PO01

POLITICA DE BIOMETRÍA

Hoja de Vida

Nº	Modificaciones efectuadas	Fecha	Realizado por	Revisado y aprobado
1	Primera Edición	11/12/2015	Flavio Tapia	Luis Chavez
2	Versión 1.2 Se incorporan referencias a auditoría externa	12/08/2016	Flavio Tapia	Luis Chavez
3	Tercera Edición	Agosto 2023	Arquitecto Líder	Comité de Seguridad

Tabla de contenido

Introducción

El objetivo de este informe es comprobar que la política de Firma Biométrica contiene los aspectos relevantes de Seguridad y están acorde a lo establecido a la política de E-Sign (PSC), involucrando a toda la cadena de instituciones dentro de la generación de este servicio.

De esta manera, se busca entregar la confianza en el uso de firma, describiendo la operatividad entre las partes involucradas donde una de éstas por normativa permite que sea un tercero que prese servicios que transparenten los procesos garantizando su invulnerabilidad.

Normativa Técnica

La normativa técnica que se tuvo a la vista para elaborar este documento, es la siguiente:

- Ley N°19.799
- Decreto 181, de 2002, de Economía
- ETSI TS 102 207 V1.1.3 (2003-08) Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services.
- ETSI TR 102 206 V.1.1.3 (2003-08) Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework.
- ETSI TR 102 203 V1.1.1 (2003-05) Mobile Signatures; Business and functional Requirements.
- ETSI TS 102 204 V1.1.4 (2003-08) Mobile Signature Service; Web Service Interface.
- ETSI TS 101 733, v.1.6.3, v1.7.3 y v.1.8.1. Electronic Signatures and Infrastructures (SEI); CMS Advanced Electronic Signatures (CAdES).
- ETSI TS 101 903, v.1.2.2, v.1.3.2 y 1.4.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).
- ETSI TS 102 778, v 1.1.2. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles;

Part 1: PAdES Overview,

Part 2: PAdES Basic - Profile based on ISO 32000-1,

Part 3: PAdES Enhanced - PAdES-BES and PAdESEPES Profiles;

Part 4: Long-term validation

- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.
- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.
- IETF RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation"

1. CLIENTES

Organizaciones

Las Organizaciones corresponde a personas jurídica o naturales, de derecho público o privado, que desean que sus clientes, afiliados o beneficiarios firmen documentos electrónicos haciendo uso de la Firma Avanzada Biométrica

En este caso el rol de la organización es el de iniciar el proceso de firma electrónica de documentos, a través del envío de un documento electrónico al suscriptor final.

De esta forma, los roles que puede ejecutar la Organización son los siguientes:

1. Generación de un documento electrónico para la firma por el Suscriptor.
2. Envío del documento electrónico a E-Sign.
3. Recepción del documento firmado por el Suscriptor, para su almacenamiento.

En este caso, las relaciones entre la Organización y el suscriptor final no se encuentran reguladas por ESign y son resorte de ambas partes, siendo en todo caso voluntario para el suscriptor:

- La firma del documento electrónico
- El rechazo del documento electrónico
- La solicitud a E-Sign de no recibir más mensajes enviados por la empresa o por la Organización, de acuerdo a lo dispuesto por la ley 19.628.

Suscriptores

Los suscriptores, dentro del Subdominio E-Sign de la E-SIGN CA NET, incluyen todos los usuarios finales (incluidas entidades) de certificados emitidos por una CA de E-Sign. Un suscriptor es la entidad señalada como Suscriptor usuario final de un certificado. Los Suscriptores usuarios finales de un certificado pueden ser individuos, organizaciones o componentes de infraestructura, como firewalls, routers, servidores confiables u otros dispositivos utilizados para comunicaciones seguras dentro de una Organización.

En ciertos casos los certificados son emitidos directamente a entidades o individuos para su propio uso. Sin embargo, pueden existir otras situaciones en las cuales la parte requirente de un certificado es distinta del sujeto al cual corresponde la credencial. Por ejemplo, una organización puede requerir certificados para permitir que sus empleados representen a la organización en transacciones o negocios electrónicos. En tales situaciones, la entidad que solicita la emisión de los certificados (es decir paga por él, ya sea a través de la suscripción a un servicio específico, o como el emisor mismo) es diferente de la entidad que es el sujeto del certificado (generalmente el titular de la credencial). En esta CPS son utilizados dos términos distintos para distinguir estos dos roles: “Suscriptor” es la entidad que contrata con E-Sign la emisión de credenciales y; “Sujeto” es la persona a la cual se encuentra asociada la credencial. El Suscriptor carga con la responsabilidad última por el uso de la credencial, pero el Sujeto es el individuo que es autenticado cuando la credencial es presentada.

Cuando se utiliza “Sujeto”, es para distinguirlo del suscriptor. Cuando se utiliza “Suscriptor”, puede significar el Suscriptor como una entidad distinta, o puede estar siendo usado para abarcar a ambas. El contexto en el cual sea usado en esta CPS permitirá distinguir su significado correcto.

Técnicamente las CAs también son suscriptores de certificados dentro de la E-SIGN CA NET, ya sea como una PCA emitiendo un certificado autofirmado para ella misma, o como una CA a la que se le emite un certificado por parte de una CA superior. Las referencias a “entidades finales” y “suscriptores” en esta CPS, sin embargo, aplican solamente a Suscriptores usuarios finales.

Terceros que Confían (Parte que Confía)

Un Tercero que Confía es un individuo o una entidad que actúa confiando en un certificado y/o en una firma digital emitida por E-Sign. Un Tercero que Confía puede o no ser también un Suscriptor de un certificado digital de E-Sign.

Beneficiarios de los certificados

Los beneficiarios de los Certificados de Firma Biométrica incluyen, pero no están limitados a:

1. El suscriptor que es parte en el Acuerdo de Suscriptor de Certificado;
2. Todos los proveedores de aplicaciones de software con los que la entidad emisora raíz se ha celebrado un contrato para la inclusión de su certificado raíz en el software distribuido por dicho proveedor de aplicación de software, y
3. Todos los Terceros que Confían que razonablemente confían en un Certificado Válido.

2. PROCEDIMIENTO DE REGISTRO

Proceso de registro, validación y emisión de FE-Biometrica

Para la operación de Harware, E-Sign cuenta con un producto de verificación biométrica compuesto por una estación y un servidor que se encargand e la administración y manejo de la información capturada, además de interactuar con el hardware necesario para la captura y validación del dato biométrico. Por el momento los componentes biométricos utilizables sólo contemplan uso de huella dactilar.

3. USOS DEL DATO BIOMÉTRICO

El objetivo principal del dato biométrico es poder generar una verificación de identidad que acredite la identidad del suscriptor basándose en mecanismos de comparación de huellas y las aplicaciones o mecanismos dispuestos por el registro civil a través de la cédula de identidad. Dentro de la cadena de valor del producto/proceso se encuentra la utilización de esta información como medio de certificación de la identidad del suscriptor para la posterior emisión de un certificado de firma electrónica biométrica en la nube de ESign.

Llaves asimétricas

La aplicación genera en el dispositivo criptográfico centralizado un par de llaves asimétricas, asociadas a un:

- Usuario (huella por ej.)

- Proveedor envía la llave pública a la CA, para su custodia en Servidor y llaves privadas en el HSM.

- Estas llaves son generadas con algoritmo optimizado con ECDSA, y vinculadas a la FEA en HSM.

Llaves asimétricas para Autenticación

Estas llaves son generadas con algoritmo optimizado de acuerdo al estándar del sistema de firma y custodia de certificados y vinculadas al certificado con las llaves en el HSM.

Son utilizadas para autenticar al dispositivo, y al descargarse en el equipo se verifica que el hash del equipo coincida con el original.

Servidor HSM

Módulo criptográfico, instalado en un servidor para estos fines en el datacenter dispuesto por ESign, en la cual se almacenan las llaves privadas de los suscriptores de certificados de firma electrónica avanzada biométrica.

Base de Datos de certificados

Las llaves privadas de FEA biométrica serán generadas en un dispositivo criptográfico (HSM) y la parte publica de dicho certificado custodiada en una Base de Datos relacionadas con las llaves privadas de los suscriptores mediante el uso de identificadores únicos por registro.

Proceso de Autenticación

- E-SIGN procedimiento de validación: autoriza & valida.
- Una vez validada la FEA:

  Descarga o activación FEA en HSM.
- Emisión

  E-SIGN emite & auto-instala la FEA en HSM.

Propósitos de Uso del Dato Biométrico

El dato biométrico se utiliza para generar un match entre lo verificado al momento de enrolarse en la BdD de E-Sign, contra la cedula emitida por el registro civil y la huella rescatada del usuario.

La generación del procedimiento de identificación permite a la aplicación biométrica poder solicitar al sistema de custodia de certificados (descrito en ET-01), la generación de un par de llaves para la emisión de una FES o FEA (en este procedimiento se explica que se utiliza FEA ya que es la firma avanzada y requiere de HSM).

De esta forma, el almacenamiento, registro de usuarios, uso del dato biométrico y el procedimiento de generación de firma se conectan con el dato biométrico utilizando un TLS (canal seguro) que permite que los datos viajen encriptados desde el origen de la validación y la BdD mediante un canal seguro.

Verificación de datos para evitar Fraudes

- ✓ Se emite un certificado digital FEA en HSM_1 centralizada para FIRMA ELECTRONICA AVANZADA BIOMÉTRICA(*key_usage=digital signature and non-repudiation*), custodiada por E-SIGN.
- ✓ Al mismo instante, se genera un par de llaves para AUTENFICACION (*key_usage=client_authentication*) optimizado y vinculadas a la FEA en HSM_2 validado y asociado al suscriptor mediando el HASH para prevenir cualquier intento de captura o fraude con la Huella capturada

4. OBLIGACIONES

Partes Involucradas

Obligaciones Suscriptor

El Suscriptor se obliga a través de un Acuerdo de Suscriptor que debe aceptar, a:

(a) identificarse a sí mismo con precisión y asegurar la exactitud de la información que usted proporciona a la entidad emisora o su representante autorizado,

(b) cumplir con los términos del Acuerdo y la CPS aplicable, que se incorpora por referencia en dicho Acuerdo

(c) no controlar, interferir o realizar ingeniería inversa de la ejecución técnica de los sistemas, y (d) no responsabilizar a E-Sign por el uso de su certificado.

Los suscriptores deben garantizar, además:

1. Cada firma digital creada utilizando la clave privada correspondiente a la clave pública listada en el Certificado es la firma digital del Suscriptor y el Certificado ha sido aceptado y está operativo (no expirado o revocado) en el momento de crear la firma digital,
2. Sus llaves privadas están protegidas y que nunca alguna persona no autorizada ha tenido acceso a la llave privada del Suscriptor,
3. Todas las declaraciones hechas por el Suscriptor en la Solicitud de Certificado enviada por el suscriptor son verdaderas.
4. Toda la información proporcionada por el Suscriptor y contenida en el Certificado es verdadera,
5. El Certificado está siendo utilizado exclusivamente para fines autorizados y legales, de conformidad con esta CPS, y
6. El Suscriptor es un suscriptor usuario final y no una CA, y no está utilizando la llave privada que corresponde a alguna de las llaves públicas incluidas en el certificado para los efectos de firmar digitalmente cualquier Certificado (o cualquier otro formato de llave pública certificada) o CRL, como CA o de cualquier otra manera.

Usos Prohibidos del Certificado de FEA

Los certificados de FEA deben ser usados solamente en la medida que su uso sea consistente con la normativa legal aplicable, y en particular, los certificados deben ser utilizados sólo de manera permitida por la normativa vigente en Chile.

Ni los certificados de E-SIGN ni los de E-Sign han sido diseñados, concebidos ni autorizados para uso o reventa como equipamiento de control en circunstancias peligrosas o para usos que requieren un rendimiento a prueba de fallas, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armas, en los que una falla podría acarrear directamente la muerte, lesiones personales o daños medioambientales graves.

E-SIGN y E-Sign regeneran periódicamente las llaves de CAs Intermedias. Las aplicaciones de terceros o plataformas que tienen una CA Intermedia incorporada como un certificado raíz, pueden no funcionar como fueron diseñadas después de que la llave de la CA Intermedia haya sido regenerada. Por lo tanto, ESign no garantiza el uso de las CA Intermedias como certificados raíz y recomienda que las CA Intermedias

Deberes de las Partes

Los certificados deben ser usados solamente en la medida que su uso sea consistente con la normativa legal aplicable, y en particular, los certificados deben ser utilizados sólo de manera permitida por la normativa sobre importaciones y exportaciones.

Ni los certificados de E-SIGN ni los de E-Sign han sido diseñados, concebidos ni autorizados para uso o reventa como equipamiento de control en circunstancias peligrosas o para usos que requieren un rendimiento a prueba de fallas, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armas, en los que una falla podría acarrear directamente la muerte, lesiones personales o daños medioambientales graves.

Obligaciones E-Sign

E-Sign garantiza al Suscriptor:

1. Derecho de Uso de los nombres de dominio o dirección IP: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar que el solicitante tenía derecho a usar, o tenía el control del nombre de dominio(s) y direcciones IP que figuran en el asunto del certificado y en la extensión subjectAltName (o se delegó a tal derecho o control por parte de alguien que tenía tal derecho a utilizar o controlar, sólo en el caso de nombres de dominio), (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

2. Autorización de Certificados: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar que el Sujeto autorizó la emisión del certificado y que el representante de la requirente está autorizado para solicitar el certificado en nombre del sujeto, (ii), seguido el procedimiento

al emitir el Certificado, y (iii) el procedimiento descrito con precisión en la Política de Certificación de la CA y / o Declaración de Prácticas de Certificación;

3. Precisión de la Información: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar la exactitud de toda la información contenida en el certificado (con la excepción de la materia: el atributo organizationalUnitName), (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

4. Certeza de la información: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para reducir la probabilidad de que la información contenida en el Certificado del sujeto (salvo el atributo organizationalUnitName) fuese engañoso, (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

5. Identidad del solicitante: Que, si el certificado contiene información sobre la identidad del sujeto, la CA (i) implementó un procedimiento para verificar la identidad del solicitante, (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

6. Acuerdo de Suscriptor: Que, si la entidad emisora y el suscriptor no son Afiliados, el suscriptor y CA son partes de un Acuerdo de Suscriptor legalmente válido y exigible que cumpla estos requisitos, o, si la entidad emisora y el suscriptor están afiliados, el Representante del solicitante haya reconocido y aceptado las Condiciones de Uso;

7. Estado: Que la CA mantiene 24 x 7 un repositorio de acceso público con información actualizada sobre el estado (válido o revocado) de todos los certificados no vencidos, y

8. Revocación: Que el CA revocará el certificado por cualquiera de las razones especificadas en las presentes prescripciones.

5. DECLARACIÓN DE LAS GARANTÍAS, SEGUROS Y RESPONSABILIDAD DE LAS PARTES

Declaraciones y Garantías de la CA

- E-Sign garantiza que:
- No hay declaraciones falsas sustanciales en el Certificado conocidas por o procedentes de las entidades que aprobaron la Solicitud de Certificado o que emitieron el Certificado,
- No hay errores en la información en el Certificado introducidos por las entidades que aprobaron la Solicitud de Certificado o que emitieron el Certificado, como resultado de no ejercer un cuidado razonable en la gestión de la Solicitud de Certificado o en la creación del Certificado,
- Sus certificados cumplen todos los requisitos materiales de esta CPS, y

- Los servicios de revocación y el uso de un repositorio se ajustan a la CPS aplicable en todos los aspectos materiales.

Garantías y obligaciones

E-Sign garantiza a los beneficiarios de certificados que, durante el período en que el certificado es válido, la CA ha cumplido con estos requisitos y con su Política de Certificados y / o Declaración de Prácticas de Certificación en la emisión y la gestión del Certificado. Las garantías de certificados incluyen específicamente, pero no se limitan a, los siguientes:

1. Derecho de Uso de los nombres de dominio o dirección IP: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar que el solicitante tenía derecho a usar, o tenía el control del nombre de dominio(s) y direcciones IP que figuran en el asunto del certificado y en la extensión subjectAltName (o se delegó a tal derecho o control por parte de alguien que tenía tal derecho a utilizar o controlar, sólo en el caso de nombres de dominio), (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

2. Autorización de Certificados: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar que el Sujeto autorizó la emisión del certificado y que el representante de la requirente está autorizado para solicitar el certificado en nombre del sujeto, (ii), seguido el procedimiento al emitir el Certificado, y (iii) el procedimiento descrito con precisión en la Política de Certificación de la CA y / o Declaración de Prácticas de Certificación;

3. Precisión de la Información: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar la exactitud de toda la información contenida en el certificado (con la excepción de la materia: el atributo organizationalUnitName), (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

4. Certeza de la información: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para reducir la probabilidad de que la información contenida en el Certificado del sujeto (salvo el atributo organizationalUnitName) fuese engañoso, (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

5. Identidad del solicitante: Que, si el certificado contiene información sobre la identidad del sujeto, la CA (i) implementó un procedimiento para verificar la identidad del solicitante, (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

6. Acuerdo de Suscriptor: Que, si la entidad emisora y el suscriptor no son Afiliados, el suscriptor y CA son partes de un Acuerdo de Suscriptor legalmente válido y exigible que cumpla estos requisitos, o, si la entidad emisora y el suscriptor están afiliados, el Representante del solicitante haya reconocido y aceptado las Condiciones de Uso;

7. Estado: Que la CA mantiene 24 x 7 un repositorio de acceso público con información actualizada sobre el estado (válido o revocado) de todos los certificados no vencidos, y

8. Revocación: Que el CA revocará el certificado por cualquiera de las razones especificadas en las presentes prescripciones.

Declaraciones y Garantías de la RA

Las RAs garantizan que:

No hay declaraciones falsas sustanciales en el Certificado, conocidas por o procedentes de las entidades que aprobaron la Solicitud de Certificado o que emitieron el Certificado,

No hay errores en la información del Certificado introducidos por las entidades que aprobaron la Solicitud de Certificado, como resultado de no ejercer un cuidado razonable en la gestión de la Solicitud de Certificado,

Sus certificados cumplen todos los requisitos materiales de esta CPS, y

Los servicios de revocación (cuando corresponda) y el uso de un repositorio se ajustan a la CPS aplicable en todos los aspectos materiales.

Declaraciones y Garantías del Suscriptor

Los suscriptores garantizan que:

- Cada firma digital creada utilizando la clave privada correspondiente a la clave pública listada en el Certificado es la firma digital del Suscriptor y el Certificado ha sido aceptado y está operativo (no expirado o revocado) en el momento de crear la firma digital,
- Sus llaves privadas están protegidas y que nunca alguna persona no autorizada ha tenido acceso a la llave privada del Suscriptor,
- Todas las declaraciones hechas por el Suscriptor en la Solicitud de Certificado enviada por el Suscriptor son verdaderas,
- Toda la información proporcionada por el Suscriptor y contenida en el Certificado es verdadera,
- El Certificado está siendo utilizado exclusivamente para fines autorizados y legales, de conformidad con esta CPS, y
- El Suscriptor es un suscriptor usuario final y no una CA, y no está utilizando la llave privada que corresponde a alguna de las llaves públicas incluidas en el certificado para los efectos de firmar digitalmente cualquier Certificado (o cualquier otro formato de llave pública certificada) o CRL, como CA o de cualquier otra manera.

Declaraciones y Garantías del Tercero que Confía

Los Acuerdos del Tercero que Confía requieren que éstos reconozcan que tienen información suficiente para tomar una decisión informada hasta un punto tal que optan por confiar en la información contenida en un Certificado, que ellos son los únicos responsables de decidir si deben o no confiar en tal información, y que ellos asumirán las consecuencias legales de su incumplimiento en el ejercicio de las obligaciones de la Tercero que Confía en términos de esta CPS.

Renuncia de Garantías

Dentro de los límites permitidos por la legislación aplicable, los Acuerdos de Suscriptor y los Acuerdos de la Tercero que Confía renunciarán a las posibles garantías de E-Sign, incluyendo cualquier garantía de comerciabilidad o idoneidad para un propósito particular.

Limitaciones de Responsabilidad

Dentro de los límites permitidos por la legislación aplicable, los Acuerdos de Suscriptor y los Acuerdos de la Tercero que Confía limitarán la responsabilidad de E-Sign. Las limitaciones de responsabilidad deberán incluir una exclusión de daños indirectos, especiales, incidentales y derivados.

La responsabilidad (y/o la limitación de la misma) de los Suscriptores será la establecida en los Acuerdos de Suscriptor aplicables.

La responsabilidad (y/o la limitación de la misma) de las RAs empresariales y de la CA aplicable deberán ser establecidas en el(los) acuerdo(s) entre ellas.

La responsabilidad (y/o la limitación de la misma) de las Terceros que Confian deberán ser las establecidas en los Acuerdos de Terceros que Confian aplicables.

Indemnizaciones

Indemnización por los Suscriptores

Dentro de los límites permitidos por la legislación aplicable, los Suscriptores tienen la obligación de indemnizar a E-Sign por:

- Falsedad o tergiversación de hecho por el Suscriptor en la Solicitud de Certificado del Suscriptor,
- La no revelación de un hecho sustancial en la Solicitud de Certificado, si la falsedad u omisión es consecuencia de negligencia o con la intención de engañar a cualquiera de las partes,
- Faltas del Suscriptor para la protección de la llave privada del Suscriptor, para utilizar un Sistema de Confianza o para tomar, en cualquier otro caso las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de la llave privada del Suscriptor, o

- El uso por parte del Suscriptor de un nombre (incluyendo, sin limitaciones dentro de un nombre común, un nombre de dominio o una dirección de correo electrónico) que infrinja los Derechos de Propiedad Intelectual de un tercero.

El Acuerdo de Suscriptor aplicable puede incluir obligaciones de indemnización adicionales.

Indemnización por las Terceros que Confían

Dentro de los límites permitidos por la legislación aplicable, los Acuerdos de la Tercero que Confía exigirá a las Terceros que Confian indemnizar a E-Sign por:

- La falta de la Tercero que Confía para llevar a cabo las obligaciones de un Tercero que Confía,
- La confianza de la Parte que Confiada en un Certificado que no es razonable bajo las circunstancias, o
- La falta de la Tercero que Confía en la comprobación del estado de tal Certificado para determinar si el Certificado está expirado o revocado.

El Acuerdo de la Tercero que Confía aplicable puede incluir obligaciones de indemnización adicionales.

6. PRIVACIDAD Y PROTECCIÓN DE LOS DATOS

Declaración de Políticas

La privacidad es una de las preocupaciones principales de la mayoría de los usuarios de Internet y un requisito fundamental para el disfrute y la satisfacción general del usuario.

E-Sign, está al tanto de las preocupaciones de privacidad de los visitantes a su sitio Web y ha preparado una declaración de privacidad para explicar al usuario qué información se recopila en el sitio Web de ESign, www.e-sign.cl, y qué se realiza con dicha información.

Protección de datos

E-Sign recopila la siguiente información sobre el Suscriptor y los visitantes a su sitio web:

Información personal

No se recopila ninguna información personal de ninguno de los visitantes del sitio de E-Sign a menos que el visitante proporcione dicha información de forma explícita y deliberada. Si simplemente está visitando el

sitio, no se le solicitará ningún tipo de información personal. La única forma por la que se recibirá información personal sobre el visitante, es si nos envía un correo que incluya dicha información o llenado en algún formulario en nuestra página web. En este último caso, el Suscriptor será debidamente informado respecto del uso que pueda darse a esta información y de su eventual comunicación al público.

Información estadística sobre visitas al Sitio Web

Cuando se visite el sitio de E-Sign, las computadoras pueden recopilar automáticamente información estadística sobre las visitas que se realizan. Esta información no permite la identificación personal, sino sólo como una visita al sitio. Es posible que E-Sign monitorice estas estadísticas tales como el número de personas que visitan el sitio, la dirección IP del usuario, las páginas visitadas, los dominios desde los que acceden los visitantes y los navegadores utilizados. Estos datos estadísticos acerca de las visitas se utilizan únicamente para obtener una visión global. Esta información estadística ayuda a mejorar el rendimiento del sitio Web.

Uso de cookies

E-Sign no utiliza cookies.

Cómo se utiliza y con quién se comparte la información recopilada

La información recopilada sólo se utiliza por E-Sign y de la manera descrita a continuación.

Facilitar el soporte, renovación y compra de nuestros productos y servicios

Es posible se utilice la información que enviada para facilitar información relativa a la adquisición, renovación y soporte de productos y servicios.

Validación de su identidad (sólo si solicita ciertos tipos de ID Digitales)

Ciertos tipos de ID Digitales requieren que parte de la información de la solicitud sea comparada con información contenida en bases de datos o fuentes de terceros. Hacemos esto para autenticar su identidad y otros atributos y además para prevenir el hurto de información. E-Sign mantiene acuerdos de confidencialidad con las terceras personas antes referidas que restringen la revelación de su información. En determinadas situaciones de carácter excepcional, tenemos contratos que permiten a estas terceras personas revelar la información a sus subcontratistas o afiliados, pero sólo para autenticar su identidad y sólo en la forma establecida en los acuerdos de confidencialidad.

Formación del contenido de una ID Digital

La información exacta que aparece en los distintos tipos de ID Digitales aparece en la página del registro pertinente y en esta declaración de políticas de privacidad. Generalmente, esta información se limita al nombre, dirección y e-mail, pero ciertos tipos de ID Digitales contienen información adicional. Por ejemplo, los Certificados SSL pueden contener el número de RUT (Rol Único Tributario) de la organización. ***Toda información contenida en un ID Digital que usted nos envíe será publicada. La publicación de las ID Digitales en un lugar accesible es fundamental para posibilitar el uso generalizado de una ID Digital. Su ID Digital será publicada en nuestros registros a fin de que terceros puedan acceder y examinar su información de ID Digital. Usted no debe esperar ningún tipo de privacidad en relación con la información contenida en su ID Digital.***

Si la ley nos obliga a revelar datos

Si la ley o un juzgado competente nos obligara a revelar información a algún organismo estatal u otro, para cumplir con la ley, lo haremos.

Encuestas

De vez en cuando podemos solicitar información a personas que nos hayan enviado información de contacto a través de encuestas. La participación en estas encuestas es totalmente voluntaria, por lo que es decisión del usuario revelar o no esta información. La información de las encuestas se utilizará con propósitos de seguimiento o para mejorar el uso y satisfacción de este sitio Web.

AUDITORÍA EN TERRENO

No existe una auditoría externa completa sobre todos los elementos de la plataforma tecnológica y de emisión de firma electrónica biométrica.

Sin embargo, se realizan auditorías externas respecto de la mayor parte de los componentes críticos de la plataforma:

a) **Auditoría ISO 27001**
   Realizada en el marco de la certificación ISO 27001, la última es de fecha 2023.

b) **Inspección Anual Ordinaria (IAO)**
   Ejecutada por la Entidad Acreditadora de la Subsecretaría de Economía y Empresas de Menor Tamaño.

Conclusiones

La Política de Firma Biométrica de E-Sign es concordante con la Política de Certificados de la empresa, y solamente refleja las diferencias específicas que posee el proceso de generación, descarga y uso de la firma electrónica avanzada a través de biometría.