

PO02

DECLARACIÓN DE PRÁCTICAS DE BIOMETRÍA



Hoja de Vida

Nº	Modificaciones efectuadas	Fecha	Realizado por	Revisado y aprobado
1	Primera Edición	27-10-2015	Flavio Tapia	Luis Chavez
2	Segunda Edición	30-03-2022	Ronald Pérez	Comité de Seguridad
3	Tercera Edición	12-10-2023	Arquitecto Líder	Comité de Seguridad
4	Cuarta edición	04-06-2025	Oficial de seguridad	Comité de seguridad

Tabla de contenido

Hoja de Vida	2
Introducción	7
Normativa Técnica.....	7
1. Existencia del Documento de Prácticas de Biometría.....	9
Declaración de Prácticas de Biometría	9
Personas involucradas	9
Autoridades Certificadoras.....	9
Autoridades de Registro.....	9
Suscriptores.....	10
Terceros que Confían (Parte que Confía).....	11
Beneficiarios de los certificados	11
Otros Participantes.....	11
Uso del Certificado	11
Certificados Emitidos a Personas (Certificados Individuales).....	12
Certificados Emitidos a Organizaciones.....	12
Niveles de seguridad	13
Usos Prohibidos del Certificado	13
Administración de Política.....	14
Organización Administradora del Documento.....	14
Persona de Contacto	15
Persona que Determina la Idoneidad de la CPS.....	15
Procedimiento de Aprobación de la CPS	15
Definiciones y Acrónimos	15
Responsabilidades de Publicación y Repositorio	16
Repositorios	16
Publicación de la Información de Certificados	16
2. Obligaciones y responsabilidades de la PSC (E-sign).....	18
Declaración de Obligaciones y deberes de E-Sign.....	18

Declaración de las Garantías, Seguros y Responsabilidad de las Partes	20
Declaraciones y Garantías de la CA	20
Garantías y obligaciones.....	21
Declaraciones y Garantías de la RA	22
3. Obligaciones y responsabilidades del solicitante a identificar digitalmente	22
Declaraciones y Garantías del Tercero que Confía	24
Renuncia de Garantías.....	24
Limitaciones de Responsabilidad	24
Indemnizaciones.....	25
Indemnización por los Suscriptores.....	25
Indemnización por las Terceros que Confían	25
Terminación de la PSC BIO	26
4. Ciclo de Vida de los Datos Biométricos.....	28
Proceso de Uso de Datos (Esquema general)	29
Quien puede enviar una Solicitud de Certificado	32
Proceso y responsabilidades del Enrolamiento	32
Procesamiento de la Solicitud de Certificado	33
Funciones de Identificación y Autenticación	33
Aprobación o Rechazo de Solicitudes de Certificado.....	33
Tiempo para procesar las Solicitudes de Certificado	33
Entrega de Certificados	34
Acciones de la CA durante la Entrega de Certificados	34
Notificación de entrega del Certificado al Suscriptor por parte de la CA.....	34
Aceptación del Certificado	34
Conducta Constitutiva de la Aceptación del Certificado.....	34
Publicación del Certificado por parte de la CA	35
Notificación de la emisión del Certificado por la CA a otras entidades	35
Uso del Par de Llaves y del Certificado	35
Uso de la Llave Privada del Suscriptor y del Certificado.....	35
Uso de Certificado y la Llave Pública por parte del Tercero que Confía.....	35

Renovación del Certificado	36
Circunstancias para la Renovación de Certificados.....	36
Quién puede solicitar la Renovación	36
Procesamiento de Solicitudes de Renovación de Certificados	37
5. Controles de Seguridad Técnica	37
Verificación de la existencia de Medidas de Seguridad	37
<i>Generación e Instalación del Par de Llaves</i>	37
Generación de Par de Llaves	37
Entrega de la Llave Privada al Suscriptor	39
Entrega de Llave Pública al Emisor del Certificado	39
Entrega de la Llave Pública de la CA a las Terceros que Confían.....	39
Tamaños de Llaves	40
Requisitos para los Tamaños de Llave	41
6. Controles de Seguridad No Técnica	43
Verificación de Mecanismo de autenticación	43
Nombres.....	43
Requisitos para Nombres	47
CountryName Emisor (requerido)	47
OrganizationName Emisor (requerido)	47
CommonName Emisor (opcional)	47
subjectAlternativeName (requerido)	48
CountryName (opcional).....	48
OrganizationName (opcional)	48
OrganizationalUnitName (opcional).....	49
commonName (opcional).....	49
domainComponent (opcional)	50
Otros atributos del Sujeto	50
Necesidad de que los Nombres sean Significativos.....	50
Anonimato o Seudónimos de los Suscriptores	50
Reglas de Interpretación de Diversas Formas de Nombre	51

Unicidad de los Nombres	51
Reconocimiento, Autenticación, y el Rol de las Marcas Comerciales	51
Validación de Identidad Inicial.....	51
Método para probar la posesión de la Llave Privada	51
Autenticación de la Identidad de una Organización	52
Deberes	53
Verificación de Mecanismos de Auditoría de Información relevante	54
Frecuencia de Procesamiento del Registro	54
Periodo de Retención para el Registro de Auditoria.....	54
Protección de Registro de Auditoria.....	54
Procedimientos de Respaldo de los Registros de Auditoria.....	54
Sistema de Recolección de Auditoria (Interna vs. Externa)	55
Notificación al Sujeto Causante del Evento.....	55
Evaluación de Vulnerabilidades	55
Archivo de Registros	55
Tipos de Registros Archivados	55
Periodo de Retención Para el Archivo	56
Protección del Archivo	56
Procedimientos de Respaldo del Archivo	56
Requisitos de Sellado de Tiempo de los Registros.....	56

Introducción

El objetivo de este informe es verificar que el PSC de Biometría disponga de un documento, que señale los procedimientos de operación tanto para usarlos Datos Biométricos como el marco de aplicación de los mismos

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, 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. Existencia del Documento de Prácticas de Biometría

Declaración de Prácticas de Biometría

El proceso de Práctica de biometría consiste en la definición el conjunto de procesos y partes involucradas, así como los tipos de certificados que a través de este modelo se pueden emitir.

De esto se puede inferir la interrelación, garantías, deberes y derechos que emanan de la generación de una firma electrónica avanzada y sus interfaces que pueden ser usadas a través de tokens físicos, dispositivos móviles y biométricos respectivamente. El modelo en este sentido es uno solo y lo que cambia solamente es el terminal. E-Sign a través de este documento por ende describe lo que su declaración de prácticas de certificación describe. Este documento se encuentra disponibilizado de forma publica en el sitio <https://www.esign-la.com/cps/>

Personas involucradas

Autoridades Certificadoras

El término de Autoridad Certificadora (CA) es un término genérico que se refiere a todas aquellas entidades autorizadas para emitir certificados de llave pública dentro de la E-SIGN CA NET. El termino CA engloba una subcategoría de emisores denominados Autoridades Primarias de Certificación ("PCA"). Las PCA actúan como raíces de tres dominios, uno por cada clase de certificado. Cada PCA es una entidad de E-SIGN. Las Autoridades Certificadoras de E-Sign que emiten certificados a suscriptores usuarios finales y otras CAs están subordinadas a las PCAs.

