Proyecto	**Servicios Cualificados de Validación de Firmas y Sellos Electrónicos**
Título	**Declaración de Practicas SVA - Servicios Cualificados de Validación de Firmas y Sellos Electrónicos (DPSVA)**

Realizado por	**LLEIDANET PKI S.L.**		
Dirigido a	**Usuarios internos y externos**		
Documento	**DOC-200216.2140915**		
Fecha aprobación	**22/05/2025**	Revisión	**6**

Firmado por: Raul Gisbert Rodas
Fecha firma: 22/05/2025 16:25:03 CEST

Firmado por: PASCUAL FERRER PONCE
Fecha firma: 22/05/2025 21:07:22 CEST

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

Les 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: 23/05/2025 15:01:44 CEST

1 DATOS DEL DOCUMENTO

Proyecto	Servicios Cualificados de Validación de Firmas y Sellos Electrónicos
Título	Declaración de Practicas SVA - Servicios Cualificados de Validación de Firmas y Sellos Electrónicos (DPSVA)
Código	DOC-200216.2140915
Tipo de documento	DOC – Documento genérico
Clasificación del documento	Público
Realizado por	LLEIDANET PKI S.L.
Dirigido a	Usuarios internos y externos
Fecha aprobación	22/05/2025
Revisión	6

2 HISTORIA DEL DOCUMENTO

Revisión	Fecha	Motivo de la modificación	Responsable
1	09/04/2021	Creación del documento.	Indenova SLU (CJ)
2	31/05/2021	Nueva ceremonia de claves de la PKI	Indenova SLU (CJ)
3	08/07/2021	Actualizar el contenido y la estructura del documento al Anexo A ETSI TS 119 441	Indenova SLU (CJ)
4	27/08/2024	Se hace referencia la política de validación que se emplea y que se indica en los reportes “QES AdESQC TL based”, se incluye la definición del Proof of Existance, se actualiza a la ETSI TS 119 172-4 y se actualiza la denominación de Indenova SL a Lleidanet PKI SL	Lleidanet PKI (CJU)

5	02/05/2025	Ajuste en el apartado Segregación de deberes Actualizar denominación a Lleidanet PKI SL	Lleidanet PKI (CJU)
6	22/05/2025	Agregar apartado Pruebas Validador de Firmas	Lleidanet PKI (CJU)

3 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Nombre: Compliance (CJ) Cargo: Responsable de calidad Fecha: 22/05/2025
Revisado por:	Nombre: Lleidanet PKI SL (SB) Cargo: Administrador del Servicio Fecha: 22/05/2025
Aprobado por:	Nombre: Comisión de Seguridad de la Información Cargo: Comisión de Seguridad de la Información Fecha: 22/05/2025

4 INTRODUCCIÓN

4.1 DESCRIPCIÓN GENERAL

Este documento describe las prácticas y políticas aplicadas por LLEIDANET PKI S.L. para la prestación del servicio cualificado de validación de firma y sellos electrónicos (SVS), en 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 la que se deroga la Directiva 1999/93/CE y siguiendo el formato indicado en el Anexo A del ETSI TS 119 441.

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.

4.1.1 Identificación de TSP

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

OID: 1.3.6.1.4.1.49959

4.1.2 Política del servicio de validación de firmas electrónicas

La Política de servicio de validación de sello y firma cualificada se identifica con el OID (OID) 1.3.6.1.4.1.49959.1.5.2

Se sigue una Política: QES AdESQC TL based la cual valida las firmas electrónicas e indica si son Firmas electrónicas avanzadas (AdES), AdES respaldadas por un Certificado Cualificado (AdES / QC) o una Firma Electrónica Cualificada (QES).

Todos los certificados y sus cadenas relacionadas que respaldan las firmas se validan con las Listas de confianza de los Estados miembros de la UE (esto incluye certificado del firmante y certificados utilizados para validar los servicios de estado de validez del certificado: CRL, OCSP y sellos de tiempo).

El presente documento es un documento público y su contenido es conforme a la especificación técnica de la ETSI TS 119 441 (y en concreto en el Anexo A) y define las políticas y prácticas en la provisión de los servicios de validación de firmas/sellos electrónicos cualificados.

4.2 COMPONENTES DEL SERVICIO DE VALIDACIÓN DE FIRMAS

4.2.1 Actores SVS

Cliente de validación de firmas (SVC)

- Componente de software que proporciona una interfaz de usuario para la aplicación utilizada por el servicio de validación de firmas.

Driver de Aplicación (DA)

- Aplicación que proporciona funcionalidad de validación de firmas al Cliente de validación de Firmas.

Servidor de servicio de validación de firmas (SVSServ)

- El componente que implementa el protocolo de validación de firmas en el lado del SVSP.

Protocolo de servicio de validación de firmas (SVP)

- Canal de comunicación seguro para intercambiar información entre el DA y el SVSServ.

Aplicación de validación de firma (SVA)

- Un componente de software que es responsable de la validación de la firma, que implementa la validación algoritmo y crea un informe de validación de firma.

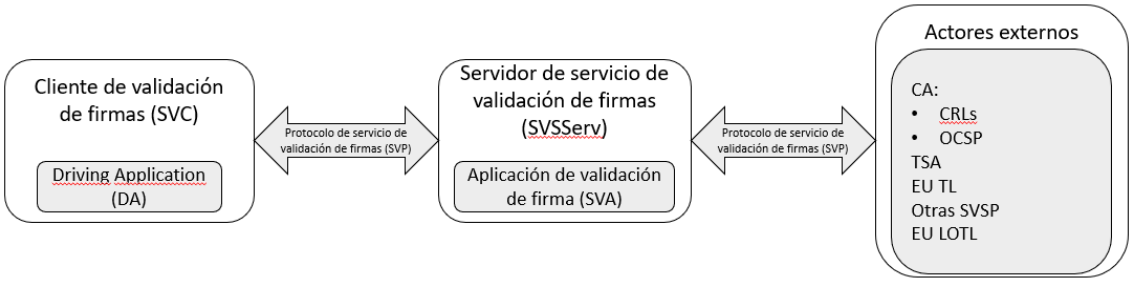
Actores externos

- Otras fuentes de confianza: autoridades de certificación, autoridades de sellado de tiempo, Lista de prestadores cualificados de servicios electrónicos de confianza (TSL), la Comisión Europea proporciona la lista de Listas de confianza que están llamadas a cumplir con sus propósitos.

En este sentido los clientes que quieran utilizar el servicio de validación de firmas de LLEIDANET PKI S.L. deberán implementar el SVC y el DA mediante las APIS que le proporcionará LLEIDANET PKI S.L. Dichas APIs permitirán utilizar el servicio de validación de firmas y conectarse al SVSServ de forma segura.

4.2.2 Arquitectura de servicio

El siguiente diagrama muestra la arquitectura simplificada del Servicio cualificado de validación de firmas.



SVC:

- Ejecuta el SVP del lado del usuario
- Crea la solicitud de validación de la firma
- Cuando corresponde, se preocupa por la presentación del informe de validación
- Puede incorporar:
    - Una interfaz de usuario para ingresar manualmente la solicitud
    - Una interfaz de máquina para solicitudes automatizadas
    - Una interfaz de usuario para presentar el informe

SVSServ:

- Ejecuta el SVP y procesa la validación de la firma en el lado del SVSP
- Ejecuta el SVA que:
    - Implementa el algoritmo de validación también definido en ETSI TS 119 102-1
    - Puede llamar a actores externos para cumplir su propósito
- Crea el SVR relacionado con la solicitud
- Construye la respuesta de validación de la firma

El canal de comunicación entre el SVC y el SVSServ transporta la validación de la firma solicita la respuesta. Cubre la autenticación del SVSP, para evitar informes falsos, y admite autenticación de cliente.

