Proyecto	**Servicio de Firma Centralizada**
Título	**Declaración de Prácticas SVA - Servicio de Firma Centralizada (DPSFC)**

Realizado por	**LLEIDANET PKI S.L.**		
Dirigido a	**Usuarios internos y externos**		
Documento	**DOC-200216.2140910**		
Fecha aprobación	**02/05/2025**	Revisión	**4**

Firmado por: Raul Gisbert Rodas
Fecha firma: 02/05/2025 9:59:31 CEST

Firmado por: PASCUAL FERRER PONCE
Fecha firma: 05/05/2025 9:52:09 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 12:08:46 CEST

1 DATOS DEL DOCUMENTO 4
2 HISTORIA DEL DOCUMENTO 4
3 ELABORACIÓN, REVISIÓN Y APROBACIÓN 5
4 INTRODUCCIÓN 6
5 REFERENCIAS 6
6 DEFINICIONES Y ABREVIACIONES 8
7 OBJETIVO 9
8 OBJETO DE LA ACREDITACIÓN 9
9 RELACIÓN ENTRE EL TSP Y EL SERVICIO DE FIRMA CENTRALIZADA 9
10 DISPOSICIONES GENERALES DE LA POLÍTICA Y DE LA DECLARACIÓN DE PRÁCTICAS 10
11 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO 10
12 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN 11
13 PKI PARTICIPANTES 12
13.1 ENTIDAD DE CERTIFICACIÓN LLEIDANET PKI S.L. (EC LLEIDANET PKI S.L.) 12
13.2 ENTIDAD DE REGISTRO LLEIDANET PKI S.L. (ER LLEIDANET PKI S.L.) 12
13.3 PROVEEDOR DE SERVICIOS DE FIRMA CENTRALIZADA Y (LLEIDANET PKI S.L.) 12
14 PRÁCTICAS DEL PROVEEDOR DE SERVICIOS DE CONFIANZA PARA EL SERVICIO DE CREACIÓN DE FIRMAS Y FIRMA CENTRALIZADA 14
14.1 RESPONSABILIDAD DE PUBLICACIÓN Y DEPÓSITO 14
14.2 INICIALIZACIÓN DE LAS CLAVES DE FIRMA 14
14.3 REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LAS CLAVES DE FIRMA 17
15 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 19
15.1 GENERACIÓN DE REGISTROS 19
15.2 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD 20
15.3 ARCHIVO DE REGISTROS 21
15.4 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE 21
16 CONTROLES DE SEGURIDAD TÉCNICA 21
16.1 GESTIÓN DE LOS SISTEMAS DE LA SEGURIDAD 21
16.2 OPERACIONES Y SISTEMAS 21
16.3 CONTROLES DE SEGURIDAD INFORMÁTICA. 22
17 GESTIÓN DE CICLO DE VIDA DE LAS CLAVES: (SISTEMAS AUTOMATIZADOS) 22

17.1 GENERACIÓN DE LAS CLAVES 22
17.2 PROTECCIÓN DE LA CLAVE PRIVADA 22
17.3 DISTRIBUCIÓN DE LA CLAVE PUBLICA 23
17.4 RE-EMISIÓN DE LA CLAVE 23
17.5 TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA 23
17.6 CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO 23
18 CONTROL DE CAMBIOS 24
19 POLÍTICA DE PRIVACIDAD 24
20 CONFIDENCIALIDAD DE LA INFORMACIÓN DE NEGOCIO 24
21 DERECHOS DE PROPIEDAD INTELECTUAL 25
22 POLÍTICA DE REEMBOLSO 25
23 RESPONSABILIDAD FINANCIERA, REPRESENTACIONES Y GARANTÍAS 25
24 ENMENDADURAS 26
25 RESOLUCIÓN DE DISPUTAS 26
26 ACUERDO ÍNTEGRO, SUBROGACIÓN Y DIVISIBILIDAD 26
27 FUERZA MAYOR Y OTRAS PROVISIONES 26
28 TARIFAS 26
29 FINALIZACIÓN DE LA SVA 26
30 AUDITORÍA 27
31 CONFORMIDAD CON LA LEY APLICABLE 27
32 BIBLIOGRAFÍA 27

1 DATOS DEL DOCUMENTO

Proyecto	Servicio de Firma Centralizada
Título	Declaración de Prácticas SVA - Servicio de Firma Centralizada (DPSFC)
Código	DOC-200216.2140910
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	4

2 HISTORIA DEL DOCUMENTO

Revisión	Fecha	Motivo de la modificación	Responsable
1	09/04/2021	Creación del documento.	Indenova SL (SBS)
2	31/05/2021	Nueva ceremonia de claves de la PKI	Indenova SL (SBS)
3	03/04/2024	Cambio de denominación de Indenova S.L. a Lleidanet PKI S.L.	Lleidanet PKI (CJU)
4	02/05/2025	Actualizar los roles de las personas que pertenecen a la comisión de seguridad de la información Actualizar el apartado del Procedimiento de registro de eventos de la DPC	Lleidanet PKI (CJU)

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. 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 electrónicos, invirtiendo en el desarrollo e implantación de las mismas el 95% de su actividad.

Como Prestador de Servicios de Valor añadido - SVA, Lleidanet PKI S.L. provee servicios través de la implementación de soluciones que utilizan los certificados digitales para asegurar las transacciones documentarias y de negocio de las organizaciones tanto en el sector privado como en el gubernamental. En este sentido, Lleidanet PKI S.L. provee las soluciones de software y el sistema de gestión necesarios para en conjunto regular y controlar la gestión de usuarios y el intercambio seguro de información, así como la generación y protección de registros auditables de las transacciones realizadas.

