica a la que se emite un Sello de tiempo y que está sujeta a las obligaciones del Suscriptor.

Sello de Tiempo: datos en formato electrónico que vinculan otros datos electrónicos a un momento particular que establece evidencia de que estos datos existían en ese momento

Política de sello de tiempo: conjunto de reglas que indica la aplicabilidad de un Sello de Tiempo a una comunidad en particular y/o clase de aplicación con requisitos de seguridad comunes

Autoridad de Sellado de Tiempo (TSA): TSP que presta servicios de Sellado de Tiempo utilizando una o más Unidades de Sellado de Tiempo

Servicio de sellado de tiempo: servicio de confianza para la emisión de sellos de tiempo

Unidad de Sellado de Tiempo (TSU): conjunto de hardware y software que se gestiona como una unidad y tiene una única clave de firma de sello de tiempo activa a la vez

Servicio de Confianza: servicio electrónico que potencia la confianza en las transacciones electrónicas

Proveedor de Servicios de Confianza (TSP): entidad que presta uno o más servicios de confianza

Declaración de divulgación de la TSA: conjunto de declaraciones sobre las políticas y prácticas de una TSA que requieren énfasis o divulgación particular a los Suscriptores y a las partes que confían, por ejemplo, para cumplir con los requisitos reglamentarios.

Declaración de prácticas de la TSA: declaración de las prácticas que emplea una TSA para emitir Sellos de Tiempo

Sistema TSA: composición de productos y componentes informáticos organizados para poder ofrecer la prestación de servicios de Sellado de tiempo

UTC(k): escala de tiempo realizada por el laboratorio "k" y mantenida en estrecho acuerdo con UTC, con el objetivo de llegar a ±100 ns.

3.2 Acrónimos

A los efectos de este documento, se aplican las abreviaturas dadas en la CPS de Entrust para Certificados Cualificados y las siguientes:

BIPM	Bureau International des Poids et Mesures
BTSP	Mejores Prácticas de la Política de Sellado de Tiempo
CA	Autoridad de Certificación
GMT	Hora del Meridiano de Greenwich
IERS	Servicio Internacional de Rotación de la Tierra y Sistema de Referencia
IT	Tecnologías de la Información
TAI	Hora Atómica Internacional
TPS	Declaración de Prácticas de la Autoridad de Sellado de Tiempo
TSA	Autoridad de Sellado de Tiempo
TSP	Proveedor de Servicios de Confianza
TSU	Unidad de Sellado de Tiempo
UTC	Tiempo Universal Coordinado

4. Conceptos generales

4.1 Conceptos generales de requisitos de política

Este documento hace referencia a ETSI EN 319 401 para los requisitos de política genéricos comunes a todas las clases de servicios de proveedores de servicios de confianza.

Estos requisitos de política se basan en el uso de criptografía de Clave Pública, certificados de Clave Pública y fuentes de tiempo confiables.

Se espera que el Suscriptor y las Partes que confían consulten esta TPS para obtener más detalles sobre cómo la TSA en particular implementa esta política de Sellado de Tiempo (por ejemplo, los protocolos utilizados para proporcionar este servicio).

4.2 Servicios de Sellado de Tiempo

La prestación de los servicios de Sellado de tiempo se desglosa en este documento en los siguientes componentes del servicio a efectos de clasificación de requisitos:

- **Provisión de Sellos de Tiempo**: Este componente del servicio genera Sellos de Tiempo.
- **Gestión de Sellado de Tiempo**: Este componente del servicio monitorea y controla el funcionamiento de los servicios de Sellado de Tiempo para asegurar que el servicio prestado es el especificado por la TSA. Este componente del servicio tiene la responsabilidad de la instalación y desinstalación del servicio de provisión de Sellado de Tiempo.

4.3 Autoridad de Sellado de Tiempo (TSA)

Un proveedor de servicios de confianza (TSP) que brinda servicios de Sellado de Tiempo al público se denomina Autoridad de Sellado de Tiempo (TSA). La TSA tiene la responsabilidad general de la prestación de los servicios de Sellado de Tiempo identificados en la cláusula 4.2. La TSA tiene la responsabilidad de la operación de una o más TSU que crea y firma en nombre de la TSA.

