ECD_CO_1001.07_Política de Servicios Cualificados de Validación de Firmas y Sellos Electrónicos

Lleida SAS
Colombia - Bogotá

Control de documentación

Histórico de versiones

Versión	Fecha	Autor	Descripción
1	07/3/2022	Gloria Salvador	Versión inicial
2	30/11/2022	Gloria Salvador	Corrección del numeral de la política
2.1	03/05/2023	Gloria Salvador	Referencias acreditación ONAC

Lista de distribución

Empresa
Lleida SAS

Clasificación y estatus

Clasificación	Estatus
Uso Interno	Aprobado

Documentos referenciados

Descripción

Tabla de contenido

1. Introducción

1.1 Objetivo

Dar a conocer al público en general los lineaminentos establecidos por Lleida SAS para prestar Servicios Cualificados de Validación de Firmas y Sellos Electrónicos como ECD de acuerdo con los establecido en la Ley 527 de 1999, Ley 1437 de 2011 y los reglamentos que los modifiquen o complementen, en el territorio de Colombia

1.2 Alcance

Todos los miembros de Lleida SAS, Entidad de Certificación Digital, así como todas las terceras partes identificadas en el alcance del Sistema de Gestión de la Entidad de Certificación Digital

1.3 Distribución

Aprobada por la Dirección de Lleida SAS, esta Política debe ser accesible a todas las personas incluidas en la lista de distribución especificada en el control documental, mediante los canales adecuados, establecidas en el procedimiento ECD_CO-3001 - Gestión del repositorio de documentación.

1.4 Revisión

La presente Política de Servicio será revisada y aprobada anualmente por parte del Comité de Seguridad de Lleida.net. No obstante, si tuvieran lugar cambios relevantes para la Organización, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento.

2. Consideraciones previas

Política de Servicios Cualificados de Validación de Firmas y Sellos Electrónicos, en adelante *Política* es un documento elaborado por Lleida SAS (en adelante Lleida.net) que, actuando como una Entidad de Certificación Digital (en adelante ECD) contiene las normas, procedimientos que Lleida.net aplica como lineamiento para prestar Servicios Cualificados de Validación de Firmas y Sellos Electrónicos de acuerdo a lo establecido en la Ley 527 de 1999, Ley 1437 de 2011 y los reglamentos que los modifiquen o complementen, en el territorio de Colombia.

La Política está conforme con los siguientes lineamientos:

- Criterios específicos de Acreditración para las Entidades de Certificación Digital CEA 3.0-07 (en adelante CEA) que deben ser cumplidos para obtener la acreditación como ECD, ante el Organismo Nacional de Acreditación de Colombia (en adelante ONAC)
- Ley 527 de 1999
- Estándares y protocolos:

  Hypertext Transfer Protocol (HTTP)

  https://www.ietf.org/rfc/rfc2616.txt

  HTTP Over TLS (HTTPS)

  https://datatracker.ietf.org/doc/html/rfc2818

  CAdES (CMS Advanced Electronic Signatures). ETSI TS 101 733

  https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v02020p.pdf

  PAdES (PDF Advanced Electronic Signatures). ETSI TS 102 778

  https://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf

  RFC 3126 Electronic Signature Formats for long term electronic signatures

  https://datatracker.ietf.org/doc/html/rfc3126

  RFC 5126 CMS Advanced Electronic Signatures (CAdES)

  https://datatracker.ietf.org/doc/html/rfc5126

  RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

  https://datatracker.ietf.org/doc/html/rfc3161

  RFC 3126 Electronic Signature Formats for long term electronic signatures

  https://datatracker.ietf.org/doc/html/rfc3126

RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

https://datatracker.ietf.org/doc/html/rfc5905

Protocolo ANSI ASC X9.95 ETSI TS 101 861 V1.2.1 Time stamping profile

https://www.etsi.org/deliver/etsi_ts/101800_101899/101861/01.04.01_60/ts_101861v010401p.pdf

ISO/IEC 19005-3:2012 Document Management - Electronic document file format for long term preservation - Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)

https://www.iso.org/standard/57229.html

DATOS DE LA ENTIDAD PRESTADORA DE SERVICIOS DE CERTIFICACIÓN LEGAL

Razón social:	LLEIDA S.A.S.
N.I.T.	900571038-3
Dirección:	Calle 81 # 11 – 55 Oficina 903
Ciudad/País	Bogotá/Colombia
Teléfono:	+5713819903
Correo electrónico:	co@lleida.net
Página web:	www.lleida.net/co
Nº Certificado Acreditación	22-ECD-009
Certificado Acreditación	22-ECD-009.pdf (onac.org.co)

DATOS DE LA ENTIDAD DE REGISTRO

La entidad de registro es la misma prestadora de servicios de certificación digital.

Peticiones, Quejas, Reclamos, Solicitudes y apelaciones

Las peticiones, quejas reclamos, solicitudes y apelaciones sobre los servicios prestados por Lleida SAS seran atendidas por varios mecanismos a disposición del subscriptor y seran resueltas por las personas pertinentes e imparciales.

- Por correo electrónico a clientes@lleida.net . Deberá adjuntarse la plantilla disponible en www.lleida.net/co ECD_CO 4501 Plantilla PQRSA Lleida SAS
- Por teléfono al +57 1 381 9903

En el plazo máximo de 15 días deberán ser resueltas y notificadas, previa radicación, análisis y redacción de reporte formal que será entregado al subscriptor.

3. Administración de políticas

La administración de las Políticas de Servicios están a cargo del proceso de Sistema Integrado de Gestión

Persona de contacto

Nombre: Eva Pané Vidal
Cargo: Supervisor de la ECD
Teléfono de contacto: +57 1 381 9903
Correo electrónico: compliance@lleida.net

Las políticas deben ser aprobadas por el Comité de Seguridad, una vez aprobadas es responsabilidad el Supervisor de la ECD la actualización en los portales web en su última versión.

3.1 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) 1.3.6.1.4.1.53589.1.5.2

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. COMPONENTES DEL SERVICIO DE VALIDACIÓN DE FIRMAS

4.1 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 digital, 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 LLEIDA.NET deberán implementar el SVC y el DA mediante las APIS que le proporcionará LLEIDA.NET Dichas APIs permitirán utilizar el servicio de validación de firmas y conectarse al SVSServ de forma segura.

4.2 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.

5. DISEÑO DEL SERVICIO DE VALIDACIÓN DE FIRMAS

La Plataforma de Validación de firmas y sellos electrónicos de LLEIDA S.A.S responde al Servicio Cualificado de validación de Firmas electrónicas y sellos electrónicos, certificado bajo marco legal, que permite generar las correspondientes evidencias de validación de certificados cualificados, firmas y sellos electrónicos.

El Servicio Cualificado de validación de Firmas electrónicas genera evidencias, teniendo en cuenta las normas y estándares fijados por la normativa legal vigente. 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.

- 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 identificación y nombre y apellidos.

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

    - En el caso de certificados de representante extracción de los datos de identificación de la persona y de la sociedad anteriormente mencionados

- Extracción de información de si el certificado es cualificado o no, en su caso.

- 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.

- La emisión de las evidencias de validación de certificados de sello electrónico será realizada en conformidad con las normas ETSI.

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

- 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 guías técnicas internacionales.

7.1 REQUISITOS DEL PROCESO DE VALIDACIÓN DE FIRMAS

LLEIDA S.A.S, 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.

LLEIDA S.A.S 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;

(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 siguientes requisitos:

a) estar vinculado al creador de manera única;

b) permitir la identificación del creador;

c) haber sido creado utilizando datos de creación que el creador puede utilizar para la creación de una firma, con un alto nivel de confianza, bajo su control exclusivo, y

d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable;

(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.

7.1.1 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.

