



POLÍTICA DE FIRMA MOVIL

Santiago, 3 de abril de 2020

E-SIGN S.A.



 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	2 de 22

Contenido

Introducción.....	3
Normativa Técnica	4
Clientes	5
Descripción de Clientes.....	5
Procedimiento de Registro	7
Proceso de registro, validación y emisión de FEA.....	7
Verificación de datos para evitar Fraudes.....	10
Obligaciones Suscriptor	11
Usos Prohibidos del Certificado de FEA.....	12
Deberes de las Partes	12
Obligaciones E-Sign.....	13
Declaración de las Garantías, Seguros y Responsabilidad de las Partes.....	14
Privacidad y Protección de los Datos	19
Declaración de Políticas	19
Protección de datos	19
Consistencia entre la política de seguridad, la CPS y la CP	21
Difusión.....	22
Revisión de las Políticas	22
Preguntas y Actualizaciones	22
Control de Documento	22

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	3 de 22

Introducción

El objetivo de este informe es comprobar que la política de Firma Móvil 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 éste servicio.

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

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	4 de 22

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 V1.1.3 (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, v.1.7.3 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 (SEI); 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 PAdESEPPES Profiles;

Part 4: Long-term validation

- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (SEI); 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.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	5 de 22

- 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"

Cientes

Descripción de 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 Móvil.

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:

Generación de un documento electrónico para la firma por el Suscriptor.

Envío del documento electrónico a E-Sign.

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 E-Sign 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.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	6 de 22

Suscriptores

Los suscriptores, dentro del Subdominio E-Sign de la E-SIGN CA NET, incluyen todos los usuarios finales (incluidos 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.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	7 de 22

Beneficiarios de los certificados

Los beneficiarios de los Certificados de Firma Móvil 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.

Procedimiento de Registro

Proceso de registro, validación y emisión de FEA

El proceso de registro, validación y emisión de firma electrónica avanzada del Suscriptor, consta de los siguientes pasos:

1. Descarga de aplicación móvil

En forma previa al enrolamiento, el suscriptor debe descargar la aplicación móvil SAFE SIGNER, desde el almacén de aplicaciones, dependiendo de la tecnología utilizada:

- Cliente instala la App móvil.
- La aplicación móvil generará un “SAFE-ID”, tipo OTP que queda “HOLD”.
- Posteriormente el Suscriptor debe ingresar el “SAFE-ID” en el enrolamiento WEB.

2. Enrolamiento

El enrolamiento consta en un registro web del Suscriptor.

Cuando el suscriptor se enrola para obtener un certificado de firma electrónica avanzada, el suscriptor debe ingresar información personal. La información personal que debe ingresar es:

- Rut

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	8 de 22

- Serie Cedula de Identidad
- Nombres (incluir todos sus nombres)
- Apellido Paterno
- Apellido Materno
- Dirección de correo electrónico. Debe cumplir con la condición que la dirección de email debe tener relación con el nombre. No puede ingresar direcciones de correo genéricas, p.e.: info@dominio.com, gerencia@dominio.com, etc. Esta exigencia no será aplicada en el caso que la verificación sea realizada por un funcionario público.
- “SAFE-ID”
- Frase Secreta o Contraseña: La contraseña será utilizada en caso que el suscriptor necesite revocar su certificado digital a través de la web de E-Sign.

Finalmente el suscriptor deberá Aceptar el Acuerdo del Suscriptor para completar el enrolamiento.

3. Validación

La validación de la identidad del Suscriptor debe ser realizada de cualquiera de las formas aceptadas por E-Sign, según el Plan de Validación vigente

- Mediante verificación de la identidad utilizando información generada por E-Sign: esta información puede haber sido generada de dos formas
 - Mediante verificación presencial del suscriptor en oficinas de E-Sign.
 - Mediante verificación biométrica de la identidad del suscriptor, contra la base de datos de huella digital de E-Sign, a través de un servicio seguro aprobado por ESign. En este caso la confirmación de la identidad del suscriptor será verificada electrónicamente con la información enviada a E-Sign desde el respectivo dispositivo biométrico.
- A través de validación presencial en Notaría Pública, y envío físico del formulario respectivo a las oficinas de E-Sign
- Mediante la confirmación de la identidad del suscriptor, otorgada en por un órgano del Estado de Chile, respecto de sus funcionarios: en caso que la identidad del suscriptor sea validada por algunos de estos servicios, haciendo uso de información que poseen en sus bases de datos para comprobar la identidad del respectivo suscriptor.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	9 de 22

4. Notificación de descarga de la FEA

a) EL Cliente es notificado de que su **certificado está listo**:

- Una vez validada la FEA:
 - Se notifica al cliente vía EMAIL (numero solicitud & PIN)
 - Se notifica vía PUSH al móvil.

