Declaración de Prácticas de la Autoridad de Sellado de tiempo (TSA)

TuID

TABLA DE CONTENIDOS

1 INTRODUCCIÓN

1.1 Descripción general

Antel es un Prestador de Servicios de Certificación Acreditada (PSCA) y un Prestador de Servicios de Confianza (PSCo) acreditado ante la Unidad de Certificación Electrónica (UCE) y para ello opera una plataforma, llamada TuID, de firma e identificación en custodia centralizada en conformidad con la normativa europea eIDAS y la reglamentación vigente en Uruguay.

Adicionalmente, Antel es una Autoridad de Sellado de Tiempo (TSA por sus siglas en inglés, *Time Stamping Authority*), brindando además el servicio a través de sus propias unidades de sellado de tiempo (TSU), y para tal fin se encuentra acreditada por la UCE, al amparo de lo dispuesto en sus políticas vigentes; del Decreto N° 436/011 de 08 de Diciembre de 2011, que reglamenta la Ley N° 18600 de 21 de setiembre de 2009 y del 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.

El presente documento forma parte de la Declaración de Prácticas de Certificación de la Autoridad Certificadora de Antel (CPS), y constituye la Declaración de Prácticas de la Autoridad de Sellado de Tiempo de Antel. Ésta declaración será utilizada para la emisión de sellos de tiempo según los protocolos y estándares estipulados por la Unidad de Certificaciones Electrónicas (UCE) para Servicios de Confianza que proveen sellado de tiempo.

El alcance de este documento, es la definición de las prácticas y procedimientos empleados por Antel en la emisión de sellos de tiempo y operación de los servicios que la hacen posible.

En esa misma línea, el presente documento contiene las definiciones y declaraciones específicas relativas al servicio de sellado de tiempo provisto por Antel en su rol de TSA. Al desarrollarse este rol en forma integrada a su rol como PSCA y como servicio de custodia centralizada, aplican a éste todas las declaraciones de procedimientos y operación de seguridad de los demás servicios, que ya se encuentran definidos en la CPS de la CA de Antel, y por lo tanto deben ser consultados allí.

A efecto de permitir a los solicitantes y usuarios conocer la reglamentación vigente, este documento y las políticas definidas por la UCE estarán disponibles en www.tuid.uy.

1.2 Identificación

Nombre: Declaración de Prácticas de la Autoridad de Sellado de Tiempo (TSA) de Antel.

Versión: 1.0

Fecha de elaboración: 20/04/2020

Fecha de última actualización: 28/12/2021

OID: 2.16.858.10000157.66565.18

Sitio web de publicación: www.tuid.uy/legal/Declaracion_Practicas_TSA_TuID.pdf

1.3 Roles y definiciones

1.3.1 Autoridad de Sellado de Tiempo

La Autoridad de Sellado de Tiempo (en adelante TSA por sus siglas en inglés, *Time Stamping Authority*) es la Autoridad independiente que se establece como fuente de tiempo, otorga sellado del mismo a los datos provistos por los solicitantes y es en ella en quien depositan su confianza los terceros aceptantes. Por este motivo, la TSA es la responsable por la correcta operación de los servicios de sellado de tiempo, incluyendo la precisión del mismo y la seguridad en la producción de los tokens que lo certifican.

El rol de Autoridad de Sellado de Tiempo es desempeñado por Antel, en conformidad con la Política de Sellado Digital de Tiempo de la UCE, y sus funciones están detalladas en el presente documento. Al ser Antel ya un PSCA emitiendo certificados de personas físicas bajo las políticas reguladas por la UCE, utilizará la misma Autoridad Certificadora para emitir los certificados a sus propias Unidades de Sellado de Tiempo (TSU), utilizando para ello el perfil de certificado especificado por la UCE en la Política de Sellado de Tiempo para Prestadores de Servicios de Confianza.

1.3.2 Unidades de Sellado de Tiempo

La política de TSA de la UCE define a las Unidades de Sellado de Tiempo (TSU) como "*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*". En el caso de Antel será el operador de sus propias TSU, por lo cual quedarán acreditadas ante la UCE bajo la propia TSA, y sus certificados de sellado de tiempo serán emitidos por la CA acreditada que Antel ya posee.

