Lleida.net Click&Sign OTP

PSC 1004 Política y declaración de prácticas de prestación del servicio de firma electrónica con OTP – Click&Sign

Lleida.net
Parc Agrobiotech | Edifici H1 2a planta, 25003 Lleida (Spain)

Control de documentación

Descripción

El presente documento tiene por objetivo describir el cumplimiento respecto a la finalidad y contenidos, con lo establecido por las normas ETSI EN 319 401 *General Policy Requirements for Trust Service Providers* así como los aspectos técnicos del servicio de entrega electrónica certificada prevenidos en el artículo 26 del Reglamento eIDAS.

Histórico de documentación

Versión	Fecha	Autor	Descripción
1	26/8/2024	Eva Pané	Versión inicial.

Clasificación y estatus del documento

Clasificación del documento	Público
Estado	Aprobado

Documentos relacionados

Descripción

Lleida.net

Contenido

1. Introducción

LLEIDANETWORKS SERVEIS TELEMÀTICS, S.A. es una operadora de comunicaciones con autorización de la Comisión del Mercado de Telecomunicaciones para la prestación de los servicios de Transmisión de datos-Proveedor de acceso a internet (10/12/1998); Servicio telefónico fijo (11/05/2005); Transmisión de datos - Almacenamiento y reenvío de mensajes (23/4/2008); y operador móvil virtual - completo (5/12/2008) estando especializada en la actualidad en la prestación de servicios de confianza dotando de seguridad a la realización de actos jurídicos en Internet así como a su remisión y notificación segura y certificada.

Con esta finalidad la empresa se constituye como Prestador de Servicios Electrónicos de Confianza, bajo la denominación de Lleida.net Lleida.net de conformidad con lo dispuesto en el Reglamento UE 910/2014 (de ahora en adelante, Reglamento eIDAS) del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE con efectos del 1 de julio de 2016.

2. Política y declaración básica de prácticas para la prestación del servicio de firma electrónica mediante OTP – Click&Sign

La presente Política regula la prestación del servicio de firma electrónica mediante OTP por Lleida.net mediante el servicio Click&Sign

2.1.Declaración básica del servicio de firma electrónica

La Declaración básica del servicio de firma electrónica mediante OTP (CLICK&SIGN) de Lleida.net recoge las condiciones y aspectos fundamentales del servicio que, junto a otras condiciones y aspectos más específicos, se recogen en este documento. En consecuencia, mediante la presente declaración básica, Lleida.net afirma que:

Titularidad

CLICK&SIGN es un servicio del LLEIDANETWORKS SERVEIS TELEMÀTICS, S.A., empresa cuyos datos de contacto se encuentran en el apartado 1.3.4 de la Declaración de Prácticas de Certificación.

Disponibilidad del servicio

La disponibilidad del servicio es la descrita en el presente documento.

Publicación de la Política

Los usuarios tendrán acceso a esta política o a la versión aplicable en cada momento en la URL https://www.lleida.net/es/politicas-y-practicas

Mecanismos criptográficos

La firma electrónica de las evidencias de remisión y recepción de envíos electrónicos se realiza calculando el hash mediante SHA256, y en base a certificados X.509 versión 3 y al RFC 3280 "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*", utilizando para ello certificados cualificados expedidos por Lleida.net PKI SLU, antes InDenova, o Firmaprofesional como proveedor de respaldo.

Validez de las evidencias de firma electrónica

CLICK&SIGN no establece otras limitaciones a la confianza que merece su servicio de firma electrónica certificada que las que son inherentes a las tecnologías utilizadas y a las presunciones legales. Lleida.net hará siempre uso de las técnicas criptográficas que se consideren más avanzadas, especialmente las indicadas en la norma TS 119 312.

Aplicabilidad

Lleida.net considera que el uso más apropiado del servicio de firma electrónica es la generación de una prueba documental que acredite la remisión, por parte un remitente, la recepción y, en su caso, la firma por parte de uno o más firmantes, de un determinado documento en formato PDF, así como del momento en que ambas se produjeron.

Obligaciones

Las obligaciones de las partes usuarias están descritas en el presente documento.

Registro de las operaciones

Lleida.net registra sus operaciones y conserva esta información en adecuadas condiciones de seguridad.