5. Descarga o activación FEA en HSM.

La FEA será descargada en una HSM de E-Sign, desde la cual se realizará el proceso de firma móvil

Este proceso podrá ser realizado de dos formas:

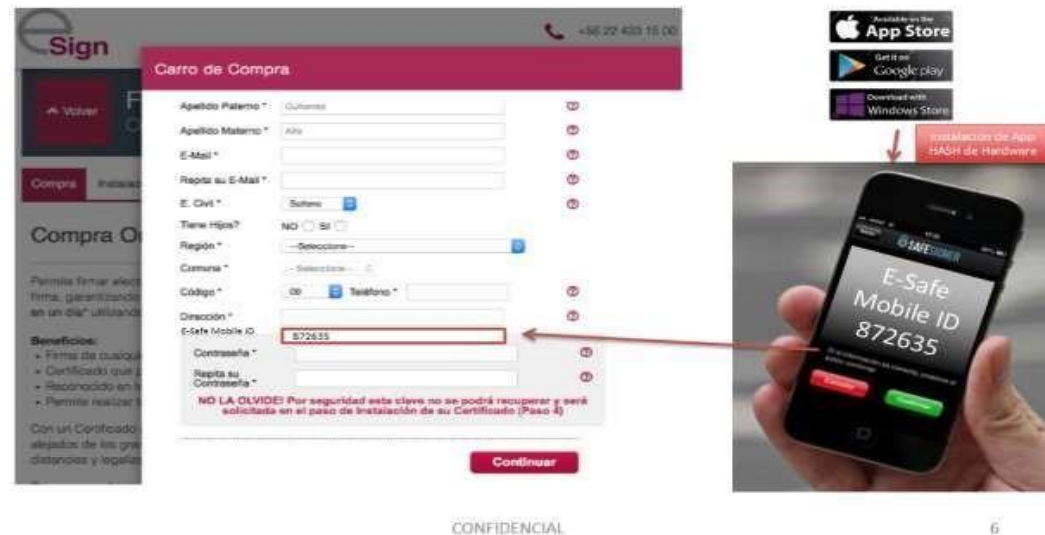
- Usuario ingresa a WEB (desde email de notificación) de Descarga N° Solicitud, PIN y Escanea Código QR.
- Usuario ingresa a Móvil (desde la notificación PUSH) y podría autorizar activación de FEA en HSM desde, ingresando el N° Solicitud y PIN.

En el proceso de descarga, se realizan las siguientes acciones

- Se valida toda la información generada (número de solicitud, frase secreta, Safeld, RUT del Suscriptor).
- E-SIGN emite y auto-instala la FEA en HSM.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL		SI-PO_006
			Fecha de Aprobación Abril 2020
			Página 10 de 22



Verificación de datos para evitar Fraudes

- ✓ Se emite un certificado digital FEA en HSM₁ centralizada para FIRMA ELECTRONICA AVANZADA (*key_usage=digital signature and non-repudiation*), custodiada por E-SIGN.
- ✓ Al mismo instante, se genera un par de llaves para AUTENTICACION (*key_usage=client_authentication*) optimizado a móvil con curva elíptica, y vinculadas a la FEA en HSM₂ (vinculada con el Safe Id), luego se envía la llave privada encriptada al móvil previamente validado y asociado al suscriptor mediante el HASH de Hardware "ESAFE MOBILE ID", y queda instalado en el móvil de manera segura.
- ✓ Vincular FEA en HSM a la llave pública o privada del teléfono Asimétrica CURVA ELIPTICA.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	11 de 22

Obligaciones

Partes Involucradas

Obligaciones Suscriptor

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

- (a) identificarse a si 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.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	12 de 22

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, E-Sign 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.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	13 de 22

Obligaciones E-Sign

E-Sign garantiza al Suscriptor:

- 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;
- 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;
- 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;
- 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;
- 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;
- 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;

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	14 de 22

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.

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

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	15 de 22

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.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	16 de 22

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.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	17 de 22

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. También deberán incluir las siguientes topes de responsabilidad que limitan los daños de E-Sign en relación a un Certificado específico:

Clase	Topes de responsabilidad
Class 1	Cien Dólares EE.UU. (\$ 100.00 EE.UU.)
Class 2	Cinco Mil Dólares EE.UU. (\$ 5,000.00 EE.UU.)
Class 3	Cien Mil Dólares EE.UU. (\$ 100,000.00 EE.UU.)

Tabla 14 - Topes de Responsabilidad

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

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	18 de 22

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 Confían deberán ser las establecidas en los Acuerdos de Terceros que Confían 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 Confían indemnizar a E-Sign por:

- La falta de la Tercero que Confía para llevar a cabo las obligaciones de un Tercero que Confía,

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	19 de 22

- 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.

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 E-Sign, 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

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	20 de 22

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.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	21 de 22

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 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.

Consistencia entre la política de seguridad, la CPS y la CP

La Política de Firma Móvil 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 móvil.

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	

 PÚBLICO	POLÍTICA DE FIRMA MOVIL	SI-PO_006	
		Fecha de Aprobación	Abril 2020
		Página	22 de 22

Difusión

La comunicación de la presente política se efectúa de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se debe hacer difusión mediante los siguientes canales:

- Publicación en sistema Redmine .
- Correo informativo a los interesados.

Revisión de las Políticas

La presente política deberá ser revisada cada tres años o cuando ocurran cambios significativos que impacten los servicios del negocio, para asegurar su continua idoneidad, eficiencia y efectividad.

Preguntas y Actualizaciones

Este documento es actualizado periódicamente, según sea necesario. Por favor envíe sus consultas, o comentarios, a comiteseguridad@esign-la.com.

Control de Documento

Versión	Descripción	Autor	Fecha	Revisión
1.0	Primera Edición	Flavio Tapia	Octubre 2015	
1.1	Actualización Formato e ítem de revisión y actualización	Ronald Pérez	Abril 2020	

Elaborado por:	Aprobado por:	Lugar de Archivo	PÚBLICO
SysAdmin	Jefe de Operaciones	Redmine – Proyecto Webtrust	