POLÍTICA DE SELLADO DE TIEMPO (TSA)

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
Fecha: 2022.10.26 07:25:20 +02'00'

CONTROL DE CAMBIOS

VERSIÓN	FECHA	CAMBIO
1.1	20/02/2018	– 5.1. Identificación. Actualización del identificador de la política. Token sello de tiempo: 1.3.6.1.4.1.14777.3.3
1.2	06/10/2021	– Se incluye nuevo epígrafe: Control de Cambios, y se elimina el documento DOC_P_Actualización_DPTSA. – Se mejora la redacción. – 5.1. Identificación. Actualización del identificador de la política. Token sello de tiempo: 1.3.6.1.4.1.14777.300.1 – 6.5 Procedimiento de emisión de un sello de tiempo. Actualización de la Cadena de Certificación de la Autoridad de Certificación subordinada CN = SUBCA QC IZENPE – TSA – 6.8.3 Perfil del certificado de la TSA. Actualización de los datos del certificado. – 6.8.4 Perfil del token de sello de tiempo. Actualización del OID OID = 1.3.6.1.4.1.14777.300.1
1.3	09/12/2021	– 6.8.2 Perfil de una petición de sello de tiempo. Especificación de algoritmos hash admitidos.
1.4	21/10/2022	– 6.8.2 Perfil de una petición de sello de tiempo: se añaden todos los hash admitidos y se especifican la preferencia de los mismos. – Actualización de los puntos 6.7.7. Compromiso de la clave privada del certificado de TSA y 6.7.8 Finalización de la TSA.

Índice

Contenido

1 INTRODUCCIÓN

Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. (en adelante, Izenpe) ofrece un servicio cualificado de sellado de tiempo como parte de sus servicios como prestado cualificado de servicios de confianza, según definición 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 (en adelante, eIDAS).

Este servicio crea y registra evidencias digitales de la existencia de un dato en un instante determinado en la línea de tiempo, de una forma fiable y de confianza, mejorando significativamente la fiabilidad de los datos electrónicos.

Izenpe ha creado una Autoridad de Sellado de Tiempo (TSA) para proporcionar el servicio de sellado de tiempo.

El presente documento describe la política de la Autoridad de Sellado de Tiempo (TSA), especificando los procesos y políticas generales de la Autoridad de Sellado de Tiempo para la generación del sello de tiempo y sus servicios. Se especifican procesos y detalles técnicos adicionales a la Declaración de Prácticas de Certificación (DPC) de Izenpe.

Los procedimientos definidos y su correcta implementación son auditados por una entidad externa, según las especificaciones definidas por ETSI a través de la norma EN 319 421.

2 DEFINICIONES Y ACRÓNIMOS

2.1 Definiciones

Esta Política referencia las definiciones y acrónimos usados en la Declaración de Prácticas de Certificación, además de:

- Autoridad de Sellado de Tiempo (TSA): autoridad que emite tokens de sello de tiempo
- Terceras partes usuarias**:** usuario que confía en un sello de tiempo proporcionado por Izenpe
- Suscriptor**:** persona que utiliza los servicios proporcionado por la TSA y que acepta de forma explícita los términos y condiciones
- Política de sellado de tiempo**:** reglas que aplican a la TSA cuando se genera un token de sello de tiempo
- Token de sello de tiempo**:** objeto de datos que relaciona la existencia de unos datos digitales a un momento concreto. Sirve como evidencia de que un dato existió en un instante determinado en la línea de tiempo.
- Unidad de sellado de tiempo**:** componentes hardware y software gestionados como una unidad que proporciona tokens de sello de tiempo desde una única fuente de tiempo. Los componentes pueden ser clonados o implementados en redundancia para conseguir alta disponibilidad
- Declaración de Prácticas de la TSA**:** políticas y prácticas de una TSA, especialmente orientado a suscriptores y terceras partes.
- Coordinated Universal Time**:** tiempo solar en el meridiano principal (0º). La escala de tiempo está basada en el segundo, según se define en ETSI TS 102.023 y en ITU-R Recommendation TF.460-5.
- UTC(k): escala de tiempo realizada por un laboratorio "k" de acuerdo con UTC, con el objetivo de conseguir una desviación máxima de +-100ns.