4.3 DEFINICIONES Y ABREVIATURAS

4.3.1 Definiciones

Nombre	Abreviación	Definición
eIDAS Regulation	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
Proveedor de servicios de confianza	TSP	Una entidad que brinda servicios de confianza.
Proveedor de servicios cualificados de confianza	QTSP	Una entidad que proporciona uno o más Servicios de Confianza Cualificados y es el Órgano de Supervisión el que le ha otorgado la cualificación.
Servicio de validación de firmas	SVS	Servicio de confianza para la validación de firmas y/o sellos.
Autoridad de certificación	CA	Proveedor de servicios cualificados de confianza que emite certificados para firmas y/o sellos electrónicos.
Sistema de Gestión de Seguridad de la Información	SGSI	Sistema de gestión de seguridad de la información de LLEIDANET PKI S.L. certificado según ISO/IEC 27001: 2014.
Comisión de Seguridad de la Información	CSI	Comisión que supervisa, desarrolla, mantiene y gestiona los programas y políticas de seguridad.
Reglamento General de Protección de Datos	RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

4.3.2 Abreviaturas

Abreviación	Abreviatura de

DA	Driving Application
PoE	Proof of Existence
QES	Qualified Electronic Signature or Qualified Electronic Seal
AdES	Advanced Electronic Signature
AdES/QC	Advanced Electronic Signature created with a Qualified Certificate
(Q)SCD	Qualified Signature Creation Device
QSVSP	Qualified Signature Validation Service Provider
SD	Signer's Document
SDO	Signed Data Object
SDR	Signed Document Representation
SVA	Signature Validation Application
SVP	Signature Validation Protocol
SVR	Signature Validation Report
SVSP	Signature Validation Service Provider
SVSServ	Signature Validation Service Server
TSA	Time stamping Authority
VPR	Signature Validation PRocess
OID	Object Identifier
PKI	Public Key Infrastructure
OCSP	Online Certificate Status Protocol
HSM	Hardware Security Module

4.4 POLÍTICAS Y PRÁCTICAS

4.4.1 Organización que administra la documentación del TSP

Este documento es administrado por LLEIDANET PKI S.L.

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

4.4.2 Persona de contacto

La persona de contacto para la gestión de este documento será el Director técnico de LLEIDANET PKI S.L.

Se puede solicitar más información a través del correo electrónico consultas@indenova.com

4.4.3 Aplicabilidad de la documentación TSP (pública)

Declaración de práctica del servicio de validación de firmas y sellos electrónicos

LLEIDANET PKI S.L. es responsable de la gestión de la Declaración de prácticas del servicio de validación de firmas y sellos electrónicos de LLEIDANET PKI S.L. Este documento deberá ser aprobado por la Comisión de Seguridad de la Información y publicado en el sitio web de LLEIDANET PKI S.L. (https://www.indenova.com/acreditaciones/eidas/).

LLEIDANET PKI S.L. notificará al organismo supervisor sobre cualquier cambio en la prestación de servicios de confianza cualificados sin demoras indebidas, pero a más tardar 3 días hábiles. LLEIDANET PKI S.L. notificará al organismo supervisor sobre la terminación prevista del servicio de confianza calificado al menos 3 meses antes de la terminación del servicio de confianza cualificado.

La notificación al organismo supervisor se enviará sin demora indebida y a más tardar 3 días hábiles después de cualquier cambio en la Declaración de prácticas del servicio de validación de firmas y sellos electrónicos de LLEIDANET PKI S.L.

Política de seguridad de la información

LLEIDANET PKI S.L. ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO/IEC-27001. LLEIDANET PKI S.L. ha logrado la certificación del SGSI de acuerdo con la norma ISO/IEC-27001 con el alcance de la certificación de "Los sistemas de información que dan soporte a las actividades relativas al diseño, desarrollo, implantación, mantenimiento y soporte de soluciones software de firma electrónica, seguridad, certificación digital y procesos electrónicos para el e-government y ebusiness, servicios de intermediación electrónica y e-business".

LLEIDANET PKI S.L. ha implementado todos los controles necesarios requeridos por las regulaciones eIDAS y RGPD y los estándares correspondientes (es decir, ETSI EN 319 401) en el SGSI.

La CSI de LLEIDANET PKI S.L. aprueba las políticas y prácticas relacionadas con la seguridad de la información.

Términos de servicio

LLEIDANET PKI S.L. pone a disposición los Términos de servicio y el Acuerdo de procesamiento de datos en el sitio web de LLEIDANET PKI S.L. (https://www.indenova.com/acreditaciones/eidas/).

5 GESTIÓN Y OPERACIÓN DEL SERVICIO DE CONFIANZA

LLEIDANET PKI S.L. ha implementado un Sistema de Gestión de Seguridad de la Información de acuerdo con la norma ISO/IEC 27001 y ha obtenido la certificación ISO/IEC 27001 por un organismo de certificación internacional acreditado.

Los párrafos siguientes resumen la gestión y las operaciones del servicio de confianza, incluidos los controles de seguridad aplicados.

5.1 ORGANIZACIÓN INTERNA

LLEIDANET PKI S.L. cumple con todas las obligaciones legales aplicables a la prestación de sus Servicios de confianza. Lleva a cabo sus operaciones de acuerdo con las políticas y prácticas adoptadas. LLEIDANET PKI S.L. garantiza que todos los requisitos definidos en la Declaración de aplicabilidad ISO27001 y esta Declaración de prácticas se implementen y sigan siendo aplicables a los Servicios de confianza proporcionados.

La prestación de servicios de confianza está sujeta a una auditoría externa realizada al menos cada 12 meses por un organismo de evaluación de la conformidad.

5.1.1 Fiabilidad de la organización

LLEIDANET PKI S.L. cuenta con la estabilidad financiera y los recursos necesarios para operar de acuerdo con este documento.

LLEIDANET PKI S.L. mantiene un seguro de responsabilidad civil de acuerdo con la legislación aplicable, para cubrir las obligaciones derivadas de sus operaciones y en línea con el artículo 13 del reglamento eIDAS.

LLEIDANET PKI S.L. cumple los requerimientos generales indicados en el artículo 19 del Reglamento eIDAS, así como lo indicado en el ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

En relación con el servicio cualificado de validación de firmas y sellos electrónicos se presta el servicio de acuerdo con el artículo 32 del Reglamento eIDAS y el ETSI 119 102-1.

LLEIDANET PKI S.L. puede proporcionar más información sobre las medidas de confiabilidad específicas de la organización a pedido legítimo especial de la parte interesada.

Los suscriptores están obligados a mantener confidencialidad en los passwords y credenciales de uso del servicio de validación y deben comunicar de forma oportuna cualquier circunstancia que hiciera sospechar de un uso ilícito de las mismas o que éstas estuvieran comprometidas.

LLEIDANET PKI S.L. es responsable sobre la disponibilidad del servicio y como se ha indicado anteriormente dispone de un seguro de responsabilidad civil de acuerdo a la legislación aplicable.

LLEIDANET PKI S.L. no es responsable por:

- Cualquier daño para un usuario del servicio que hubiera fallado en mantener el debido secreto sobre las credenciales de uso del servicio.
- La disponibilidad del servicio, si dicha disponibilidad depende de servicios de terceros o terceras entidades.
- El no cumplimiento de las obligaciones es debida a una causa de fuerza mayor.

5.1.2 Segregación de deberes

El sistema de gestión de seguridad de la información implementado y certificado de acuerdo con la ISO/IEC 27001 garantiza que la segregación de funciones se verifique y mantenga. Específicamente: los roles del Responsable del SGSI y de auditor interno están separados, véase apartado 8.2.4 Roles que requieren segregación de funciones de la DPC LLEIDANET PKI S.L.

5.2 RECURSOS HUMANOS

El sistema de gestión de seguridad de la información implementado y certificado según ISO/IEC 27001 garantiza que LLEIDANET PKI S.L. haya implementado todos los controles necesarios para

operaciones seguras. Los empleados y contratistas reciben la formación adecuada y tienen toda la experiencia necesaria para llevar a cabo las tareas especificadas en los contratos de empleo o contratistas, según se define en el Procedimiento de Aspectos Organizativos de la Seguridad de LLEIDANET PKI S.L. y en la Política de Seguridad de LLEIDANET PKI S.L.

Control ISO 27001		Cumplimiento
A.7.1	Antes de la contratación	
A.7.1.1	Investigación de antecedentes	El equipo de RRHH comprueba los antecedentes de todos los candidatos al puesto de trabajo, de los contratistas y de terceros, de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos considerados. En el caso de personas que vayan a ocupar puestos clave para la organización, se realizará una comprobación exhaustiva de todos los datos relativos a la formación y el empleo antes de su contratación.
A.7.1.2	Términos y condiciones de contratación	Los empleados reciben copia de la ficha de puesto y anexo “Acuerdo de confidencialidad”. Como parte de sus obligaciones contractuales, los empleados, deben aceptar y firmar los términos y condiciones de su contrato de trabajo, que debe establecer sus responsabilidades y las de la organización en lo relativo a seguridad de la información.
A.7.2	Durante la contratación	
A.7.2.1	Responsabilidades de gestión	La dirección gobierna y apoya las actividades del SGSI. Los detalles se proporcionan en la política de seguridad.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y los usuarios de terceros (este último, si procede según requisitos de seguridad detectados) reciben la formación adecuada y las actualizaciones regulares de las políticas y procedimientos de la organización, incluyendo requisitos de seguridad,

		responsabilidades legales y otros controles del negocio, así como prácticas en el uso correcto de los recursos de tratamiento de información: procedimientos de conexión, uso de paquetes de software, etc., antes de obtener acceso a la información o los servicios. La formación se proporciona en el Plan de formación anual que realiza LLEIDANET PKI S.L.
A.7.2.3	Proceso disciplinario	Dirección instará el procedimiento disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad. El proceso disciplinario se llevará a cabo basándose en los requerimientos del R.D. Leg. 1/1995 de 24 Mar. Estatuto de los Trabajadores, que en su Sección 4 "Extinción del contrato", artículo 54, hace referencia a la posibilidad de la apertura de un proceso disciplinario para los trabajadores.
A.7.3	Cese del empleo o cambio de puesto de trabajo	
A.7.3.1	Cese o cambio de puesto de trabajo	La terminación o cambio de responsabilidades laborales, de acuerdo a los contratos con empleados, las declaraciones de confidencialidad siguen siendo válidos después de la terminación del empleo. La política de seguridad del proveedor define recomendaciones sobre qué aspectos de seguridad de la información se recomienda abordar en los contratos.

5.3 GESTIÓN DE ACTIVOS

5.3.1 Requerimientos generales

LLEIDANET PKI S.L. mantiene listas de activos actualizadas, incluidos los activos de información. La Gestión de Riesgos se basa en el análisis y la evaluación del riesgo asociado a los activos de la organización y llevar a cabo los planes de tratamiento de riesgos para todos aquéllos activos cuyo nivel de riesgo se encuentre por encima del nivel de riesgo aceptado por la Comisión de Seguridad de la Información. Más específicamente:

Control ISO 27001		Cumplimiento
A.8.1	Responsabilidad sobre los activos	
A.8.1.1	Inventario de activos	Área de Sistemas/Responsable de SGSI mantienen actualizado el inventario de activos, el área de Sistemas mantiene las categorías de inventario relativas a activos hardware o software y el Responsable de SGSI mantiene las categorías de inventario no relativas a activos hardware o software.
A.8.1.2	Propiedad de los activos	El responsable del activo se ocupa de asegurar que la información y los activos asociados a los medios de procesamiento están adecuadamente clasificados.
A.8.1.3	Uso aceptable de los activos	Se siguen las reglas de uso aceptable de la información y de los recursos para el tratamiento de la información, que se recogen en Guía de buenas prácticas en SI.
A.8.1.4	Devolución de los activos	Los empleados deben devolver a la organización todos los activos que hubieran estado utilizando.

5.3.2 MANEJO DE LOS SOPORTES DE ALMACENAMIENTO

Los medios que contienen información confidencial se manejan de forma segura y de acuerdo con la Política general de almacenamiento de archivos de trabajo de LLEIDANET PKI S.L. de SGSI y los Procedimientos operativos de LLEIDANET PKI S.L. para las TIC. Más específicamente:

Control ISO 27001		Cumplimiento
A.8.3	Manejo de los soportes de almacenamiento	
A.8.3.1	Gestión de los soportes extraíbles	Política general de almacenamiento de archivos de trabajo define cómo manejar la información, incluida la información electrónica dentro de los

		sistemas de información, correos electrónicos, almacenamiento (extraíble).
A.8.3.2	Eliminación de los soportes	Los soportes son retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos.
A.8.3.3	Soportes físicos en tránsito	La Política general de almacenamiento de archivos de trabajo y los Procedimientos internos definen las reglas sobre cómo manejar la transferencia de medios.

5.4 CONTROL DE ACCESO

La Política de control de acceso de LLEIDANET PKI S.L., que forma parte del SGSI de LLEIDANET PKI S.L., garantiza que el acceso al sistema se limitará a las personas autorizadas y que se implementen todos los controles necesarios para un control de acceso seguro. Más específicamente:

Control ISO 27001		Cumplimiento
A.9.1	Requisitos de negocio para el control de accesos	
A.9.1.1	Política de control de accesos	El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido ("denegado por defecto"), a menos que se permita expresamente ("necesidad de saber") a usuarios individuales o grupos de usuarios. Más detalles están disponibles en la Política de control de acceso de LLEIDANET PKI S.L.
A.9.1.2	Control de acceso a las redes y servicios asociados	En LLEIDANET PKI S.L. se controla la seguridad en la conexión entre la red de LLEIDANET PKI S.L. y otras redes públicas o privadas. Más detalles están disponibles en la Política de control de acceso de LLEIDANET PKI S.L.
A.9.2	Gestión de acceso de usuario	
A.9.2.1	Gestión de altas/bajas en el registro de usuarios	Se proporcionan a los usuarios únicamente el acceso a los servicios para los que han sido específicamente autorizados. Como regla general,

		los usuarios tendrán acceso autorizado únicamente a aquella información y recursos que precisen para el desempeño de sus funciones. Los Procedimientos internos definen las reglas para las altas y baja del registro de usuarios.
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	Para ello LLEIDANET PKI S.L. lleva un proceso de aprovisionamiento de acceso de usuario el cual se llevará a cabo para asignar o revocar los derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	Los privilegios especiales o los perfiles con funciones más avanzadas, como creación de usuarios o asignación de contraseñas iniciales, sólo se asignan a administradores y a quién realmente las necesiten, en función de las tareas que les hayan encomendado
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	Se controla la asignación de contraseñas mediante un proceso de gestión formal. La asignación de la información secreta de autenticación es controlada a través de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Se realiza una revisión periódica de los derechos de acceso de los usuarios, para ello se sigue un procedimiento interno.
A.9.2.6	Retirada o adaptación de los derechos de acceso	Se restringe el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.
A.9.3	Responsabilidades del usuario	
A.9.3.1	Uso de información confidencial para la autenticación	Se exige a los usuarios que sigan las prácticas de la organización en el uso de información secreta de autenticación. Se previene el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de la información o de los recursos de procesamiento de la información.
A.9.4	Control de acceso a sistemas y aplicaciones	

A.9.4.1	Restricción del acceso a la información	Se restringe el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.
A.9.4.2	Procedimientos seguros de inicio de sesión	De acuerdo a lo que se exige en la política de control de acceso, el acceso a los sistemas y aplicaciones son controlados por un procedimiento de inicio de sesión seguro.
A.9.4.3	Gestión de contraseñas de usuario	Los sistemas de gestión de contraseña son interactivos y aseguran contraseñas de calidad
A.9.4.4	Uso de herramientas de administración de sistemas	El uso de programas de utilidades que podrían ser capaces de anular sistemas y aplicaciones de control se limitan y se controlan.
A.9.4.5	Control de acceso al código fuente de los programas	Se restringe el acceso al código fuente de las aplicaciones software.

5.5 CONTROLES CRIPTOGRÁFICOS

Control ISO 27001		Cumplimiento
A.10.1	Controles criptográficos	
A.10.1.1	Política de uso de los controles criptográficos	LLEIDANET PKI S.L. determina en la Política de uso de los controles criptográficos, los controles criptográficos.
A.10.1.2	Gestión de claves	Las claves se almacenan en dispositivos criptográficos FIPS 140-2.

5.6 SEGURIDAD FÍSICA Y AMBIENTAL

Control ISO 27001	Cumplimiento

A.11.1	Áreas seguras	
A.11.1.1	Perímetro de seguridad física	Con la identificación del perímetro de seguridad física prevenimos los accesos físicos no autorizados, los daños, las intromisiones en las instalaciones y en la información, pérdidas, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización. Protegiendo el acceso a las instalaciones se protege el acceso físico a los sistemas de información.
A.11.1.2	Controles físicos de entrada	Las áreas seguras se encuentran protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado. Se ha establecido un perímetro de seguridad física que impide el acceso no autorizado mediante la implantación de una serie de controles físicos de acceso en las zonas de entrada: puertas con control de entrada, sistema de registro de entrada de trabajadores, acceso solo para socios y personas designadas fuera del horario laboral, sistemas de detección de intrusos con alarma.
A.11.1.3	Seguridad de oficinas, despachos e instalaciones	Los controles de seguridad para las instalaciones de la oficina se evalúan durante la evaluación de riesgos y se toman las acciones necesarias cuando se evalúan áreas de riesgos superiores a los tolerables.
A.11.1.4	Protección contra las amenazas externas y de origen ambiental	Se protege contra amenazas externas y de origen ambiental.
A.11.1.5	Trabajo en áreas seguras	Los controles de seguridad para las instalaciones de la oficina se evalúan durante la evaluación de riesgos y se toman las acciones necesarias cuando se evalúan áreas de riesgos superiores a los tolerables.
A.11.1.6	Áreas de acceso público y de carga y descarga	Se controlan los puntos de acceso tales como las áreas de carga y descarga y otros puntos, a través de los que el personal no autorizado puede acceder a las instalaciones, y si es posible, dichos puntos se encuentran aislados de los recursos de tratamiento

		de la información para evitar los accesos no autorizados.

5.7 SEGURIDAD DE LA OPERACIÓN

Control ISO 27001		Cumplimiento
A.12.1	Responsabilidades y procedimientos de operación	
A.12.1.1	Documentación de los procedimientos de operación	Los procedimientos de operación en materia de gestión de los recursos de tratamiento y comunicación de la información son documentados mantenidos. Son difundidos entre los empleados que vayan a implicarse en el procedimiento que corresponda y puestos a disposición de todos los usuarios que los necesiten a través de los sistemas internos de LLEIDANET PKI S.L. Son documentados con detalle las pautas de actuación de la entidad para dar cobertura a la gestión de la información dentro del alcance del SGSI.
A.12.1.2	Gestión de cambios	Para controlar los cambios en los sistemas y recursos de tratamiento de información se han implantado responsabilidades y procedimientos formales de gestión; de este modo se asegura un control satisfactorio de todos los cambios en los equipos, el software o los procedimientos.
A.12.1.3	Gestión de capacidades	La utilización de los recursos se supervisa y ajusta, así como también se realizan proyecciones de los requisitos futuros de capacidad, para garantizar el comportamiento requerido del sistema. Para el correcto funcionamiento de los sistemas, se realiza una planificación por adelantado que asegure su capacidad y disponibilidad. El uso de los recursos de la empresa está controlado y se ajusta a las necesidades identificadas para cada actividad; por tanto, para que se prevean los requisitos de capacidad de los

		sistemas para asegurar el comportamiento requerido, teniendo en cuenta nuevas actividades que puedan surgir, o actualizaciones de los sistemas ya existentes.
A.12.1.4	Separación de los entornos de desarrollo, prueba y producción	Se separan los recursos de desarrollo (pruebas internas de equipo), test (pruebas internas de integración), preproducción (interno o de cliente) y de producción (interno o de cliente), para reducir los riesgos de acceso no autorizado o los cambios en los sistemas (internos o de cliente). Los desarrolladores tienen acceso a los sistemas en producción internos o de preproducción/producción de los clientes. En los entornos de desarrollo, test y preproducción se usan datos lo más parecido posible, por volumen y exactitud a los de producción, aunque no se usarán los datos reales si se trata de datos sensibles.
A.12.2	Protección contra código malicioso	Se han implantado los controles de detección, prevención y recuperación que sirvan como protección contra código malicioso y se han implantado procedimientos adecuados de concienciación del usuario.
A.12.2.1	Controles contra el código malicioso	LLEIDANET PKI S.L. posee una configuración que garantiza que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida y con ello se evita que se ejecute el código no autorizado.
A.12.3	Copias de seguridad	
A.12.3.1.	Copias de seguridad de la información	De forma automática se hacen copias diarias de las máquinas virtuales existentes, shares, bases de datos y datos de configuración de los sistemas que contengan información relevante.
A.12.4	Registro de actividad y supervisión	
A.12.4.1	Registro y gestión de eventos de actividad	Se realizan registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se mantienen estos

		registros durante el periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.
A.12.4.2	Protección de los registros de la información	Los dispositivos de registro y la información de los registros son protegidos contra manipulaciones indebidas y accesos no autorizados.
A.12.4.3	Registros de actividad del administrador y operador del sistema	Se registran las actividades del administrador del sistema y de la operación del sistema.
A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de la información dentro de la organización o de un dominio de seguridad, se encuentran sincronizados.
A.12.5	Control del software en explotación	
A.12.5.1	Instalación del software en sistemas en producción	Se establece la prohibición de instalación o uso de software que sea autorizado por LLEIDANET PKI S.L., y se llevan a cabo revisiones periódicas del software instalado en los equipos para comprobar que no existen elementos no autorizados; para ello se han instalado herramientas antivirus y detección de código malicioso. Además, anualmente se elabora un Informe con el resultado de las comprobaciones realizadas.
A.12.6	Gestión de la vulnerabilidad técnica	
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se realizan periódicamente, pruebas de intrusión externa e internas por el personal que cumpla con las competencias requeridas, los hallazgos detectados son tratados para su resolución.
A.12.6.2	Restricciones en la instalación de software	Para ello disponemos de la Política de autorización de instalación de software.
A.12.7	Consideraciones de las auditorías de los sistemas de información	

A.12.7.1	Controles de la auditoría de los sistemas de información	Se realiza un proceso de auditoría de los sistemas de información para alcanzar la máxima eficacia y para verificar que los sistemas de información cumplen las normas de aplicación de la seguridad.

5.8 SEGURIDAD DE LA RED

Control ISO 27001		Cumplimiento
A.13.1	Gestión de la seguridad en las redes	
A.13.1.1	Controles de red	Las redes se encuentran adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo la información en tránsito.
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	Se aplican medidas de seguridad para garantizar la seguridad del servicio de acceso a las aplicaciones de tratamiento, para ello se gestionan todos los controles sobre los servicios de red existentes.
A.13.1.3	Segregación de redes	Se segregan los grupos de usuarios, servicios y sistemas de información en las redes.

5.9 GESTIÓN DE INCIDENTES

Control ISO 27001		Cumplimiento
A.16.1	Gestión de incidentes de seguridad de la información y mejoras	

A.16.1.1	Responsabilidades y procedimientos	El grupo de gestión se encarga de las actividades de preparación para hacer frente a posibles incidencias. Además, se garantiza de que el registro y la supervisión son adecuados, así como las lecciones aprendidas de incidentes anteriores, se integran en las operaciones de LLEIDANET PKI S.L.
A.16.1.2	Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información son notificados a través de los canales adecuados de gestión lo antes posible.
A.16.1.3	Notificación de los puntos débiles de la seguridad	Todos los empleados, contratistas y terceros que sean usuarios de los sistemas y servicios de información se encuentran obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios. El procedimiento a seguir es el mismo que en el caso de las incidencias de seguridad.
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	Los eventos de seguridad de la información generados por los sistemas son valorados y registrados para emprender las acciones pertinentes.
A.16.1.5	Respuesta a los incidentes de seguridad	Si se produjera algún incidente de seguridad de alto impacto, LLEIDANET PKI S.L. notificará a todos los afectados en los plazos que el reglamento, las leyes y las normas lo indiquen.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se lleva a cabo un análisis periódico de las incidencias registradas con la finalidad de determinar qué acciones pueden desarrollarse para evitar la materialización de un potencial evento que pudiese afectar a la seguridad de la información.
A.16.1.7	Recopilación de evidencias	Los informes, alertas, y toda la documentación relativa a los incidentes de seguridad son almacenados de forma segura en previsión de que puedan ser utilizados en caso de emprenderse acciones legales o administrativas a la hora de depurar responsabilidades.

5.10 RECOLECCIÓN DE EVIDENCIA

LLEIDANET PKI S.L. aplica los requisitos especificados en la cláusula 7.10 de ETSI EN 319 401 con respecto a la recopilación de evidencia. Estos registros solo se divulgarán a las autoridades policiales bajo orden judicial y a las personas con la solicitud legítima.

5.11 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

LLEIDANET PKI S.L. ha implementado un procedimiento de gestión de la continuidad del negocio, que forma parte del SGSI de LLEIDANET PKI S.L. y cubre procedimientos de evaluación de riesgos, respuestas a incidentes, desastres y sus planes de recuperación incluyendo pruebas.

Los planes incluyen todos los recursos y procesos necesarios para la recuperación y cubre toda la información aspectos de seguridad de la gestión de la continuidad del negocio. El objetivo de dichos planes es completar la recuperación de servicios dentro del objetivo de tiempo de recuperación (RTO) establecido. Los planes de recuperación se prueban anualmente. Más específicamente.

Control ISO 27001		Cumplimiento
A.17.1	Continuidad de la seguridad de la información	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La Seguridad de la Información de LLEIDANET PKI S.L. ha sido considerada, a la hora de diseñar un plan de acción para garantizar la Gestión de Continuidad del Negocio, en caso de fallos importantes o catastróficos. A tal efecto, se define el Plan de continuidad de negocio. En dicho plan se describen los procesos que permiten asegurar la continuidad de los servicios prestados por la organización.
A.17.1.2	Implantación de la continuidad de la seguridad de la información	Se desarrolla e implanta los planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requerido, después de una interrupción o un fallo de los procesos de negocio críticos.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	LLEIDANET PKI S.L. asegura de que todo el personal implicado en el Plan de Continuidad reciba la formación técnica necesaria para realizar su labor.

5.12 PLANES DE TERMINACIÓN Y TERMINACIÓN DE TSP

En caso de terminación de la prestación del servicio, LLEIDANET PKI S.L. se regirá por lo dispuesto en la normativa vigente sobre firma electrónica.

LLEIDANET PKI S.L. Informará debidamente a los Suscriptores y Titulares de los Certificados, así como a los Usuarios de los servicios afectados, sobre sus intenciones de terminar su actividad como Prestador de Servicios de Confianza al menos con dos (2) meses de antelación al cese de esta actividad

Terminará cualquier subcontratación que tenga al objeto de la prestación de funciones en nombre de la LLEIDANET PKI S.L. del servicio a cesar.

Podrá transferir, una vez acreditada la ausencia de oposición de los Suscriptores, aquellos Certificados que sigan siendo válidos en la fecha efectiva de cese de actividad a otro Prestador de Servicios de Confianza que los asuma. De no ser posible esta transferencia los Certificados se extinguirán.

Sea cual fuere el servicio en cese, LLEIDANET PKI S.L. transferirá a un tercero los registros de eventos, la información de registro, la información de estado de revocación y auditoría, así como los Certificados empleados en la prestación del servicio, por un periodo suficiente a los efectos que dictamine la legislación vigente.

Comunicará al Organismo de supervisión el cese de su actividad y el destino que vaya a dar a los Certificados, especificando en su caso: si los va a transferir, a quién, o si los dejará sin efecto. La notificación a dicho organismo se realizará con al menos dos (2) meses de antelación, en documento firmado manuscrita o electrónicamente. Además, se remitirá a dicho organismo la información relativa a los Certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos pertinentes.

Se transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios

Se destruirán las Claves privadas, de forma que no puedan recuperarse.

Todas estas actividades estarán recogidas en el documento interno: DOC-200216.20B2309 Plan de Cese de los Servicios de Certificación

5.13 CUMPLIMIENTO

Control ISO 27001		Cumplimiento
A.18.1	Cumplimiento de los requisitos legales y contractuales	
A.18.1.1	Identificación de la legislación aplicable	Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplir dichos requisitos, se encuentran definidos, documentados y se

		mantienen actualizados de forma explícita para cada sistema de información de la organización.
A.18.1.2	Derechos de propiedad intelectual	LLEIDANET PKI S.L. implanta procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software propietario.
A.18.1.3	Protección de los registros de la organización	Los documentos importantes se encuentran protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, regulatorios, contractuales y empresariales.
A.18.1.4	Protección de datos y privacidad de la información personal	LLEIDANET PKI S.L. garantiza la protección y la privacidad de los datos según se requiera en la legislación y las regulaciones y, en su caso, en las cláusulas contractuales pertinentes.
A.18.1.5	Regulación de controles criptográficos	Los controles criptográficos son utilizados de acuerdo con todos los contratos, leyes y regulaciones pertinentes

6 DISEÑO DEL SERVICIO DE VALIDACIÓN DE FIRMAS

La Plataforma de Validación de firmas y sellos electrónicos de LLEIDANET PKI S.L. responde al Servicio Cualificado de validación de Firmas electrónicas y sellos electrónicos, certificado bajo reglamento eIDAS, que permite generar las correspondientes evidencias de validación de certificados cualificados, firmas y sellos electrónicos. El servicio, trabaja teniendo en cuenta las publicaciones de la Comisión Europea, por lo que su uso y servicio atiende a todos los países de la UE.

El Servicio Cualificado de validación de Firmas electrónicas genera evidencias, teniendo en cuenta las normas y estándares fijados por la normativa legal vigente de la UE, Reglamento eIDAS. Se realizan comprobaciones del estado de calificación del certificado en el momento, día y hora de su emisión. En caso de existir Sello de Tiempo electrónico, se realiza también su comprobación. De igual manera, se realiza comprobación del estado del certificado en el momento de la firma. De todos los procesos, se generan las correspondientes evidencias.

Permite que el consumidor tenga pleno conocimiento sobre la validez, vigencia y cumplimiento normativo de la firma sometida a validación y le permite establecer políticas internas para blindarse frente

a documentos o archivos firmados por clientes, proveedores o trabajadores que no cumplan con lo dispuesto en la normativa.

Características de la plataforma de validación:

- Validación de certificados bajo el reglamento eIDAS.

- Validación de confianza, caducidad y revocación de los certificados

- Validación de todos los certificados recogidos por la TSL: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

- Extracción de información de los certificados (identificación de personas físicas y jurídicas).

- En el caso de certificados de personas físicas extracción de CIF y nombre y apellidos.

- En el caso de certificados de sello extracción de CIF y razón social

- En el caso de certificados de representante extracción de CIF y nombre y apellidos del representante y CIF y razón social de la empresa.

- Extracción de información de si el certificado es cualificado o no.

- Sellos de tiempo.

- Periodo de validez de los Sellos de Tiempo. Mínimo 15 años.

- La emisión de las evidencias de validación de certificados de firma electrónica será realizada en conformidad con las normas ETSI aprobadas en el marco de la regulación eIDAS.

- La emisión de las evidencias de validación de certificados de sello electrónico será realizada en conformidad con las normas ETSI aprobadas en el marco de la regulación eIDAS.

- La verificación de los sellos de tiempo que puedan ser recibidos para verificación, así como los certificados electrónicos a validar, deberán cumplir las normas del Reglamento eIDAS.

- Generación y emisión de evidencias.

Además de los servicios de validación de firmas electrónicas, se proporciona a las aplicaciones integradas la capacidad de extender las firmas electrónicas tanto ASN.1 como XML y PDF a formatos longevos. El Servicio recupera las evidencias de validación necesarias para la extensión al formato longevo deseado, y construye la firma resultante.

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, esta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Esto implica que, si queremos tener una firma que pueda ser validada a lo largo del tiempo, la firma electrónica que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas existe un servicio que mantiene dichas evidencias, y realiza la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

Los pasos que realiza el servicio son:

1. En primer lugar, se verifica la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES, y las referencias.

2. Se realiza un proceso de completado de la firma electrónica, consistente en lo siguiente:

a. Obtener las referencias a los certificados, así como almacenar los certificados del firmante.

b. Obtener las referencias a las informaciones de estado de los certificados, como las listas de revocación de certificados (CRLs) o las respuestas OCSP, así como almacenarlas.

3. Se sellan las referencias a los certificados y a las informaciones de estado.

El almacenamiento de los certificados y las informaciones de estado se realiza dentro del documento resultante de la firma electrónica, siguiendo las modalidades de firmas AdES –X o -A.

Para el archivado y gestión de documentos electrónicos se seguirán las recomendaciones de las guías técnicas de desarrollo del Esquema Nacional de Interoperabilidad (Real Decreto 4/2010, de 8 de enero).

La validación de una firma requiere una prueba de la existencia o Proof of Existence (PoE) de esa firma en un momento dado.

Tal prueba de existencia puede darse en forma de un timestamp.

Un timestamp digital es una afirmación de prueba de que un objeto de datos existió en un momento particular. Esto generalmente toma la forma de un vínculo entre un hash de un objeto de datos y una fecha y hora emitida y firmada por una autoridad de timestamping confiable.

Al firmar digitalmente, una fecha y hora pueden incluirse ya en la firma, pero corresponde a la hora local de la computadora del firmante. Esta última puede ser fácilmente modificada antes de firmar, de modo que la hora de la firma no sea la real. Por lo tanto, este tiempo de firma no puede ser confiable. Se debe utilizar un timestamp digital confiable para probar la existencia de la firma (y sus datos asociados) en un cierto momento.

Este principio también existe para las firmas manuscritas. Cuando un documento se firma manualmente, se hace en presencia de un notario confiable, quien verifica no solo la identidad del firmante, sino también la fecha y hora de la firma.

Antes de explicar el proceso de timestamping, a continuación definimos algunos conceptos que están involucrados en este proceso.

• Una Autoridad de Timestamping (TSA) es un Proveedor de Servicios de Confianza que crea tokens de timestamp utilizando una o más Unidades de Timestamping. La TSA debe cumplir con las especificaciones del IETF RFC 3161.

• Una Unidad de Timestamping (TU) es un conjunto de hardware y software que contiene una única clave de firma utilizada por una TSA.

Además, en el contexto de las firmas digitales, usualmente distinguimos los timestamps dependiendo de los datos para los cuales proporcionan una prueba de existencia:

• Un timestamp de contenido es un timestamp que se calcula sobre los datos originales que son firmados por una firma. Proporciona una prueba de existencia de los datos originales, pero no de la firma.

• Un timestamp de firma es un timestamp que se calcula sobre el valor de la firma digital (en algunos casos sobre todo el objeto de datos firmado). Proporciona una prueba de existencia del valor de la firma.

• Un timestamp de archivo es un timestamp que se calcula sobre el material de validación de una firma (es decir, los datos necesarios para validar una firma, como CRLs, respuestas OCSP, cadena de certificados, etc.). Al menos proporcionan una prueba de existencia de ese material de validación, pero como a menudo se calculan en realidad sobre todo el objeto de datos firmado en el que se ha añadido ese material de validación, a menudo proporcionan una prueba de existencia de los datos originales, el valor de la firma, el timestamp de la firma, el material de validación y otros posibles timestamps de archivo que están cubiertos por ellos.

El timestamping, el proceso de añadir un timestamp a una firma, se puede desglosar en los siguientes pasos:

1. El usuario crea un hash de los datos para los cuales se requiere una afirmación de timestamp (por ejemplo, el valor de la firma para un timestamp de firma).

2. El usuario envía el hash y el algoritmo de resumen a un TSA.

3. El TSA agrupa el hash, la hora de estampado (fecha y hora actuales) y la identidad del TSA y lo firma con una clave privada contenida en un TU.

4. El token de timestamp resultante del paso anterior se devuelve al cliente.

5. El token de timestamp se añade a la firma de los datos que se enviaron como un hash en el primer paso.

El token de timestamp creado por una TSA puede considerarse confiable porque

• la TSA es independiente del proceso de firma;

• el reloj de la TSA está sincronizado con una fuente de tiempo autorizada;

• el timestamp está firmado digitalmente por la TSA;

• la TSA debe seguir especificaciones estrictas.

6.1 REQUISITOS DEL PROCESO DE VALIDACIÓN DE FIRMAS

LLEIDANET PKI S.L., de conformidad con el Reglamento 910/2014, aprueba las siguientes firmas/sellos avanzados en formatos CADES, XADES y PADES en los niveles de cumplimiento B, T y LT, los cuales se encuentran reconocidos por los Estados miembros.

LLEIDANET PKI S.L. aprueba las condiciones y políticas bajo las cuales se confirma la validez de una firma / sello electrónico avanzado, siguiendo lo indicado en ETSI TS 119 101:

(1) el certificado que respalda la firma electrónica avanzada era válido en el momento de la firma, y cuando la firma electrónica avanzada está respaldada por un certificado cualificado, el certificado cualificado que respalda la firma electrónica avanzada era, en el momento de la firma, un certificado

cualificado de firma electrónica que cumple con el Anexo I del Reglamento (UE) No 910/2014 y que fue emitido por un proveedor de servicios de confianza cualificado;

(2) los datos de validación de la firma corresponden a los datos proporcionados a la parte que confía;

(3) el conjunto único de datos que representa al usuario se proporciona correctamente a la parte que confía;

(4) el uso de cualquier seudónimo se indica claramente a la parte que confía si se usó un seudónimo en el momento de la firma;

(5) cuando la firma electrónica avanzada es creada por un dispositivo de creación de firma electrónica cualificado, el uso de dicho dispositivo se indica claramente a la parte que confía;

(6) la integridad de los datos firmados no se ha visto comprometida;

(7) en el momento de la firma se cumplían los requisitos establecidos en el artículo 36 del Reglamento (UE) no 910/2014;

(8) el sistema utilizado para validar la firma electrónica avanzada proporciona, a la parte que confía, el resultado correcto del proceso de validación y permite que la parte que confía detecte cualquier problema de seguridad relevante.

6.1.1 Modelo de validación

Según ETSI EN 319 102-1, el modelo conceptual de validación de QES / QESeal o AdES_QC / AdESeal_QC, se presenta en la Ilustración 1.

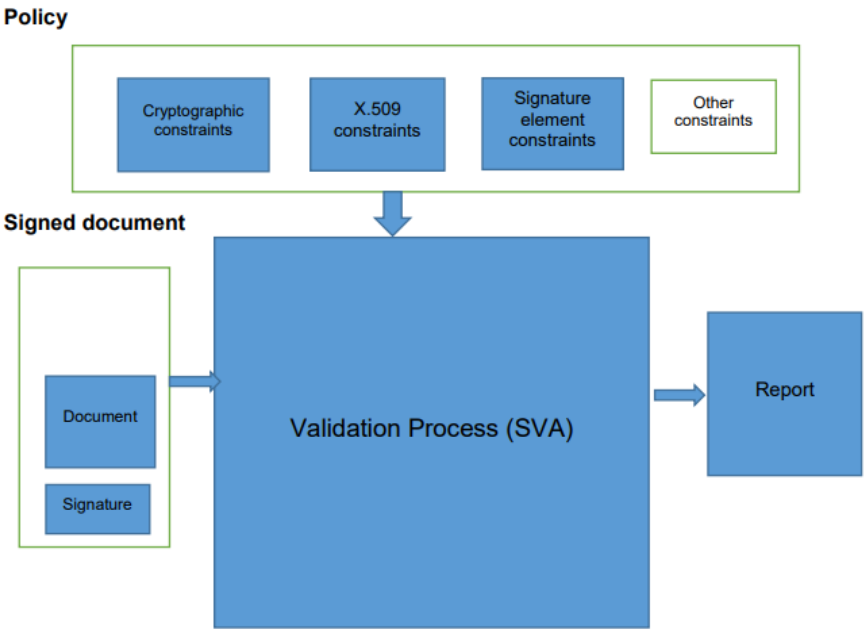


Ilustración 1: Modelo conceptual de validación

En el modelo, el componente SVA recibe la firma/sello y, de acuerdo con la Política de Validación (conjunto de restricciones), valida y genera un indicador de estado y un informe de validación que es interpretado por un usuario (parte de confianza) para la aplicabilidad de la firma/sello.

Para validar el formato de firma/sello, se ejecutan varios subprocesos dentro del proceso SVA (proceso de validación para el formato/nivel seleccionado): verificación de formato, verificación de control de calidad, verificación criptográfica, etc. el proceso es APROBADO, FALLIDO o INDETERMINADO.

Los estados que proporciona el proceso SVA después de validar el formato/nivel particular de acuerdo con la Política de Validación son:

- APROBADO: las verificaciones de todas las características/parámetros criptográficos de la firma/sello son exitosas de acuerdo con la Política; Cabe indicar que el servicio indica que la firma/sello es técnicamente válido, pero esto no significa que sea aplicable al propósito comercial particular;
- FALLIDO: las comprobaciones de todas las características/parámetros criptográficos de la firma/sello no son satisfactorias, la firma/sello se creó después de la revocación del control de calidad, o el formato no coincidía con uno de los formatos de referencia especificados;
- INDETERMINADO: los resultados de las comprobaciones individuales no permiten que la firma/sello se evalúe como APROBADO o FALLIDO; la aceptación de la firma/sello es prerrogativa del usuario/parte que Confía.

Para cada nivel/formato de firma electrónica/sello electrónico, la SVA realiza una secuencia lógica de subprocesos que comprenden los siguientes procesos de validación:

- Proceso de validación para formato básico de firma/sello - BASELINE_B. La SVA realiza este proceso si el tiempo de validación está dentro del período de validez del QC y no se revoca, o el tiempo de validación está fuera del período de validez del QC y la CA ha proporcionado información sobre su revocación / cancelación;
- Proceso de validación para el nivel básico de firma / sello BASELINE_T y BASELINE_LT - la SVA realiza este proceso de validación de firma básica de una firma / sello con tiempo certificado (_T) y de firma / sello con tiempo certificado y estado de un QC (_LT);
- Proceso de validación para el nivel de firma / sello BASELINE_LTA - la SVA realiza este proceso de validación de firma básica de una firma / sello con tiempo certificado (_T), de firma / sello con tiempo certificado y estado de un QC (_LT) y de una firma / sello con material de archivo (LTA);

6.1.2 Proceso de validación

EL proceso que sigue el SVA es:

(1) Si la firma/sello para la validación es:
- con perfil BASELINE_B - el SVA deberá realizar (4)
- con perfil BASELINE_T o BASELINE_LT - el SVA deberá realizar (3)
- con perfil BASELINE_LTA: el SVA deberá realizar (2)

(2) Si el SVA no admite la validación de firma/sello con el perfil BASELINE_LTA, el SVA deberá realizar (3); de lo contrario, la SVA realizará un proceso de validación de firma/sello con perfil BASELINE_LTA y pasará a (5);

(3) Si el SVA no admite la validación de firma/sello con los perfiles BASELINE_LTA, BASELINE_T y BASELINE_LT, el SVA deberá realizar (4); de lo contrario, la SVA realizará un proceso de validación de firma/sello con el perfil BASELINE_T y BASELINE_LT y pasará a (5);

(4) La SVA realizará un proceso de validación de sello/firma de formato básico (perfil BASELINE_B) y pasará a (5);

(5) Cuando el estado de validación del proceso de validación seleccionado sea APROBADO, la SVA devolverá un indicador de estado TOTAL PASSED y un informe de validación en formato XML como respuesta del servicio web;

(6) Cuando el estado de validación del proceso de validación seleccionado es FALLIDO, el SVA devolverá un indicador de estado TOTAL-FALLIDO y un informe de validación en formato XML como respuesta del servicio web;

(7) En otro caso, el SVA devolverá el indicador de estado INDETERMINADO y un informe de validación en formato XML como respuesta del servicio web.

Las solicitudes de validación de firmas/sellos y las respuestas a estas solicitudes utilizan el canal de comunicación seguro entre Cliente y Servidor. El intercambio está protegido por el soporte de la

autenticación del servidor y se puede mantener la autenticación del cliente. El protocolo de validación (solicitudes y respuestas) cumple con ETSI EN 119 442.

De acuerdo con ETSI TS 119 172-4, el SVA realiza el proceso de validación en los siguientes pasos:

Paso 1: El Cliente genera y envía una solicitud de validación que contiene los documento (si la firma/sello está envuelto o envuelto); Las restricciones de validación son establecidas implícitamente por el software SVA y el proceso de validación las ejecuta de acuerdo con el formato de la firma/sello entregado en la solicitud.

Paso 2: El SVA realiza la validación de firma/sello; la implementación de este paso implica el uso de servicios de confianza internos adicionales de LLEIDANET PKI S.L. (CRL/OCSP,) o, si es necesario, de otros proveedores externos.

Paso 3: El SVA genera, prepara y envía una respuesta XML como informe de validación en respuesta a una solicitud de validación de firma/sello; el informe de validación detallado contiene el indicador de estado (SI/NO) de la validación de cada restricción y sus efectos en función del proceso de validación seleccionado del SVA, cumple con la especificación técnica ETSI TS 119 102-2.

Paso 4: Sobre la base de la respuesta XML del informe de validación, el Usuario/Confianza acepta o rechaza la validez técnica de la firma/sello.

El servicio realiza los siguientes procesos de validación, dependiendo del perfil de la firma/sello presentado:

- Proceso de validación de firma/sello con perfil BASELINE_B;
- Proceso de validación del sello de tiempo;
- Proceso de validación de firma/sello con perfiles BASELINE_T y BASELINE_LT; este proceso es el mismo para ambos perfiles;
- Proceso de validación de firma/sello con perfil BASELINE_LTA.

La elección del proceso de validación del SVA sigue las instrucciones de la sección 12.2del modelo de validación y el proceso seleccionado realiza los pasos anteriores, incluidos los procedimientos funcionales básicos (subprocesos), que construyen la secuencia lógica de verificaciones en el marco del proceso de validación de la firma/sello.

6.1.3 Resultado de la validación

El proceso de validación de firma / sello finaliza con:

- Indicador de estado de validación (APROBADO, FALLIDO, INDETERMINADO);
- Identificador de la política de validación (o descripción de las limitaciones);
- Fecha y hora de validación y datos de validación (firma / certificado de sello;
- El proceso de validación seleccionado (según el perfil de firma / sello);
- Informe de validación.

6.2 REQUISITOS DEL PROTOCOLO DE VALIDACIÓN DE FIRMAS

Actualmente se consideran formatos admitidos:

- Formato XAdES (XML Advanced Electronic Signatures), según especificación técnica ETSI TS 101 903, versión 1.2.2, versión 1.3.2. y versión 1.4.1. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

- Formato CAdES (CMS Advanced Electronic Signatures), según especificación técnica ETSI TS 101 733, versión 1.6.3, versión 1.7 y versión 1.8.1. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

- Formato PAdES (PDF Advanced Electronic Signatures), según especificación técnica ETSI TS 102 778-3, versión 1.2.1 (se admitirán versiones posteriores siempre que no impliquen cambios significativos en la sintaxis de los tags usados en la presente política) y la ETSI TS 102 778-4 para el caso de firmas longevas en PADES (PAdES Long Term). En caso contrario se aprobará la adaptación del perfil a la nueva versión del estándar a través de una adenda a esta política de firma.

6.3 INTERFACES

6.3.1 Canal de comunicación

LLEIDANET PKI S.L. opera y respalda el SERVICIO como un servicio web al que se accede a través de:

- API Servicio calificado de validación de firmas o sellos electrónicos: https://app.swaggerhub.com/apis/eSignaBox/circuits-api/2.0.3#/Signatures/checkSignatures

La interfaz utiliza un canal de transporte/comunicación seguro que admite la autenticación del cliente.

EL SERVICIO se autentica mediante el uso de tokens y protocolos Open ID Connect:

- Autorización API: https://app.swaggerhub.com/apis/eSignaBox/authorization-api/2.0.1

6.3.2 SVSP - otro TSP

En ciertos casos, el SERVICIO requiere acceso a fuentes externas de certificados relacionados con el proceso de validación de firma/sello a un documento firmado/sellado. Dichos participantes externos (indirectos) en el proceso de validación son:

- Depósitos de certificados mantenidos por otros QTSP: registros públicos, fuentes CRL/OCSP; autoridades certificadoras de sellado de tiempo;
- Lista de confianza nacional, listas de confianza (TL) externas (Estados miembros);
- Lista de listas de confianza (LoTL).

EL SERVICIO utiliza interfaces de software estandarizadas para acceder a estas fuentes externas de certificados calificados, que verifica durante el proceso de validación de QES/QESeal y/o AdES/AdESeal_QC.

La LoTL es una publicación de la Comisión Europea. Este archivo XML contiene las Listas de confianza de los Estados miembros, incluida la Lista de confianza nacional.

Puede encontrar información sobre quién firma y publica LoTL en: http://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52015XC1224(01)&from=EN.

El formato de firma de la LoTL y la TL nacional es XAdES BASELINE_B. El SERVICIO confía en LoTL verificando la firma a través del certificado publicado en la dirección anterior.

6.4 REQUISITOS DEL INFORME DE VALIDACIÓN DE FIRMAS

El proceso de validación de firma / sello finaliza con:

- Indicador de estado de validación (APROBADO, FALLIDO, INDETERMINADO);
- Identificador de la política de validación (o descripción de las limitaciones);
- Fecha y hora de validación y datos de validación (firma / certificado de sello;
- El proceso de validación seleccionado (según el perfil de firma / sello);
- Informe de validación.

6.5 PRUEBAS DEL VALIDADOR DE FIRMAS

Con el objetivo de asegurar la corrección de las validaciones realizadas por el servicio de validación de firmas, periódicamente se realizan una serie de pruebas automatizadas y se genera un reporte de resultados de estas pruebas.

Los tests que se realizan sobre el servicio, incluyen combinaciones de, entre otras variables:

- Perfiles de certificado (persona natural, pertenencia a administración pública, pertenencia a organización, etc.)
- Formatos de firma (PAdES, CAdES, XAdES)
- Niveles de certificado (Cualificado y no cualificado)
- Tipos de certificado (de firma y de sello)
- Tipos de documento firmado (pdf y texto xml)
- Tipos de reporte obtenido (pdf, json)

7 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

(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.

(7) ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services

(8) ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers