Proyecto	**Autoridad de Sellado de Tiempo (TSA)**
Título	**Declaración de Prácticas**

Realizado por	**LLEIDANET PKI S.L.**		
Dirigido a	**Usuarios internos y externos**		
Documento	**DOC-200216.20A0210**		
Fecha aprobación	**02/05/2025**	Revisión	**5**

Firmado por: Raul Gisbert Rodas
Fecha firma: 05/05/2025 9:05:49 CEST

Firmado por: PASCUAL FERRER PONCE
Fecha firma: 05/05/2025 9:22:59 CEST

ER-1140/2011 NMS-0009/2012 SI-0024/2013 ES-1140/2011

Carrer Els Traginers, 14 - 2°B
Pol. Ind. Vara de Quart
46014 Valencia
Tel. (34) 96 381 99 47
Fax (34) 96 381 99 48
info@lleida.net
www.lleida.net

Firmado por: JORDI GISBERT RODAS
Fecha firma: 05/05/2025 12:05:50 CEST

1 DATOS DEL DOCUMENTO

Proyecto	Autoridad de Sellado de Tiempo (TSA)
Título	Declaración de Prácticas
Código	DOC-200216.20A0210
Tipo de documento	DOC - Documento genérico
Clasificación del documento	Público
Realizado por	LLEIDANET PKI S.L.
Dirigido a	Usuarios internos y externos
Fecha aprobación	02/05/2025
Revisión	5

2 HISTORIA DEL DOCUMENTO

Revisión	Fecha	Motivo de la modificación	Responsable
1	02/10/2020	Creación del documento	Indenova SL (SBS)
2	26/02/2021	Ingresar tipos de algoritmos soportados	Indenova SL (CJU)
3	24/05/2021	Actualización del documento	Indenova SL (CJU)
4	31/05/2021	Actualización por la nueva jerarquía: OID para el servicio de la TSA. Las características de la subordinada de Sellado de Tiempo de Indenova y la TSU de Indenova.	Indenova SL (CJU)
5	02/05/2025	Se ajusta el apartado de Conformidad Se actualiza la denominación a Lleidanet PKI S.L.	Lleidanet PKI (CJ)

3 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Nombre: Compliance (CJ) Cargo: Responsable de Calidad Fecha: 02/05/2025
Revisado por:	Nombre: Lleidanet PKI SL (SB) Cargo: Administrador del Servicio Fecha: 02/05/2025
Aprobado por:	Nombre: Comisión de Seguridad de la Información Cargo: Comisión de Seguridad de la Información Fecha: 02/05/2025

4 INTRODUCCIÓN

Lleidanet PKI S.L.U. es una empresa con domicilio en España que brinda servicios de certificación digital, software de firma digital, servicios de intermediación digital, así como servicios de emisión de Sellos de Tiempo (Timestamp), conformes a la regulación vigente.

Lleidanet PKI S.L.U. es una empresa trasnacional que nació con vocación de desarrollar, innovar y generar soluciones tecnológicas TIC en el ámbito empresarial e institucional. Está especializada en soluciones de firma electrónica, securización de archivos y comunicaciones y cifrado de datos, criptografía, movilidad, certificados digitales y procedimientos electrónico, invirtiendo en el desarrollo e implantación de las mismas el 95% de su actividad.

Como Autoridad de Sellado de Tiempo - TSA, Lleidanet PKI S.L.U. provee los servicios de emisión de sellado de tiempo, utilizando una infraestructura periódicamente auditada para cumplir la certificación ISO 27001.

Junto a los servicios de certificación digital, Lleidanet PKI S.L.U. brinda los servicios de registro o verificación de sus clientes, tanto en el caso de personas jurídicas como naturales.

El planteamiento es ofrecer una oferta diferenciada, generadora de soluciones y servicios innovadores, con el objetivo de crear valor. Para ello combinamos un alto grado de conocimiento de los directivos y profesionales, con su amplia experiencia en certificados digitales y firma electrónica para eCommerce y eAdministración y el uso de tecnología avanzada.