2.2 Acrónimos

- TSA: Time Stamp Authority
- TSU: Time Stamp Unit
- TST: Time Stamp Token
- UTC: Coordinated Universal Time
- eIDAS: 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
- DPC: Declaración de Prácticas de Certificación

3 ÁMBITO

El presente documento define las prácticas, operacionales de gestión de (TSA) para que los suscriptores y terceros de confianza puedan evaluar la fiabilidad de los servicios de sellado de tiempo.

Los requisitos de la política de la TSA son conformes a las disposiciones del Reglamento Europeo eIDAS. Los servicios de sellado de tiempo de Izenpe pueden aplicarse a una firma electrónica o a cualquier aplicación que requiera una evidencia de la existencia de datos digitales en un punto particular en el tiempo. Estos requisitos de la política están basados en criptografía de clave pública, certificados de clave pública (X.509) y fuentes de tiempo fiables.

El presente documento, junto a la DPC de Izenpe, puede ser utilizado organismos independientes para evaluar la fiabilidad de esta TSA y sus servicios de sellado de tiempo.

4 CONCEPTOS GENERALES

4.1 Servicios de sellado de tiempo

Los Servicios de sellado de tiempo incluyen dos componentes:

- Provisión de sellos de tiempo: componente técnico encargado de generar los tokens de sello de tiempo
- Administración sellos de tiempo: componente del servicio que monitoriza y controla la operación de los servicios de sellado de tiempo. La gestión de sellado de tiempo garantiza que los relojes utilizados en el sellado de tiempo están correctamente sincronizados con UTC.

4.2 Autoridad de sellado de tiempo

La TSA de Izenpe emite tokens de sello de tiempo (TST) seguros para usuarios de servicios de sellado de tiempo (como por ejemplo suscriptores o terceras partes).

La TSA de Izenpe asume toda la responsabilidad sobre la provisión de los servicios de sellado de tiempo indicados en el apartado “6.4 Responsabilidades”. La TSA de Izenpe puede operar varias unidades identificables de sello de tiempo (TSU’s), y cada TSU puede tener una clave diferente (ver apartado “6.8.4 Perfil del token de sello de tiempo”).

Dentro de un TSU se permite clonar claves y utilizarlo en componentes redundantes para cumplir con requerimientos de alta disponibilidad.

La TSA de Izenpe está identificada en el certificado digital usado por los servicios de sellado de tiempo. El perfil está disponible en el apartado “6.8.3 Perfil del certificado de la TSA”.

4.3 Suscriptor

El suscriptor puede ser una organización o un particular.

- Si el suscriptor es una organización, las obligaciones que aplican a esa organización también aplican a sus usuarios finales asociados.

  La organización debe informar adecuadamente a sus usuarios finales., siendo responsable si los usuarios finales no cumplen correctamente las obligaciones.

- Si el suscriptor es un usuario particular, el usuario final será responsable directamente del cumplimiento de las obligaciones.

4.4 Política de Sellado de Tiempo y Declaración de Prácticas de la TSA

4.4.1 Propósito

La Política y Declaración de Prácticas de sellado de tiempo se definen como:

- La Política de la TSA define los aspectos de deben ser cumplidos tanto por el suscriptor como por la Autoridad emisora de sellos de tiempo. Se incluyen las reglas y procesos que aplica la TSA cuando genera un token de sello de tiempo.
- La Declaración de Prácticas (DPC) es una declaración de cómo está implementado el servicio de sellado de tiempo para cumplir con los requerimientos de la política.

- De forma complementaria a los procesos descritos en la DPC de Izenpe, esta política de TSA describe procesos y políticas específicas.

4.4.2 Nivel de especificidad

La política de TSA especifica los procesos utilizados para proporcionar los servicios de sellado de tiempo, extendiendo los procesos descritos en la DPC.

4.4.3 Enfoque

La política de TSA se enfoca a procesos generales: detalles técnicos como la estructura organizativa, procedimientos operativos, e infraestructura de comunicaciones están especificados en la DPC o en documentos internos. Los documentos internos no están disponibles al público.

5 INTRODUCCIÓN A LA POLÍTICA DE LA TSA Y REQUERIMIENTOS GENERALES

5.1 Identificación

Izenpe incluye el siguiente identificador de política (OID) a todos los tokens de sello de tiempo emitidos por su TSA.