1.3.3 Solicitantes

Los Solicitantes del Servicio de Sellado de Tiempo son personas físicas, jurídicas o incluso equipamiento informático, que utiliza el Servicio de Sellado de Tiempo de la TSA, el cual garantiza que un conjunto de datos se encontraba en cierto estado conocido en un momento dado, representado por el resultado de un hash y consignado por la estampa de tiempo otorgada por las TSU de la TSA.

1.3.4 Terceros Aceptantes

Personas físicas, jurídicas o equipamiento informático, que luego de realizadas las verificaciones de firmas y certificados correspondientes confían en los sellos de tiempo emitidos a los solicitantes por la TSA.

1.4 Usos y ámbito de aplicación

Usos Permitidos de los Sellos de Tiempo

Los sellos de tiempo pueden ser utilizados por los solicitantes para demostrar a los terceros aceptantes que un documento o cualquier conjunto de datos digitales existía en esa forma y contenido en un cierto momento en el tiempo, demostrando el momento en que se realizaron actos digitales, e incluso permitiendo en algún caso verificar una firma en un tiempo posterior al fin de la validez del certificado que la produjo.

1.5 Administración de la Declaración de Prácticas

Aplica lo estipulado en la Declaración de Prácticas de Certificación de la AC de TuID.

1.6 Definiciones y abreviaturas

Autoridad Certificadora (AC o CA): refiere a la entidad de confianza responsable de emitir o revocar los certificados electrónicos, se utiliza como sinónimo de ACPA (Autoridad Certificadora del Prestador Acreditado).

Autoridad de Sellado de Tiempo (TSA- PSCo): 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.

Declaración de Prácticas de Certificación (CPS – Certificate Practice Statement): declaración de las prácticas que emplea una entidad certificadora en la gestión de los certificados emitidos por ella (emisión, revocación, renovación, etc.).

European Telecommunications Standards Institute (ETSI): organización de estandarización independiente, sin fines de lucro de la industria de las telecomunicaciones de Europa, con proyección mundial.

HASH: algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija y alta variabilidad (entropía) según la entrada, garantizando así que pueda ser utilizada como función de identidad y verificación de integridad.

Network Time Protocol (NTP): protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable. En el contexto del presente documento, es el protocolo que se utiliza para mantener la estabilidad en la determinación de la hora del servicio de sellado de tiempo.

Prestador de Servicios de Certificación Acreditado (PSCA): entidad acreditada ante la UCE y responsable de la operación de una Autoridad de Certificación de PKI Uruguay.

Prestador de Servicios de Confianza (PSCo): entidad acreditada ante la UCE para brindar uno o más servicios de confianza. En el contexto del presente documento, corresponde tanto al prestador del servicio de firma e identificación en custodia centralizada como al prestador de servicios de sellado de tiempo.

Servicio de Sellado de Tiempo: servicio que recepciona 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 declaración (Sección 4.7).

Solicitantes: los solicitantes del servicio de sellado de tiempo son los organismos 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 brindado por el servicio de sellado. 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.

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

Timestamps: secuencia de caracteres que denotan la hora y fecha (o alguna de ellas) en la/s que ocurrió determinado evento.

Token de sellado de tiempo (TST): es la estructura de datos que contiene una representación (hash) 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 en esa forma 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)*".

Unidad de sellado de tiempo (TSU): es el conjunto de hardware y software gestionado como una unidad. Se trata de 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.

2 Responsabilidad y Obligaciones

2.1 Obligaciones de la TSA y las TSU

Antel opera la TSA y es responsable por el cumplimiento de las obligaciones estipuladas para tal fin en la Política de sellado de tiempo de la UCE, en los estándares técnicos aplicables y en particular con lo estipulado en la sección 4 del presente documento.

En particular, Antel asume las siguientes obligaciones y responsabilidades hacia los suscriptores y terceras partes en todo lo relativo a la prestación de los servicios de Sellado de Tiempo:

- Implementar y operar las TSU siguiendo los estándares de seguridad y políticas aplicables.
- Realizar la emisión de sellos de tiempo en base a la información provista por el solicitante exclusivamente, en forma libre de errores de entrada de datos, y con llaves privadas dedicadas exclusivamente para tal fin.
- Realizar la generación de llaves de las TSU en un entorno seguro, mediante personal autorizado, de acuerdo con los estándares técnicos vigentes y a los procedimientos establecidos en la sección 4 del presente documento.
- Emitir los certificados de las TSU sólo en base a peticiones de certificación (CSR) emitidas de acuerdo a lo estipulado en el punto anterior.
- Firmar los tokens de tiempo usando la llave privada generada exclusivamente para este fin, y no utilizar la llave privada de la TSU para ninguna otra finalidad.
- Determinar con precisión la fecha y hora a la que se emiten los sellos de tiempo, con una precisión mayor a 1 segundo respecto al tiempo UTC, no emitiendo sellos si la desviación fuese mayor.
- No emitir sellos de tiempo con TSU cuyo certificado se encuentre expirado o revocado.
- Almacenar las claves públicas de las TSU por el período de operación de estas.
- Comunicar a los solicitantes en forma oportuna y mediante declaraciones públicas las condiciones en las que se presta el servicio.
- Llevar adelante auditorías internas y externas para garantizar el cumplimiento de lo estipulado en la presente declaración y en las políticas y estándares técnicos aplicables.
- Proveer acceso permanente a las TSU, excepto en casos de interrupciones programadas, y ante casos de interrupciones inesperadas, dedicar los recursos adecuados para el restablecimiento del servicio en el menor tiempo posible. El uptime general del servicio de sellado deberá ser superior al 99,8%.
- Proteger toda información confidencial o privada que le sea conferida a Antel en el curso de su prestación del servicio de sellado de tiempo. No se considera información confidencial los hashes de las peticiones recibidas de solicitantes cuando estos no se encuentran asociados al conjunto de datos que los origina.
- Antel no se hace responsable por el contenido del documento, sólo da certeza que un documento o cualquier conjunto de datos digitales existía en esa forma y contenido en un cierto momento en el tiempo, y la emisión de un token de tiempo para dicho documento no puede ser considerada una aceptación o conocimiento de su contenido por parte de Antel.

2.2 Obligaciones de los Suscriptores/Solicitantes

Los suscriptores deberán verificar la firma de los sellos de tiempo para garantizar su integridad, y verificar el estado de vigencia del certificado de la TSU firmante contra los servicios de OCSP o CRL de Antel.

2.3 Obligaciones de Terceros Aceptantes

Los Terceros Aceptantes deberán verificar la firma de los sellos de tiempo para garantizar su integridad, y verificar el estado de vigencia del certificado de la TSU firmante contra los servicios de OCSP o CRL de Antel.

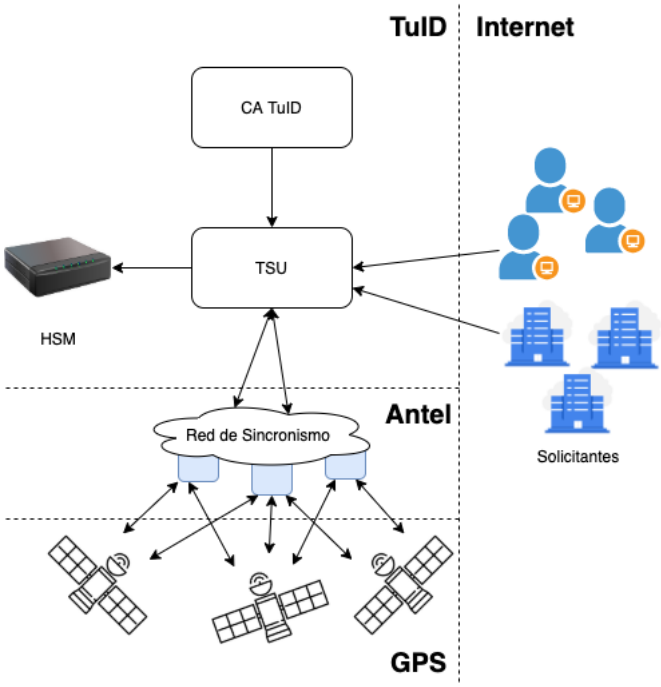
2.4 Obligaciones de la UCE

Las obligaciones de la UCE con respecto a los servicios de sellado de tiempo son estipuladas en la Política de Servicios de Sellado de Tiempo de la UCE.

3 Descripción general de la TSA.

La presente declaración se basa en la Política para Servicios de Sellado de Tiempo de la UCE, y sigue todos los lineamientos del estándar ETSI EN 319 421 - *Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*.

Antel, en su calidad de TSA, emite los certificados para sus TSU utilizando la CA acreditada de TuID, de acuerdo a todo lo establecido en su Declaración de Prácticas de Certificación (CPS), y de acuerdo a lo estipulado en la Política de Sellado de Tiempo de la UCE para la emisión de certificado de las TSU, especialmente en lo que refiere al perfil de certificado. De esta forma, un token de tiempo emitido por la TSU puede ser verificado con su certificado, que a su vez puede ser verificado con el certificado de la CA de Antel, y este finalmente puede ser verificado con el certificado de la ACRN, completando así la cadena de confianza de la Infraestructura Nacional de Certificación Electrónica.



Las TSU firman digitalmente los time-stamps, utilizando claves privadas especialmente dedicadas para tal fin. Dichas llaves privadas se almacenan siempre en módulos criptográficos de seguridad (HSM) reservados para tal propósito. A su vez, estas unidades realizan la sincronización de hora mediante protocolo NTP contra una red de sincronismo de Antel, que es utilizada para el sincronismo de horas de los servicios de telefonía, entre otras. Esta red cuenta con equipos de sincronismo que obtienen la hora realizando lecturas directamente de los servicios globales de GPS, por lo que se consideran una fuente de hora Stratum 1. Su precisión real se estima en el orden de los microsegundos, y por lo tanto la precisión de las TSU se estima en el orden de los milisegundos.

Los suscriptores solicitan a la TSU los sellos de tiempo a través del protocolo especificado en el RFC 3161 (*Time Stamping Protocol*), utilizando como transporte preferido HTTPS, con opción a utilizar en algunos casos HTTP, como excepción, si aplicasen restricciones de hardware o software del lado de los clientes. Los clientes se autentican con credenciales entregadas para tal fin. Cada sello de tiempo es firmado por la TSU y calificado con la política de sellado de tiempo utilizada.

Antel aplica condiciones comerciales para el acceso al servicio por parte de los suscriptores, pudiendo brindar el servicio bajo un costo, en forma gratuita o incluso reservándose el derecho de brindarlo en forma completamente abierta en algún contexto.

Los terceros aceptantes cuentan con los certificados de las TSU presentes en los sellos de tiempo y en el portal público de TuID para realizar la validación de las firmas de los mismos. Además, cuentan con los servicios públicos de OCSP y la CRL de TuID para la validación del estado de revocación de esos certificados, así como con la CRL de la ACRN para la validación del estado del certificado de TuID.

Antel se encuentra acreditado ante la UCE para la prestación de los servicios de sellado de tiempo, y realiza auditorías periódicas para garantizar el cumplimiento con sus políticas, con los estándares técnicos aplicables y con todo lo estipulado en la presente declaración.

4 Gestión y Operación de la TSA

En la presente sección se estipulan los controles aplicados en la gestión y operación de la TSA y las TSU asociadas. Dado que la TSA se implementa dentro del mismo marco de gestión que la CA de TuID, la mayoría de los elementos ya se encuentran definidos en la CPS de la CA de TuID.

4.1 Gestión de riesgos y políticas de seguridad

Los aspectos específicos del Servicio de Sellado de Tiempo forman parte del marco de gestión de riesgos de la CA y la infraestructura de custodia centralizada.

4.2 Organización Interna

Aplica todo lo estipulado en la CPS de la CA de TuID. La TSA es parte de la plataforma TuID, que es parte de Antel.

4.3 Seguridad ligada al personal

Estipulado en la CPS de la CA de TuID en la sección 5.3.

4.4 Gestión de Activos

Estipulado en la CPS de la CA de TuID en la sección 5.2.

4.5 Control de Acceso

Estipulado en la CPS de la CA de TuID en la sección 6.

4.6 Controles Criptográficos

4.6.1 Generación de llaves de las TSU

Antel genera las claves criptográficas utilizadas para la firma de los sellos de tiempo en un todo de acuerdo con lo estipulado en ETSI EN 319 421. Esto implica que realiza la generación en dispositivos HSM certificados con FIPS 140-2 Level 3, mediante personal autorizado, con control por oposición, y dentro del entorno físico seguro de la TSA, CA e infraestructura de custodia centralizada. Las TSU emiten sellos de tiempo firmados con claves RSA de al menos 2048 bits, y con algoritmos de hash a elección del solicitante, pero soportando SHA256, SHA384 y SHA512.

4.6.2 Protección de las llaves de las TSU

Antel adopta medidas específicas para asegurar que las claves privadas utilizadas para el sello de tiempo mantengan su integridad y confidencialidad. Dichas medidas incluyen el uso de HSMs certificados con FIPS 140-2 Level 3. Las copias de seguridad de estas claves sólo son realizadas con la finalidad de instalar la misma clave en más de un HSM en uso por la misma TSU para garantizar alta disponibilidad, y se realizan utilizando los mecanismos de cifrado de los fabricantes de los HSM, garantizando de esa forma que las claves se exportan en forma cifrada, nunca abandonando los HSM en claro. Estos procedimientos son realizados por personal autorizado, bajo control por oposición, y dentro del entorno seguro.

4.6.3 Certificados Públicos de las TSU

De acuerdo con lo estipulado en ETSI EN 319 421, las claves públicas de una TSU deben estar protegidas por un certificado, y el mismo debe ser emitido por una autoridad certificadora operando bajo ETSI EN 319 411-1 - *Policy and security requirements for Trust Service Providers issuing certificates, Part 1 - General*

Requirements. Este requisito se satisface ya que las claves de las TSU se protegen por un certificado emitido por la CA de TuID, que es una CA acreditada para la emisión de certificados bajo la regulación de la UCE y en un todo de acuerdo con el estándar mencionado anteriormente. Los certificados públicos de las TSU se publican en el sitio de TuID, además de ser incluidos en los mismos sellos emitidos, a menos que el solicitante explícitamente pida un sello sin el certificado embebido para hacerlo más liviano.

Las TSU no emiten nunca sellos con fechas de validez anteriores a la fecha de comienzo de validez de su certificado, ni tampoco emiten sellos con su clave privada si el certificado público no ha sido instalado en la TSU, momento en el cual la TSU además verifica que el certificado que va a comenzar a utilizar esté adecuadamente firmado por la CA de Antel y se verifique la cadena de confianza a la ACRN.

4.6.4 Cambio de claves y certificados de las TSU

Los certificados de las TSU se emiten con un período de validez de cinco (5) años. No obstante, las claves de las TSU tienen una validez de un (1) año desde su generación. Luego de ese período, las mismas ya no son utilizadas para la generación de nuevos sellos. Esto se consigna emitiendo los certificados con la extensión "*private key usage period*" a un año luego de la emisión. Este esquema de utilización de claves por un período menor a la validez de certificados está estipulado en ETSI EN 319 421.

Toda operación de cambio de claves y certificados es realizada luego de una reevaluación de la robustez de los mecanismos criptográficos en ese momento según las guías que ofrezcan organismos de estandarización como el NIST, para ser cambiados si se encuentran considerados como riesgosos. De la misma forma, si en cualquier momento de la validez de los certificados se detecta una obsolescencia de los mecanismos criptográficos subyacentes como colisiones en los hashes, debilidades en el algoritmo de cifrado o insuficiencias en el largo de las claves, Antel tomará las medidas necesarias para la sustitución prematura de los certificados de las TSU por otros que se basen en elementos criptográficos más robustos.

4.6.5 Fin de ciclo de vida de claves de las TSU

Una vez concluido el período de uso de las claves privadas (*private key usage period*), las mismas son sustituídas por claves y certificados nuevos, siendo además destruidas para prevenir que se continúe con su uso. Nunca se emitirán *timestamps* utilizando claves expiradas, por lo que los terceros aceptantes deberán verificar que además de encontrarse vigente el certificado en el momento de emisión del sello, se encontrase vigente la clave privada según el período de validez estipulado en la extensión *private key usage period*.

4.6.6 Ciclo de vida del equipamiento criptográfico

Los HSM y otros dispositivos criptográficos utilizados en las TSU han sido instalados en una ceremonia controlada con presencia de personal de la UCE y AGESIC. Dicho procedimiento incluyó la inicialización de estos equipos a su configuración de fábrica previo a su configuración, que además fue realizada por personal autorizado, con control por oposición y dentro del entorno seguro, para garantizar su integridad y por consiguiente la integridad del servicio de sellado. Si surgiera la necesidad de enviar un HSM a mantenimiento, el mismo es reinicializado en forma previa para garantizar que ya no posea las claves de la TSU, y de ser terminado su uso el mismo es destruído en forma irrecuperable.