Nuestros SERVICIOS están dirigidos a la Administración Electrónica y Comercio electrónico y, en general, para proyectos de “oficina sin papeles”, tiene como componente central la Plataforma eSigna®, a partir del cual se apoyan el resto de nuestros productos y soluciones, entendidos como módulos independientes y a su vez interconectados, según las necesidades del proyecto a implantar.

5 RESPONSABILIDADES

Lleidanet PKI S.L.U. asume las responsabilidades de representación de los servicios de sello de tiempo, a fin de ejecutar las garantías y cláusulas contractuales con los clientes. En tal sentido establece y garantiza el cumplimiento de los niveles de servicio y requerimientos contractuales acordados con cada cliente.

6 DEFINICIONES Y ABREVIACIONES

6.1 DEFINICIONES

Tercero que confía	Persona natural o jurídica que recibe un documento con un sello de tiempo y confía en la validez de dicho sello provisto por la TSA de Lleidanet PKI S.L.U.
Suscriptor	Persona natural o jurídica que requiere los servicios provistos por una Autoridad emisora de sellos de tiempo – TSA y que está de acuerdo con los acuerdos y obligaciones descritos en la Declaración de Prácticas y la Política de Sellado de Tiempo.
Política de sellado de tiempo	Conjunto de directivas que dirigen la aplicabilidad y requisitos en la administración de un servicio de sello de tiempo para una determinada comunidad de usuarios y un determinado alcance.
Sello de tiempo	Conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez. El sello de tiempo incluye: - La firma digital de la entidad de sellado de tiempo - Identificador electrónico único del documento (HASH o resumen) - Fecha y hora recogida de una fuente fiable de tiempo
Autoridad de Sellado de tiempo	Autoridad que emite los sellos de tiempo, en los cuales confían los suscriptores y terceros que confían.
Declaración de Prácticas	Conjunto de declaraciones acerca de políticas y prácticas que dirigen las actividades y procesos de la TSA y que son publicadas para conocimiento de suscriptores y terceros que confían.
Sistemas de la TSA	Sistemas de tecnologías de la información que soportan l provisión de servicios de sellado de tiempo. Componentes de hardware y software que son administrado como una unidad para proveer sellos de tiempo desde un fuente de tiempo.
Unidad de Sellado de tiempo	Componentes de hardware y software que son administrados como una unidad para proveer sellos de tiempo desde una fuente de tiempo.

6.2 ABREVIACIONES

BIPM	International Bureau of Weights and Measures (Bureau International Des Poids et Mesures
GMT	Greenwich Mean Time
IERS	International Earth Rotation Service
TAI	International Atomic Time (Temps Atomique international)
TSA	Time-Stamping Authority
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

7 PARTICIPANTES

7.1 AUTORIDAD DE SELLADO DE TIEMPO DE LLEIDANET PKI S.L.U. (TSA LLEIDANET PKI S.L.U.)

Lleidanet PKI S.L.U., en su papel de Autoridad de Sellado de Tiempo, es la persona jurídica privada que presta indistintamente servicios de emisión de sellados de tiempo.

7.2 PROVEEDOR DEL CERTIFICADO DIGITAL (EC LLEIDANET PKI S.L.U.)

Los servicios de sellado de tiempo son provistos en la infraestructura y bajo la administración de Lleidanet PKI S.L.U.. El certificado digital es provisto por la EC Lleidanet PKI S.L.U., es una Entidad de Certificación autorizada por el Organismo supervisor. Como parte de la cobertura de seguridad del certificado digital de sellado de tiempo, Lleidanet PKI S.L.U. ampara las transacciones de sellado de tiempo mediante la cobertura del Seguro de Responsabilidad Civil.

8 POLÍTICA DE SELLADO DE TIEMPO

Lleidanet PKI S.L.U. gestiona las actividades de sellado de tiempo conforme con la RFC 3628.