Token sello de tiempo	1.3.6.1.4.1.14777.300.1

5.2 Comunidad de usuarios y aplicabilidad

Los usuarios del servicio de sellado de tiempo serán suscriptores y terceras partes que requieran del servicio. Existe una limitación por número de peticiones mensuales, a partir de las cuales el servicio tiene un coste asociado. Contactar con Izenpe para consultar condiciones y tarifas.

5.3 Conformidad

El cumplimiento de esta Política de Sellado de Tiempo está sujeto a auditorías periódicas independientes, tanto internas como externas.

Izenpe cumple con las obligaciones definidas en el apartado “Obligaciones y Responsabilidades” y asegura la implementación de controles apropiados.

6 POLÍTICA DE SELLADO DE TIEMPO

6.1 Despliegue y mantenimiento de sistemas de confianza

Las claves de la TSA y sus servicios son producidas en un entorno de confianza. Los sistemas y productos usados por Izenpe proporcionan los servicios adecuados de acuerdo a los niveles requeridos de aseguramiento. Izenpe lleva a cabo un análisis adecuado de los requisitos de seguridad y dispone de procedimientos de control de cambios.

6.2 Política de Sellado de Tiempo

La TSA opera sus servicios de acuerdo a las reglas establecidas en la presente Política, la DPC y documentos internos adicionales que definen los requerimientos técnicos, operativos y procedimentales. Izenpe puede de forma discrecional ofrecer servicios de TSA específicos a un solicitante.

La Política define cómo Izenpe se adhiere a los requerimientos identificados en la DPC y otros documentos internos.

Los procedimientos definidos y su correcta implementación son auditados anualmente por una entidad externa independiente.

La TSA y otra documentación relevante está disponible en www.izenpe.eus.

La Declaración de divulgación de TSA está incluida en el punto "**¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**". Los documentos internos no se publican. Las modificaciones sobre las prácticas de TSA o cualquier otro documento publicado son implementadas según las especificaciones de la DPC.

Los términos y condiciones establecidos en este documento, son vinculantes para todos los suscriptores y terceras partes que utilicen los servicios de sellado de tiempo de Izenpe.

Se pueden encontrar otros documentos que complementan a esta Política como la DPC, en www.izenpe.eus

- La TSA de Izenpe es un servicio cualificado de sellado de tiempo según eIDAS
- Para información de contacto consultar el apartado "1.5.2 Datos de contacto" de la DPC
- Las obligaciones de la entidad emisora de sellos de tiempo están definidas en el apartado 6.3.1 *Obligaciones de la Entidad Emisora de Sellos de Tiempo* de este documento.
- Las obligaciones del suscriptor están definidas en el punto 6.3.2 *Obligaciones del suscriptor de sellos de tiempo* de este documento
- Las obligaciones de terceros están definidas en el punto 6.3.3 *Obligaciones de terceras partes verificadoras de sellos de tiempo* de este documento
- Las responsabilidades de la Autoridad de Sellado de Tiempo están definidas en el punto 6.4 *Responsabilidades* de este documento
- El servicio tiene un coste según tarifas de catálogo de precios de Izenpe.
- Izenpe mantiene registros de todas las operaciones de la TSA, según se indica en el punto 6.13 *Recogida de evidencias* de este documento.

- Para posibles reclamaciones y resolución de disputas consultar punto 9.12 *Reclamaciones y resolución de disputas* de la DPC.
- Suscriptores y terceras partes aceptan las condiciones de uso definidas por Izenpe
- El certificado de la TSA de Izenpe está emitido por una Autoridad de Certificación cuya política de certificación sigue las directrices indicadas en la DPC de Izenpe.
- Cada token de sello de tiempo emitido por el servicio TSA de Izenpe incluye el identificador de objeto definido en el apartado 6.8.4 *Perfil del token de sello de tiempo.*
- Los algoritmos de hash permitidos están indicados en el apartado 6.8.2 *Perfil de una petición de sello de tiempo.* El algoritmo de firma del token TSA está definido en el apartado 6.8.4 *Perfil del token de sello de tiempo.*
- La TSA asegura la precisión de tiempo compatible con los estándares mínimos de tiempo UTC de +/- 1 segundo. La TSA de Izenpe no emitirá tokens de sello de tiempo si no se puede asegurar dicha precisión.
- Las limitaciones de responsabilidad están definidas en el apartado 6.4 *Responsabilidades* de este documento, en la DPC y en otros acuerdos de servicio mantenidos con usuarios.

6.3 Obligaciones y responsabilidades

Izenpe, como Entidad que emite sellos de tiempo de acuerdo con la presente Política de Sellado de Tiempo asume las siguientes obligaciones.

6.3.1 Obligaciones de la Entidad Emisora de Sellos de Tiempo

La Autoridad de Sellado de Tiempo de Izenpe,

- Emite tokens de sello de tiempo (TST) seguros para usuarios de servicios de sellado de tiempo (se incluyen tanto suscriptores como terceras partes.
- Asume la responsabilidad de proporcionar los servicios de sellado de tiempo.
- Puede operar con diferentes unidades identificables de sellado de tiempo (TSU's), cada una de las cuales puede tener su propia clave de firma.
- Está identificada en el certificado digital utilizado para los servicios de sellado de tiempo.
- Ofrece sus servicios a todos los suscriptores y terceras partes verificadoras de sellos de tiempo que se comprometan a cumplir con sus obligaciones.

6.3.2 Obligaciones del suscriptor de sellos de tiempo

El suscriptor de sellos de tiempo puede utilizar el Servicio de Sellado de Tiempo únicamente según especificaciones de ETSI EN 319 422.

El suscriptor debe verificar que el token de sello de tiempo ha sido correctamente firmado por la autoridad de sellado de tiempo, y que la clave privada utilizada para firmar el token de sello de tiempo no ha sido revocado.

El suscriptor debe cumplir con la presente Política de Sellado de Tiempo de Izenpe, disponible en www.izenpe.eus

6.3.3 Obligaciones de terceras partes verificadoras de sellos de tiempo

Cuando se recibe un token de sello de tiempo, la tercera parte debe verificar que el token está correctamente firmado y que la clave privada utilizada para firmar el sello de tiempo no ha sido revocada.

Mientras el certificado utilizado para generar sellos de tiempo no esté caducado, es posible comprobar su validez en la CRL correspondiente.

En el caso de que la verificación se realice después del periodo de validez del certificado, la tercera parte deberá comprobar que la función hash empleada, los algoritmos y longitud de claves criptográficas se pueden seguir considerando seguras.

6.4 Responsabilidades

- Izenpe opera su TSA de acuerdo con la política de TSA de Izenpe, su DPC, y los términos de cualquier otro acuerdo vinculante entre Izenpe y usuarios del servicio de sellado de tiempo.
- Izenpe realiza esfuerzos para proporcionar alta disponibilidad en sus servicios, pero no ofrece una garantía total en cuanto a disponibilidad, ni la precisión en los sellos de tiempo. Izenpe no es responsable en ningún caso de pérdida de beneficios, daños indirectos o consecuentes, o pérdida de datos, en la medida en que la legislación vigente lo permita.
- Izenpe no será responsable de daños consecuencia de infracciones cometidas por el suscriptor o terceras partes en los términos y condiciones aplicables.
- Izenpe no será bajo ninguna circunstancia responsable de daños consecuencia de eventos de fuerza mayor como desastres naturales, caídas de electricidad o telecomunicaciones, fuego, interacciones externas no predecibles como virus o ataques de hackers, acciones gubernamentales, o huelgas.
- En cualquier caso Izenpe realizará todas las medidas razonables para mitigar los efectos de tales eventos. Cualquier daño consecuencia de un retraso causado por un evento de fuerza mayor no será cubierto por Izenpe.

6.5 Procedimiento de emisión de un sello de tiempo

Con objeto de la prestación del Servicio de Sellado de Tiempo, Izenpe realiza la gestión de las claves correspondientes de conformidad con lo descrito en el apartado 6.7 *Controles criptográficos* de este documento.

Los Sellos de Tiempo emitidos bajo esta política son firmados por certificados específicos, emitidos bajo la Cadena de Certificación de la Autoridad de Certificación subordinada con CN = SUBCA QC IZENPE – TSA.

Para obtener más información sobre la citada Cadena de Certificación de la Autoridad de Certificación raíz consultar el apartado 1.3.1 *Autoridades de Certificación* de la DPC.

6.5.1 Provisión y disponibilidad del servicio de sellado de tiempo

La emisión de Sellos de Tiempo se realizará ante la petición de la entidad usuaria. Cuando ésta desee obtener un Sello de Tiempo para un documento electrónico, calculará un valor o conjunto de valores hash a partir de este. Éste se incluirá en una estructura de petición de sello de tiempo, y será enviado a Izenpe para que proceda a la emisión del Sello de Tiempo correspondiente.

Este Sello de Tiempo vinculará, a través de la firma electrónica de Izenpe, los datos recibidos y la fecha y hora de la recepción.

Los algoritmos admitidos están descritos en el apartado 6.8.2 *Perfil de una petición de sello de tiempo* de este documento.

Izenpe no realizará comprobación o tratamiento alguno sobre la representación de los datos a sellar recibidos más allá de su inclusión en el propio Sello de Tiempo y en los sistemas de registro de eventos. Izenpe no verificará en modo alguno el contenido, ni la veracidad de la representación de los datos a sellar ni del origen de los mismos.

El Servicio de Sellado de Tiempo estará disponible las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a Izenpe u operaciones de mantenimiento. Izenpe notificará esta última circunstancia con la antelación suficiente y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

Tanto las peticiones de Sellado de Tiempo como las respuestas se gestionan conforme a lo descrito en la recomendación IETF RFC 3161.

6.5.2 Petición de un sellado de tiempo

Las peticiones de Sellado de Tiempo se envían a la dirección http://tsa.izenpe.com encapsuladas como Content-Type: application/timestamp-query, codificadas en DER y descritas en ASN.1 (Ver IETF RFC 3161)

6.5.3 Respuesta a una petición de sellado de tiempo

Las respuestas a una petición de Fechado Digital se reciben de la dirección http://tsa.izenpe.eus encapsuladas como Content-Type: application/timestamp-reply, codificadas en DER y descritas en ASN.1.

El contenido de la respuesta es una estructura ASN.1 en la que se incluye el resultado de la operación (status), es decir, si la operación se ha realizado de manera satisfactoria o no, y una estructura CMSSignedData (timeStampToken) en la que se incluye el fechado digital (TSTInfo) firmado por la Autoridad de Fechado Digital.

El certificado de la Autoridad de Sellado Digital es un certificado emitido por la CA con la extensión id-kp-timestamping que indica que este certificado se utilizará con el fin exclusivo de fechar documentos digitales.

6.6 Administración y operación de la TSA

6.6.1 Gestión de la Seguridad

La gestión de la seguridad de la TSA de Izenpe está descrita en el apartado 5. *Controles de seguridad física, de procedimiento y de personal* de la DPC.

6.6.2 Clasificación y gestión de activos

La TSA de Izenpe asegura que la información y otros activos reciben el tratamiento apropiado en cuanto a seguridad, según se define en el apartado 5.7 *Plan de Contingencias* de la DPC.

6.6.3 Seguridad del personal

Los controles de seguridad del personal están definidos en el apartado 5. *Controles de seguridad física, de procedimiento y de personal* de la DPC.

6.7 Controles criptográficos

6.7.1 Generación de la clave de la TSA

Izenpe genera las claves criptográficas en un entorno físicamente securizado y realizado por personal con roles de confianza. Las claves de la TSA de Izenpe son generadas siguiendo un procedimiento específico. La duración máxima del certificado de la TSA será de 5 años.

6.7.2 Protección de la clave privada de la TSU

La TSA de Izenpe asegura que se mantiene la confidencialidad e integridad de sus claves. En particular el HSM cumple con los requerimientos de FIPS 140-2 nivel 3 y el nivel de aseguramiento EAL4+ del perfil correspondiente. En ese sentido las claves de la TSA se mantienen con un nivel de seguridad equivalente al descrito en la DPC para las CAs subordinadas de Izenpe.

6.7.3 Distribución de la clave pública de la TSU

El certificado de la TSA de Izenpe está publicado en www.izenpe.eus.

6.7.4 Renovación con regeneración de la clave de la TSU

Las claves de la TSA de Izenpe deben ser reemplazadas antes de la expiración del certificado si el algoritmo, longitud de clave o cualquier otra medida de seguridad deja de ser considerado fiable por la industria. En cualquier caso, se regenerarán las claves y se emitirá un nuevo certificado cada dos años.

6.7.5 Fin del ciclo de vida de la clave de la TSU

La TSA de Izenpe no permite firmar respuestas timestamp con un certificado caducado o revocado. En el caso de finalización de servicios de la TSA de Izenpe, todas las claves privadas de los certificados de la TSA incluyendo copias de seguridad serán destruidas de forma que dichas claves sean irrecuperables.

6.7.6 Gestión del ciclo de vida del módulo criptográfico usado para firmas los sellos de tiempo

Izenpe establece procedimientos para garantizar que los servicios de no repudio de los módulos de seguridad de hardware (HSM) no son manipulados durante el envío y almacenamiento.

La instalación y activación de las claves de firma contenidas en el hardware criptográfico es realizado únicamente por el personal con roles de confianza. Operación, procedimientos y gestión de ciclo de vida de los HSM están descritos en documentación interna de Izenpe.

6.7.7 Compromiso de la clave privada del certificado de TSA

En caso de compromiso de una clave privada del servicio TSA de Izenpe se aplicará el procedimiento indicado en el punto 5.7.3 *Procedimiento ante compromiso de una clave privada* de la DPC, así como, lo indicado en el punto *8.4 Servicio VA/TSA del Plan de Contingencia*, entre otros:

- No se emitirán tokens timestamp.
- En el caso de comprometerse la precisión mínima de +/- 1 segundo definida no se emitirán sellos de tiempo hasta que se corrija la calibración.

La TSA garantiza que en caso de que se produzca un evento de seguridad en los servicios de sellado de tiempo, incluyendo el compromiso de su clave privada o la pérdida de calibración respecto a la UTC, informará a los suscriptores y las terceras partes en la página web de Izenpe.

Existen procedimientos específicos de contingencia para los sistemas de TSA, que garantizan la recuperación de las operaciones y la respuesta ante compromisos de claves de TSU y pérdida de sincronismo.

En caso de un compromiso al menos IZENPE:

- Informará a los suscriptores y usuarios del compromiso.
- Revocará el certificado de TSA/TSU y publicará la correspondiente lista de revocación.
- Planificará la generación de un nuevo certificado de TSA para evitar la pérdida de servicio, siempre que no existan problemas de seguridad para ello.
- Investigará las causas del compromiso y tomará medidas adecuadas para evitar que se repitan.

En caso de una pérdida de sincronización, al menos IZENPE:

- Parará la emisión de sellos de tiempo.
- Informará a los suscriptores y usuarios de la pérdida de sincronismo.
- Re-establecerá el servicio lo más rápidamente posible

6.7.8 Finalización de la TSA

La terminación de la TSA de Izenpe se realizará según los procedimientos definidos en el apartado3.8 Cese de la TSA del documento PR_G_Plan_de_Cese_de_Servicios_de_Izenpe.

6.8 Sellado de tiempo

6.8.1 Fuente de tiempo empleada para la prestación del servicio

Izenpe obtiene el tiempo de sus sistemas de una conexión al Real Observatorio de la Armada (ROA) siguiendo el protocolo NTP a través de la conexión establecida con el Gobierno Vasco. La descripción del protocolo NTP se puede encontrar en el estándar de IETF RFC 5905.

Basándose en este servicio interno, Izenpe ofrece un servicio de sellado de tiempo (TSA) que puede ser utilizado para crear sellos de tiempo sobre documentos arbitrarios, según IETF RFC 3161.

6.8.2 Perfil de una petición de sello de tiempo

- La petición de sello de tiempo deberá seguir la estructura definida en IETF RFC 3161.
- La petición debe seguir las indicaciones de ETSI TS 101 861.
- Los algoritmos de hash soportados son: md2; md5; sha256; sha1; sha384; sha512. Siendo los SHA1 y SHA256 los más indicados. En cualquier caso, Izenpe sigue las recomendaciones de la industria en cuanto a suites criptográficas.

6.8.3 Perfil del certificado de la TSA

Los datos de creación de firma de la TSA están vinculados al siguiente Certificado:

EXTENSION ATTRIBUTE	VALUE	COMMENT
Subject	CN = tsa.izenpe.com 2.5.4.97 = VATES-A01337260 O = IZENPE S.A. C = ES	
Issuer Name	CN = SUBCA QC IZENPE - TSA 2.5.4.97 = VATES-A01337260 O = IZENPE S.A. C = ES	
Key Usage	Firma digital (80)	
Extended Key Usage	Impresión de fecha (1.3.6.1.5.5.7.3.8)	
Subject key Identifier	<key identifier of this CA's public key>	
Authority key identifier	<key identifier of the issuing CA's public key>	
CRL Distribution Point	http://crl.izenpe.eus/cgi-bin/izenpeTSA	URLs of the CRL Distribution points
Certificate Policy	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.14777.10.1 [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.izenpe.eus/cps [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado	
Subject Information Access	[1]Acceso a información de autoridad Método de acceso=Método de acceso desconocido (1.3.6.1.5.5.7.48.3) Nombre alternativo: Dirección URL=http://tsa.izenpe.eus/	

6.8.4 Perfil del token de sello de tiempo

- Para el protocolo de sello de tiempo se siguen las normas IETF RFC 3161 y RFC 5816.
- Para el perfil de sello y políticas se siguen las normas ETSI EN 319 421 (Policy and Security Requirements for Trust Service Providers issuing Time-Stamps) y ETSI EN 319 422 (Time-stamping protocol and time-stamp token profiles).
- Todos los tokens de sellado de tiempo emitidos por Izenpe incluyen el objeto identificador de política (OID) 1.3.6.1.4.1.14777.300.1.
- Todos los tokens de sellado de tiempo emitidos por Izenpe incluyen el certificado Timestamp empleado para firmar el token.
- El certificado que se utiliza para firmar está generado con sha256WithRSAEncryption, con longitud de clave de 4096 bits, y es de uso exclusivo para el servicio de TSA.
- El algoritmo hash del token es SHA-256.

6.8.5 Sincronización del reloj con UTC

- La TSA de Izenpe utiliza su propio servidor de tiempo, el cual está sincronizado con el ROA (Real Observatorio de la Armada).
- Existen controles para detectar cambios en la calibración y/o problemas de sincronización que puedan comprometer la precisión definida.
- La TSA asegura la precisión de tiempo compatible con las normas de precisión de tiempo UTC mínimos de +/- 1 segundo. La Izenpe TSA no emitirá tokens de sello de tiempo si la precisión de tiempo no está asegurada
- La TSA de Izenpe asegura el correcto tratamiento de los segundos intercalares durante el último minuto del día en el que está planificado el ajuste.

6.9 Seguridad física y ambiental

Izenpe asegura la seguridad física y ambiental de su TSA según se define en el apartado 5. *Controles de seguridad física, de procedimiento y de personal* de la DPC.

6.10 Gestión de operaciones

La TSA de Izenpe mantiene controles apropiados de operación según directrices de ETSI EN 319 421. Estos documentos y políticas son internos y no están disponibles al público y son comprobados periódicamente por revisiones internas y externas para asegurar el cumplimiento y efectividad de estos controles.

6.11 Seguridad de red

La seguridad de red está basada en el concepto de zonificación multi-nivel utilizando múltiples firewalls redundantes. La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL/TLS.

6.12 Gestión de incidentes

Los definidos en el apartado 5.7.1 *Procedimientos de gestión de incidencias* de la DPC.

6.13 Recogida de evidencias

Los indicados en el apartado 5.*4 Audit de la DPC*.

6.14 Archivado de información relacionada con la operación de los servicios de sellado de tiempo

Los registros relacionados con la operación del servicio de sellado de tiempo son generados y almacenados de la misma forma que los registros relacionados con la operación de la Autoridad de Certificación. Los respectivos controles aseguran la integridad, confidencialidad y el archivado requerido de todos los registros según se especifica en el apartado 5.5 *Archivado de Registros* de la DPC.

Izenpe asegura que existen las medidas adecuadas para evitar el procesamiento inadecuado de sus registros.

6.15 Gestión de accesos a sistemas

La TSA de Izenpe dispone de los controles de acceso adecuados según se define en el apartado 5. *Controles de seguridad física, de procedimiento y de personal* la DPC.

6.16 Cumplimiento con los requerimientos legales

Los servicios de la TSA de Izenpe cumplen con los requerimientos de eIDAS. Izenpe asegura que se toman las medidas adecuadas para evitar el procesamiento no autorizado de datos de carácter personal. Izenpe también asegura la confidencialidad de datos personales y otra información proporcionada por usuarios a la TSA.

6.17 Organizativo

La organización que mantiene la TSA de Izenpe es la misma que mantiene las CAs subordinadas. Las medidas de seguridad organizativa, técnica y de personal están definidas en la DPC, y son conformes a otras leyes y regulaciones según se define en la presente política.