La TSA puede hacer uso de otras partes para proporcionar componentes de los servicios de Sellado de Tiempo. Sin embargo, la TSA siempre mantiene la responsabilidad general (según la cláusula 6.5) y garantiza que se cumplan los requisitos de la política identificados en este documento.

4.4 Subscriptor

Cuando el Suscriptor es una organización, comprende varios usuarios finales o un usuario final individual y algunas de las obligaciones que se aplican a esa organización deberán aplicarse también a los usuarios finales. En cualquier caso, la organización será responsable si las obligaciones de los usuarios finales no se cumplen correctamente y, por lo tanto, se espera que dicha organización informe adecuadamente a sus usuarios finales.

Cuando el Suscriptor sea un usuario final, el usuario final será directamente responsable si no cumple correctamente con sus obligaciones.

4.5 Política de Sellado de Tiempo y declaración de prácticas de TSA

Esta cláusula explica los roles relativos de la política de Sellado de Tiempo y esta TPS. No impone ninguna restricción en la forma de una política de Sellado de Tiempo o especificación de declaración de prácticas.

Una política de Sellado de Tiempo es una forma de política de servicio de confianza, tal como se especifica en ETSI EN 319 401, aplicable a los proveedores de servicios de confianza que emiten Sellos de Tiempo. La TPS es una forma de Declaración de Prácticas de Servicios de Confianza como se especifica en ETSI EN 319 401 aplicable a los proveedores de servicios de confianza que emiten Sellos de Tiempo.

Esta TPS especifica una política de Sello de Tiempo y una declaración de prácticas para la TSA de Entrust.

5. Introducción a las políticas de sellado de tiempo y requisitos generales

5.1 General

Este documento define un conjunto de reglas a las que se adhiere Entrust al emitir Sellos de Tiempo, respaldados por certificados de Clave Pública, con una precisión de un (1) segundo o mejor con respecto a UTC.

5.2 Identificación

El identificador de la política de Sellado de Tiempo especificado en este documento es:

```
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023)  policy-identifiers(1) best-practices-ts-policy (1)
```

Al incluir uno de estos identificadores de objeto en un Sello de Tiempo, la TSA declara conformidad con la política de Sello de Tiempo identificada.

5.3 Comunidad de usuarios y aplicabilidad

Mejores prácticas en política de Sello de Tiempo

Esta política tiene como objetivo cumplir con los requisitos de Sellado de Tiempo para una validez a largo plazo, pero es aplicable en general a cualquier uso que tenga un requisito de calidad equivalente.

Esta política puede ser utilizada para servicios públicos de Sellado de Tiempo o Servicios de Sellado de tiempo utilizados dentro de una comunidad cerrada.

6. Políticas y prácticas

6.1 Análisis de vulnerabilidad

Ver apartado 5.4.8 de la CPS de Entrust para Certificados Cualificados.

6.2 Declaración de Prácticas de Servicios de Confianza

Entrust asegura la calidad, desempeño y operación del servicio de Sellado de Tiempo a través de la implementación de diversas políticas y controles de seguridad.

Las políticas y controles de seguridad son revisados periódicamente por un organismo independiente, mientras que personal capacitado y confiable verifica el cumplimiento de las políticas por parte de los controles de seguridad.

6.2.1 Formato de Sello de Tiempo

Los Sellos de Tiempo emitidos cumplen con RFC 3161 y ETSI EN 319 422. El servicio emite Sellos de Tiempo RSA 4096 que utilizan el algoritmo hash SHA256. El servicio acepta solicitudes de Sello de Tiempo con algoritmos hash SHA256, SHA384 o SHA512.

6.2.2 Precisión de la hora

El servicio de Sellado de Tiempo utiliza una fuente de tiempo confiable de un conjunto de servidores NTP de laboratorio UTC(k) y monitorea la deriva de estas fuentes usando un monitor de tiempo NTP.

El servicio de Sellado de Tiempo alcanza una precisión de la hora muy por debajo de +/-1s con respecto al UTC.

Téngase en cuenta que el tiempo de Sellado de Tiempo no es el momento de aceptación de la solicitud de sellado de tiempo, sino el momento de procesamiento del sistema de Sellado de Tiempo.

6.2.3 Limitaciones en el uso del servicio de sellado de tiempo

No está estipulado.

6.2.4 Obligaciones del Suscriptor

Los Suscriptores deben verificar que el token de Sello de Tiempo se haya firmado correctamente y verificar los servicios de validación de Entrust EU (es decir, CRL u OCSP) para confirmar que el certificado de Sello de Tiempo no ha sido revocado.

Los suscriptores deben utilizar funciones criptográficas seguras para las solicitudes de Sellado de Tiempo o software para crear Sellos de Tiempo.

Si un Suscriptor agotó su cuota y el servidor devuelve un estado HTTP "429 Too Many Requests", el Suscriptor debe respetar el encabezado HTTP " Retry-After".

Consúltese el Acuerdo de Suscriptor para obtener información adicional.

6.2.5 Obligaciones de las partes que confían

Antes de confiar en un Sello de Tiempo, la Parte que confía debe verificar que el Sello de Tiempo se haya firmado correctamente y que el certificado de Sello de Tiempo no haya sido revocado en el momento de la firma.

6.2.6 Verificación del sello de tiempo

6.2.6.1 Verificación del emisor del sello de tiempo

Las Claves Públicas de los certificados utilizados, incluidos los certificados TSU y CA, se publican para permitir una verificación de que el Sello de Tiempo ha sido firmado correctamente por la TSA.

6.2.6.2 Verificación del estado de revocación del sello de tiempo

La validez de las Claves Públicas de los certificados utilizados, incluidos los certificados TSU y CA, debe comprobarse mediante el respondedor CRL u OCSP incluido en dichos certificados.

6.2.7 Ley aplicable

Ver apartado 9.14 de la CPS de Entrust para Certificados Cualificados.

6.2.8 Disponibilidad del servicio

Entrust ha implementado las siguientes medidas para garantizar la disponibilidad del servicio:

- Configuración redundante de sistemas de TI, incluida la infraestructura de HSM, para evitar puntos únicos de falla
- Instalaciones redundantes para evitar pérdidas de servicio
- Uso de sistemas de alimentación ininterrumpida

Entrust tiene como objetivo proporcionar una disponibilidad del servicio del 99,9% por año.

6.3 Términos y condiciones

Ver el apartado 9 de la CPS de Entrust para Certificados Cualificados..

6.4 Política de seguridad de la información

Véase la sección 5.3.8 de la CPS de Entrust para Certificados Cualificados..

6.5 Obligaciones de la TSA

6.5.1 General

Entrust es responsable de:

- El cumplimiento de esta TPS y sus políticas y procedimientos internos o publicados.
- El cumplimiento de las leyes y reglamentos aplicables.

6.5.2 Obligaciones de la TSA para con los suscriptores

Esta TPS no impone ninguna obligación específica al Suscriptor más allá de las establecidas en el Acuerdo del Suscriptor.

6.6 Información para las partes que confían

Las obligaciones de las Partes que Confían están cubiertas en el acuerdo de la Parte que Confía. Además, la Parte que Confía deberá hacer lo siguiente:

- verificar que el Sello de Tiempo se haya firmado correctamente y que la Clave Privada utilizada para firmar el Sello de Tiempo no se haya visto comprometida hasta el momento de la verificación;
- tener en cuenta cualquier limitación en el uso del Sello de Tiempo indicado por la política de Sello de Tiempo; y
- tener en cuenta cualquier otra precaución prescrita en acuerdos o en otros lugares.

7. Gestión y operación de la TSA

7.1 Introducción

Entrust ha implementado políticas de seguridad de la información y procedimientos operativos para mantener la seguridad del servicio.

7.2 Organización interna

Para las operaciones adecuadas del servicio de Sellado de Tiempo, Entrust mantiene documentación no divulgada que especifica todos los controles operativos relacionados con la seguridad del personal, controles de acceso, evaluación de riesgos, etc. Estos documentos internos son utilizados por organismos independientes para confirmar el cumplimiento del servicio con respecto a ETSI EN 319 421.

a) La TSA es proporcionada por: Entrust

b) La gestión de la seguridad de la información y la gestión de la calidad del servicio se realiza dentro del concepto de seguridad del servicio.

c) La TSA ha contratado personal suficiente con la formación, conocimientos técnicos y experiencia necesarios para gestionar y operar el servicio de Sellado de tiempo.

7.3 Controles de personal

Ver apartado 5.3 de la CPS de Entrust para Certificados Cualificados.

7.4 Gestión de activos

Toda la información y los activos físicos asociados con las instalaciones de procesamiento de información utilizadas dentro del servicio están claramente identificados, categorizados y archivados de acuerdo con la Política de Gestión de Activos de Entrust..

7.5 Control de acceso

Distintas capas de seguridad en cuanto a acceso físico y acceso lógico aseguran un funcionamiento seguro del servicio de Sellado de Tiempo.

El acceso a la información, las instalaciones de procesamiento de información y los procesos comerciales deben controlarse en función de la Política de Control de Acceso de Entrust. Esta política considera:

- Acceso a la red y servicios de red
- Gestión de acceso de usuarios, que incluye:

  - Altas, bajas y suministro
  - Derechos de acceso privilegiado
  - Segregación de funciones
  - Revisión de los derechos de acceso
  - Eliminación o ajuste de los derechos de acceso
- Responsabilidades
- Control de acceso a sistemas y aplicaciones, que incluye:
  - Restricciones de acceso a la información
  - Procedimientos seguros de inicio de sesión
  - Sistema de gestión de contraseñas
  - Uso de programas de servicios privilegiados
  - Control de acceso al código fuente del programa

7.6 Controles criptográficos

7.6.1 General

Ver apartado 6.2 de la CPS de Entrust para Certificados Cualificados.

7.6.2 Generación de pares de claves TSU

La generación de Pares de Claves TSU se realiza según la sección 6.1.1.3 de la CPS de Entrust para Certificados Cualificados. El algoritmo de generación de Pares de Claves TSU, la longitud de la clave y el algoritmo de firma se especifican en la CPS de Entrust para Certificados Cualificados.

La clave privada TSU no se importará en diferentes módulos criptográficos. La TSU solo tiene una clave privada activa a la vez.

7.6.3 Protección de la clave privada de TSU

Ver apartado 6.2 de la CPS de Entrust para Certificados Cualificados.

7.6.4 Certificado de clave pública TSU

Entrust garantiza la integridad y autenticidad de las claves (públicas) de verificación de firma de TSU de la siguiente manera:

Las claves (públicas) de verificación de firma de TSU están disponibles para las partes de confianza en certificados disponibles públicamente. Los certificados se pueden encontrar en el sitio web de Entrust en https://entrust.net/cps

La TSU no emite un Sello de Tiempo antes de que se cargue su certificado (de Clave Pública) de verificación de firma en la TSU o su dispositivo criptográfico. Al obtener un certificado (de Clave Pública) de verificación de firma, Entrust verifica que este certificado se haya firmado correctamente (incluida la verificación de la cadena de certificados a su autoridad de certificación de confianza).

7.6.5 Cambio de clave de la TSU

El período de validez del certificado de la TSU no será mayor que el período de tiempo en que el algoritmo elegido y la longitud de la clave se reconozcan como aptos para su propósito. El periodo de validez del certificado de la TSU se especifica en el apartado 6.3.2 de la CPS de Entrust para Certificados Cualificados.

7.6.6 Gestión del ciclo de vida del hardware criptográfico de firma

El personal con Funciones de Confianza inspeccionará el hardware criptográfico durante el proceso de puesta en marcha para garantizar la integridad y que no se haya encontrado evidencia de manipulación mientras estaba almacenado.

La instalación, activación y duplicación de las claves de firma de TSU en el hardware criptográfico debe realizarlas únicamente el personal con Funciones de Confianza mediante el control dual en un entorno físicamente seguro.

Las Claves Privadas de TSU almacenadas en el módulo criptográfico de TSU se borran al retirar el dispositivo.

7.6.7 Fin del ciclo de vida de la clave TSU

El período de uso de la Clave Privada TSU se estipula en la sección 6.3.2 de la CPS de Entrust para Certificados Cualificados. El período de uso de las Claves Privadas no excederá la validez de los certificados emitidos con esas Claves Privadas.

Después del final del período de uso de la Clave Privada, las Claves Privadas dentro del hardware criptográfico se destruyen de tal manera que las Claves Privadas ya no se pueden recuperar ni utilizar.

7.7 Sellado de tiempo

7.7.1 Emisión de sellos de tiempo

El Servicio Cualificado de Sellado de Tiempo de Entrust emite Sellos de Tiempo calificados de la siguiente manera:

- Los Sellos de Tiempo se ajustan al perfil de Sello de Tiempo definido en ETSI EN 319 422.

- Los Sellos de Tiempo incluyen la hora correcta, que es rastreable a al menos un valor en tiempo real distribuido por un laboratorio UTC(k).
- Los problemas de precisión y sincronización horaria se abordan en la sección 7.7.2 de este documento.
- Si se detecta que el reloj del Sello de Tiempo está fuera de la precisión indicada, no se emitirán los Sellos de Tiempo.
- Los Sellos de Tiempo se firman con una clave generada específicamente para este fin.
- El servicio de Sello de Tiempo no emitirá Sellos de Tiempo más allá del período de validez de la clave privada.

7.7.2 Sincronización de reloj con UTC

El reloj de la TSU está sincronizado con el UTC tal y como se especifica en el apartado 6.2.2 de este documento, en concreto:

- Los relojes de TSU se mantienen de tal manera que los relojes no se desvían fuera de la precisión declarada. La precisión declarada es de 1 segundo o mejor.
- Los relojes TSU están protegidos contra amenazas que podrían resultar en un cambio no detectado en el reloj que lo sacara de su calibración.
- El TSA detecta si la hora que se indicaría en un Sello de Tiempo se desvía o salta fuera de sincronización con UTC.
- Si se detecta que la hora que se indicaría en un Sello de Tiempo se desvía o salta de la sincronización con el UTC, la TSU detendrá la emisión del sello de tiempo.
- La sincronización del reloj se mantiene cuando se produce un segundo intercalar notificado por el organismo correspondiente y el cambio para tener en cuenta el segundo intercalar se produce durante el último minuto del día en el que está previsto que se produzca el segundo intercalar. Se mantendrá un registro de la hora exacta (dentro de la precisión declarada) cuando ocurrió este cambio.

7.8 Seguridad física y ambiental

Ver apartado 5.1 de la CPS de Entrust para Certificados Cualificados.

7.9 Seguridad de la operación

Ver capítulo 5 de la CPS de Entrust para Certificados Cualificados.

7.10 Seguridad de la red

Ver capítulo 5 de la CPS de Entrust para Certificados Cualificados.

7.11 Gestión de incidencias

Ver apartado 5.7.1 de la CPS de Entrust para Certificados Cualificados.

7.12 Recopilación de evidencias

Ver apartados 5.4 y 5.5 de la CPS de Entrust para Certificados Cualificados.

Además se recogen las siguientes pruebas:

- Sincronización del reloj de una TSU a UTC
- Registros de todos los eventos relacionados con la detección de pérdida de sincronización

7.13 Gestión de la continuidad del negocio

Ver apartado 5.7 de la CPS de Entrust para Certificados Cualificados.

7.14 Terminación de la TSA y planes de terminación

Ver apartado 5.8 de la CPS de Entrust para Certificados Cualificados.

Además, cuando la TSA termine sus servicios, la TSA revocará los certificados de la TSU..

7.15 Cumplimiento

Entrust garantiza el cumplimiento de la legislación aplicable en todo momento.

Concretamente, Entrust TSA cumple con:

a) REGLAMENTO (UE) Nº 910/2014

b) ETSI EN 319 401, ETSI EN 319 421, ETSI EN 319 422

c) IETF RFC 3161

Entrust mantiene su cumplimiento con los estándares eIDAS identificados anteriormente a través de un auditor cualificado de forma bienal (eIDAS) y continua. La auditoría la realiza un organismo de evaluación de la conformidad acreditado por un organismo nacional de acreditación de un estado miembro de la Unión Europea sobre la base de EN ISO/IEC 17065 según lo perfilado por ETSI EN 319 403 y, en particular, considerando los requisitos definidos en el Reglamento eIDAS (UE) n.º 910/2014.

8. Requisitos adicionales para sellos de tiempo cualificados

8.1 Certificado de clave pública TSU

El certificado TSU será emitido por una CA que cumpla con la política QCP-l y BTSP. Las Claves Privadas de los certificados TSU firmarán Sellos de Tiempo cualificados como lo indica el qcStatement “esi4-qtstStatement-1”.

8.2 TSA que emite sellos de tiempo electrónicos cualificados y no cualificados

Las TSUs no emitirán Sellos de Tiempo electrónicos no cualificados.