Política de sellado digital de tiempo

Índice

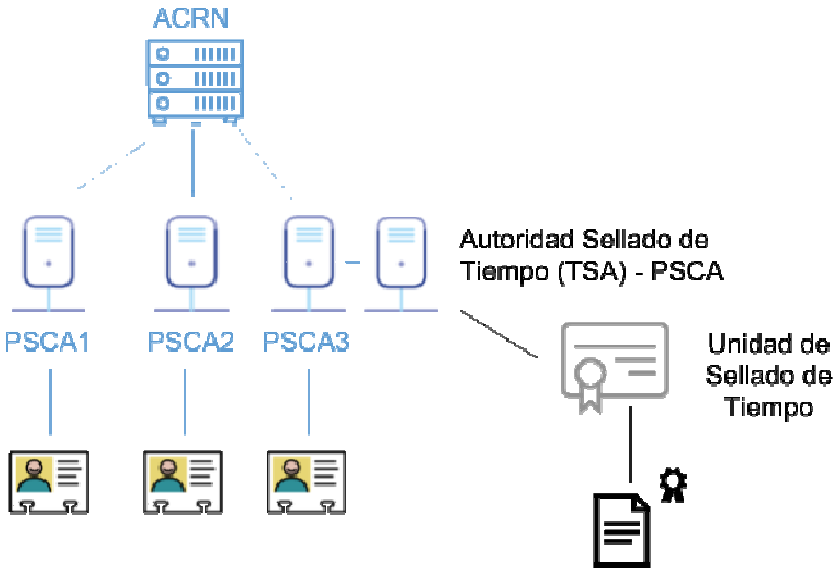
1. Introducción

1.1. Descripción general

El sellado digital de tiempo (*Timestamping*) o fechado digital es un mecanismo informático para certificar que un documento electrónico existía en una fecha y hora determinada asegurando el "no repudio".

A partir del Decreto N° 436/011 de 08 de Diciembre de 2011, que reglamenta la Ley N° 18.600 de 21 de setiembre de 2009 y el Decreto N° 70/018 de 19 de marzo de 2018, que reglamenta los artículos 31 al 33 de la Ley N° 18.600, en la redacción dada por el artículo 28 de la Ley N° 19.535 de 28 de setiembre 2017, respecto a los servicios de confianza de identificación digital y firma electrónica avanzada con custodia centralizada, queda encomendado a la Unidad de Certificación Electrónica (UCE), el proceso de acreditación y elaboración de políticas relativas al sellado de tiempo, tanto para Prestadores de Certificación Acreditado (PSCA) como para los Prestadores de Servicios de Confianza (PSCo).

El servicio de sellado de tiempo puede ser brindado por un Prestador de Servicios de Certificación (PSCA) o a un Prestador de Servicio de Confianza (PSCo), donde la Autoridad de Sellado de Tiempo forma parte del PCSA ó PCSo, en un esquema similar al de la figura.



1.2. Objetivo

La presente Política es elaborada con el fin de regular las condiciones necesarias que permiten a un PSCA o a un PSCo brindar el servicio digital de sellado de tiempo (*Timestamping*) acreditándose ante la UCE como Autoridad de Sellado de Tiempo (TSA).

2. Definiciones, abreviaturas y conceptos generales

Autoridad de Sellado de Tiempo (TSA): Es la autoridad en la que confían los usuarios de los servicios de sellado de tiempo (solicitantes y partes que confían) para la emisión de los sellos de tiempo.
Una TSA puede operar diferentes unidades de sellado de tiempo, donde cada unidad tiene un par de llaves diferentes. Es decir, una TSA puede tener simultáneamente varios certificados de sellado de tiempo, según sean sus necesidades.
La TSA provee uno o más servicios de sellado de tiempo a través de unidades de sellado de tiempo. Una TSA actúa como una "Autoridad de Fechado Electrónico" (AFE) definida en el Decreto 436/2011.

Unidad de sellado de tiempo (TSU): Es el conjunto de hardware y software que es gestionado como una unidad, tiene un certificado de sellado de tiempo firmado por una llave privada de la TSA, a partir del cual genera los *tokens* de sellado de tiempo.

Tiempo Universal Coordinado (UTC - *Universal Time Coordinated):* El tiempo coordinado UTC está basado en relojes atómicos que se sincronizan para obtener una alta precisión en la fecha y hora, y es el sistema de tiempo utilizado como estándar por la *World Wide Web*. Se define en la recomendación de ITU TF.460-6.