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 REFERENCIAS

[DPSFC] - Declaración de Prácticas SVA - Servicio de Firma Centralizada (DPSFC) (https://www.indenova.com/acreditaciones/eidas/)

[ETSI EN 319 401] - General Policy Requirements for Trust Service Providers

[ETSI EN 319 411-1] - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[ETSI TS 119 431-1] - TSP service components operating a remote QSCD / SCDev

[CEN EN 419 241-1]: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

Para el desarrollo de su contenido, se ha tenido en cuenta las siguientes especificaciones técnicas:

- ETSI TS 101 733 Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).

- ETSI TS 101 903 Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).

- ETSI TS 102 778 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview, Part 2: PAdES Basic - Profile based on ISO 32000-1, Part 3: PAdES Enhanced - PAdES-BES and PAdESEPES Profiles; Part 4: Long-term validation.

- ETSI TS 102 176-1 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

- ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

- ETSI TS 101 861 Time stamping profile.

- ETSI TR 102 038 Electronic Signatures and Infrastructures (SEI); XML format for signature policies.

- ETSI TR 102 041 Electronic Signatures and Infrastructures (SEI); Signature policies report.

- ETSI TR 102 045 Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.

- ETSI TR 102 272 Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP.

- IETF RFC 3125, Electronic Signature Policies.

- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).

ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

6 DEFINICIONES Y ABREVIACIONES

A las definiciones dispuestas en la DPSFC, para la interpretación del presente documento se añaden los siguientes términos y abreviaturas tal y como se definen en ETSI TS 119 431-1.

- Autenticación: un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico
- Identificación electrónica (eid): el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.
- Medios de identificación electrónica: una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.
- Referencia a medios de identificación electrónica: datos usados en el ssasc como referencia a unos medios de identificación electrónica que permiten autenticar a un firmante.
- Servicio de confianza: servicio electrónico consistente en la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo, servicios de entrega electrónica certificada y certificados de estos servicios; o la creación, verificación y validación de certificados para la autenticación de sitios web; o la preservación de firmas, sellos o certificados electrónicos.
- Proveedor de servicios de confianza (TSP): entidad que provee de servicios de confianza.
- Dispositivo cualificado de creación de firma / sello electrónico (qscd): dispositivo de creación de firma que cumple con los requisitos del anexo ii del reglamento(eu) no 910/2014.
- Dispositivo remoto de creación de firma: dispositivo de creación de firma utilizado a distancia por el firmante y operado en su nombre bajo su control exclusivo de uso.
- Componente de servicio de aplicación de firma en servidor (SSASC): componente de servicio operado por un TSP, compuesto de una aplicación de firma en servidor (SSA) y un QSCD / SCdev, empleado para la creación de firmas electrónicas en nombre del firmante.
- Proveedor de servicio de aplicación de firma en servidor (SSASP): TSP que opera un SSASC.
- Dispositivo de creación de firma (SCDev o SCD): un equipo o programa informático configurado que se utiliza para crear una firma electrónica.
- SAD Signature Activation Data SAM Signature Activation Module SAML Security Access Markup Language SCA Signature Creation Application SCAL Sole Control Assurance Level SCAL1 Sole Control Assurance Level 1
- SCASC Signature Creation Application Service Component SCDev Signature Creation Device SCS Signature Creation Service SCSP Signature Creation Service Provider SD Signer's Document SDO Signed Data Object

- SSA Server Signing Application SSASC Server Signing Application Service Component TSP Trust Service Provider

7 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza Lleidanet PKI S.L. para la administración de sus servicios como Prestador Cualificado de Servicios de Confianza, en el marco del cumplimiento de los requerimientos del "Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo" o también como es conocido "Reglamento eIDAS" establecida por el Parlamento Europeo.

8 OBJETO DE LA ACREDITACIÓN

Lleidanet PKI S.L., es un Prestador cualificado de Servicios de Confianza de conformidad con el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

Este documento contiene la Política y Declaración Prácticas Servicio de Firma Centralizada.

- La creación de firmas mediante sistemas de firma centralizada, en el cual Lleidanet PKI S.L. gestiona en nombre del firmante su dispositivo de creación de firma permitiéndole generar firmas electrónicas cualificadas asegurando el control exclusivo del firmante sobre sus claves de firma, ya sea mediante mecanismos de autenticación más OTP (usuario y password y PIN OTP), huella dactilar o mediante el uso de la APP móvil Lleidanet Wallet, de acuerdo a la especificación técnica ETSI TS 119 431-1.

El presente documento es un documento público que su contenido es de acuerdo a la especificación técnica ETSI TS 119 431-1 y define las políticas y prácticas en la provisión de los servicios de firma centralizada.

9 RELACIÓN ENTRE EL TSP Y EL SERVICIO DE FIRMA CENTRALIZADA

Lleidanet PKI S.L. es un proveedor de servicios de confianza cualificado que emite certificados y sellos electrónicos cualificados de acuerdo con la legislación vigente.

El servicio de SSASC forma parte de los servicios operados por Lleidanet PKI S.L. y permite prestar el servicio de firma electrónica centralizada a los firmantes que cuentan con un certificado electrónico definido para firma centralizada en su correspondiente Declaración Prácticas Servicio de Firma Centralizada.

En el presente documento Lleidanet PKI S.L. es identificado como el SSASP.

10 DISPOSICIONES GENERALES DE LA POLÍTICA Y DE LA DECLARACIÓN DE PRÁCTICAS

Lleidanet PKI S.L. en la prestación de su servicio de firma centralizada emplea dispositivos criptográficos de creación y protección de firmas catalogados como cualificados (QSCD) de conformidad con el 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 el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

Los HSM son operados de acuerdo con su certificación FIPS 140-2 y/o Common Criteria EAL 4+ y la solución SSASC empleada está alineada con los requisitos de seguridad definidos en la norma EN 419 241-1 para poder actuar como un Trustworthy System Supporting Server Signing (TW4S) con Sole Control Level 2 (SCAL2).

11 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Lleidanet PKI S.L. administra los documentos de Declaración de Prácticas, y todos los documentos normativos de la SVA.

Para cualquier consulta contactar:

Nombre: Lleidanet PKI S.L.
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

12 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Este documento es la "Política y Declaración Prácticas Servicio de Firma Centralizada" de Lleidanet PKI S.L.

1. Para el servicio de firma centralizada tiene asignado el OID: 1.3.6.1.4.1.49959.1.5.1
   - La política es conforme a la política "NSCP: Normalized SSASC Policy" definida en ETSI TS 119 431-1 que tiene asignado el siguiente OID: 0.4.0.19431.1.1.2.
   - La política es conforme a la política "EUSCP: EU SSASC Policy" definida en ETSI TS 119 431-1 que tiene asignado el siguiente OID: 0.4.0.19431.1.1.3.

Lleidanet PKI S.L. revisa periódicamente la conformidad de sus políticas con respecto a la especificación ETSI TS 119 431-1 y cambiará el identificador de sus políticas ante cualquier cambio en las políticas definidas en la sección 4.3.2 de dicha especificación.

La Declaración de Prácticas de Servicios de Valor Añadido de Lleidanet PKI S.L., la Política y Plan de Privacidad y otra documentación relevante son publicados en la siguiente dirección: https://www.indenova.com/acreditaciones/eidas/

Los miembros de la Comunidad Electrónica y los Usuarios de los servicios tienen la obligación comprobar regularmente los documentos declarativos correspondientes (Políticas y/o Prácticas de Certificación de aplicación), solicitando cuanta información consideren oportuna a Lleidanet PKI S.L.

No obstante, de cara a facilitar a los Usuarios destinatarios (Entidad usuaria y Suscriptor) el conocimiento de la existencia de novedades, cuando las modificaciones practicadas en cualquiera de las Declaraciones de Prácticas de Certificación y Políticas de Certificación afecten directamente a los derechos y obligaciones de las partes integrantes de la Comunidad Electrónica, o bien restrinjan el ámbito de aplicación de los Certificados, Lleidanet PKI S.L. notificará a los interesados con una antelación mínima de treinta (30) días a la entrada en vigor de los cambios, con la finalidad que los miembros de la Comunidad Electrónica adopten la decisión que a su derecho convenga. Lleidanet PKI S.L. no asumirá ningún compromiso indemnizatorio por las modificaciones o supresiones operadas en la Declaración en el ejercicio de sus derechos como Prestador de Servicios Certificación.

Las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por la Comisión de Seguridad de la SVA de Lleidanet PKI S.L. antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Los documentos referidos a la Declaración de Prácticas y Políticas de Certificación de los proveedores de Lleidanet PKI S.L., así como la Declaración de Prácticas de la SVA con las que tiene filiación serán accesibles también para las personas con discapacidad y estos serán publicados en la siguiente dirección:

https://www.indenova.com/acreditaciones/eidas/

13 PKI PARTICIPANTES

13.1 ENTIDAD DE CERTIFICACIÓN LLEIDANET PKI S.L. (EC LLEIDANET PKI S.L.)

Lleidanet PKI S.L., en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

13.2 ENTIDAD DE REGISTRO LLEIDANET PKI S.L. (ER LLEIDANET PKI S.L.)

Lleidanet PKI S.L., brinda también los servicios de Entidad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

Las funciones de ER podrán ser tercerizadas. En este caso la ER de Lleidanet PKI S.L. evaluará el cumplimiento de sus políticas realizando evaluaciones internas que determinen su cumplimiento a dicho tercero.

La ER puede tercerizar las funciones de verificación y registro sin ningún límite ni restricción, siempre dejando claro que el responsable final es la ER, siempre que se asegure la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación. Sin embargo, la responsabilidad legal frente al Organismo de supervisión, los suscriptores, titulares y terceros que confían es de la entidad solicitante de la acreditación de la Entidad de Registro. El tercero debe garantizar la seguridad y protección de los datos personales y confidenciales de la ER, así como la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, durante la ejecución de las actividades de tercerización, quedando claro que ante el Organismo de supervisión el responsable ante terceros es la ER.

Cabe indicar que Lleidanet PKI S.L. suministra al tercero la Plataforma de ER para la creación de la solicitud y la emisión de los certificados, asegurando la integridad en todo el proceso, accediendo a la plataforma eSignaPKI con el certificado digital del operador.

13.3 PROVEEDOR DE SERVICIOS DE FIRMA CENTRALIZADA Y (LLEIDANET PKI S.L.)

Lleidanet PKI S.L. actúa como proveedor del servicio de aplicación de firma centralizada (SSASP) y no delega ninguna parte del servicio a entidades terceras.

13.3.1 Titular

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos publicados en la DPC de Lleidanet PKI S.L.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por Lleidanet PKI S.L. conforme lo establecido en la Política de Certificación.

13.3.2 Suscriptor

El Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

13.3.3 Solicitante

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo la DPC de Lleidanet PKI S.L.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

13.3.4 Tercero que confía

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación Lleidanet PKI S.L. a un titular. El Tercero que confía, a su vez puede ser o no titular.

13.3.5 Entidad a la cual se encuentra vinculado el titular

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el Certificado.

13.3.6 Otros participantes

13.3.6.1 El comité de Seguridad

El comité de seguridad es un organismo interno de la Entidad de Certificación LLEIDANET PKI S.L., conformado por el Director de nuevos negocios, el Administrador del Sistema y el Director técnico y tiene entre otras funciones la aprobación de la CPS como documento inicial, así como autorizar los cambios o

modificaciones requeridas sobre la CPS aprobada y autorizar su publicación. El comité de Seguridad es el responsable de integrar la CPS, a la CPS de terceros prestadores de servicios de certificación.

14 PRÁCTICAS DEL PROVEEDOR DE SERVICIOS DE CONFIANZA PARA EL SERVICIO DE CREACIÓN DE FIRMAS Y FIRMA CENTRALIZADA

14.1 RESPONSABILIDAD DE PUBLICACIÓN Y DEPÓSITO

Véase apartado de la DPC.

14.2 INICIALIZACIÓN DE LAS CLAVES DE FIRMA

14.2.1 Generación de claves de firma

El SSASC utiliza la aplicación de firma en servidor "eSignaCrypto" en combinación con un módulo criptográfico (HSM) que actúa como SCDev / QSCD, el cual es un dispositivo cualificado de creación de firma.

El SSASC utiliza HSMs con certificación FIPS PUB 140-2 y Common Criteria EAL 4+ para realizar todas las operaciones criptográficas con las claves de los firmantes.

Las claves de los firmantes son claves RSA con una longitud de clave de 2048 bits.

Fuera del módulo HSM las claves se almacenan cifradas con el algoritmo AES y una longitud de clave de 128 bits. La clave de cifrado es única y se deriva de una clave maestra del módulo HSM y de una clave de firmante derivada o del PIN de activación que es transportado cifrado dentro del SAD.

Las operaciones de administración del módulo criptográfico requieren de control dual.

Antes de generar el certificado del firmante el par de claves del firmante no se encuentran activas en el servicio de firma centralizada y el SSA no permite su uso.

Junto a la clave del firmante se genera una petición de certificado en formato CSR o PKCS #10 que sirve como prueba de posesión de la clave privada del firmante en el proceso de registro del certificado y emisión del certificado por parte de la Autoridad de Certificación.

14.2.2 Asociación de los medios de identificación electrónica del firmante

El proceso de generación de claves se realiza durante el enrolamiento del usuario. Todo el proceso se encuentra cifrado mediante SSL y a nivel de aplicación. El proceso seguido es el siguiente:

1. El Operador de ER de Lleidanet PKI S.L. se autentica en la ER empleando su certificado electrónico.
2. A continuación, toma los datos requeridos para crear la identidad digital del usuario. La Autoridad de Registro validará la identidad del firmante de acuerdo con los requisitos establecidos en la Declaración de Prácticas de Certificación del certificado solicitado por el firmante con un nivel de garantía alto según los requisitos establecidos en UE 2015/1502.
3. Lleidanet PKI S.L. no delega el proceso de identificación y autenticación del firmante a terceras partes.
4. Una vez tomados los datos, se realiza un primer registro de la información que desencadena la creación de un token de seguridad (código único) de un solo uso, necesario para completar el proceso de generación de claves e identidad.
5. Una representación del token (código único) se envía por correo electrónico al Usuario, dependiendo del perfil empleado, representado con un código QR o código de activación. Dicho token es escaneado o introducido por el Usuario con su dispositivo móvil y la aplicación Lleidanet Wallet en el caso de firma centralizada en Lleidanet Wallet o desde un computador en el caso de firma centralizada con huella dactilar o usuario/password.
6. La aplicación solicita al Usuario que seleccione una Contraseña de seguridad que protegerá el material criptográfico. Dicha contraseña nunca viaja fuera del dispositivo móvil o computador del usuario ni se almacenará en el TSP.
7. Al elegir la Contraseña de seguridad se generan las claves criptográficas de dispositivo, un par de claves pública/privada, y se envía una solicitud a la EC para iniciar el proceso de creación de identidad. La solicitud va firmada con la clave privada y la EC verifica la solicitud y asocia la clave pública del dispositivo.
8. La EC crea las claves pública y privada de identidad del usuario en el HSM FIPS 140-2 y catalogado como QSCD, siguiendo el protocolo interno de generación del HSM. Seguidamente, se desnaturaliza la clave privada. En el caso de firmas centralizadas con el perfil de Lleidanet Wallet se crean 2 fragmentos A y B. El fragmento A se enviará cifrado al celular para que se almacene de forma segura y el fragmento B se almacena en la base de datos de la PKI cifrado con la clave maestra del servicio de firma centralizada residente en el mismo HSM. En el caso de firmas centralizadas con el perfil de Usuario/password y huella dactilar, la clave privada se cifra con esta misma clave maestra del HSM y con el PIN que introduce el usuario con cifrado AES. Finalmente, la EC devuelve los datos necesarios para crear el CSR o PKCS#10 (Certificate Signing Request), junto con el algoritmo de generación de claves y otros datos de control.
9. La identidad de firma se compone de un par de claves RSA con longitud 2048 y el certificado electrónico que vincula la clave pública a la identidad del firmante
10. Hasta la efectiva asociación del certificado con su correspondiente par de claves, la identidad de firma es incompleta y el SSASC no permitirá el uso de las claves.

11. El SAA emplea los datos para crear las claves pública y privada de identidad del usuario y generar el CSR que envía a la PKI.
12. La ER verifica el CSR y genera un certificado asociado a la solicitud. Finalmente devuelve el certificado al SAA
13. SAA almacena el certificado y desnaturaliza la clave privada de dispositivo e identidad del usuario. En el caso de firmas centralizadas con el perfil de Lleidanet Wallet se crean 2 fragmentos A y B. El fragmento A se almacena cifrado en el celular de forma segura y el fragmento B se almacena de nuevo cifrado en la PKI en un HSM FIPS 140-2. En el caso de firmas centralizadas con el perfil de Usuario/password y huella dactilar, la clave privada se cifra con la clave maestra del HSM y con el PIN que introduce el usuario con cifrado AES.
14. Con este proceso se finaliza la generación y avisa a Operador y Usuario.

Para poder hacer uso de la identidad, en el caso de Firma Centralizada con Lleidanet Wallet el Usuario debe contar con el celular empleado en el proceso de enrolamiento que contiene el fragmento A de material criptográfico, realizar una autenticación contra la PKI para recuperar el fragmento B y poder regenerar el material criptgráfico con el fragmento A almacenado en el dispositivo.

Este mecanismo protege al Usuario y su identidad de una forma novedosa, con autenticación de doble factor.

Se adjunta diagrama de secuencia con el proceso de generación de claves.

Para el caso de firma centralizada con usuario/password o Huella dactilar se sigue el siguiente proceso:

1. Durante la emisión del certificado (operación que está autenticada por el operador de registro), se establece un canal seguro SSL de comunicación entre eSignaDesktop y el servidor de PKI y Firma Centralizada, se crea una conexión segura del Web Service seguro y adicionalmente se genera un canal seguro a nivel de aplicación entre eSignaCentralizedSign Module y el HSM, empleando una clave derivada S1.
2. eSignaDesktop envía al servidor de Firma Centralizada la clave S1 y el Usuario y Password usando la clave pública de Firma Centralizada del HSM para proteger todo el contenido.
3. El servidor de Firma Centralizada entrega la información encriptada al HSM, el cual desencripta mediante su clave privada la información y la almacena durante la operación de generación.
4. El HSM cifra mediante su Master Key (MK HSM (AES-256)) de Firma Centralizada, el Usuario-Password y se almacena en la base de datos encriptada.
5. Se genera en HSM un UUID y se deriva una clave DUUID. Se cifra el UUID también con la MK y se almacena por separado en otra tabla de la base de datos y relacionándola con el registro del Usuario-Password encriptado.
6. En este momento se generan las claves pública y privada de Usuario y se crea el certificado, momento en el que se cifran mediante S1 y se envían al cliente.
7. El cliente desencripta las claves mediante S1 y deriva una clave a partir del PIN del Usuario, se procesa las claves públicas y privadas para eliminar información e inutilizarlas y posteriormente se encripta el resultado, generando K.

8. Una vez hecho esto se envía K encriptado al HSM mediante S1, que desencripta K y lo encripta mediante DUUID.
9. Se almacena el resultado en la base de datos encriptada y se destruye todo el material criptográfico temporal del HSM y del cliente eSignaDesktop.

No se delegan partes del proceso de identificación y autenticación del firmante a terceras partes.

El SSA almacena la clave pública de activación en los metadatos asociados al par de claves del firmante. El PIN de activación se utiliza como parte para derivar la clave de cifrado con la que se protegen las claves del firmante.

El SSA protege la integridad de las claves de los firmantes y sus metadatos asociados mediante el cómputo de una función HMAC.

14.2.3 Asociación del certificado del firmante

La identidad de firma se compone de un par de claves RSA con longitud 2048 y el certificado electrónico que vincula la clave pública a la identidad del firmante.

Hasta la efectiva asociación del certificado con su correspondiente par de claves, la identidad de firma es incompleta y el SSASC no permitirá el uso de las claves.

El SSASC solicitará al dispositivo QSCD la generación del par de claves de los firmantes antes de la emisión del certificado electrónico. Como requisito previo a la generación de las claves, el firmante deberá establecer el PIN/contraseña de activación de firma.

Así mismo, el SSASC solicitará a la correspondiente Autoridad de Certificación la emisión del certificado, el cual se pondrá a disposición del firmante a través del Portal de Gestión de Identidades.

El SSASC verifica que el certificado del firmante y la clave pública almacenada en el sistema se corresponden. En caso de que ambas claves públicas coincidan, el certificado queda vinculado al par de claves del firmante, completando la identidad de firma. La clave del firmante queda a partir de este momento operativa para realizar operaciones de firma.

La integridad de cada identidad de firma se garantiza mediante la firma electrónica de cada registro en el repositorio donde se almacenan.

14.3 REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LAS CLAVES DE FIRMA

14.3.1 Activación de las claves de firma

El módulo SAM dentro del entorno protegido aplicará el control de acceso del usuario sobre sus claves de firma. Esto se materializará por medio de un protocolo de activación de la firma (SAP, Signature Activation Protocol) con el que se generará unos datos de activación de firma (SAD, Signature Activation

Data) sobre los que el SAM aplicará las condiciones de acceso al material de firma en el QSCD, lo cual se realizará mediante la aplicación móvil Lleidanet Wallet o eSignaDesktop

Las claves del firmante solo se pueden activar dentro del módulo HSM. La clave de un firmante sólo se podrá activar si completa el protocolo de activación autenticándose con sus credenciales de identidad, mediante su usuario/password, su huella dactilar o Lleidanet Wallet según sea el caso. En todos los casos, la activación de las claves de firma requerirá el PIN/contraseña de firma, establecido previamente por el firmante.

El protocolo de activación de firma (SAP) está diseñado para prevenir ataques de man-in the middle y replay. Además de esto el mensaje SAD incorpora protecciones contra suplantación, robo de sesión, duplicación, robo de credenciales, phishing y adivinación, mediante la combinación de técnicas de cifrado, firma electrónica, funciones resumen, incorporación de números aleatorios y uso de dos factores de autenticación de diferente naturaleza.

Todas las comunicaciones con el SSASC son protegidas mediante el protocolo TLS 1.2.

Los controles de acceso implementados en el SSA garantizan que un firmante no tiene acceso las claves de otros firmantes ni a otros objetos y funciones del sistema que no sean las funciones de firma, ya que éstas se encuentran cifradas con el SAD introducido por el usuario y que sólo conoce él, además de por la MASTERKEY del HSM.

Una vez se activa la clave del firmante el SSASC solo permite un único uso para firmar el resumen criptográfico contenido en el mensaje SAD utilizado para la activación. Tras la realización de la operación de firma solicitada, se requerirá un nuevo SAD para generar una nueva firma.

Las claves de los firmantes se almacenan cifradas en la base de datos del SSA utilizando el algoritmo de cifrado AES y una longitud de clave de 256 bits. La clave de cifrado para cada clave y firmante es diferente y se deriva a partir de una clave maestra del módulo criptográfico y el PIN/contraseña de activación de clave que establece el firmante.

El SSA permite generar firmas electrónicas con el algoritmo RSA PKCS#1 v1.5 y algoritmo resumen SHA-256.

14.3.2 Gestión de los datos de activación de firma

El mensaje con los datos de activación de firma (SAD) es generado en la aplicación SAA instalada en el teléfono inteligente del firmante o en la aplicación eSignaDesktop instalado en el computador del usuario.

El mensaje del SAD contiene el resumen(es) criptográfico(s) de los datos a firmar, referencias que permiten identificar la clave seleccionada e identificar al firmante, el PIN de activación de firma cifrado. Todo el mensaje del SAD se firma con la clave privada de activación de firma en la aplicación SAA para autenticar al firmante.

El SSASC solo permite que el firmante pueda utilizar su clave de activación de firma desde un único teléfono inteligente evitando así su duplicado.

La combinación de dos factores de autenticación de diferente naturaleza, la clave de activación y el PIN de activación, aseguran que el firmante tiene control exclusivo de sus datos de activación de firma.

El SAP consiste en la transmisión de un solo mensaje SAD a través de un canal seguro hasta el SSA. El módulo de activación de firma (SAM) es un sub-modulo del SSA.

14.3.3 Borrado de las claves de firma

Las claves del firmante son borradas de forma inmediata, cuando el certificado del firmante es revocado.

Periódicamente Lleidanet PKI S.L. ejecuta un proceso de borrado de la base de datos de aquellas claves de los firmantes cuyo certificado asociado ha caducado.

Los firmantes podrán solicitar la revocación de su certificado electrónico siguiendo los mecanismos establecidos en la Declaración de Prácticas de Certificación correspondiente. La revocación y caducidad del certificado supone en todos los casos la destrucción las claves asociadas.

14.3.4 Copia de seguridad y restauración de las claves de firma

Se mantienen copias de seguridad periódicas de la base de datos donde se encuentra las claves de los firmantes, y del resto de claves de infraestructura necesarias para garantizar la continuidad del servicio en caso de incidente. El número de copias de seguridad es el mínimo para garantizar la continuidad del servicio.

Las claves de infraestructura del SSASC son siempre almacenadas en contenedores cifrados.

El módulo criptográfico que contiene la clave maestra del SSASC que protege las claves de todos los firmantes requiere de control dual para su operación, copia de seguridad y restauración. La clave maestra del SSASC nunca abandona el módulo criptográfico en claro.

15 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

Véase punto 5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIÓN de la DPC.

15.1 GENERACIÓN DE REGISTROS

Se registran todos los eventos significativos de seguridad, incluyendo en cada registro la fecha y hora exacta de su realización, la cual no debe estar posibilitada de ser eliminada ni modificada del registro.

Los sistemas permiten la generación de los siguientes registros:

a) Intentos fallidos y exitosos de inicializar un usuario, renovar, habilitar, deshabilitar y actualizar o recuperar usuarios.
b) Intentos fallidos o exitosos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema, intentos de entrada y salida del sistema.

c) Intentos no autorizados de acceso a los registros o bases de datos del sistema.
d) Encendido y apagado del sistema principal.

El registro de auditoria de eventos debe registrar la hora, fecha e identificadores software y hardware.

Los registros generados durante la ejecución de los servicios, como son los cambios en la configuración, el personal e incidentes de acceso físico, deben ser gestionados por las organizaciones cliente que utiliza los sistemas de la SVA.

Compete a las organizaciones cliente la revisión, mantenimiento y protección del archivo de registros, así como los procesos de auditoría de estos registros.

15.2 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

Véase apartado 8.4 PROCEDIMIENTO DE REGISTRO DE EVENTOS de la DPC. Además, en particular, en la prestación del servicio de firma electrónica en servidor:

1. El SSA guarda registro, al menos, de los siguientes eventos: - Inicialización de sistema, arranque, parada y cambios de configuración. - Eventos de gestión de claves del firmante (generación, activación, uso, desactivación y destrucción) - Uso de claves de los firmantes. - Autenticación de los firmantes (incluyendo intentos fallidos). - Gestión de los datos de activación de firma del firmante (cambios de PIN/contraseña) - Accesos al sistema por parte de los usuarios administradores.
2. El SSA genera un registro de auditoría continuo en el que solo es posible añadir nuevos eventos y no es posible eliminar o modificar los eventos anteriores. 61. El SSA protege los eventos del registro de auditoría a nivel de entrada y de todo el registro aplicando una función HMAC que encadena cada registro con el anterior.
3. Todos los registros de eventos del registro de auditoría del SSA incluyen la siguiente información: - Fecha y hora del evento. - Tipo de evento. - Identidad de la entidad (firmante, administrador o proceso) responsable de la acción. - Resultado del evento (éxito o error)
4. El SSA comprueba en el arranque y periódicamente la integridad del registro de auditoría para detectar el borrado o modificación. Adicionalmente el SSA dispone de una funcionalidad para verificar la integridad del registro de auditoría a petición de un usuario con rol de auditor en el sistema.
5. Para garantizar la precisión de la fecha y hora de los eventos de auditoría el reloj de los sistemas se encuentra sincronizado por NTP utilizando como referencia el ROA (Real Observatorio de la Armada). Existen controles para detectar problemas que puedan comprometer la sincronización.

15.3 ARCHIVO DE REGISTROS

Véase apartado 8.4 PROCEDIMIENTO DE REGISTRO DE EVENTOS de la DPC.

15.4 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

Lleidanet PKI S.L. proporciona servicios de soporte de segundo nivel para la gestión de incidentes y recuperación de los sistemas de software que sustentan los servicios.

Corresponde a las organizaciones clientes, la implementación del Plan de Contingencias para el soporte del primer nivel y la recuperación en caso de incidentes en la infraestructura de hardware, firmware, comunicaciones y entorno.

16 CONTROLES DE SEGURIDAD TÉCNICA

16.1 GESTIÓN DE LOS SISTEMAS DE LA SEGURIDAD

El SSA implementa los siguientes roles de gestión:

- Responsable de seguridad (security officer): tiene la responsabilidad general de administrar e implementar las políticas de seguridad y tiene acceso a la información de seguridad.
- Administrador del sistema (system administrators): es el responsable de instalar, configurar y mantener el TW4S pero con acceso controlado a la información de seguridad.
- Operador del sistema (system operators): es el responsable de la operación del día a día del TW4S y las operaciones de copia de seguridad y restauración.
- Auditor del sistema (system auditor): está autorizado para revisar los archivos y registros de auditoría del TW4S para auditar que las operaciones del sistema están alineadas con la política de seguridad.

Lleidanet PKI S.L. asigna estos roles a personal cualificado e implementa todos los controles de segregación de funciones definidos en la sección 6.2.1.2 de la norma CEN EN 419 241-1. 6.5.2.

16.2 OPERACIONES Y SISTEMAS

La entidad dispone de procedimientos para operar de forma correcta y segura el SSASC.

El componte software SSA y el módulo HSM son operados de acuerdo con sus manuales para su instalación, administración y operación para cumplir con los objetivos de seguridad definidos su certificación como dispositivo QSCD.

16.3 CONTROLES DE SEGURIDAD INFORMÁTICA.

Véase apartado 9.5 Controles de Seguridad Informática de la DPC.

17 GESTIÓN DE CICLO DE VIDA DE LAS CLAVES: (SISTEMAS AUTOMATIZADOS)

En relación a los controles de seguridad (generación e instalación de par de claves, protección de clave privada y controles de ingeniería de los módulos criptográficos, datos de activación, controles técnicos de ciclo de vida, ...) se encuentran ampliamente desarrollados en la DPC

17.1 GENERACIÓN DE LAS CLAVES

La Generación de las claves de firma del sistema automatizado deberá ser realizada en un ambiente asegurado físicamente, por personal que ocupa roles de confianza, bajo al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del SVA.

La generación de la clave de firma del sistema automatizado deberá ser realizada en un módulo criptográfico que:

- Cumpla con los requerimientos FIPS 140-2 o Common Criteria EAL 4+
- Cumpla los requerimientos identificados en el CEN Workshop Agreement 14167-2 (CWA 14167-2)

El algoritmo de generación, la longitud de la clave firma y el algoritmo de firma usado para firmar los sellos de tiempo deberán ser reconocidos por el Organismo supervisor.

17.2 PROTECCIÓN DE LA CLAVE PRIVADA

La clave privada de firma permanece confidencial y que se mantiene su integridad. La clave de firma del sistema automatizado estará protegida en un módulo criptográfico que:

- Cumpla con los requerimientos FIPS 140-2 o Common Criteria EAL 4+,
- Cumpla los requerimientos identificados en el CEN Workshop Agreement 14167-2 (CWA 14167-2)

Si se realiza un respaldo de la clave de firma, esta deberá ser copiada, almacenada y recuperada sólo por personal que ocupa roles de confianza, usando al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del SVA.

Cualquier copia de la clave deberá ser protegida por la clave secreta del módulo criptográfico antes de ser almacenada fuera del dispositivo.

17.3 DISTRIBUCIÓN DE LA CLAVE PUBLICA

La clave pública de firma debe ser disponible para los terceros que confían en un certificado de clave pública.

El certificado puede ser emitido por la misma entidad que opera el SVA o por otra EC reconocida por el Organismo supervisor.

El certificado debe ser emitido por una EC bajo una política que provea un nivel de seguridad equivalente o superior a la DPSVA.

Este certificado deberá ser reconocido por el Organismo supervisor.

17.4 RE-EMISIÓN DE LA CLAVE

El tiempo de vigencia del certificado no debe ser mayor que el periodo de vigencia de los algoritmos y tamaños de claves, conforme al reconocimiento del Organismo supervisor.

17.5 TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA

Las claves privadas no pueden ser usadas tras la expiración de su ciclo de vida:

a. Se establecen procedimientos técnicos u operacionales para asegurar que son generadas y utilizadas nuevas claves.
b. La clave privada de firma, o cualquier parte de la clave será destruida de tal modo que no pueda ser recuperada.
c. El sistema de generación de sellos de tiempos debe rechazar cualquier intento de emitir sellos de tiempo si la clave privada de firma ha expirado o se encuentra revocada.

17.6 CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

Durante la Gestión del ciclo de vida del módulo criptográfico se cumple que:

- El hardware del módulo criptográfico no debe ser manipulado durante su transporte.
- El hardware del módulo criptográfico no debe ser manipulado durante su almacenamiento.
- La instalación, activación y duplicación de la clave de firma en el hardware del módulo criptográfico deberá ser realizado solo por personal que ocupa roles de confianza, usando al menos un control de acceso de dos personas en un ambiente físico seguro.

- El hardware de firma de sellos de tiempo funciona correctamente.
- Las claves de firma que son almacenadas en un módulo criptográfico son borradas antes de que el dispositivo sea retirado.

18 CONTROL DE CAMBIOS

Se debe implementar procedimientos de control de cambios para poner en producción modificaciones o parches de emergencia de aplicaciones críticas de software del SVA, a fin de evitar posteriores fallas o incompatibilidad con otros sistemas.

Lleidanet PKI S.L. realiza la gestión de cambios siguiendo el procedimiento interno PR-032 Gestión de comunicaciones y operaciones. En este se describen los tipos de cambios, la gestión de los mismos y los controles a tener en cuenta.

19 POLÍTICA DE PRIVACIDAD

La SVA brinda sus servicios a personas jurídicas y no tiene acceso a la información personal proporcionada por los suscriptores de los servicios de valor añadido. Lleidanet PKI S.L. no se responsabiliza por la información que los suscriptores entregan a las organizaciones clientes. Corresponde a las organizaciones clientes, la implementación de controles para la protección de los datos personales de sus suscriptores.

20 CONFIDENCIALIDAD DE LA INFORMACIÓN DE NEGOCIO

Todo el personal de Lleidanet PKI S.L. que participa de la administración de los sistemas de la SVA, ha firmado un Convenio de Confidencialidad para proteger la información confidencial de los proyectos de las organizaciones clientes.

La información crítica y sensible, que es archivada y protegida contra daño ambiental o intencional, así como acceso de lectura y modificación no autorizados.

En particular se protege la siguiente información:

- Material comercialmente reservado de la SVA, de las organizaciones cliente, incluyendo términos contractuales, planes de negocio y propiedad intelectual;

- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores de empresa y/o terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los usuarios, titulares o terceros que confían.
- Información que pudiera perjudicar la normal realización de las operaciones de la SVA

21 DERECHOS DE PROPIEDAD INTELECTUAL

La totalidad de los componentes de la SVA de Lleidanet PKI S.L., es decir, aplicaciones, políticas, procedimientos, sitios web, diagramas, textos, imágenes, ficheros, fotografías, logotipos, gráficos, marcas, iconos, combinaciones de colores, o cualquier otro elemento, su estructura y diseño, la selección y forma de presentación de los materiales, links y demás contenidos audiovisuales o sonoros, así como su diseño gráfico y códigos fuentes necesarios para su funcionamiento, acceso y utilización, están protegidos por derechos de propiedad industrial e intelectual, titularidad de Lleidanet PKI S.L., sin que puedan entenderse cedidos los derechos de explotación sobre los mismos más allá de lo estrictamente necesario para su correcto uso.

En particular, quedan prohibidas la reproducción, la transformación, distribución, comunicación pública, puesta a disposición del público y en general cualquier otra forma de explotación, por cualquier procedimiento, de todo o parte de los contenidos de los componentes de la SVA, así como de su diseño y la selección y forma de presentación de los materiales incluidos en la misma. Estos actos de explotación sólo podrán ser realizados si media la autorización expresa de Lleidanet PKI S.L.

Queda asimismo prohibido descompilar, desensamblar, realizar ingeniería inversa, sublicenciar o transmitir de cualquier modo, traducir o realizar obras derivadas de los programas de ordenador necesarios para el funcionamiento, acceso y utilización de las aplicaciones y de los servicios en él contenidos, así como realizar, respecto a todo o parte de tales programas, cualesquiera de los actos de explotación descritos en el párrafo anterior. El usuario del sitio web deberá abstenerse en todo caso de suprimir, alterar, eludir o manipular cualquier dispositivo de protección o sistemas de seguridad que puedan estar instalados en el mismo.

22 POLÍTICA DE REEMBOLSO

Las condiciones de reembolso serán definidas con cada organización cliente en los respectivos contratos con la SVA.

23 RESPONSABILIDAD FINANCIERA, REPRESENTACIONES Y GARANTÍAS

La cobertura de seguro, las provisiones de garantía y responsabilidad, así como las indemnizaciones son definidas en los contratos con las organizaciones clientes.

24 ENMENDADURAS

Los procedimientos para la resolución de enmendaduras serán definidas en los contratos con las organizaciones clientes.

25 RESOLUCIÓN DE DISPUTAS

Los procedimientos para la resolución de disputas serán definidas en los contratos con las organizaciones clientes.

26 ACUERDO ÍNTEGRO, SUBROGACIÓN Y DIVISIBILIDAD

Las cláusulas de acuerdo íntegro, subrogación y divisibilidad serán definidas en los contratos con las organizaciones clientes.

27 FUERZA MAYOR Y OTRAS PROVISIONES

Las cláusulas de fuerza mayor y otras provisiones aplicables a la entrega de los servicios de valor añadido serán definidas en los contratos con las organizaciones clientes.

28 TARIFAS

Las tarifas por los servicios serán definidas en los contratos con las organizaciones clientes.

29 FINALIZACIÓN DE LA SVA

Antes de que la SVA termine sus servicios realizará las siguientes medidas:

- Con 30 días de anticipación se informará a todos las organizaciones clientes y suscriptores, la finalización de las operaciones de la SVA.

- Se pondrá a disponibilidad de todas las organizaciones cliente la información concerniente a su terminación y las limitaciones de responsabilidad
- Se concluirán los permisos de autorización de funciones de todos los subcontratados para actuar en nombre de la SVA
- Se mantendrán o transferirán a los terceros que confían sus obligaciones de verificar los documentos generados.
- Las claves privadas de la SVA, incluyendo copias, serán destruidas de manera segura de modo que no pueda ser recuperada
- Se tomarán medidas para que los certificados de la SVA sean revocados
- Las provisiones sobre término y terminación, así como las cláusulas de supervivencia serán definidas en los contratos de las organizaciones cliente. Además, las modificaciones realizadas deben ser comunicadas a los suscriptores, titulares y terceros que confían.

30 AUDITORÍA

Lleidanet PKI S.L. se somete a servicios de auditoría periódica por parte del Organismo de evaluación de la conformidad para el mantenimiento de la acreditación de la SVA.

El auditor debe:

- Ser autorizado por el Organismo supervisor.
- Ser independiente del PSVA, y no haber realizado trabajos para ella dentro de los 2 años anteriores a la ejecución de la auditoría.

Dentro de esta revisión anual se realizará un análisis de los requerimientos de seguridad que deben ser cubiertos en las etapas de diseño y especificación de los proyectos de desarrollo de sistemas del SVA, para asegurar que dichos requerimientos son considerados en los sistemas críticos.

31 CONFORMIDAD CON LA LEY APLICABLE

Lleidanet PKI S.L. es afecta y cumple con las obligaciones establecidas por el Organismo supervisor, de los requerimientos del "Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo" o también como es conocido "Reglamento eIDAS" establecida por el Parlamento Europeo y a la Ley de Firmas Electrónica, para el reconocimiento legal de los sellos de tiempo emitidos bajos las directrices definidas en el presente documento.

32 BIBLIOGRAFÍA

(1) REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO (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
(5) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
(6) Real Decreto 505/2007, de 20 de abril, por el que se aprueban las condiciones básicas de accesibilidad y no discriminación de las personas con discapacidad para el acceso y utilización de los espacios públicos urbanizados y edificaciones.