9 IDENTIFICACIÓN

La Política de Sellado de Tiempo de Lleidanet PKI S.L.U. tiene como identificador único:

1.3.6.1.4.1.49959.1.1.5.3

9.1 CERTIFICADO SUBORDINADA SELLADO DE TIEMPO LLEIDANET PKI S.L.U.

El DN del 'issuer name' del certificado de la subordinada de sellado de tiempo de Lleidanet PKI S.L.U., tiene las siguientes características:

CN = Certification Authority Root Indenova SL

O = Indenova SL

SERIALNUMBER = B97458996

OU = Certification Authority Indenova SL

L = Valencia

C = ES

En el DN del 'subject name' se incluyen los siguientes campos:

Description = inDenova SL Timestamping Certificate 003

CN = inDenova TSA 003

O = inDenova SL

2.5.4.97 = VATES-B97458996

SERIALNUMBER = B97458996

OU = Trusted Timestamp Service inDenova SL

T = Service Timestamping inDenova SL

L = VALENCIA

C = ES

Número de serie = 56 DE 6C 77 1D 42

Huella digital = BC 38 04 88 EB 44 6C 18 4A 56 E6 56 23 12 E0 A9 1D 92 8B 73

SHA-256 = 63889399BF34E7A5C21CFE81F3B893AB5BE9EA7303D69C877433E0FF94740252

9.2 CERTIFICADO TSU LLEIDANET PKI S.L.U.

El DN del 'issuer name' del certificado de la TSU de Lleidanet PKI S.L.U., tiene las siguientes características:

Description = inDenova SL Timestamping Certificate 003

CN = inDenova TSA 003

O = inDenova SL

2.5.4.97 = VATES-B97458996

SERIALNUMBER = B97458996

OU = Trusted Timestamp Service inDenova SL

T = Service Timestamping inDenova SL

L = VALENCIA

C = ES

En el DN del 'subject name' se incluyen los siguientes campos:

Description = inDenova SL Timestamping Certificate 003

CN = inDenova TSU 003

O = inDenova SL

2.5.4.97 = VATES-B97458996

SERIALNUMBER = B97458996

OU = Trusted Timestamp Service inDenova SL

T = Service Timestamping inDenova SL

L = VALENCIA

C = ES

Número de serie = 33 84 4E 4D 5A C4

Huella digital = 0D 43 07 3A E0 FD 71 02 91 35 35 64 A8 90 15 36 C5 F3 57 A7

SHA-256 = C516FB49B01CCB2ACBE337AD13D29CC98A59788E81B549B36D8915AD61378386

10 COMUNIDAD DE USUARIOS Y APLICABILIDAD

Lleidanet PKI S.L.U. no limita la comunidad de usuarios de los servicios de sellado de tiempo, estos pueden ser personas jurídicas del sector privado o estatal que deseen utilizar los sellos de tiempo y que estén de acuerdo con su Declaración de Prácticas y su Política de Sellado de Tiempo.

11 OBLIGACIONES Y RESPONSABILIDAD

Lleidanet PKI S.L.U. asegura que los sistemas, personas y procesos que conforman los servicios de sellado de tiempo, cumplan con los requerimientos definidos en la RFC 3628, verificando su cumplimiento con periodicidad.

En este sentido, Lleidanet PKI S.L.U. se hace responsable de cumplir con las obligaciones contractuales y niveles de servicio, las cuales se especifican en los términos y condiciones (https://www.indenova.com/acreditaciones/eidas/), acordados con cada cliente.

Asimismo, Lleidanet PKI S.L.U. no es responsable de publicar las prácticas y políticas de los terceros proveedores de los servicios de sellado de tiempo.

12 OBLIGACIONES DE LA TSA EN RELACIÓN A LOS SUSCRIPTORES

Lleidanet PKI S.L.U. entregará los servicios con la confiabilidad y exactitud establecida en los respectivos contratos, en las respectivas políticas de sellado de tiempo y en la presente Declaración de Prácticas.

13 OBLIGACIONES DE LOS SUSCRIPTORES

Es responsabilidad de los suscriptores utilizar una aplicación de software, que realice las peticiones e interprete las respuestas conforme al formato establecido en la RFC 3161, las verificaciones del estado del certificado, así como realizar la correcta configuración de la hora local en estas aplicaciones.

La emisión de sellos de la TSA de Lleidanet PKI S.L.U. es conforme al protocolo y el perfil definido en la norma ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

Petición de un sello de tiempo El cliente debe realizar las peticiones de sello de tiempo de acuerdo con la estructura definida en el RFC 3161.

El protocolo para el envío de la petición de sello de tiempo al servicio será HTTP o HTTPS de acuerdo con la definición del apartado 3.4 del RFC 3161.

14 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Los terceros que confían son responsables de verificar que los documentos sean firmados con un sello de tiempo, con un certificado digital reconocido por Lleidanet PKI S.L.U. y que estos sellos tengan como parte de su número de identificación el OID.

Asimismo, deben verificar que el certificado de sello de tiempo se encuentra firmado y que la clave privada no estuvo comprometida en el momento en el que se realizó el sellado de tiempo.

15 REQUERIMIENTOS EN LAS PRÁCTICAS DE LA TSA

Lleidanet PKI S.L.U. cumple los requerimientos de la RFC 3628, conforme a lo exigido en la legislación vigente de Entidades de Valor Añadido.

15.1 DECLARACIÓN Y PUBLICACIÓN DE PRÁCTICAS

Lleidanet PKI S.L.U. demuestra que cuenta con la confiabilidad necesaria para proveer los servicios de sellado de tiempo a sus clientes, a través del sometimiento de sus servicios a la evaluación provista por el organismo supervisor.

La infraestructura de software y hardware utilizados en los servicios de emisión de sellos de tiempo son provistos por Lleidanet PKI S.L.U., cuya infraestructura y administración es rigurosamente evaluada por las auditoría para el logro de la certificación ISO 27001. Asimismo, el certificado de sellado de tiempo.

16 CONDICIONES Y TÉRMINOS DE USO

Las condiciones y términos de uso de los servicios de sellado de tiempo para todos los suscriptores y terceros corresponden serán definidos con cada cliente en los contratos con los suscriptores.

Será responsabilidad del suscriptor difundir, conforme corresponda en términos de confidencialidad, las condiciones adicionales que sean establecidas en el contrato, a toda la comunidad de usuarios que defina para el uso de los servicios contratados.

17 APROBACIÓN DEL DOCUMENTO DE DECLARACIÓN DE PRÁCTICAS

La presente Declaración de Prácticas y las Políticas de Sellado de Tiempo, son aprobadas y reconocidas por la Comisión de Seguridad de Lleidanet PKI S.L.U. y su cumplimiento es supervisado por la autoridad máxima dentro de la TSA.

18 EVALUACIÓN DE CUMPLIMIENTO

Lleidanet PKI S.L.U., como Autoridad emisora de sellos de tiempo, se somete a auditorías periódicas por parte del Organismo de evaluación de la conformidad. A su vez, Lleidanet PKI S.L.U., y del estándar ISO 27001 para su infraestructura de sellado de tiempo.

19 NOTIFICACIÓN DE CAMBIOS

Lleidanet PKI S.L.U. notificará los cambios realizados a este documento a los suscriptores, terceros que confían y demás interesados en sus servicios de sellado de tiempo, y publicará las nuevas versiones en su sitio web (https://www.indenova.com/acreditaciones/eidas/).

20 INFORMACIÓN DE CONTACTO

Autoridad de Sellado de Tiempo:

Nombre: Lleidanet PKI S.L.U.
Dirección: Carrer Dels Traginers, 14 - 2° B C.P 46014, Valencia, España
Tel: (+34) 96 381 99 47
Correo electrónico: consultas@indenova.com
Página Web: www.indenova.com

21 LIMITACIONES DE USO

Las limitaciones de uso de los servicios de sellado de tiempo serán definidos en los términos y condiciones (https://www.indenova.com/acreditaciones/eidas/), acordados con cada cliente.

22 VERIFICACIÓN DE LA CONFIABILIDAD DE UN CERTIFICADO

Para verificar la confiabilidad de un sello de tiempo, el tercero que confía deberá verificar si el certificado digital utilizado estuvo vigente y no revocado en la fecha en la que se realizó la firma, así como si el certificado utilizado ha sido firmado a su vez por una Entidad Certificadora con reconocimiento legal en el país. Además, el tercero que confía deberá verificar que el sello contiene el objeto identificador OID de la respectiva política.