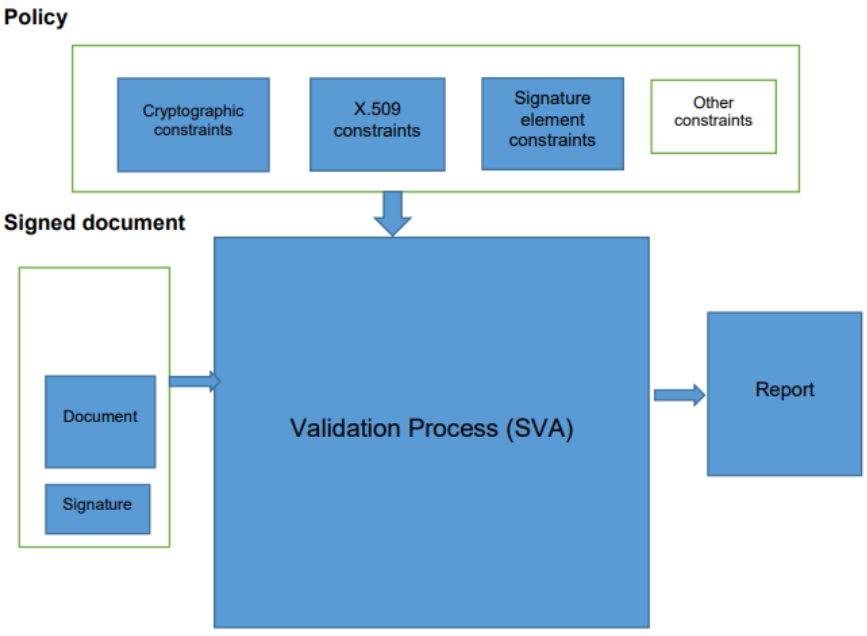

Ilustración 1: Modelo conceptual de validación

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);

7.1.2 PROCESO DE VALIDACIÓN

EL proceso que sigue el SVA sigue 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 319 172-1, 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 LLEIDA S.A.S(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.

7.1.3 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.

7.2 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.

7.3 INTERFACES

7.3.1 CANAL DE COMUNICACIÓN

LLEIDA S.A.S 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

7.3.2 SVSP - OTRO ECD

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 ECD: registros públicos, fuentes CRL/OCSP; autoridades certificadoras de sellado de tiempo;

- Listas de confianza (TL) externas (Estados miembros de la UE);

- 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.

7.3.3 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. Políticas de seguridad del servicio

El servicio y el sistema que la gestiona atiendo a los distintos aspectos de seguridad:

- Seguro

El sistema no permite los accesos no autorizados a la información, a través de la plataforma y de ataques directos sobre los servidores sobre los que funciona.

- Trazable

Todas las acciones de los usuarios que implican una modificación en un documento se registran.
En algunos servicios la auditoría de eventos se firma y sella con TSA para asegurar su autenticidad.

- Fidedigno

No se modifican los originales de los documentos

- Integridad

Las evidencias periciales generadas, no se modifican.

- Buenas prácticas de Seguridad de la Información

El Sistema de Gestión de los Servicio de Correo electrónico certificado es auditado periódicamente según los estándares de ISO 27001.

- Auditado

Además ser realizan revisiones técnicas y de Ethical Hacking acorde con OWASP.

7. TARIFAS

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

8. Obligaciones

Obligaciones de la ECD Lleida.net

Lleida.net como entidad de prestación de servicios de certificación está obligada según normativa vigente en lo dispuesto en las Políticas de Servicio y en la DPC a:

1. Respetar lo dispuesto en la normatividad vigente, la DPC y en las Políticas de Certificado.
2. Publicar la DPC y cada una de las Políticas de Servicio en la página Web de Lleida.net
3. Informar a ONAC sobre las modificaciones de la DPC y de las Políticas de Certificado.
4. Mantener la DPC y Políticas de Servicio con su última versión publicadas en la página Web de Lleida.net.
5. Emitir el servicio conforme a las Políticas de Servicio y a los estándares definidos

9. Mapa de controles

Norma	Apartado
CEA- 3.0-07	10.11