4.7 Sellado de Tiempo

4.7.1 Prestación del servicio de sellado

El servicio de sellado es otorgado a usuarios autenticados, para los cuales aplican condiciones comerciales y precios que son definidos por Antel fuera del alcance del presente documento. Antel se reserva el derecho de brindar alguna versión del servicio en forma gratuita, e incluso mediante algún endpoint completamente libre de acceso, para el cual podrán aplicar criterios de niveles de servicio diferenciales, siempre en cumplimiento de las políticas vigentes.

4.7.2 Emisión de sellos de tiempo

Los sellos de tiempo son emitidos de acuerdo con el perfil de timestamping especificado en ETSI EN 319 422, en la sección 8 de la Política de Sellado de Tiempo de la UCE, y en cumplimiento con el RFC 3161 "*Time Stamp Protocol (TSP)*". La solicitud se realiza sobre HTTPS, que debe ser protegido con un certificado reconocido por los principales truststores de la industria. Antel no brinda el servicio sobre HTTP salvo a través de redes privadas, o por excepciones debidamente justificadas y motivadas por sistemas legados o similares.

Cada token de tiempo (TST) contiene:

- el hash de los datos enviados para sellar,
- el identificador de la política de *timestamping*,
- un número de serie único que lo identifica unívocamente dentro de la TSA,
- el valor de la hora UTC con una precisión inferior a un segundo y
- el certificado de la TSU firmante si el cliente así lo solicita en su petición.

Las TSU aceptan requests usando SHA256, SHA384 y SHA512. Las claves de firma de las TSU son siempre RSA de 2048 bits y sólo son utilizadas para firmar los TST. Para cada solicitud de sello de tiempo, las TSU generan registros de auditoría que incluyen datos como el timestamp de la solicitud, el resultado de la misma, el TST emitido y un HMAC para garantizar la integridad de esos registros.

Las TSU no emiten ningún TST con certificados que hayan llegado al fin de su validez, o si la diferencia de tiempo del sistema contra UTC es detectada como superior a un segundo.

4.7.3 Sincronización UTC

La hora es sincronizada en forma periódica por las TSU contra la red de sincronismo de Antel mediante el protocolo NTP. En cada una de esas sincronizaciones se genera una evidencia firmada por la TSU con un HMAC que indica el resultado de la sincronización y el "drift" de ese momento con respecto a UTC. Si el drift fuese mayor a 1 segundo, además de registrar el evento se deja de emitir sellos y se genera una alerta para atención del personal correspondiente. Las trazas de auditoría quedan almacenadas y firmadas para luego analizar las causas del hecho.

La fuente de tiempo es la propia red de sincronismo de tiempo que Antel emplea para su infraestructura de telefonía, y la parte a usar para la TSA consiste en un conjunto de tres servidores NTP que se comunican con las TSU mediante un enlace privado gigabit de baja latencia. Estos servidores NTP se implementan mediante equipos especialmente diseñados para sincronismo horario que obtienen directamente UTC desde el sistema GPS. Estos equipos son carrier class, con redundancia de fuente y controladora, y además cuentan con 2 antenas y dos cableados GPS, lo que permite contar con alta disponibilidad en todos los puntos del sistema de sincronismo. Al tomar la hora directamente del sistema GPS, se trata de fuentes de hora Stratum 1, y al realizar las estampas de tiempo por hardware cuentan con una precisión de microsegundos, logrando que la precisión efectiva de las TSU sea del orden de unos pocos milisegundos. Esta sincronización ya incluye el manejo de Leap Seconds.

4.7.4 Servicio de Validación

La validación de los TST se hace utilizando el certificado de la TSU y la validación estándar de la Infraestructura Nacional de Certificación Electrónica. Para ello, TuID cuenta con los servicios de estado OCSP y CRL para verificar la validez de los certificados de las TSU.

4.7.5 Validación Longeva

Si el certificado de la TSU firmante no se encuentra expirado ni revocado, la verificación se realiza siguiendo las reglas de una PKI normal. Para la verificación de firmas más allá del período de validez del

certificado de la TSU e incluso más allá de la validez del certificado de la CA, se deben seguir las recomendaciones estipuladas en la Política de Sellado de Tiempo de la UCE y en ETSI EN 319 421. En ambos lugares 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 cuyo sello ya está expirado por estar expirado su certificado firmante, Antel recomienda a los solicitantes que realicen un nuevo sello de tiempo contra la TSU, que ya contará con nuevos certificados, y si correspondiere también con nuevos certificados de la CA de TuID y de la ACRN, refrescando así la validez del nuevo timestamp.

4.8 Seguridad Física y del Entorno

Estipulado en la CPS de la CA de TuID en la sección 5.1.

4.9 Seguridad en las Operaciones

Estipulado en la CPS de la CA de TuID en la sección 5.2.

4.10 Seguridad de las Redes

Estipulado en la CPS de la CA de TuID en la sección 6.7.

4.11 Gestión de Incidentes

Estipulado en la CPS de la CA de TuID en la sección 5.7.

4.12 Auditoría y recolección de evidencias

Estipulado en la CPS de la CA de TuID en las secciones 5.4 y 5.5.

Se auditan explícitamente todas las transacciones de sincronización que realicen las TSU y los *request* de sellos de tiempo que hagan los solicitantes finales, incluyendo el TST emitido. En ambos casos los registros son almacenados firmados por un HMAC realizado por las TSU, y la retención de los registros podrá variar pero no será inferior a 5 años en ningún caso.

4.13 Gestión de la Continuidad del Negocio

Estipulado en la CPS de la CA de TuID en la sección 5.7. Las TSU cuentan con redundancia para proveer alta disponibilidad ante fallas menores y moderadas. Se cuenta con redundancia geográfica en stand-by para activar el servicio desde otra locación como estrategia de continuidad ante desastres de mayor impacto.

4.14 Terminación de la TSA

De terminarse el servicio de TSA, Antel notificará a la UCE y publicará el hecho en el Diario Oficial. Antel cesará entonces inmediatamente la emisión de sellos de tiempo, retendrá los registros de auditoría por el plazo requerido, y continuará brindando los servicios de validación de estado de certificados de TSU como parte del servicio de estado de certificados emitidos por la CA de TuID. De aplicar también la terminación de los servicios de CA, aplican las condiciones estipuladas en la CPS de la CA de TuID, en las cuales Antel continuará el servicio o tomará las medidas que correspondan, en acuerdo con la UCE, para transferir estos servicios a un tercero.

4.15 Cumplimiento

Antel toma todas las medidas razonables para garantizar el cumplimiento de la TSA y las TSU con la legislación vigente de Uruguay, regulación y políticas exigidas por la UCE, con todos los estándares técnicos aplicables y todas las definiciones de la presente Declaración. Dicho cumplimiento es monitoreado y asegurado mediante la realización de autorías periódicas, tanto internas como externas.

5 Perfiles de Certificados y TSTs

El formato de los certificados cumple con lo especificado en el estándar ITU-T X.509 versión 3[2] (*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*), definido en su versión más reciente en el RFC 5280[3].

5.1 Perfil de Certificado de la CA

La CA es la CA de TuID ya implementada, y su perfil de certificado se encuentra estipulado en la CPS de la CA de TuID y en la Política de Certificación de la ACRN.

5.2 Perfil de Certificado de las TSU

Atributos	***Contenido***
Versión	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 = TuID Sellado de Tiempo NN (NN es un número único de cada TSU) O = Antel OU = TuID C = UY
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 2048 bits

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/contentCommitment = 1 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 0 CRLSign = 0 EncipherOnly = 0

	DecipherOnly = 0
Uso de Claves Extendido (Extended Key Usage)	timeStamping
Private key usage period	1 año (en formato desde/hasta)
Políticas de Certificación (Certificate Policies)	OID: 2.16.858.10000157.66565.16 URI: www.uce.gub.uy/informacion-tecnica/politicas/cp_sellado_de_tiempo.pdf OID: 2.16.858.10000157.66565.18 URI: www.tuid.uy/legal/Declaracion_Practicas_TSA_TuID.pdf
Restricciones Básicas (Basic Constraints)	CA = FALSE
Puntos de distribución de las CRL (CRL Distribution Points)	URI = URL primaria de publicación de la CRL
Authority Information Access	CA: https://www.tuid.uy/cer/Autoridad_Certificadora_TuID.cer OCSP: ocsp.tuid.uy
CRL Distribution Points	crl.tuid.uy/crls

5.3 Perfil de TST

Los TST son emitidos según el TimeStamping Protocol estipulado en el RFC 3161, y de acuerdo a lo estipulado por ETSI EN 319 422.

A los tokens se les agrega la extensión **qcStatements** con el valor esi4-qtstStatement1 para marcarlos como tokens de tiempo cualificados, según el formato estipulado en el RFC 3739.