23 CONTEXTO Y OBLIGACIONES LEGALES

A fin de obtener el reconocimiento legal de sus sellos de tiempo, Lleidanet PKI S.L.U., como Autoridad emisora de sellos de tiempo, cumple los requerimientos establecidos en la legislación vigente.

24 LIMITACIONES DE RESPONSABILIDAD

Lleidanet PKI S.L.U. no se hace responsable por los casos de fraude y suplantación de sellos de tiempo que no contengan el identificador único de la Política de Sellado de Tiempo y la firma digital de los sellos de tiempo firmados por la raíz de Lleidanet PKI S.L.U.

Asimismo, Lleidanet PKI S.L.U. no se hace responsable de horas locales mal configuradas en el software de los usuarios de los clientes.

25 PROCEDIMIENTOS PARA LA SOLUCIÓN DE RECLAMOS Y CONTROVERSIAS

Los procedimientos para la solución de reclamos y controversias serán definidos con cada cliente, en su respectivo contrato.

26 DECLARACIÓN DE NIVELES DE DISPONIBILIDAD DEL SERVICIO Y TIEMPO DE RESPUESTA

El servicio de sellado de tiempo tiene una disponibilidad permanente las 24 horas durante todos los días del año.

Lleidanet PKI S.L.U. realizará todos los esfuerzos necesarios para que el servicio nunca se encuentre inaccesible de forma continua más de 24 horas, siendo este un servicio crítico de Lleidanet PKI S.L.U. y por lo tanto tratado de forma adecuada en el Plan de contingencias y de continuidad de negocio.

27 PROVISIONES PARA LA RECUPERACIÓN DEL SERVICIO EN CASO DE DESASTRES

Lleidanet PKI S.L.U. implementa controles de contingencia en caso de falla de equipos, corrupción de información, interrupción de comunicaciones, y demás eventos operacionales conforme a la RFC 3628.

En el caso de compromiso de la clave privada de la TSA o si la exactitud de desviación del tiempo UTC es mayor que +/- 1, no serán emitidos sellos de tiempo.

En el caso de eventos que puedan afectar la seguridad de los servicios de sellado de tiempo, como compromiso de la clave o pérdida de sincronización fuera de los niveles de desviación permitidos, la información relevante será comunicada a los suscriptores mediante correo electrónico por parte de Lleidanet PKI S.L.U. En el caso de compromiso, o sospecha de compromiso o pérdida de calibración, se pondrá a disposición de los suscriptores y terceros que confían la información que permita identificar los sellos de tiempo afectados, a menos que esto viole la privacidad de los usuarios o la seguridad de los servicios de la TSA.

28 CICLO DE VIDA DE LA GESTIÓN DE LA CLAVE

28.1 GENERACIÓN DE LA CLAVE DE LA TSA

La generación de la clave privada del certificado digital con el cual se firman los sellos de tiempo es realizada en un ambiente físico seguro (conforme a la sección 7.4.4 de la RFC 3628), por personal confiable (sección 7.4.3 de la RFC 3628) bajo, al menos, autorización de dos personas.

La generación de la clave privada se realiza en un módulo hardware de seguridad – HSM con certificaciones FIPS 140-2 nivel 3 o Common Criteria EAL 4+ y su administración es protegida por al menos dos personas.

28.2 CARACTERÍSTICAS TÉCNICAS DEL CERTIFICADO DIGITAL Y DE LOS ALGORITMOS UTILIZADOS

Las características del certificado digital y de los algoritmos utilizados en los servicios de sellado de tiempo son: SHA-1, SHA-256, SHA-384, SHA-512. Se desaconseja a sus subscriptores el uso de SHA-1 como algoritmo de resumen, que se mantiene por motivos de compatibilidad.

28.3 PROTECCIÓN DE LA CLAVE PRIVADA DE LA TSA

La clave privada del certificado de firma de cada sello de tiempo es resguardada durante su uso dentro de un módulo hardware criptográfico con certificación FIPS 140-2 nivel 3. Las copias de respaldo se almacenan en un módulo criptográfico del mismo nivel de seguridad.

28.4 DISTRIBUCIÓN DE LA CLAVE PÚBLICA TSU

La clave pública está contenida dentro de un certificado X.509 v3, firmada digitalmente por una Entidad de Certificación Digital de Lleidanet PKI S.L.U. regulada por su Declaración de Prácticas.

28.5 RE-EMISIÓN DE LA CLAVE DEL TSU

La clave privada de la TSA será reemplazada antes de la expiración de su periodo de validez y en caso de obsolescencia o vulnerabilidad declarada del algoritmo, el tamaño de la clave u otra medida de seguridad relevante.

28.6 ALMACENAMIENTO DE LOS REGISTROS DE AUDITORÍA

Los registros concernientes a la operación del servicio de sellado de tiempo, incluyendo eventos relacionados a la sincronización del reloj con la fuente confiable de tiempo y la gestión de las claves de la TSA son salvaguardados contra modificación no autorizada.

Los registros son almacenados y protegidos por un periodo de 1 año adicional al periodo de vigencia del certificado digital con el que el sello de tiempo fue creado. En caso de que la clave privada de la TSA se vea comprometida, entonces el periodo de almacenamiento de registros será mayor que los sellos de tiempo más afectados.

28.7 TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA DEL TSU

Las claves privadas con las cuales se firman los sellos de tiempo reconocidos por Lleidanet PKI S.L.U., no serán usadas luego de terminado su ciclo de vida sino que será emitida una nueva clave y puesta en operación, realizando el cambio de un certificado digital por otro, incluyendo la generación segura y la publicación del nuevo certificado.

La clave de la TSA que ha expirado o ha sido revocada o cualquier parte de ella, incluyendo cualquier copia será destruida de modo que no pueda ser recuperada.

29 GESTIÓN DEL CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO USADO PARA FIRMAR LOS SELLOS DE TIEMPO

Los módulos hardware criptográficos que se utilizan para almacenar y proteger las claves privadas con las cuales se firman los sellos de tiempo reconocidos por Lleidanet PKI S.L.U., son protegidos contra manipulación no autorizada durante todo su ciclo de vida, incluyendo transporte, generación de la clave, uso y almacenamiento.

La instalación, activación y duplicación de las claves de la TSU en el hardware criptográfico sólo puede ser realizada por el personal que tiene asignado un rol de confianza, usando al menos un control dual en un ambiente físico seguro (conforme a la sección 7.4.4 de la RFC 3628) con control de acceso físico de al menos dos personas.

Se monitoreará el funcionamiento correcto del hardware criptográfico.

En los casos que se decida desechar el equipo las claves privadas de la TSA serán borradas para evitar su uso no autorizado. Considerando el respaldo seguro de la clave si aún se encuentra vigente.

30 SELLO DE TIEMPO

Los sellos de tiempo cumplen lo siguiente:

- Los sellos de tiempo son conformes a la RFC 3161.
- Se utiliza un servicio de sincronización a la fuente de tiempo confiable.
- El sello de tiempo incluye un identificador de la política de sello de tiempo, en concordancia con la TSA.
- Cada sello de tiempo tiene asignado un único identificador.
- El tiempo incluido en el sello de tiempo será sincronizado con la UTC dentro de la exactitud de +/- 1 segundo.
- El sello de tiempo incluye un resumen de los datos firmados (HASH).
- El sello de tiempo deberá ser firmado por una clave generada para este propósito, correspondiente a la TSA.
- Si se detecta que el reloj del proveedor del sello de tiempo se encuentra fuera de la precisión indicada los sellos de tiempo no deben emitirse.

30.1 EMISIÓN DE SELLOS DE TIEMPOS

La emisión de sellos de la TSA de Lleidanet PKI S.L.U. es conforme al protocolo y el perfil definido en la norma ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

30.2 PETICIÓN DE UN SELLO DE TIEMPO

El cliente debe realizar las peticiones de sello de tiempo de acuerdo con la estructura definida en el RFC 3161 [6].

El protocolo para el envío de la petición de sello de tiempo al servicio será HTTP o HTTPS de acuerdo con la definición del apartado 3.4 del RFC 3161 [6].

Los algoritmos de resumen criptográfico aceptados por la TSA de Lleidanet PKI S.L.U. son: SHA-256, SHA512 y SHA-1. Lleidanet PKI S.L.U. desaconseja a sus subscriptores el uso de SHA-1 como algoritmo de resumen, que mantiene por motivos de compatibilidad.

30.3 RESPUESTA A UNA PETICIÓN DE SELLO DE TIEMPO

Los sellos de tiempo generados por la TSA se adecuan al perfil definido en el apartado 5.2 de ETSI EN 319 422 [5].

El algoritmo de resumen de los sello de tiempo es SHA-256.

El algoritmo de firma del sello de tiempo es sha256WithRSAEncryption.

El sello de tiempo incluye una extensión del tipo qcStatements con la declaración esi4qtstStatement-1 de acuerdo el apartado 9.1 de ETSI EN 319 422 para indicar que el sello de tiempo es cualificado.

El sello de tiempo incluye el certificado electrónico de la clave pública de firma de la TSU.

30.4 PERFIL DEL CERTIFICADO

El certificado de la TSU está emitido por la entidad de certificación “Lleidanet PKI S.L.U.”.

La duración del certificado es de 5 años.

31 SINCRONIZACIÓN DEL RELOJ CON LA UTC

Lleidanet PKI S.L.U. adopta medidas para asegurar que su reloj es sincronizado con la UTC dentro de la exactitud declarada:

- La calibración de los relojes será monitoreada y mantenida de modo que no se desvíen de la precisión de +/- 1 segundo. Protegiendo el reloj de la TSU contra amenazas que podrían provocar un cambio no detectable luego de la calibración. Y monitoreando la exactitud declarada, para detectar cualquier desviación.

- En caso de desviación los terceros que confían afectados serán informados mediante una publicación en la página web de Lleidanet PKI S.L.U. o mediante correo electrónico a todos los clientes del servicio, a fin de que estos comuniquen a los terceros que confían.
- Cuando un cambio en el tiempo sea notificado por una autoridad competente, los respectivos cambios serán realizados el último minuto del día cuando el cambio en el tiempo haya sido planificado para ocurrir. En este escenario se mantendrá un registro del tiempo exacto (dentro de la exactitud declarada) y será notificado a los terceros que confían mediante una publicación en la página web de Lleidanet PKI S.L.U. o mediante correo electrónico a todos los clientes del servicio, a fin de que estos comuniquen a los terceros que confían.

32 GESTIÓN DE LA SEGURIDAD

Lleidanet PKI S.L.U. implementa un Sistema de Gestión de Seguridad de la Información y adopta medidas de seguridad conforme a la certificación ISO 27001.

33 POLÍTICA DE PRIVACIDAD

Puesto que los servicios de sellado de tiempo son independientes de los usuarios finales, y la única información recabada es la definida en la RFC 3161, Lleidanet PKI S.L.U. no recogen información privada de personas naturales ni de sus clientes, en lo que respecta a servicios de sellado de tiempo.

34 TÉRMINO DE LA TSA

Lleidanet PKI S.L.U. adopta medidas para asegurar que las interrupciones potenciales a los suscriptores y terceros que confían sean minimizadas, en particular asegurar el mantenimiento continuo de la información requerida para verificar los sellos de tiempo. Antes de que Lleidanet PKI S.L.U. termine sus servicios, se adoptarán las siguientes medidas:

- Se pondrá a disponibilidad de todos los suscriptores y terceros que confían la información concerniente a su terminación.
- Se concluirán los permisos de autorización de funciones de todos los subcontratados para actuar en nombre de la TSA, respecto de la emisión de los sellos de tiempo.
- Se transferirán las obligaciones a los terceros que confían de mantener los registros de eventos y archivos auditables necesarios para demostrar la correcta operación de la TSA por un periodo razonable.
- Se mantendrán o transferirán a los terceros que confían sus obligaciones de hacer disponible su clave pública o su certificado por un periodo razonable.
- La clave privada de la TSU, incluyendo copias, será destruida de manera segura de modo que no pueda ser recuperada.

- La TSA celebrará acuerdos para cubrir los costos de cumplir con estos requisitos mínimos, en caso de que la TSA se declara en quiebra o por otras razones es incapaz de cubrir los costos por sí mismo.
- Se tomarán medidas para que los certificados de los TSU sean revocados.

35 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

35.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

El cumplimiento de los controles que garanticen la seguridad en la emisión de los sellos de tiempo se evaluará por medio de una Auditoria anual realizada por una firma de auditoría reconocida y la certificación ISO 27001.

36 OTROS ASUNTOS LEGALES Y COMERCIALES

36.1 TARIFAS

37 Tarifas de emisión de sellado de tiempo

Las tarifas serán definidas por Lleidanet PKI S.L.U. de acuerdo a los contratos celebrados con sus clientes.

38 Tarifas de otros servicios

Una vez se ofrezcan otros servicios por parte de Lleidanet PKI S.L.U., se publicarán en la dirección www.indenova.com

39 Política de reembolso

Las políticas de reembolso serán definidas por Lleidanet PKI S.L.U. de acuerdo a los contratos celebrados con sus clientes.

40 RESPONSABILIDADES FINANCIERAS

40.1 COBERTURA DEL SEGURO

El seguro cubre todos los perjuicios contractuales y extracontractuales de los titulares clientes de Lleidanet PKI S.L.U., que confían exenta de culpa derivados de errores y omisiones, o de actos de mala fe

de los administradores, representantes legales o empleados de la Entidad de Certificación Lleidanet PKI S.L.U. en el desarrollo de las actividades para las cuales cuenta con autorización.

La cobertura de seguro es internacional y protege a los titulares clientes de Lleidanet PKI S.L.U..

41 DERECHOS DE PROPIEDAD INTELECTUAL

Se prohíbe la reproducción, divulgación, comunicación pública y transformación de cualquiera de los elementos contenidos en la presente Declaración de Prácticas, que son propiedad exclusiva de Lleidanet PKI S.L.U., sin su autorización expresa.

42 CUMPLIMIENTO DE REQUERIMIENTOS LEGALES

Lleidanet PKI S.L.U., como Autoridad emisora de sellos de tiempo, cumple los requerimientos establecidos en la cumple los requerimientos establecidos en la legislación vigente.

Lleidanet PKI S.L.U. no recoge información personal de los usuarios (personas naturales) de los servicios de sellado de tiempo.

Lleidanet PKI S.L.U., se debe someter a procesos de auditoría periódica por parte del organismo de evaluación de la conformidad para el mantenimiento de la acreditación de la TSA.

43 REVISIÓN, ACTUALIZACIÓN Y PUBLICACIÓN DEL PLAN

La Política de Seguridad, Política de Privacidad y la Política de Sellado de tiempo de la TSA serán revisados y actualizados al menos una vez por año.

Así mismo, se publicará en la web de Lleidanet PKI S.L.U. dicho documento para conocimiento público (https://www.indenova.com/acreditaciones/eidas/).

44 RESPONSABILIDADES

Lleidanet PKI S.L.U. asume las responsabilidades de representación de los servicios de sello de tiempo, a fin de ejecutar las garantías y cláusulas contractuales con los clientes. En tal sentido establece y garantiza el cumplimiento de los niveles de servicio y requerimientos contractuales acordados con cada cliente.

El Responsable de Seguridad de la información de Lleidanet PKI S.L.U. gestiona la implementación y vela por el cumplimiento del presente plan, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

45 CONFORMIDAD

Este documento ha sido revisado por el Administrador del Servicio y aprobado por la Comisión de Seguridad de la Información de LLEIDANET PKI S.L., y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

Dentro del organigrama, se define la estructura o comisión encargada de la implementación de la TSA y dentro de ella su política.

46 BIBLIOGRAFÍA

(1) REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 (Reglamento eIDAS)
(2) Reglamento (UE) 2016/679 (Reglamento general de protección de datos)
(3) Ley 59/2003, de 19 de diciembre, de firma electrónica.
(4) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza