Política de sellado de tiempo para Prestadores de Servicios de Confianza

Índice

1. Introducción

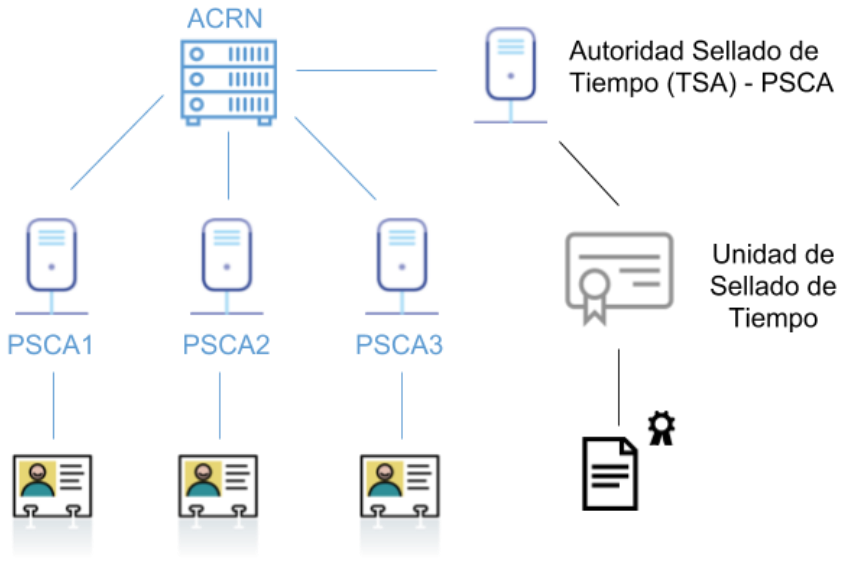
1.1. Descripción general

El sellado digital de tiempo 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 de el Decreto N° 436/011 de 08 de Diciembre de 2011, que reglamenta la Ley N° 18600 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 remitido a la 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).

Se distingue entonces cuando el servicio de sellado de tiempo es brindado por un PSCA a cuando es brindado por un PSCo, elaborándose una política para cada tipo de servicio brindado.

En el caso del servicio de sellado de tiempo brindado por un PSCA, el o los certificados de sello de tiempo forman parte de la Infraestructura Nacional de Certificación Electrónica en un esquema similar al de la siguiente figura.



En el caso de un servicio de sellado de tiempo brindado por el PSCo, el o los certificados de sello de tiempo no provienen de la Autoridad Certificadora Raíz Nacional, especificándose en la presente política las condiciones necesarias para proveer este servicio de sellado de tiempo.

1.2. Objetivo

La presente política es elaborada con el fin de regular las condiciones necesarias que permiten a un Prestador de Servicio de Confianza (PSCo) brindar el servicio de sellado de tiempo (*Timestamping*).

2. Definiciones, abreviaturas y conceptos generales

Autoridad de Sellado de Tiempo (TSA-PSCo).
La TSA-PSCo 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-PSCo puede operar diferentes unidades de sellado de tiempo, donde cada unidad tiene un par de llaves diferentes. Es decir, una TSA-PSCo puede tener varios certificados de sellado de tiempo según sean sus necesidades.

La TSA-PSCo provee uno o más servicios de sellado de tiempo a través de unidades de sellado de tiempo. Una TSA-PSCo 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 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, verifica los parámetros de la solicitud y genera 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 o entidades finales que utilizan el servicio de sellado de tiempo del PSCo.

Terceros aceptantes
Son los receptores del TST que confían en el servicio de sellado de tiempo brindado por los PSCo. Los terceros validan la firma del sello de tiempo y comprueban el estado de vigencia del certificado de la TSA-PSCo 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 subscriptor del servicio realiza una petición de sellado de tiempo a una TSA-PSCo incluyendo en la solicitud una referencia al dato a sellar (*hash*). Esta solicitud se realiza de acuerdo con el "*Timestamp Request*" definido en el RFC 3161.