Los clientes empresariales de E-Sign pueden operar sus propias CAs como una CA subordinada a una PCA de ESign. Dichos clientes entablan una relación contractual con E-Sign, en virtud de la cual deben atenerse a todos los requerimientos de las CP E-SIGN CA NET y de la CPS de E-Sign. Estas CAs subordinadas pueden, sin embargo, implementar prácticas más estrictas de acuerdo a sus requerimientos internos.

Autoridades de Registro

Una Autoridad de Registro (RA) es una entidad que ejecuta labores de identificación y autenticación de solicitantes de Certificados de usuario final, inicia o transmite solicitudes de revocación de certificados de usuario final, y aprueba solicitudes de renovación o regeneración de llaves de certificados, en nombre de una CA de la E-SIGN CA NET. E-Sign puede actuar como RA para los certificados que emite.

Terceras personas que entablan una relación contractual con E-Sign, pueden operar sus propias RA y autorizar la emisión de certificados por una CA de E-Sign. Las RAs de terceras partes deben cumplir con todos los requisitos de la CP de la E-SIGN CA NET, la CPS de E-Sign y los términos del acuerdo contractual de servicios empresariales con E-Sign. Sin embargo, las RAs pueden implementar prácticas más restrictivas, de acuerdo a sus requerimientos internos¹.

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.

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 bajo el subdominio E-Sign. Un Tercero que Confía puede o no ser también un Suscriptor bajo el subdominio E-Sign.

Beneficiarios de los certificados

Los beneficiarios de los Certificados de las CA de E-Sign 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

Otros Participantes

Los Clientes Empresa son organizaciones que pueden operar sus propias entidades emisoras como una CA bajo E-SIGN CA NET, para las personas que forman parte de su organización.

Uso del Certificado

Uso Adecuado de los Certificados

Certificados Emitidos a Personas (Certificados Individuales)

Los Certificados Individuales son usados normalmente por individuos para firmar o encriptar correos electrónicos (e-mail) y para autenticarse en aplicaciones (autenticación de cliente). Aun cuando los usos más comunes para un certificado individual están incluidos en la Tabla 1 de más abajo, un certificado individual puede ser utilizado para propósitos distintos, a condición de que el Tercero que Confía pueda confiar razonablemente en que el certificado y su uso no está en modo alguno prohibido por la ley, la CP E-SIGN CA NET, la CPS bajo las cuales ha sido emitido dicho certificado o cualquiera de los acuerdos con Suscriptores.

Clase de Certificado	Nivel de Seguridad			U		
	Nivel de Seguridad Bajo	Nivel de Seguridad Medio	Nivel de Seguridad Alto	Firmado	Encriptación	Autenticación
Certificados Class 1						
Certificados Class 2						
Certificados Class 3						

Tabla 1. Usabilidad de Certificados Individuales

Certificados Emitidos a Organizaciones

Los Certificados organizacionales son emitidos a organizaciones luego de haber sido verificado que la Organización existe legalmente, y que los otros atributos de la Organización incluidos en el certificado (excluyendo la información no verificada del suscriptor) hayan sido autenticados, como por ej. la propiedad de un dominio de Internet o de correo electrónico. No es el objetivo de esta CPS el limitar los usos que pueden darse a los Certificados organizacionales. Mientras que los usos más comunes se encuentran señalados en la Tabla 2 de más abajo, un Certificado organizacional puede ser utilizado para otros propósitos, siempre y cuando

una tercera Tercero que Confía puede razonablemente confiar en que el certificado y su uso no se encuentra prohibido en modo alguno por la ley, por la CP de E-SIGN CA NET, por cualquier CPS bajo la cual haya sido emitido el certificado, o cualquier acuerdo con Suscriptores.

Niveles de seguridad

Los **Certificados de bajo nivel de seguridad** son certificados que no deben ser usados para autenticar o asegurar no repudio. La firma digital provee un nivel modesto de seguridad de que el e-mail proviene de un remitente con una dirección e-mail cierta. El Certificado, no obstante, no entrega garantía de la identidad del Suscriptor. La aplicación de cifrado permite a un Tercero que Confía el uso del Certificado de un Suscriptor para cifrar los mensajes al Suscriptor, si bien la Tercero que Confía remitente no puede estar segura de que el destinatario es de hecho la persona nombrada en el certificado.

Los **certificados de nivel medio de seguridad** son certificados adecuados para garantizar algunas comunicaciones vía e-mail inter e intra organizacional, comercial y personal que requieren un nivel medio de seguridad respecto de la identidad del Suscriptor, en relación a los certificados Class 1 y 3.

Los **certificados de nivel alto de seguridad** son certificados Class 3 individuales y organizacionales, que proporcionan un alto nivel de seguridad sobre la identidad del suscriptor, en comparación con los certificados Class 1 y 2.

Usos Prohibidos del Certificado

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. Además, los Certificados Class 1 no deberán utilizarse como prueba de identidad o como soporte de no repudio de identidad o autoridad. Los

Certificados de Cliente están destinados a aplicaciones de cliente y no deberán utilizarse como Certificados de servidor o Certificados Organizacionales.

Los certificados de CA no son utilizados para una función distinta de las funciones de CA. Asimismo, los certificados para Suscriptores usuarios finales no son usados como certificados de CA.

E-Sign regenera 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 no sean embebidas en aplicaciones y/o plataformas como certificados raíz. E-Sign recomienda el uso de raíces PCA como certificados raíz.

Administración de Política

Organización Administradora del Documento

E-Sign S.A.

Avenida Apoquindo 6550, oficina 501

Las Condes

Santiago

Chile

At: Desarrollo de Prácticas - CPS Fonos: (56)

(2) 2433.1500, (56) (2) 2433.1501 practicas@esign-la.com

Persona de Contacto

Administrador de la Política de Certificados (PMA) E-Sign

S.A.

Avenida Apoquindo 6550, oficina 501 Las Condes

Santiago

Chile

+56 (2) 24331500 +56 (2) 24331501 practicas@esign-la.com

Persona que Determina la Idoneidad de la CPS

El Administrador de la Política de Certificados es responsable de determinar si esta CPS y otros documentos de la naturaleza de esta declaración, complementaria o subordinada a las CPS, son idóneas bajo la CP y esta CPS.

Procedimiento de Aprobación de la CPS

La aprobación de esta CPS y sus posteriores modificaciones se harán por el PMA.

Las modificaciones constarán en un documento que contenga una forma modificada de la CPS o un aviso de actualización. Las versiones modificadas o actualizaciones estarán vinculadas a la sección Actualizaciones y Avisos de las Prácticas del Repositorio E-Sign, la que se encuentra en la sección de Actualización de Prácticas: <https://www.esign-la.com/cps>.

Definiciones y Acrónimos

Ver Apéndice A para las definiciones y acrónimos.

Responsabilidades de Publicación y Repositorio

Repositorios

E-Sign es responsable por las funciones de repositorio para sus propias CA y para las CA de sus Clientes Empresa. E-Sign publica los certificados que emite para Suscriptores usuarios finales en el repositorio de acuerdo con CPS 2.2.

Después de la revocación de un Certificado de Suscriptor usuario final, E-Sign publica un aviso de tal revocación en el repositorio. E-Sign emite CRLs para sus propias CAs y para las CAs de los clientes empresariales dentro de su Subdominio, de conformidad con las disposiciones de esta CPS. Además, respecto de los clientes empresariales que han contratado el servicio de Online Certificate Status Protocol ("OCSP"), E-Sign ofrece servicios OCSP de conformidad con las disposiciones de esta CPS.

