Declaración de Prácticas y Políticas del Servicio de Entrega Cualificada

Servicios de Confianza

Evicertia
Octubre de 2021

Público

1 Tabla de Contenidos

2 Introducción

2.1 Presentación

Evicertia, S.L. (Evicertia) es un Prestador de Servicios de Cualificación (PSC) que presta "Servicios Cualificados de Entrega Electrónica Certificada" (QERDS) de acuerdo a lo indicado en la Sección 7 del 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.

2.2 Nombre del documento e identificación

Este documento es la "Declaración de Prácticas y Políticas del Servicio de Entrega Cualificada" de Evicertia en los sucesivo "DPPSEC".

Este documento debe ser leído a la par que la Declaración de Prácticas (DPC) de Evicertia, a la cual está subordinada. A lo largo de la presente DPPSEC se hace referencia a apartados de dicha DPC que sirven para completar el presente documento.

2.3 Participantes en los servicios de certificación

Revisar este apartado en la DPC de Evicertia.

2.4 Uso del servicio de entrega cualificada

2.4.1 Usos permitidos

El servicio de entrega cualificada genera y expide affidavits[1] con el fin de probar que una serie de datos referentes a la comunicación entre emisor y receptor han existido y no han sido alterados a partir de un instante específico en el tiempo. Su uso se limita a las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios.

2.4.2 Límites y prohibiciones de uso

El servicio de entrega cualificada no se utilizará para fines distintos de los especificados en el presente documento. Del mismo modo, el servicio deberá emplearse únicamente de acuerdo con la regulación aplicable.

2.5 Administración de la política

2.5.1 Organización que administra el documento

Los datos de la sociedad son los siguiente:

- Evicertia, S.L. (Evicertia)
- NIF: ESB86021839

[1] *Affidavit*: documento legal que sirve como testimonio o declaración jurada ante un tribunal, o como garantía o aval en otros casos. © Diccionario panhispánico del español jurídico.

- Registro Mercantil de Madrid Tomo: 28127, Libro: 0, Folio 11, Sección 8, Hoja M-506734, Inscripción 1.

2.5.2 Datos de contacto de la organización

Los datos de contacto de Evicertia, S.L., son los siguientes:

- Web: https://www.evicertia.com
- Email: info@evicertia.com
- Teléfono: +34914237080
- Fax: +34911410144
- Domicilio postal: c/ Lagasca, 95. 28006, Madrid

2.5.3 Procedimientos de gestión del documento

El sistema documental y de organización de Evicertia garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

3 Control de versiones

Ver.	Fecha	Observaciones
1.0	12/05/2021	Se aprueba la primera versión de este documento.
1.1	22/10/2021	• Se modifican los periodos de conservación de los affidavits para indicar que son 15 años mínimos en los apartados 4.1 y 6.2. • Se mejora la información sobre los PSC emisores de certificados en el apartado 8.1.1.

4 Publicación y preservación

4.1 Depósito

Evicertia custodia de manera segura todos los *affidavits* generados un mínimo de 15 años. Asimismo, dispone de un Depósito, en el que se publican las informaciones relativas al servicio de entrega cualificada. El depósito de publicación se puede consultar en https://www.evicertia.com/.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de Evicertia, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo de acuerdo con los plazos y procedimientos establecidos con respecto de la continuidad del negocio.

4.2 Publicación de información del prestador de servicios de certificación

Evicertia publicará las siguientes informaciones, en su depósito:

- La Declaración de Prácticas de Certificación de Evicertia.
- El texto de divulgación, en lo sucesivo "TD" del servicio de entrega cualificada.
- Las claves públicas de los certificados utilizados para la firma de los *affidavits*.

4.3 Frecuencia de publicación

La información del PSC, incluyendo el TD, la DPC y esta DPPSEC , se publica en cuanto se encuentra disponible.

Los cambios en la DPPSEC se rigen por lo establecido en el procedimiento de gestión de este documento y de acuerdo a la normativa de aplicación.

4.4 Control de acceso

Revisar este apartado en la DPC de Evicertia**.**

5 Identificación y autenticación

5.1 Identificación

Para poder usar los servicios de entrega cualificada de Evicertia será necesario que tanto el emisor como el receptor de las comunicaciones hayan pasado por el proceso de verificación de identidad de Evicertia, siendo necesario que las dos partes sean suscriptores del servicio.