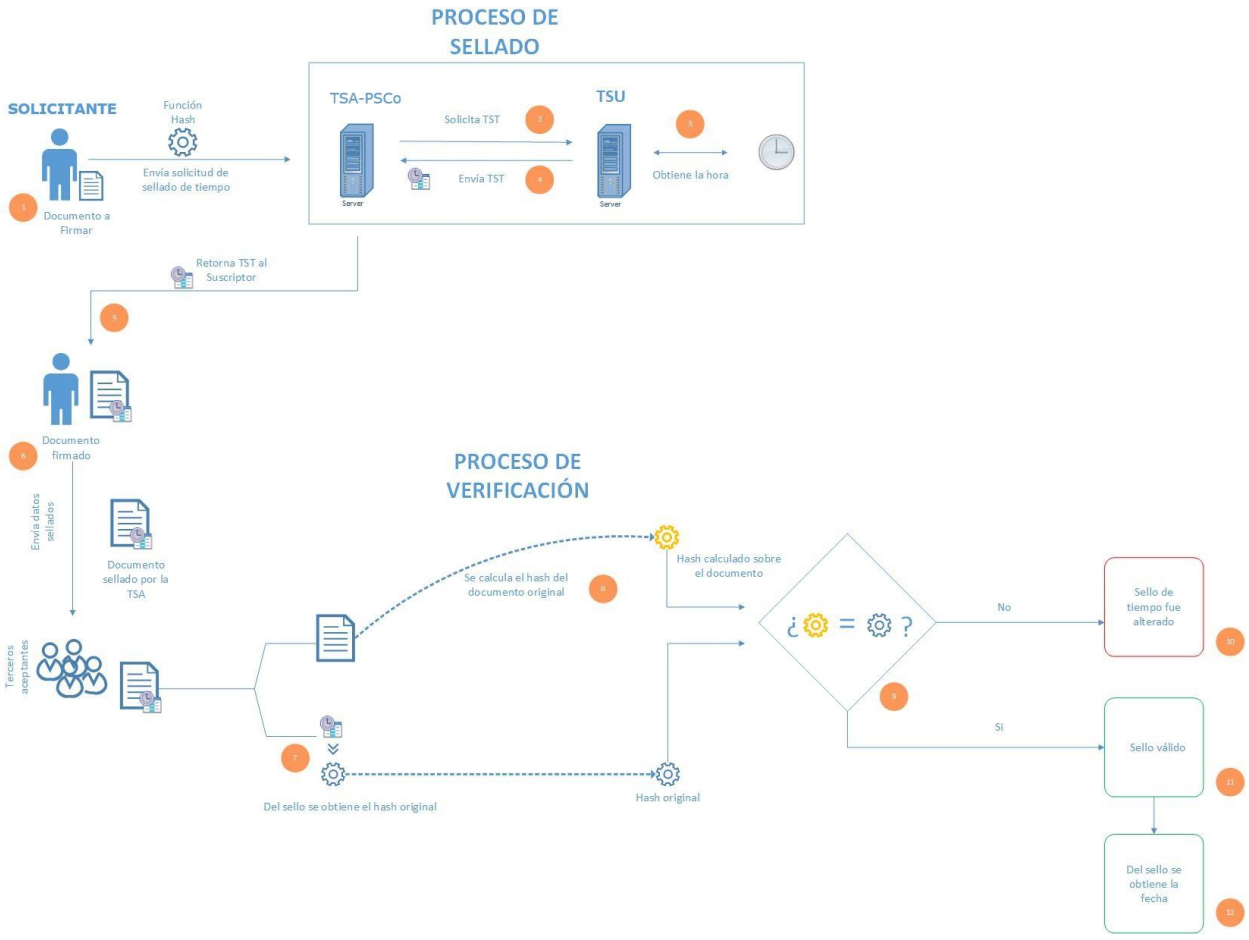
2. La autoridad de sellado de tiempo (TSA-PSCo) revisa si la petición está completa y correcta. Si el resultado es positivo, el dato (*hash*) se envía como entrada a la TSU.

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 el dato (*hash*).

4. La autoridad de sellado de tiempo (TSA-PSCo) 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

4.1. Consideraciones Generales

En el contexto de la presente política la TSA-PSCo debe residir en Uruguay pudiendo las TSU ser independientes a ésta. Es decir, consiste en la presencia de una TSA-PSCo con personería jurídica en Uruguay que puede tercerizar los servicios de la TSU.

La TSA-PSCo será responsable de todas las actividades realizadas por la TSU en su nombre en el territorio nacional y para ellos deberá contar con los contratos y autorizaciones que correspondan.

5. Obligaciones

5.1. Obligaciones de la TSA-PSCo

A continuación, incluimos las obligaciones a cumplir por la TSA-PSCo:

- 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-PSCo. En el mismo acto deberá presentarse la documentación correspondiente a los contratos y autorizaciones para la prestación del servicio.
- 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.
- No emitir sellos de tiempo si el certificado de la TSU está expirado o revocado.
- Almacenar las claves públicas por el período de la prestación de servicios como autoridad de sellado de tiempo y comunicar a la UCE, que las publicará en su sitio web.
- Comunicar al solicitante las responsabilidades y obligaciones aceptadas en el acuerdo de servicio de sellado de tiempo.
- Proteger la información confidencial o privada.

A continuación, incluimos los requerimientos que debe exigir la TSA-PSCo a la TSU:

- Contar con certificaciones internacionales para la emisión de sellos de tiempo.
- 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 usando una llave privada generada exclusivamente para este propósito. Ésta 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.

5.2. Obligaciones de los solicitantes

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

5.3. Carga de los terceros aceptantes

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

5.4. Obligaciones de la UCE

La UCE deberá llevar un registro de los proveedores de sellado de tiempo, de su período de habilitación y sus claves públicas.

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

6. Declaración de prácticas de TSU

La declaración de prácticas de la TSU 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 ser 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 debe ser aprobada 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 aplica para toda la jerarquía de certificadores registrados.
Se 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.

Almacenar las claves públicas por el período de la prestación de servicios como autoridad de sellado de tiempo y comunicar a la UCE.

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 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. 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 son emitidos en forma segura y que incluyen la hora oficial de Uruguay. En particular cada sello de tiempo emitido por la TSA-PSCo debe incluir:

- Un identificador único dentro de la TSA-PSCo.
- Valores de fecha y hora identificables, mediante los cuales se puede llegar al valor de tiempo UTC.
- El *hash* del documento a ser firmado deberá ser provisto por el solicitante.
- El identificador de la TSU que emite.

Adicionalmente la TSA-PSCo debe garantizar que:

- El sello de tiempo no podrá ser emitido en caso de no tener la precisión establecida en la presente política.
- El *token* de sellado de tiempo es firmado por una llave generada exclusivamente para este propósito.

8.2 Sincronización UTC

La TSA-PSCo debe asegurar que:

- El o los relojes utilizados por la TSU estén sincronizados con el tiempo UTC, con una exactitud con un margen de error menor a un segundo
- El reloj de la TSU debe ser 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 sean detectadas. El cálculo de tiempo cumple con las recomendaciones de NTP (*Network Time Protocol*) basados en el RFC 5905.
- La sincronización del reloj es mantenida cuando se presenten "segundos intercalares" (*leap second*) de acuerdo con el RFC 7164 Sección 3.

8.3 Servicio de validación

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

La TSU deberá contar con mecanismos de validación de estado de revocación de certificados, como OCSP, pero ninguno de estos puede sustituir a la CRL como mecanismo obligatorio.

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

10. Auditorias

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

11. Cese de actividades de una TSA-PSCo

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