Normativa

La prestación del servicio de firma electrónica (CLICK&SIGN) por parte de Lleida.net se realiza de acuerdo con la legislación española y europea aplicable a la materia, con las presentes Políticas y declaración de prácticas y con la normativa interna de Lleida.net.

Responsabilidad

Las responsabilidades de Lleida.net y las limitaciones establecidas sobre la misma se describen más arriba en el presente documento.

Reclamaciones

Todas las reclamaciones de usuarios y terceros sobre la prestación del servicio de entrega electrónica certificada deberán serle comunicadas según lo establecido en el presente documento. En el caso de que no se llegara a un acuerdo entre las partes estas se someterán a los juzgados y tribunales indicados en el apartado "Jurisdicción"

Garantía y auditorías

Lleida.net garantiza que la prestación del servicio de entrega electrónica certificada es conforme con las estipulaciones incluidas en estas Políticas y declaración de prácticas. En este sentido, Lleida.net llevará a cabo auditorías periódicas del funcionamiento de Lleida.net, de acuerdo con las directrices establecidas en el presente documento.

Tarifas

Lleida.net podrá pedir una contraprestación económica por la prestación del servicio de entrega electrónica certificada, de acuerdo con las tarifas que en cada momento se encuentren publicadas en su web.

Partners

Lleida.net puede distribuir el servicio a través de terceros, los cuales deberán cumplir con la Declaración de Prácticas de Certificación y las Política del servicio que distribuya. Asimismo se acordará en un contrato sus obligaciones y responsabilidades.

Proveedores

Lleida.net utiliza los servicios de proveedores para la prestación del servicio, en concreto son los siguientes:

- Lleida.net PKI SLU, antes InDenova.

2.2. Comunidad de usuarios

La comunidad de usuarios para la firma electrónica son los remitentes del documento y los firmantes, o terceros que actúen su nombre, y que acrediten interés legítimo. También forman parte de la comunidad las personas y entidades que confían en las evidencia expedidas por Lleida.net

Lleida.net es responsable de la remisión o puesta a disposición de los firmantes de los documentos y del registro fehaciente de la firma de los mismos, cuando ésta se produzca. También es responsable de la generación y emisión de las evidencias firmadas acreditando estos hechos y el momento en el que se produjeron.

Son partes usuarias quienes solicitan a Lleida.net la realización de una firma electrónica, así como los firmantes que aceptan recibirla. Asimismo, aquellas personas que confían en las evidencias de firma electrónica generadas por Lleida.net.

Todos ellos estarán sujetos a lo dispuesto en la presente Política.

2.3. Usos del servicio

El uso más apropiado del servicio de firma electrónica avanzada es la generación de una prueba documental que acredite la remisión, por parte de Lleida.net o una tercera parte, y la recepción, por parte de uno o más firmantes, de un determinado envío electrónico, así como del momento en que ambas se produjeron y, en su caso, acceso a documentación adjunta o su descarga, con la finalidad principal de que pueda ser utilizada en contextos de resolución de controversias.

2.4. Obligaciones

Además de las obligaciones establecidas por la ley y de las ya enumeradas, se establecen las siguientes obligaciones específicas para la prestación del servicio de entrega electrónica certificada.

Lleida.net

1. Dar fe de la remisión de los envíos o ponerlos a disposición del firmante o firmantes en la forma dispuesta en esta Política, emitiendo la correspondiente certificación.
2. Disponer los medios apropiados para que el firmante o firmantes del envío puedan generar de forma segura el correspondiente acuse de recibo.
3. Validar, en su caso, la firma o firmas electrónicas de los firmantes en la forma exigida por las correspondientes Políticas de Certificación.
4. Recibir y conservar los certificados de estado de entrega, generando en base a los mismos la certificación de entrega y poniendo ésta a disposición del remitente.
5. Utilizar medios de firma electrónica y sellos de tiempo apropiados para la generación de las certificaciones.
6. Garantizar la confidencialidad de los envíos, utilizando para ello técnicas decifrado cuando sea de aplicación.

Partes usuarias

1. Garantizar que los envíos remitidos obedecen a una relación jurídica con los firmantes y que no son comunicaciones no deseadas por los mismos, salvo cuando el envío esté amparado por lo dispuesto en una ley.
2. Proporcionar a Lleida.net datos de contacto de los firmantes que sean fiables y estén actualizados.
3. Cuando la parte usuaria sea el aceptante de un envío, utilizar medios de firma electrónica apropiados para la generación del correspondiente acuse de recibo y, en su caso, para el acceso al contenido cifrado.
4. Verificar la validez de las firmas electrónicas y sellos de tiempo incorporados en las certificaciones de remisión y recepción de envíos.
5. Notificar cualquier hecho o situación anómala relativa al servicio de entrega electrónica certificada, o a las certificaciones emitidas, y que pueda ser considerado como causa de la perdida de fiabilidad de las mismas.

Partes proveedoras

1. Garantizar que los servicios de firma digital utilizados para el servicio de entrega electrónica certificada ostenten la consideración de cualificados según el reglamento eIDAS.
2. Garantizar que los servicios de sellado de tiempo utilizados para el servicio de entrega electrónica certificada ostenten la consideración de cualificados según el reglamento eIDAS.
3. Proporcionar a Lleida.net los certificados digitales necesarios para la firma electrónica y sellado de tiempo de la documentación emitida por el proceso de entrega electrónica certificada.
4. Proporcionar a Lleida.net el servicio de sellado de tiempo para el proceso de entrega electrónica certificada.
5. Los citados servicios podrán ser prestados internamente por Lleida.net una vez que amplíe la funcionalidad de su infraestructura de servicios de confianza.

2.5. Registro de información referente al servicio

Lleida.net mantiene registros de toda la información relevante referente a sus operaciones por un periodo de 5 años des de la finalización de la prestación del servicio. Los registros se protegen para garantizar su integridad y confidencialidad.

Los registros están a disposición de quienes ostenten un interés legítimo para el acceso a los mismos y de las autoridades y tribunales que los requieran de acuerdo con lo dispuesto en las leyes.

En particular se mantienen registros, que incluyen el momento en que se produjeron, sobre los siguientes eventos:

Peticiones de entrega de envíos y resultado de las mismas;
Acuses de recibo emitidos por los firmantes;
Evidencias de recepción, reenvío y entrega;

Los procedimientos para la generación y conservación de los mencionados registros se detallan en la documentación interna de gestión de CLICK&SIGN.

2.6. Prestación del servicio

2.6.1. Acceso al servicio

Los usuarios pueden solicitar la entrega electrónica certificada de uno o más envíos en las formas previstas en la documentación interna de gestión de CLICK&SIGN. La dirección de acceso al servicio es https://admin.clickandsign.eu

2.6.2. Disponibilidad del servicio

El servicio de firma electrónica está disponible de forma ininterrumpida, salvo mantenimiento programado, caídas debidas a servicios de terceros, caso fortuito y fuerza mayor en cuyo caso la interrupción no excederá de 99,5% en una ventana de medición mensual.

2.6.3. Características del servicio

El servicio de firma electrónica Click&Sign mediante OTP se prestará de la siguiente manera:

El remitente utiliza medios electrónicos para proporcionar a LLEIDA.NET el contenido del contrato y los pertinentes identificadores de contacto electrónico, como el número de teléfono móvil y/o la dirección electrónica, recopilados en el proceso de identificación.

Una funcionalidad de seguridad separa la generación de los datos de creación de una firma con OTP (contraseña de un solo uso), al mismo tiempo que se envía al firmante el mensaje que contiene la URL que permite iniciar el procedimiento de firma.

El código OTP no se almacena como texto normal en ningún momento antes de que el signatario lo utilice para expresar su consentimiento introduciendo el código en la forma presentada en el punto final de la firma, produciendo así la firma electrónica, de manera que la OTP queda bajo el control exclusivo del firmante. Cuando el sistema de Lleida.net genera la OTP, se guarda un hash de la OTP. Cuando el firmante introduce la OTP, se calcula su hash y se compara con el hash almacenado en el sistema de Lleida.net.

Una vez generada la firma, los datos de creación de la firma OTP se almacenarán en texto normal en la acreditación, como prueba para que el firmante reconozca la firma y como evidencia jurídica para el ordenante y las partes que confían.

El algoritmo utilizado para generar el hash de la página de aterrizaje (identificación única de URL del punto final del servicio que gestiona la firma avanzada) tiene en cuenta el valor del hash de los distintos documentos que van a firmarse así como los datos identificadores del firmante, lo que hace que los datos de la firma sean únicos y garantiza la integridad de los datos que van a validarse, así como la vinculación del documento con el firmante.

El procedimiento de inicio de firma de Lleida.net validará y garantizará que todos los datos recibidos tengan el formato correcto y autorizará la operación, procediendo a guardar los documentos en un almacenamiento cifrado y en una base de datos.

Durante la operación de almacenamiento de los documentos electrónicos, se calculará su valor de hash (sin los metadatos del certificado en PDF, para ser compatible con una

firma biométrica manuscrita, otro servicio de Lleida.net) y se guardará en una tabla, junto con el resto de datos relevantes que identifican de forma única el documento.

La URL del servicio de firma incluirá una dirección de dominio con un prefijo que identificará el servicio de Lleida.net (por ejemplo, https://sign.clickandsign.eu/h/) y una parte calculada para identificar al firmante y el documento a firmar: esta parte única, denominada aquí "landing_hash", se calculará a partir de los datos personales del firmante recibidos por el servicio de firma de Lleida.net, y el valor del hash del documento o documentos.

La pantalla del servicio de firma que aparece cuando se accede a la URL muestra un mensaje de descargo de responsabilidad que indica que la firma se aplicará a todos los documentos mostrados en la página de aterrizaje del servicio de firma. Esta pantalla también incluye información sobre los términos y condiciones del propio servicio de firma avanzada y de los aspectos destacados del documento subyacente que va a firmarse y que son relevantes para la formalización del consentimiento.

El "landing_hash" se calcula mediante un algoritmo SHA256 con los datos siguientes:

- Se calculará un document_hash para cada documento a firmar. Cada document_hash estará relacionado con un identificador único de los ficheros de la tabla.
- Una cadena formada por el conjunto de datos asociado al firmante en formato de cadena JSON. Suele incluir el número de teléfono, la dirección electrónica, el nombre y apellido, el documento de identidad, etc., entre otros datos. El ordenante/oferente es quien proporciona estos datos en el momento de iniciar el proceso de solicitud de firma y será responsabilidad suya, como AR, vincularlos a la identificación del firmante.
- contract_id: identificador único del oferente que identifica el proceso de firma.
- La fecha de registro de la solicitud para iniciar el proceso de firma en formato de sello de tiempo UNIX.
- Identificador único del firmante, signatory_id.
- Identificador único de la multifirma, signature_id. Identifica de forma única un proceso de firma (puede haber varios firmantes en el mismo proceso de firma).

En todo caso el remitente deberá facilitar a Lleida.net, bajo su responsabilidad, la dirección de correo electrónico del destinatario o destinatarios del envío,

La evidencia que se emite a las partes usuarias estará en formato y tendrá, como mínimo el siguiente contenido:

- Un número de serie único;
- Una evidencia de estado del proceso y de su carácter probatorio
- Los datos asociados al remitente;
- Los datos asociados al firmante;

La fecha y horas de los eventos de todo el proceso

Lleida.net adopta las medidas técnicas precisas para garantizar que las evidencias que se emiten a las partes usuarias de recibo son seguros e incluyen un sello electrónico cualificado y un sello de tiempo que acredita el momento en el que se generó la misma, con la fecha y hora correctas.

2.7. Medidas de seguridad

Lleida.net tiene implantado un sistema de gestión de la seguridad de la información certificado contra la norma ISO/IEC 27001 que alcanza los servicios de confianza objeto de esta política.

A tal efecto, Lleida.net ha documentado, adoptado e implantado, tras la realización de un análisis de riesgos, una política de seguridad, una organización para la seguridad, así como los controles de seguridad necesarios para mitigar el riesgo identificado en las siguientes áreas:

1. Adopción de una política de seguridad con inclusión de las directrices de la Dirección en seguridad de la información, el conjunto de políticas para la seguridad de la información, así como su revisión.

2. Implantación de controles en cuanto a aspectos organizativos de la seguridad de la información, con asignación de responsabilidades para la seguridad, implantación de segregación de tareas, seguridad de la información en la gestión de proyectos e implantación de controles en movilidad. Concienciación, educación y capacitación en seguridad de la información.

3. Implantación de procesos para la gestión de activos, estableciendo un inventario de los mismos con indicación del uso aceptable en atención a la clasificación de la información tratada o almacenada

4. Implantación de procesos de gestión de control de accesos físico y lógico, control de acceso a las redes y servicios asociados, gestión de acceso de usuario, gestión de altas/bajas en el registro de usuarios, gestión de los derechos de acceso asignados a usuarios, gestión de los derechos de acceso con privilegios especiales.

5. Gestión de información confidencial de autenticación de usuarios, revisión, retirada o adaptación de los derechos de acceso de los usuarios, así como del uso de información confidencial para la autenticación.

6. Control de acceso a sistemas y aplicaciones, con controles de restricción del acceso a la información, procedimientos seguros de inicio de sesión, gestión de contraseñas de usuario, uso de herramientas de administración de sistemas y control de acceso al código fuente de los programas

7. Implantación de medidas de seguridad física y ambiental, estableciendo un perímetro de seguridad física, controles físicos de entrada, seguridad de oficinas, despachos y recursos, así como protección contra las amenazas externas y ambientales.

8. Medidas de control de la seguridad de los equipos, implantación de controles de emplazamiento y protección de equipos, instalaciones de suministro, seguridad del cableado, mantenimiento de los equipos, así como procedimientos de salida de activos fuera de las dependencias de la empresa y de seguridad de los equipos y activos fuera de las instalaciones.

9. Establecimiento de responsabilidades, documentación y procedimientos de operación, gestión de cambios, gestión de capacidades, separación de entornos de desarrollo, prueba y producción, protección contra código malicioso

10. Políticas de copias de seguridad, registro de actividad y supervisión, registro y gestión de eventos de actividad.

11. Gestión de vulnerabilidades técnicas y gestión de incidentes de seguridad de la información y mejoras, respuesta a los incidentes de seguridad y planificación de la continuidad de la seguridad de la información.

Los procedimientos mencionados se detallan en la documentación interna de gestión de CLICK&SIGN de carácter confidencial.

2.8. Notificación de cambios

Lleida.net procederá a notificar los cambios que pudieran afectar a la aceptación del servicio respecto a su comunidad de usuarios de la siguiente manera:

- Obligatoriamente, se remitirá un correo electrónico explicativo del cambio a los usuarios remitentes.
- Solamente en algunos casos, dependiendo de la magnitud de la modificación, se publicará en la página web una advertencia destacada por el tiempo que se considere razonable.

3. Terminación

En caso de que Lleida.net cesara en la operación de los servicios descritos en esta política, procederá a su notificación a la Autoridad de Supervisión correspondiente, a la entidad de certificación que haya realizado su última evaluación de conformidad, así como a todos sus clientes presentes y que lo hayan sido en los últimos cinco años, con una antelación de, al menos, cuarenta y cinco (45) días naturales previos a la finalización del servicio.

En el plazo de preaviso, los clientes podrán solicitar el acceso, a su cargo, a las evidencias generadas en sus transacciones con Lleida.net, quien las facilitará en un formato legible por humanos. En todo caso, y a los efectos legales procedentes, y a partir de la expiración del periodo de preaviso, Lleida.net procederá al archivo de las evidencias en formato PDF conforme los procedimientos internos de generación y preservación de evidencias vigentes.

Dada la naturaleza de las propias evidencias generadas y del hecho de su envío a los clientes y el mantenimiento de la clave pública utilizada para la firma de evidencias por el proveedor de firma digital, no es necesaria la transferencia de los derechos y obligaciones del servicio a un tercero en el supuesto de extinción de Lleida.net como persona jurídica.

Las acciones a realizar para la ejecución de la terminación serán las siguientes:

- Notificación a clientes de los servicios, presentes y que lo hayan sido en los últimos cinco años, con una antelación de, al menos, cuarenta y cinco (45) días naturales previos a la finalización del servicio.
- Notificación a proveedores de los servicios.
- Notificación al Ministerio de Industria.
- Borrado de la clave privada utilizada para la firma de evidencias.