El proceso de verificación de la identidad de los suscriptores será mediante presencia física en cualquiera de las oficinas de registro de Evicertia.

Será necesaria la entrega de la documentación (DNI, Pasaporte) que acredita que la persona es quien dice ser, o el representante legal (escritura pública o poder) en caso de una persona jurídica (empresas, entidades, corporaciones, ...).

Una vez comprobada la identidad de la persona se activará para dicho usuario las funcionalidades correspondientes del servicio de entrega cualificada de Evicertia.

5.2 Autenticación del emisor

La autenticación del emisor para enviar comunicaciones se hará mediante usuario (vinculando a su correo electrónico) y contraseña, proveyendo el servicio medios para aplicar políticas complejas de contraseñas y reseteos seguros de las mismas.

5.3 Autenticación del receptor

La autenticación del receptor se realiza mediante doble factor de autenticación con una URL temporal aleatoria, y un OTP (One-Time Password) que será enviado al email o teléfono móvil del receptor.

6 Requisitos operacionales

6.1 Acceso al servicio

El acceso a las diferentes URL del servicio de entrega cualificada siempre se realizará mediante protocolos seguros y comunicaciones cifradas.

6.2 Eventos y evidencias

Como se indican en el artículo 3.36 del reglamento eIDAS el servicio de entrega electrónica cualificada es *<<un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada;>>*, por lo tanto el servicio de Evicertia permite recopilar evidencias que permitan asegurar que los mensajes electrónicos del emisor son entregados al receptor de los mismos garantizando la integridad de la evidencia y la veracidad de la misma.

El encargado de garantizar esta integridad y veracidad es el propio PSC, a través de una serie de procesos criptográficos como la aplicación de firmas electrónicas y sellos de tiempo cualificados. Tanto los procesos de firma como los sellos de tiempo son proporcionados por PSC cualificados de acuerdo a lo indicado en el reglamento eIDAS.

Las evidencias en Evicertia se denominan *affidavits* y son documentos en los que se recopila toda la información pericial que permita demostrar que un evento se ha producido, y no ha sido modificado con posterioridad. En los *affidavits* se puede encontrar:

- Datos de información del emisor y receptor de los mensajes electrónicos.
- El contenido emitido, junto con los documentos adjuntos procesados, además se incorporan resúmenes criptográficos de los mismos.
- En los *affidavits* se puede encontrar información sobre los siguientes eventos:
    - Envío y emisión al servidor de correo del destinatario.
    - Entrega al servidor de correo del destinatario o fallo si no se pudiera entregar.
    - Apertura del mensaje.
    - O acciones posteriores del receptor (si es que se producen).
    - La referencia temporal estará indicada en horario *Coordinated Universal Time* (UTC).

Cada *affidavit* es firmado electrónicamente por el servicio, y se le incluye un sello de tiempo cualificado, para de esta manera garantizar la integridad del documento y que éste no haya sido modificado con posterioridad.

El emisor tendrá acceso a todos sus *affidavits* en el servicio de entrega cualificada, durante el periodo de custodia contratado con un periodo mínimo de quince años. El receptor podrá acceder a los *affidavits* a través del servicio de soporte o por información del emisor. Una vez que el periodo de vigencia contratado haya concluido ninguna de las partes tendrá acceso a los *affidavits*.

En el caso de producirse un fallo con la integridad de los *affidavits*, o se produjera cualquier incidencia asociada a la integridad del contenido durante el proceso de entrega se comunicará desde el servicio de soporte de Evicertia a las partes interesadas.

7 Controles de seguridad física, de gestión y de operaciones

Revisar este apartado en la DPC de Evicertia**.**

8 Controles de seguridad técnica

Evicertia emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

8.1 Generación e instalación del par de claves

8.1.1 Generación del par de claves

Los certificados electrónicos cualificados del servicio de entrega serán generados por Prestadores de Servicios Cualificados eIDAS como Firma Profesional (www.firmaprofesional.com), de acuerdo con su Declaración de Prácticas de Certificación y su Texto de Divulgación, encontrándose disponibles en su página web.

Asimismo, se han seguido los procedimientos de ceremonia de claves de Evicertia, dentro del perímetro de alta seguridad destinado a esta tarea. Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por Evicertia.

Para la generación de claves de los certificados electrónicos cualificados del servicio de entrega se utilizan dispositivos con las certificaciones *FIPS 140-2 level 3* o *Common Criteria EAL4+*.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

Certificados electrónicos cualificados del servicio de entrega	2.048 bits	Hasta 5 años

8.1.2 Envío de la clave pública al emisor del certificado

Los métodos para la remisión de la clave pública al prestador de servicios electrónicos de confianza es *PKCS#10*, otra prueba criptográfica equivalente o cualquier otro método aprobado por Evicertia.

8.1.3 Distribución de la clave pública del prestador de servicios de certificación

Las claves públicas de Evicertia son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las autoridades de certificación raíz y subordinadas estarán a disposición de los usuarios en la página web de Evicertia.

8.1.4 Tamaños de claves

La longitud de las claves de los certificados utilizados para la firma de los *affidavits* será como mínimo de 2048 bits.

8.1.5 Generación de parámetros de clave pública

La clave pública de los certificados utilizados para la firma de los *affidavits* está codificada preferentemente de acuerdo con RFC 5280.

8.1.6 Comprobación de calidad de parámetros de clave pública

La calidad de los parámetro de la clave pública será por lo menos:

- Longitud del Módulo = 4096 bits
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

8.1.7 Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en el apartado “Generación del par de claves”.

8.2 Protección de la clave privada

Revisar este apartado en la DPC de Evicertia**.**

8.3 Controles de seguridad informática

Revisar este apartado en la DPC de Evicertia**.**

8.4 Controles técnicos del ciclo de vida

Revisar este apartado en la DPC de Evicertia**.**

8.5 Controles de seguridad de red

Revisar este apartado en la DPC de Evicertia.

8.6 Controles de ingeniería de módulos criptográficos

Revisar este apartado en la DPC de Evicertia.

8.7 Fuentes de Tiempo

Revisar este apartado en la DPC de Evicertia.

9 Auditoría de conformidad

Revisar este apartado en la DPC de Evicertia.

10 Requisitos comerciales y legales

Revisar este apartado en la DPC de Evicertia.

11 Anexo I - Acrónimos

A continuación se muestran los acrónimos utilizados en la presente DPC.

- AC: Autoridad de Certificación
- CA: Certification Authority. Autoridad de Certificación
- RA: Autoridad de Registro
- CN: Common Name
- CP: Certificate Policy
- CPD: Centro de Procesamiento de Datos
- CPS: Certification Practice Statement. Declaración de Prácticas de Certificación
- CRL: Certificate Revocation List. Lista de certificados revocados
- CSR: Certificate Signing Request. Petición de firma de certificado
- DES: Data Encryption Standard. Estándar de cifrado de datos
- DN: Distinguished Name. Nombre distintivo dentro del certificado digital
- DPC: Declaración de Prácticas de Certificación
- DSA: Digital Signature Algorithm. Estándar de algoritmo de firma
- DCCF: Dispositivo Cualificado de Creación de Firma
- ETSI: European Telecommunications Standards Institute o Instituto Europeo de Normas de Telecomunicaciones
- QSCD: Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma
- FIPS: Federal Information Processing Standard Publication
- ISO: International Organization for Standardization. Organismo Internacional de Estandarización
- LRC: Listas de Revocación de Certificados
- LDAP: Lightweight Directory Access Protocol. Protocolo de acceso a directorios
- NTP: Network Time Protocol

- OCSP: On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
- OID: Object Identifier. Identificador de objeto
- OTP: One-Time Password
- PA: Policy Authority. Autoridad de Políticas
- PC: Política de Certificación
- PDS: Texto de divulgación
- PIN: Personal Identification Number. Número de identificación personal
- PKCS: Public-Key Cryptography Standards
- PKI: Public Key Infrastructure. Infraestructura de clave pública
- PSC: Prestador de Servicios Electrónicos de Certificación / Confianza
- RSA: Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
- SHA: Secure Hash Algorithm. Algoritmo seguro de Hash
- SSL: Secure Sockets Layer
- TCP/IP: Transmission Control. Protocol/Internet Protocol
- TSA: Autoridad de Sellado de Tiempo
- TSU: Unidad de Sellado de Tiempo
- URL: Uniform Resource Locator o localizador de recursos uniforme.