Token de sellado de tiempo (TST): Estructura de datos que contiene una representación de la información a certificar, la fecha y hora de la certificación y la firma del generador del *token* (TSU), que permite establecer evidencia de que la información certificada existía antes de ese tiempo. Los *tokens* de sellado de tiempo deben emitirse de acuerdo con el RFC 3161 "*Internet X.509 Public Key Infrastructure Time Stamp Protocol* (TSP)".

Servicio de Sellado de Tiempo: Se encarga de recibir la solicitud de sellado de tiempo de un solicitante, verificar los parámetros de la solicitud y generar el *token* de sellado de tiempo, de acuerdo con lo establecido en la presente política. Sección 4.

Solicitantes: Los solicitantes del servicio de sellado de tiempo son los organismos, personas o entidades finales que utilizan el servicio de sellado de tiempo.

Terceros aceptantes: Son los receptores del TST que confían en el servicio de sellado de tiempo. Los terceros validan la firma del sello de tiempo y comprueban el estado de vigencia del certificado de la TSA y su período de validez.

3. Proceso de sellado de tiempo y verificación

El proceso de sellado de tiempo tiene los siguientes pasos:

1. El suscriptor del servicio realiza una petición de sellado de tiempo a una TSA incluyendo en la solicitud una referencia (*hash*) al dato a sellar. Esta solicitud se realiza de acuerdo con el "*Timestamp Request*" definido en el RFC 3161.

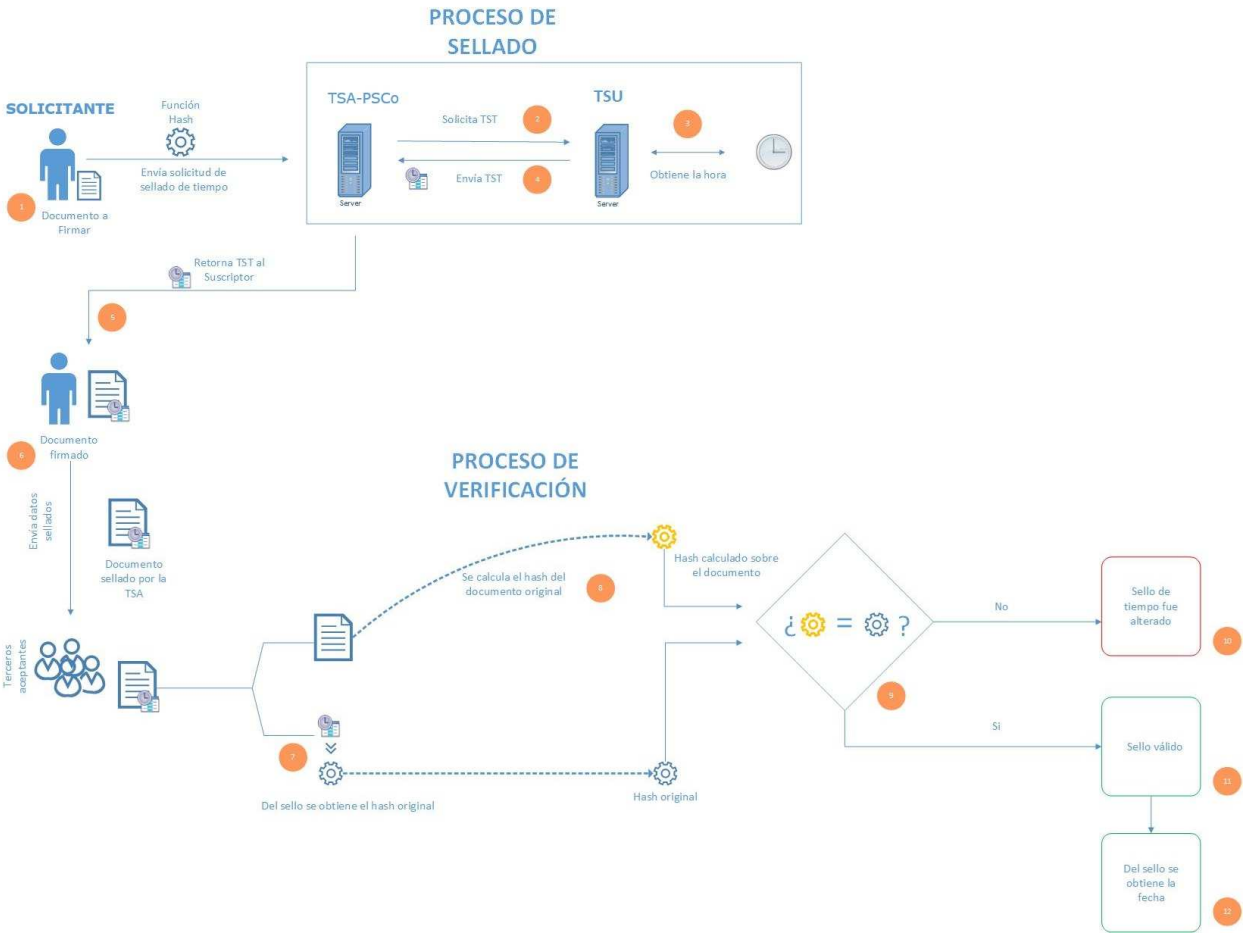
2. La autoridad de sellado de tiempo (TSA) revisa si la petición está completa y correcta. Si el resultado es positivo, la referencia al dato (*hash*) se envía como entrada a la TSU.

3. La TSU obtiene la hora UTC de una fuente confiable de tiempo y crea un *token* de sello de tiempo (TST) que asocia el instante de tiempo actual, un número de serie único y la referencia al dato (*hash*).

4. La autoridad de sellado de tiempo (TSA) recibe el *token* de sello de tiempo (TST) de la unidad de sellado de tiempo (TSU) y lo envía al solicitante.

5. El solicitante recibe el *token* de sellado de tiempo (TST) y lo adjunta al dato.

6. Para validar la autenticidad de un sello de tiempo, los terceros aceptantes separarán el dato original de su sello, calcularán el *hash* del dato y compararán el resultado con el hash incluido en el sello de tiempo (TST). Si ambos coinciden, la validación se considera exitosa.



4. Modalidad del servicio

En el contexto de la presente política la TSA debe residir en Uruguay, pudiendo sus TSU estar integradas a la TSA o ser entidades independientes de la TSA. La TSA debe tener personería jurídica en Uruguay, pero puede tercerizar las funciones de TSU con otras entidades, nacionales o extranjeras. En caso de tercerización de TSU, la TSA será responsable de todas las actividades realizadas por la TSU en su nombre en el territorio nacional y para ello deberá contar con los contratos y autorizaciones que correspondan.

5. Obligaciones

5.1. Obligaciones de la TSA

- Las claves públicas de una TSU deben estar protegidas por un certificado emitido por un PCSA o PCSo.

- Determinar con precisión la fecha y la hora a la que se emitió un sello de tiempo. La desviación máxima de los sellos emitidos no podrá superar 1 segundo respecto al tiempo UTC.

- Obtener la conformidad del solicitante sobre las responsabilidades y obligaciones estipuladas en el acuerdo de servicio de sellado de tiempo. Publicar estas obligaciones para conocimiento de de terceros aceptantes.

- Garantizar el acceso permanente a los servicios de sellado de tiempo con un tiempo de servicio (*uptime*) superior al 99,8%.

- Contar con una declaración de prácticas para el ciclo de vida de los certificados.

- Disponer de servicios públicos para la verificación del estado de los certificados (ej.: CRL, OCSP).

- Emitir sellos de tiempo de acuerdo con la información conocida en el momento de su emisión y libre de errores de entrada de datos.

- Emitir sellos de tiempo de forma que se puedan identificar unívocamente.

- Firmar los sellados de tiempo usando una llave privada generada exclusivamente para este propósito. Esta llave deberá cumplir con los requerimientos de gestión del ciclo de vida determinados en la sección 7.

- Implementar los controles operativos, de seguridad y técnicos de las buenas prácticas internacionales para la gestión de entidades de *timestamping*.

- Proteger la información confidencial o privada.

En caso de que los servicios de la TSU sean tercerizados:

- TSA deberá exigir a la TSU contratada el cumplimiento de los requisitos pertinentes para poder cumplir con las obligaciones antes detalladas.

- Las TSU utilizadas deben cumplir con garantías asimilables a las establecidas en la Ley N° 18600, para los prestadores de servicio de certificación (CA), debiendo presentar la documentación al momento de solicitar su acreditación como TSA. En el mismo acto deberá presentarse la documentación correspondiente a los contratos y autorizaciones para la prestación del servicio.

5.2. Obligaciones de los solicitantes

Verificar la firma electrónica del sello de tiempo emitido por la TSA y comprobar el estado de revocación del certifica-do de la TSA.

5.3. Carga de los terceros aceptantes

Las partes que confían tienen la carga de comprobar el estado del certificado de la TSA y su período de validez.

5.4. Obligaciones de la UCE

La UCE deberá llevar un registro de las TSA, de su período de habilitación y sus claves públicas.

Verificar la documentación presentada por los PCSA y PSCo y el cumplimiento de las obligaciones referidas en la sección 5.1.

6. Declaración de prácticas de TSA

La declaración de prácticas de la TSA deberá explicitar los roles relativos a la política de sellado de tiempo, que deben ser consistentes con esta política. Esta declaración deberá considerar los requerimientos de los estándares internaciones como el ETSI TS 101 456 "*Policy Requirements for Certification Authorities Issuing Qualified Certificates*" y el ETSI TS 101 861 "*Time-stamping Profile*".

El cumplimiento de los procedimientos, su adherencia a las políticas, competencia técnica y administrativa deben ser aprobados por la UCE.

7. Gestión del ciclo de vida de las llaves

7.1. Generación de la llave

El proceso de generación de llaves ejecutado previene la pérdida, divulgación, modificación o acceso no autorizado a las llaves privadas que son generadas. Este requerimiento se aplica para toda la jerarquía de certificadores registrados.

El PSCA o PSCo debe disponer de un módulo criptográfico (HSM) para el resguardo del material criptográfico utilizado para la emisión de los sellos de tiempo. Este módulo debe generar las llaves utilizadas para la generación de sellos de tiempo de forma interna y estas deberán ser utilizadas dentro del contexto del HSM.

El PSCA o PSCo debe almacenar las claves públicas por el período de la prestación de servicios como autoridad de sellado de tiempo.

7.2. Protección de la llave privada

Los niveles de seguridad para la protección de las llaves deben cumplir con los siguientes requisitos:

- Mantener controles para asegurar que sus llaves permanecen confidenciales y mantienen su integridad. El acceso al hardware criptográfico (HSM) estará limitado a individuos autorizados.
- Respaldar, guardar y recuperar las llaves por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro.
- Las copias de respaldo de las llaves privadas deben estar sujetas al mismo o mayor nivel de controles de seguridad que las llaves en uso.
- La recuperación de las llaves respaldadas debe llevarse a cabo de una forma tan segura como el proceso de respaldo. El estándar de módulos criptográficos es el "*Security Requirements for Cryptographic Modules*" (actualmente FIPS140). Los módulos deben certificarse como mínimo con el FIPS 140–2 nivel 3.

7.3. Otros Aspectos de la gestión de pares de claves

El período de validez máximo del certificado es de 5 años. El período de validez de la clave privada deberá ser máximo un año. Esta configuración permite validar los sellos de tiempo por un período extenso, exponiendo la clave privada por periodos más cortos.

7.4. Terminación del ciclo de vida de la llave

Debe asegurarse que:

- Las llaves privadas utilizadas en la emisión de sellos de tiempo no puedan ser utilizadas más allá del periodo de expiración.
- El procedimiento para la destrucción de llaves debe incluir la autorización para destruirla.

Debe destruir los respaldos de las llaves privadas que han expirado. Para los módulos criptográficos de hardware (HSM), estos deben ser limpiados por medio de inicialización de ceros (Zeroize Command).

8. Sellado de tiempo

8.1. *Token* de sellado de tiempo

La TSA debe garantizar que todos los *tokens* de sellado de tiempo se emiten en forma segura y que incluyen la hora UTC. En particular cada sello de tiempo emitido por la TSA debe incluir:

- Un identificador único dentro de la TSA
- Valor de tiempo UTC
- El hash del documento a ser firmado, que deberá ser provisto por el solicitante.
- Incluir el campo extensión *QCStaments* con el valor *esi4-qtstStaments1* de forma de indicar que el sello es emitido por una entidad acreditada.
- Adicionalmente la TSA debe garantizar que:

1. El sello de tiempo no podrá ser emitido en caso de no tener la precisión establecida en la presente política
2. El token de sellado de tiempo es firmado por una llave generada exclusivamente para este propósito.
3. Las API de la TSU se publica sobre HTTPS

8.2. Sincronización UTC

La TSA debe asegurar que:

- El o los relojes utilizados por la TSU estén sincronizados con el tiempo UTC, con un margen de error menor a un segundo.
- El reloj de la TSU está protegido contra amenazas que podrían resultar en el cambio del tiempo fuera de la calibración o por la manipulación física de los sistemas.
- Las diferencias entre el sistema del tiempo de la TSU y el tiempo UTC son detectadas.
- El cálculo de tiempo cumple con las recomendaciones de NTP (Network Time Protocol) basados en el RFC 5905.
- La sincronización del reloj se mantiene cuando se presenten "segundos intercalares" (*leap seconds*) de acuerdo con el RFC 7164 Sección 3.

8.3. Servicio de validación

Para la validación de un sello de tiempo, la TSA debe implementar obligatoriamente el mecanismo de CRL.

8.4. Verificación longeva de sellado de tiempo

Para la verificación de firmas más allá del período de validez del certificado de la TSA e incluso más allá de la validez del certificado de la CA, se estipula que si el certificado de la TSU se encuentra expirado, e incluso el de la CA (y la Root) también, pero no hubo evidencias de compromiso de la llave de la TSU ni de la CA, los algoritmos de hashing no presentan colisiones conocidas en ese momento y el algoritmo criptográfico de la firma y el largo de clave siguen siendo criptográficamente aceptados, el token puede ser considerado de confianza. En caso de requerir garantías adicionales sobre algún documento o transacción particular, se deberá realizar un nuevo sellado de tiempo con certificados de TSU, CA y ROOT actualizados.

8.5. Referencias

Los aspectos no especificados en la presente Política se regirán por las disposiciones establecidas en los siguientes estándares:

- ETSI EN 319 421 - https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf

- ETSI EN 319 422 - https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf

9. Perfil del Certificado

Atributos	Contenido
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la ACPA emisora
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	DN de la ACPA emisora tal cual figura en su certificado

Validez (Valid From / Valid To)	5 años (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	CN = Nombre de Fantasía de la Organización O = Nombre legal de la Organización C = UY
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 2048 bits o más
Extensiones	
Identificador de la clave del suscriptor (Subject Key Identifier)	Hash de 20 bytes del atributo Subject Public Key
Identificador de la clave de la autoridad (Authority Key Identifier)	Valor de la Extensión Subject Key Identifier del certificado de la ACPA emisora
Uso de Claves (Key Usage)	DigitalSignature = 1 NonRepudiation = 1
Uso de Claves Extendido (Extended Key Usage)	timeStamping
Private Key Usage Period	1 año (en formato desde/hasta)
Políticas de Certificación (Certificate Policies)	OID: OID: 2.16.858.10000157.66565.16 URI: www.uce.gub.uy/informacion-tecnica/politicas/cp_Sellado de tiempo.pdf OID: OID asignado a la CPS del PSCA para la ACPA emisora URI: URL de publicación de la CPS
Restricciones Básicas (Basic Constraints)	CA = FALSE
Puntos de distribución de las CRL (CRL Distribution Points)	URI = URL primaria de publicación de la CRL URI = URL secundaria de publicación de la CRL
Nombre Alternativo del Sujeto (Subject Alternative Name)	Campo de tipo directoryName con la identificación del Referente: CN = Nombre Completo del Referente C = País de emisión de su documento de identificación

10. Registros de auditoría (logs)

Los registros de auditorías deberán cumplir con los siguientes aspectos:

- Los datos y eventos específicos a ser registrados en bitácoras deben ser documentados por la TSA.
- La confidencialidad e integridad de los registros actuales y los archivados relativos a la operación de servicios de la TSA deben ser mantenidos.
- Los eventos de auditoría deben ser registrados al sistema de manera que no puedan ser fácilmente alterados, eliminados o destruidos.

11. Auditorias

La UCE podrá solicitar evidencias que demuestren el cumplimiento de los procedimientos y estándares declarados por la TSA para su operación. Estas evidencias podrán implicar la solicitud de auditorías específicas, de certificaciones o de informes de auditorías de cumplimiento independientes.

12. Cese de actividades de una TSA

La TSA que cese sus actividades estará obligada a notificar a la UCE. Deberá también publicar el cese de actividades a través del Diario Oficial y de cualquier otro medio electrónico o tradicional que considere pertinente.