Publicación de la Información de Certificados

E-Sign mantiene un repositorio basado en web que permite a las Terceros que Confían hacer consultas en línea sobre la emisión y revocación y otra información del estado del Certificado. E-Sign entrega a las Terceros que Confían información sobre cómo encontrar el repositorio adecuado para comprobar el estado del Certificado y si el servicio de OCSP (Online Certificate Status Protocol) está disponible, sobre cómo encontrar el respondedor OCSP correcto.

E-Sign publica los Certificados que emite en nombre de sus propias CAs. Después de la revocación de un certificado de suscriptor usuario final, E-Sign publicará el aviso de dicha revocación en el repositorio. Además, E-Sign emite Listas de Certificados Revocados (CRL) y, si están disponibles, proporciona servicios de OCSP (Online Certificate Status Protocol) para sus propias CAs.

E-Sign publicará siempre una versión actualizada de los siguientes documentos:

- La CP E-SIGN CA NET
- La CPS de E-Sign,
- Acuerdos de Suscriptor de Certificado Digital

- Acuerdos de Tercero que Confía

E-Sign es responsable de la función de repositorio para las CAs de E-Sign y CAs de Clientes Empresariales que emiten certificados en el Sub.-dominio de E-Sign de la E-SIGN CA NET

E-Sign publica toda la documentación pública de la CA en la sección de repositorio del sitio web de E-Sign en <https://www.esign-la.com/cps>

E-Sign publica los Certificados Digitales emitidos de acuerdo con la siguiente Tabla:

Tipo de certificado	Requerimientos de publicación
PCA E-SIGN CA NET y CAs Raíz Emisoras de la E-SIGN CA NET	Disponible para la Tercero que Confía mediante inclusión en el software actual de navegación y como parte de la Cadena de Certificación que puede ser obtenida con el Certificado de Suscriptor usuario final, a través de las funciones de búsqueda descritas más adelante.
Certificados de CA emisoras de E-Sign	Disponible para la Tercero que Confía como parte de la cadena de certificados que puede ser obtenida con el Certificado de Suscriptor usuario final, a través de las funciones de búsqueda descritas más adelante.
Certificado de la CA de E-Sign que soporta los Certificados de de CA de los Clientes Empresa	Disponible para la Tercero que Confía como parte de la cadena de certificados que puede ser obtenida con el Certificado de Suscriptor usuario final, a través de las funciones de búsqueda descritas más adelante.
Certificados de Respondedores OCSP E-SIGN	Disponible a través de la búsqueda en el servidor de directorio LDAP en..... esign-la.com

Certificados de Suscriptores usuarios finales excepto por ciertos Certificado s Class 3 dependiendo de su uso	Publicados opcionalmente y disponibles para Partes de Confían mediante funciones de búsqueda en el repositorio E-Sign en https://digitalid.e-sign.cl/c2/client/search.htm, https://digitalid.e-sign.cl/fea/client/search.htm, https://arech.e-sign.cl/eu/client/search.htm, https://arech.e-sign.cl/ro/client/search.htm y consulta en el servidor de directorio LDAP de E-SIGN en directory.verisign.com .
Certificados de Suscriptores usuarios finales, emitidos a través de Clientes Empresa	Disponible a través de las funciones de búsqueda descritas anteriormente, aunque a discreción del Cliente Empresa, el Certificado puede ser accesible sólo mediante búsqueda usando el número de serie del Certificado.

2. Obligaciones y responsabilidades de la PSC (E-sign)

Declaración de Obligaciones y deberes de 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.
9. Procedimiento de protección de la información de los solicitantes de datos biométricos: Los datos personales y biométricos capturados a través de la estación y desplegados en la aplicación de administración web son usados únicamente por E-Sign para validar la identidad del suscriptor y la información contenida no es de uso público, no es distribuida ni entregada a terceros y no es extraíble para fines no relativos a la verificación de identidad biométrica.

Los datos biométricos almacenados se encuentran alojados en bases de datos redundantes, si bien personal autorizado puede acceder a la base de datos para fines administrativos y de auditoría y mantenimiento, la API

Biométrica tiene por objetivo manejar y administrar la información contenida mediante lógicas de negocio y programación definidas por el negocio. Independiente del mecanismo de integración a la solución las operaciones y protección de datos siempre están del lado del servidor biométrico por lo que la información sensible es procesada por el servidor y no expuesta a terceros.

Las bases de datos utilizadas para generar el match son internas (propias de E-Sign) y en casos como operaciones de match on card se utiliza la huella capturada del usuario para realizar el match contra la aplicación residente dentro del chip de la cédula.

Para cualquier caso, la aplicación de escritorio integrada a la API envía los datos encriptados a través de TLS los cuales son verificados para autenticar su integridad. Así mismo el uso de los servicios hacia terceros dependerá del establecimiento de relaciones contractuales y habilitación de usuarios y estaciones para operar en un entorno controlado.

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.

3. Obligaciones y responsabilidades del solicitante a identificar digitalmente.

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. 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.

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,

- 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.

Terminación de la PSC BIO

En caso de un escenario de término de la PSC de Biometría, ya sea por origen contractual o técnico, E-sign debe iniciar el procedimiento de término de la PSC de Biometría, ejecutando la siguiente secuencia de pasos:

- Los subscriptores y clientes deben ser notificados individualmente del término de la PSC de Biometría (costos asumidos por E-SIGN). Los subscriptores, y clientes serán notificados a través de los medios de comunicación disponibles y más eficientes respecto de la situación de la PSC de Biometría y los procedimientos a ejecutar para su término. Se informa a los subscriptores, y clientes, sus responsabilidades, acciones a ejecutar, así como las de E-sign. Esta comunicación es originada por el Gerente de Tecnología y es enviada a las contrapartes técnicas y/o comerciales vigentes definidas en etapas de enrolamiento de antecedentes de usuarios.
- Las partes que confían son notificadas a través de la CRL y del servicio OCSP.
- Se deben revocar los certificados de la PSC de Biometría. El equipo de validación procesará la revocación de los certificados digitales y dejará registro de estas actividades utilizando el mismo procedimiento regular de revocación definido en el plan de validación y manual interno de validación.
- Se debe mantener los archivos y registros de la PSC según requerimiento de la CPS. Tal como lo establece la Declaración de Prácticas de Biometría, Manual de validación y plan de validación, E-sign mantendrá registro de los archivos y registros del proceso en relación a cada subscritor, con la estructura de indexación vigente, para ser traspasado a la entidad que corresponda y según sea necesario.
- Se deben mantener operativos los servicios de CRL y OCSP. Los servicios de consulta OCSP y/o CRL vigentes quedarán disponibles por un plazo que sea necesario y no más allá de 60 días desde el vencimiento de del último certificado. Un respaldo de la CRL será enviado a la Entidad Acreditadora para que sea ella quien mantenga la disponibilidad de esta información a quien la requiera.

- E-Sign colaborará en todos los aspectos comerciales y técnicos a los subscriptores, partes que confían y clientes, con el objetivo de no afectar sus procesos productivos, comerciales, de imagen u otros que puedan ser perjudiciales.

En el caso de cesar E-Sign en su actividad, transferirá los datos de sus certificados de firma electrónica avanzada Biométrica a otro prestador de servicios de certificación digital acreditado ante la Subsecretaría de Economía y Empresas de Menor Tamaño, en la fecha en que el cese se produzca. En caso de existir oposición de los titulares de los certificados, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

4. Ciclo de Vida de los Datos Biométricos

Los datos biométricos correspondientes a la persona que realiza el enrolamiento y verificación de identidad mediante el uso de biometría dactilar están sujetos a los mecanismos de operación definidos por la prestadora de servicios de identidad biométrica.

Los datos biométricos son capturados por la estación de enrolamiento y verificación que se encargan de interactuar con los dispositivos físicos dispuestos para las operaciones de enrolamiento; pistola lectora de códigos, lector NFC y dispositivo biométrico dactilar (huellero). Tanto la información extraída de la cédula, como la huella capturada al momento de obtener la información para el match entre huellas (cédula contra huella viva) son almacenadas en el servidor biométrico.

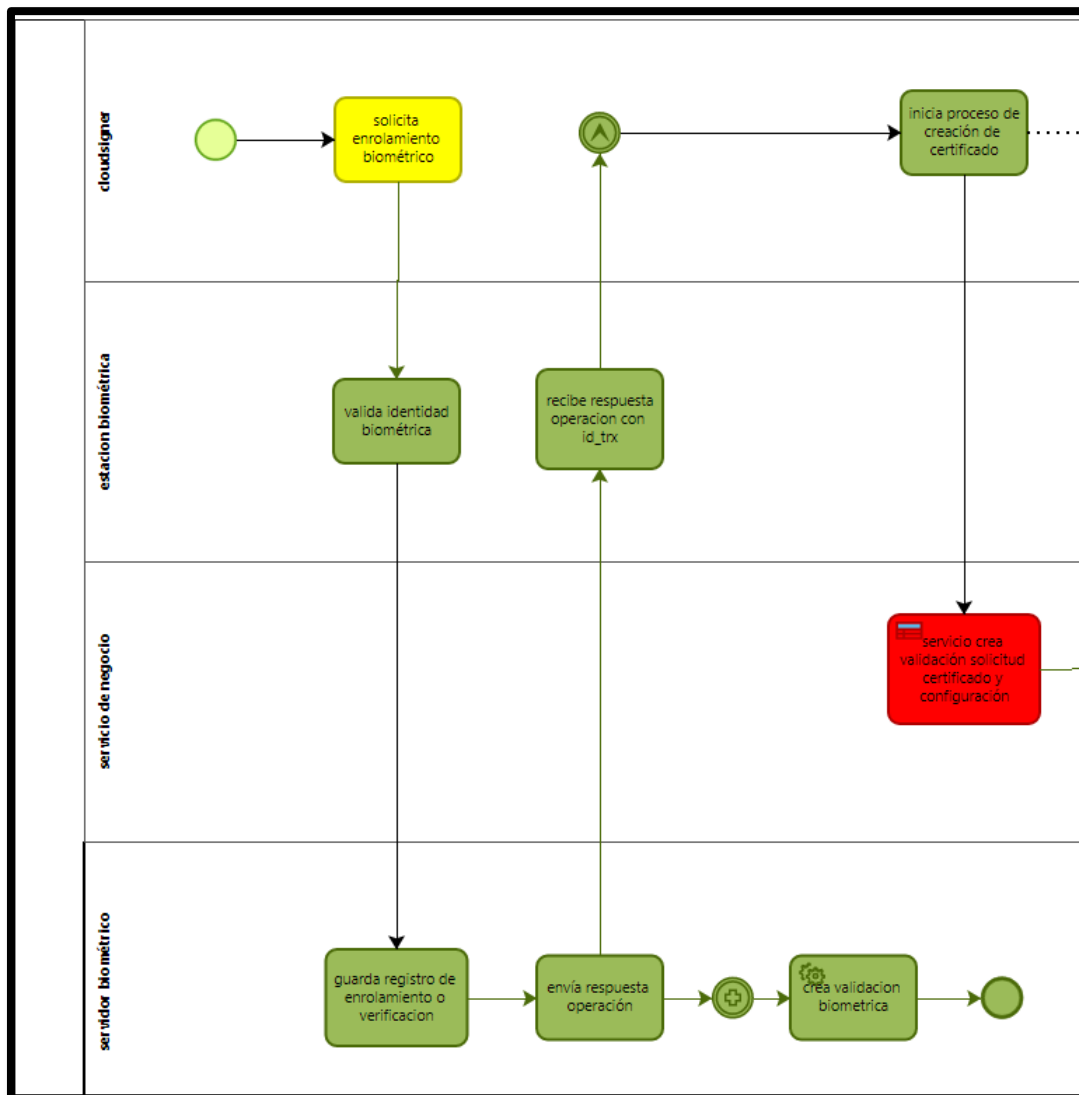
Los datos de la persona son utilizados para complementar la información mínima requerida para la generación de la solicitud y posterior emisión del certificado, así como para identificar a la persona mediante la presentación de su huella frente al dispositivo biométrico.

Las huellas almacenadas en la base de datos correspondiente al servidor biométrico se utilizan para realizar las operaciones de match entre las futuras capturas de huellas asociadas al rut y los templates de huellas o conjuntos de minucias son usados para que por cada operación de validación biométrica se pueda identificar a la persona y obtener su información personal de forma inequívoca a la hora de transcribirla.

Proceso de Uso de Datos (Esquema general)

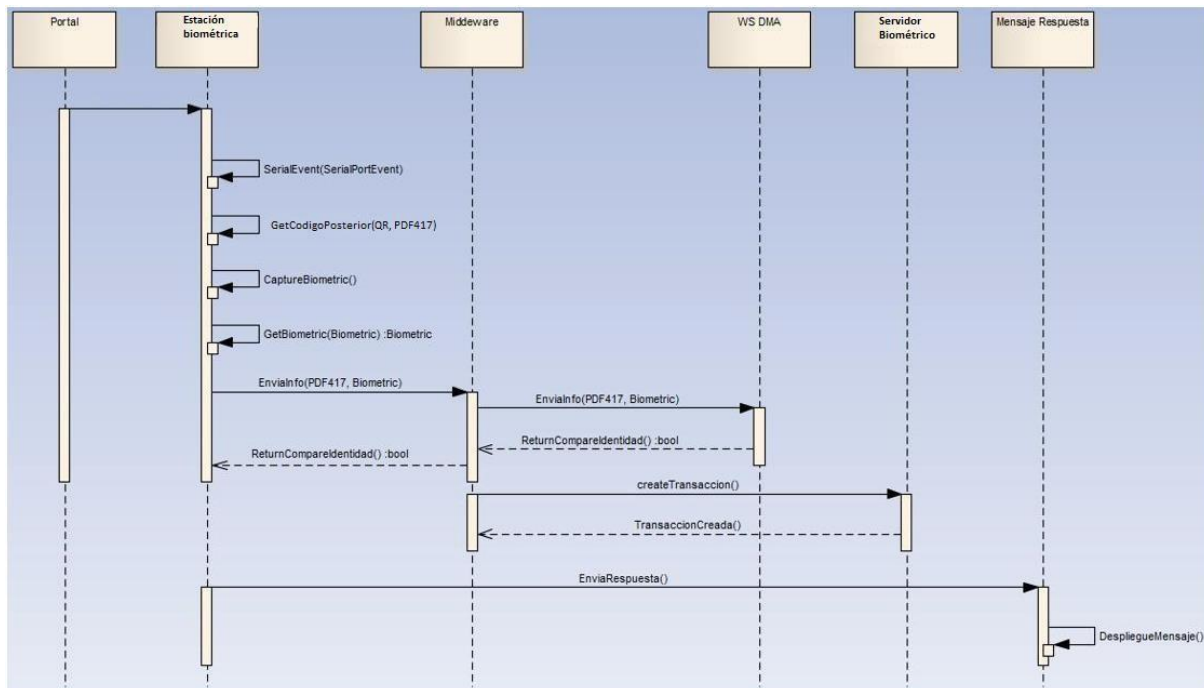
Para la creación de los datos biométricos dentro del sistema biométrico de E-Sign se realiza inicialmente el proceso de enrolamiento mediante el cual se comprueba la identidad del suscriptor en base a la cédula provista y presentada al sistema contra la huella viva, es decir, la huella capturada al momento de realizar la operación de enrolamiento.

El presente diagrama describe un flujo de interacción entre el sistema y sus componentes para la gestión de una solicitud de enrolamiento biométrico.



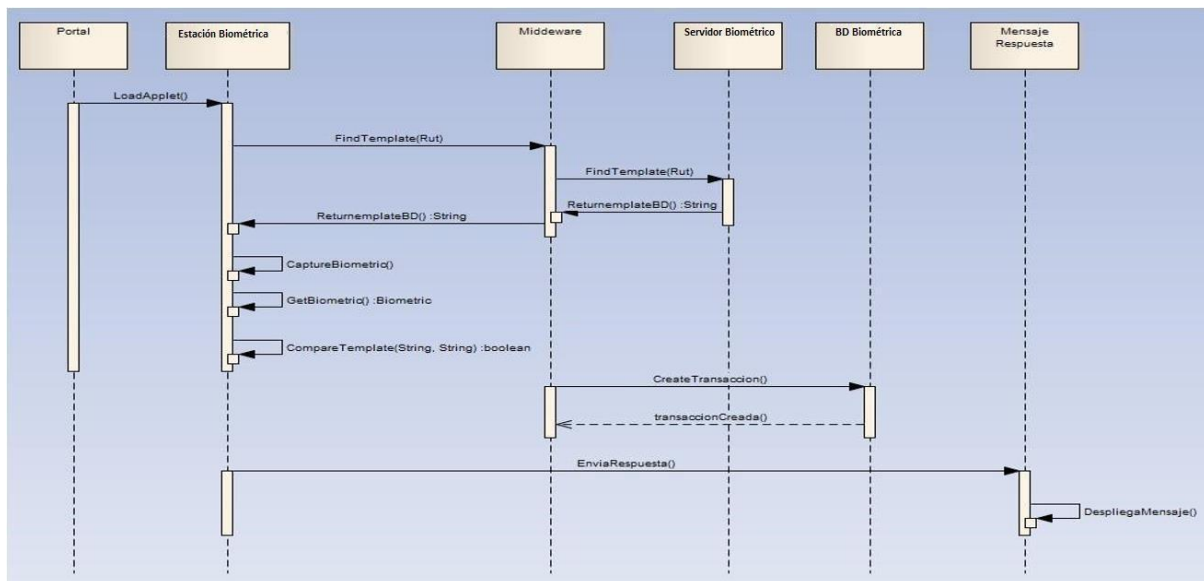
Verificación de identidad contra datos enrolados

El presente diagrama muestra la interacción entre el sitio web cliente, integrado a la estación biométrica que se encuentra preconfigurada en la estación de trabajo donde operan los dispositivos, indicando los mensajes que interactúan entre la estación, el servidor biométrico, la base de datos y el sitio integrador de la solución para efectos de verificación.



Enrolamiento de usuario en la plataforma

El presente diagrama muestra la interacción entre el sitio web cliente, integrado a la estación biométrica que se encuentra preconfigurada en la estación de trabajo donde operan los dispositivos, indicando los mensajes que interactúan entre la estación, el servidor biométrico, la base de datos y el sitio integrador de la solución para efectos de autenticación.



Quien puede enviar una Solicitud de Certificado

- A continuación, se muestra una lista de personas que pueden presentar solicitudes de Certificado:
 - o Cualquier persona que sea el asunto del Certificado,
 - o Cualquier representante de una organización o entidad,
 - o Cualquier representante autorizado de una CA, ☐ Cualquier representante autorizado de una RA.

Proceso y responsabilidades del Enrolamiento

Suscriptores de Certificado de Usuario Final

Todos los Suscriptores de Certificados de usuario final deben manifestar explícita o tácitamente su consentimiento con el Acuerdo de Suscripción que contiene las declaraciones y garantías descritas en la Sección 9.6.3 y se someten a un proceso de enrolamiento, que considera las siguientes obligaciones:

- completar la Solicitud de Certificado y aportar información veraz y correcta,
- generar, o aceptar la generación, del par de llaves
- entregar su, o sus llaves públicas, directamente o a través de la RA, a E-Sign o sus Asociados,
- demostrar la posesión y / o el control exclusivo de la llave privada, físicamente o por medios lógicos, correspondiente a la llave pública entregada a E-Sign y sus Asociados.

Certificados de CA y RA

Los Suscriptores de Certificados de CA y RA celebran un contrato con E-Sign o sus Asociados. Los Solicitantes de la CA y RA deben proporcionar sus credenciales para demostrar su identidad y proporcionar información de contacto durante el proceso de contratación. Durante este proceso de contratación o, a más tardar antes de la Ceremonia de Generación de Llaves para crear un par de llaves de CA o RA, el solicitante debe proporcionar a E-Sign o sus Asociados los elementos para determinar el nombre completo y adecuado del contenido de los Certificados que deban otorgarse al solicitante.

Procesamiento de la Solicitud de Certificado

Funciones de Identificación y Autenticación

Una RA debe realizar la identificación y autenticación de información de los Suscriptores, el solicitante del Certificado debe demostrar que legítimamente posee la llave privada correspondiente a la llave pública que se incluye en el Certificado.

El método para probar la posesión de una llave privada es PKCS # 10, otra demostración criptográficamente equivalente, u otro método aprobado por E-Sign. Este requisito no se aplica cuando un par de llaves es generado por una CA en nombre de un Suscriptor, por ejemplo, cuando las llaves pre-generadas se colocan en tarjetas inteligentes o dispositivos criptográficos seguros.

Aprobación o Rechazo de Solicitudes de Certificado

Una RA aprobará una solicitud de Certificado si se cumplen los siguientes criterios:

- Identificación y autenticación exitosa de la información del Suscriptor que se describe en las funciones de Identificación y Autenticación. □ Que el pago haya sido recibido (si procede)

Una RA rechazará una solicitud de Certificado si:

- Identificación y autenticación exitosa de la información del Suscriptor que se describe en las funciones de Identificación y Autenticación no se puede completar o
- el Suscriptor no presenta la documentación de apoyo,
- el Suscriptor no responde a los avisos en un plazo determinado
- el pago (si aplica) no ha sido recibido,
- la RA cree que la emisión de un Certificado al Suscriptor puede acarrear descredito a la E-SIGN CA NET

Tiempo para procesar las Solicitudes de Certificado

Las CAs y RAs comienzan la tramitación de Solicitudes de Certificado en un plazo razonable luego de la recepción de dichas solicitudes. No existe ninguna estipulación de tiempo para completar la tramitación de una solicitud, a menos que se indique lo contrario en el acuerdo de suscriptor pertinente, CPS u otro acuerdo entre los participantes de la E-SIGN CA NET.

La Solicitud del Certificado se mantiene activa hasta que es rechazada, o transcurra un plazo razonable sin que el solicitante envíe los antecedentes necesarios para su aprobación.

Entrega de Certificados

Acciones de la CA durante la Entrega de Certificados

El Certificado es creado y entregado luego de la aprobación de la Solicitud de Certificado por la CA, o bien, luego de la recepción de un requerimiento de la RA, para que se emita el Certificado.

La CA crea y envía al Solicitante, o a la persona o entidad que éste haya indicado, su Certificado emitido basándose en la información contenida en la Solicitud de Certificado luego de la aprobación de tal Solicitud.

Notificación de entrega del Certificado al Suscriptor por parte de la CA

Las CA emisoras de Certificados a los Suscriptores, ya sea directamente o a través de un RA, notificarán a los Suscriptores, que se han creado los Certificados, y ofrecerán a los Suscriptores el acceso a estos, notificándoles que sus Certificados están disponibles y los medios para su obtención. Los Certificados deberán estar disponibles para los Suscriptores, ya sea permitiéndoles descargarlos desde un sitio web, a través de un mensaje conteniendo el Certificado o a través de la entrega de los medios físicos en los cuales se el certificado. Los certificados pueden ser descargados en forma individual en dispositivos individuales, o de manera centralizada y segura.

Aceptación del Certificado

Conducta Constitutiva de la Aceptación del Certificado

Son conductas constitutivas de aceptación del Certificado, y del respectivo acuerdo de suscriptor:

- Descargar, instalar o usar el Certificado.
- No oponerse expresamente al Certificado o a su contenido.

- Existirá siempre un registro de la aceptación del acuerdo por parte del suscriptor.

Publicación del Certificado por parte de la CA

E-Sign o su Asociado respectivo publica los Certificados emitidos en un repositorio de acceso público.

Notificación de la emisión del Certificado por la CA a otras entidades

Las RAs pueden recibir la notificación de la emisión de Certificados que han aprobado.

Uso del Par de Llaves y del Certificado

Uso de la Llave Privada del Suscriptor y del Certificado

El uso de la llave privada correspondiente a la llave pública del Certificado sólo será permitido una vez que el Suscriptor ha aceptado el Acuerdo de Suscriptor y aceptado el Certificado. El Certificado deberá ser utilizado legalmente en conformidad con el Acuerdo del Suscriptor de E-Sign, los términos de esta CP y la CPS correspondientes. El uso de Certificados debe ser consistente con la extensión del campo KeyUsage, incluido en el Certificado (por ejemplo, si la firma digital no está habilitada, el Certificado no debe ser utilizado para la firma).

Los Suscriptores deben proteger sus llaves privadas de uso no autorizado y se debe dejar de utilizar luego de la expiración o revocación del Certificado.

Uso de Certificado y la Llave Pública por parte del Tercero que Confía

Los Terceros que Confían podrán revisar los términos de uso del Certificado, revisando las CPS específicas indicadas en el contenido del Certificado mismo, y el Acuerdo de Tercera Parte que Confía.

La confianza en un Certificado debe ser razonable bajo las circunstancias. Si las circunstancias indican la necesidad de garantías adicionales, los Terceros que Confían debe obtener tales garantías para que tal confianza se considere razonable.

Antes de realizar cualquier acto de confianza, las partes que confían evaluarán de forma independiente:

- la conveniencia de la utilización de un Certificado para cualquier propósito determinado y determinar que el Certificado, de hecho, se utilizará para un propósito adecuado que no esté prohibido o restringido por la CP. E-Sign, CA y RA no son responsables de evaluar la conveniencia de la utilización de un Certificado.
- Que el Certificado este siendo utilizado de acuerdo con las extensiones del campo *KeyUsage* incluido en el Certificado (por ejemplo, si la firma digital no está habilitada, el Certificado no puede ser invocado para validar la firma de un Suscriptor).
- El estado del Certificado y todas las CAs en la cadena del el Certificado. Si alguno de los Certificados en la Cadena de Certificados ha sido revocado, los Terceros que Confían son los únicos responsables de investigar si la dependencia de una firma digital realizada por un Certificado de Suscriptor antes de la revocación de un Certificado en la cadena de Certificados es razonable. Dicha dependencia se realiza únicamente a riesgo de los Terceros que Confían.

Suponiendo que el uso del Certificado es apropiado, la partes que confían utilizarán el software y/o hardware apropiado para realizar la verificación de firma digital u otras operaciones criptográficas que deseen realizar, como condición para confiar en Certificados que tengan relación con cada operación de este tipo. Dichas operaciones incluyen la identificación de la Cadena de Certificados y la verificación de las firmas digitales en todos los Certificados de la Cadena de Certificados.

Renovación del Certificado

La renovación del Certificado es la emisión de un nuevo Certificado al Suscriptor sin tener que cambiar la llave pública o cualquier otra información en el Certificado. La Renovación del Certificado esta soportada para Certificados de Class 3, donde se genera el par de llaves en un servidor web.

Circunstancias para la Renovación de Certificados

Antes de la expiración de un Certificado de Suscriptor, es necesario que éste haga su renovación de tal forma de mantener la continuidad del uso del Certificado. Un Certificado puede ser renovado después de su expiración.

Quién puede solicitar la Renovación

Sólo el Suscriptor de un Certificado individual o un representante autorizado de una organización puede solicitar la renovación de Certificados

Procesamiento de Solicitudes de Renovación de Certificados

Los procedimientos de renovación aseguran que la persona u organización que persigue la renovación del Certificado sea de hecho sea el Suscriptor del Certificado o la persona autorizada por el Suscriptor.

Un procedimiento aceptable es el uso de una Frase de Comprobación (o su equivalente), o la prueba de posesión de la llave privada.

Los Suscriptores eligen y envían junto con su información de enrolamiento una Frase de Comprobación (o su equivalente). En el momento de la renovación de un Certificado, si el Suscriptor envía acertadamente la Frase de Comprobación (o su equivalente) con información de reinscripción del Suscriptor, y la información de enrolamiento (incluyendo la información del contacto) no ha cambiado, el Certificado renovado se emite automáticamente. Luego de ser renovado el certificado, o al menos luego de la renovación posterior, la CA o RA confirmará la identidad del Suscriptor de acuerdo con los requisitos especificados en la presente CP para la autenticación de una Solicitud de Certificado original.

Aparte de este procedimiento u otro procedimiento aprobado por E-Sign, los requerimientos para la autenticación de una Solicitud de Certificado original se deben utilizar para la renovación de un Certificado de Suscriptor de usuario final.

5. Controles de Seguridad Técnica

Verificación de la existencia de Medidas de Seguridad

Generación e Instalación del Par de Llaves

La infraestructura de CA de E-Sign es operada en la infraestructura segura de E-SIGN, por lo cual la gestión de las llaves de CA de E-Sign es llevada a cabo por E-SIGN de acuerdo a los procedimientos establecidos en esta CPS.

Generación de Par de Llaves

La generación de par de llaves de una CA es desarrollada por varios individuos preseleccionados, capacitados, y confiables que utilizan Sistemas de Confianza y procesos que entregan la seguridad y fuerza criptográfica requerida para las llaves generadas. Para la CA Primarias y las CA de Raíz Emisoras, los módulos criptográficos usados para la generación de las llaves cumplen los requerimientos del FIPS 140-1 nivel 3. Para otras CA (incluyendo las CA de E-Sign y las CA de Clientes de Managed PKI), los módulos criptográficos usados cumplen requerimientos de FIPS 140-1 nivel 2.

Todos los pares de llaves de la CA son generados en Ceremonias de Generación de Llave planificadas con antelación de acuerdo a los requerimientos de la Guía de Referencia de Ceremonia de Llaves, la Guía CA Key Management Tool User's Guide, y la Guía de SAR de E-SIGN. Las actividades ejecutadas en cada ceremonia de generación de llave son registradas, fechadas y firmadas por todos los individuos involucrados. Estos registros se guardan para fines de auditoría y seguimiento durante un plazo estimado apropiado por la administración de E-Sign.

La generación del par de llaves de una RA es realizada generalmente por la RA utilizando un módulo criptográfico certificado según estándares FIPS 140-1 nivel 1 provisto por su software de navegación Web.

Los Clientes Empresariales generan el par de llaves utilizado por sus servidores de Automated Administration. E-Sign recomienda que la generación del par de llaves del servidor de Automated Administration sea realizada utilizando un módulo criptográfico certificado FIPS 140-1 nivel 2.

La generación de pares de llaves de un Suscriptor Usuario Final es llevada a cabo generalmente por el Suscriptor. Para certificados Class 1, certificados Class 2 y certificados Class 3 de firma de código/objeto, el Suscriptor usa típicamente un módulo criptográfico certificado FIPS 140-1 nivel 1 provisto con el software navegación Web para la generación de la llave. Para Certificados de servidor, el suscriptor típicamente usa la utilidad de generación de llave entregada con el software de servidor Web. Para Certificados de Firma Electrónica Avanzada, el Suscriptor debe usar un módulo de hardware certificado FIPS 140-1 nivel 2 o Common Criteria EAL 3.

Para Certificados ACS Application ID, E-Sign genera un par de claves en nombre del suscriptor con una semilla de números aleatorios generados en un módulo criptográfico que, como mínimo, cumpla con los requisitos de FIPS 140-1 nivel 3.

Entrega de la Llave Privada al Suscriptor

Cuando los pares de llaves de un Suscriptor usuario final son generados por el Suscriptor usuario final, la entrega de la llave privada a un Suscriptor no es aplicable. Para los Certificados ACS Application ID, la entrega la llave privada a un Suscriptor tampoco es aplicable.

En caso de que los pares de llaves de la RA o del Suscriptor usuario final sean pre-generados por E-Sign en tokens de hardware o tarjetas inteligentes, tales dispositivos son distribuidos a la RA o al Suscriptor usuario final utilizando un servicio de despacho comercial y un embalaje que evidencie la intrusión. Los datos necesarios para activar el dispositivo son comunicados a la RA o al Suscriptor usuario final mediante un proceso fuera de banda. La distribución de los tales dispositivos es registrada por E-Sign.

Cuando los pares de llaves del Suscriptor usuario final son pre-generados por Clientes Empresariales en tokens de hardware o tarjetas inteligentes, tales dispositivos son distribuidos a los Suscriptores del usuarios finales utilizando un servicio de despacho comercial y un embalaje que evidencie la intrusión. Los datos necesarios para activar el dispositivo son comunicados a la RA o al Suscriptor usuario final mediante un proceso fuera de banda. La distribución de los tales dispositivos es registrada por el Cliente Empresarial.

Para los Clientes Empresariales que usan Managed PKI Key Manager para los servicios de recuperación de claves, el Cliente puede generar los pares de llaves de cifrado (en nombre de los Suscriptores cuyas Solicitudes de Certificados aprueba) y transmitir tales pares de llaves a los Suscriptores a través de un archivo PKCS #12 protegido por contraseña.

Entrega de Llave Pública al Emisor del Certificado

Los Suscriptores usuarios finales y las RA envían electrónicamente su llave pública a E-Sign para la certificación mediante el uso de una Solicitud de Firma de Certificado PKCS#10 (CSR) u otro paquete firmado digitalmente en una sesión protegida por TLS. En caso de que los pares de llaves de la CA, de la RA o del Suscriptor usuario final sean generados por E-SIGN, este requisito no es aplicable.

Entrega de la Llave Pública de la CA a los Terceros que Confían

E-Sign forma parte de la E-SIGN CA NET de E-SIGN por lo que las CA de E-Sign dependen jerárquicamente de la CA Primaria de E-SIGN, lo que implica que, en la práctica, la llave pública de la raíz de la jerarquía de E-Sign corresponde a la llave pública de la CA Primaria de E-SIGN.

E-Sign pone los Certificados de CA para su CAs Primarias y CAs raíces a disposición de los Suscriptores y Terceros que Confían a través de su inclusión en el software de navegación Web. En la medida en que son generados nuevos Certificados de CA Primaria y de CA raíz, E-SIGN entrega estos nuevos certificados a los fabricantes de navegadores Web para su inclusión en las versiones nuevas y en actualizaciones del navegador Web.

E-Sign generalmente entrega la cadena total de certificado (incluyendo su CA emisora y todas las CA en la cadena) al Suscriptor usuario final en el acto de la emisión del Certificado. Los Certificados de las CA de E-Sign también puede ser descargados del Directorio LDAP en: directory.verisign.com.

Tamaños de Llaves

Los pares de llaves deberán tener una longitud suficiente para evitar que otros calculen la llave privada del par de llaves utilizando criptoanálisis durante el período de utilización esperado de dichos pares de llaves. La norma E-Sign para el tamaño mínimo de las llaves es el uso de pares de llaves equivalentes en fuerza a 2048 bits RSA para CA Primarias y CAs².

La tercera y quinta generación de CA Primarias de E-SIGN (G3, G4, G5, G6 y G7) tienen pares de llaves RSA de 2048 bits.

E-SIGN emite certificados para RA y entidades finales con pares de llaves de un tamaño mínimo equivalente en fuerza a RSA de 2048 bits.

²

La confianza de la CA está extendida para las Raíces de Confianza desfasadas de primera y segunda generación (G1 y G2) de Symantec con pares de llaves RSA de 1024 bits para soporte de plataformas desfasadas de cliente y pueden ser emitidos certificados de usuario final de 1024 bits RSA con expiración en o antes del 31 de Diciembre de 2011. Para preservar la continuidad de negocios de aplicaciones desfasadas más allá del 2011, serán permitidas excepciones individuales adicionales con aprobación previa para afiliados de Symantec Corporation que operen las capacidades de software de Processing.Center de acuerdo con la sección respectiva.

La cuarta generación (G4) de Class 3 PCA de E-SIGN (CA de Raíz Universal ECC) incluye una llave ECC de 384 bits.

Todas las Clases de certificados de CA Primarias, de CAs, de RAs y de entidad final de E-Sign y de la E-SIGN CA NET utilizan ya sea SHA-1 o SHA-2 para el algoritmo de hash de la firma digital y algunas versiones de Processing Center de E-SIGN soportan el uso de algoritmos de hash SHA-256 y SHA-384 en Certificados de Suscriptor entidad final.

Requisitos para los Tamaños de Llave

Los Certificados de CA Raíz debe cumplir con los siguientes requisitos para el tipo de algoritmo y el tamaño de la llave:

Algoritmo de Digest	SHA-1 *, SHA-256, SHA-384 o SHA-512
Mínimo tamaño del módulo RSA (bits)	2048
Curva ECC	NIST P-256, P-384 o P-521

Tabla 4A - Algoritmos y tamaños de llave para Certificados de CA Raíz

Los Certificados de CAs subordinadas deben cumplir con los siguientes requisitos para el tipo de algoritmo y el tamaño de la llave:

Algoritmo de Digest	SHA-1 *, SHA-256, SHA-384 o SHA-512
---------------------	-------------------------------------

Mínimo tamaño del módulo RSA (bits)	2048
Curva ECC	NIST P-256, P-384 o P-521

Tabla 4B – Algoritmos y tamaños de llave para Certificados de CA Subordinada

La CA sólo deberá emitir certificados de Suscriptor con llaves que contengan los siguientes tipos de algoritmo y tamaños de clave.

Algoritmo de Digest	SHA-1 *, SHA-256, SHA-384 o SHA-512
Mínimo tamaño del módulo RSA (bits)	2048
Curva ECC	NIST P-256, P-384 o P-521

Tabla 4C - Algoritmos y tamaños de llave CA/Browser Forum para Certificados de Suscriptor

* SHA-1 podrá ser utilizado hasta que SHA-256 sea ampliamente soportado por los navegadores utilizados por una parte sustancial de Terceros que Confían en todo el mundo.

** Un Certificado de CA Raíz emitido antes del 31 Diciembre 2010 con un tamaño de llave RSA menor a 2048 bits aún puede servir como un ancla de confianza para Certificados de Suscriptor emitidos en acuerdo con estos Requisitos.

La CA de E-Sign deberá rechazar una solicitud de certificado, si la Llave Pública solicitada no cumple con los tamaños de llave de algoritmos mínimos establecidos en esta sección.

6. Controles de Seguridad No Técnica

Verificación de Mecanismo de autenticación

Nombres

Los certificados de CA de E-Sign contienen Nombres Distinguidos X.501 en los campos Emisor y Sujeto. Los Nombres Distinguidos de las CA de E-Sign constan de los componentes especificados en la Tabla siguiente.

Atributo	Valor
País (C) =	"CL", "CO", "PE", "EC" o el código ISO del país donde opera la CA.
Organización (O) =	"E-SIGN" o "E-Sign S.A." o nombre de la organización ¹ .
Unidad Organizacional(OU) =	Los certificados CA de E-Sign pueden contener varios atributos OU. Tales atributos pueden contener uno o más de los siguientes: • Nombre del CA • E-SIGN • Una declaración haciendo referencia a los términos del Acuerdo de la Tercero que Confía aplicable que rigen el uso del certificado • Un aviso de copyright. • Texto para describir el tipo de certificado.

¹ Para una AC dedicada a una organización cliente, el componente (o =) será el nombre legal de la organización

Estado o provincia (S)=	No se utiliza.
-------------------------	----------------

Localidad (L) =	No se usa.
Nombre común (CN) =	Este atributo incluye el nombre de CA (si el nombre de CA no está especificado en un atributo OU) o no es utilizado.

Tabla 3 - Atributos de Nombre Distinguido en los certificados de CA

Los Certificados de Suscriptor usuario final contienen un nombre distinguido X.501 en el campo nombre del sujeto que consiste en los componentes especificados en la tabla 5 a continuación.

Atributo	Valor
----------	-------

País (C) =	"CL", "CO", "PE", "EC" o el código ISO del país donde opera la CA o no se utiliza.
Organización (O) =	El atributo Organización se utiliza de la siguiente manera: "E-Sign S.A." para respondedores OCSP y, opcionalmente, para los Certificados individuales que no tienen afiliación a una organización. - Nombre de la organización suscriptora para los Certificados de servidor Web y Certificados individuales que tienen afiliación a una organización.

Unidad Organizacional(OU) =	Los Certificados de Suscriptor de usuario final E-Sign pueden contener múltiples atributos OU. Tales atributos pueden contener uno o más de los siguientes: • Unidad Organizacional suscriptora (para los Certificados organizacionales y Certificados individuales que tienen afiliación a una organización) • E-SIGN • Una declaración con referencia al Acuerdo de Tercero que Confía aplicable que rige los términos de uso del Certificado • Un aviso sobre propiedad intelectual • "Persona No Validada" para Certificados Individuales Class 1 • Texto para describir el tipo de Certificado.
--------------------------------	--

Estado o provincia (S)= Indica el Estado o Provincia del Suscriptor (Estado no es un campo obligatorio en certificados emitidos a personas).

Localidad (L) = Indica la Localidad o Ciudad del Suscriptor (Localidad no es un campo obligatorio en certificados emitidos a personas).

Nombre común (CN) =	Este atributo incluye: • El Nombre de Respondedor OCSP (para Certificados de Respondedor OCSP) • Nombres de dominio (para Certificados de servidor Web) • Nombre de la organización (para Certificados de firma de código/objeto)		
<table><tr><th>Atributo</th><th>Valor</th></tr></table>		Atributo	Valor
Atributo	Valor		
País (C) =	“CL”, “CO”, “PE”, “EC” o el código ISO del país donde opera la CA o no se utiliza.		

Organización (O) =	El atributo Organización se utiliza de la siguiente manera: • "E-Sign S.A." para respondedores OCSP y, opcionalmente, para los Certificados individuales que no tienen afiliación a una organización. • Nombre de la organización suscriptora para los Certificados de servidor Web y Certificados individuales que tienen afiliación a una organización.
Unidad Organizacional(OU) =	Los Certificados de Suscriptor de usuario final E-Sign pueden contener múltiples atributos OU. Tales atributos pueden contener uno o más de los siguientes: • Unidad Organizacional suscriptora (para los Certificados organizacionales y Certificados individuales que tienen afiliación a una organización) • E-SIGN • Una declaración con referencia al Acuerdo de Tercero que Confía aplicable que rige los términos de uso del Certificado • Un aviso sobre propiedad intelectual • "Persona No Validada" para Certificados Individuales Class 1 • Texto para describir el tipo de Certificado.

Estado o provincia (S)= Indica el Estado o Provincia del Suscriptor (Estado no es un campo obligatorio en certificados emitidos a personas).

	• Nombre (para Certificados individuales).
E-Mail (E) =	Dirección de correo electrónico para Certificados Individuales

Tabla 4 - Atributos del Nombre Distinguido en Certificados de Suscriptor de usuario final

El componente Nombre Común (CN=), del nombre distinguido del Sujeto de los Certificados Suscriptor de usuario final es autenticado en el caso de Certificados Class 2- Class 3.

- El valor autenticado del Nombre Común incluido en el DN del Sujeto de Certificados Organizacionales es un nombre de dominio o el nombre legal de la organización o unidad dentro de la organización.
- El valor de Nombre Común incluido en el DN del Sujeto de Certificados individuales es el nombre generalmente aceptado de la persona natural.

Requisitos para Nombres

Los siguientes atributos de nombre deberán ser usados para completar el Emisor en Certificados emitidos bajo esta CPS:

CountryName Emisor (requerido)

El componente countryName (C =), es requerido y contiene el código de país de dos letras ISO 3166-1 para el país en el que se encuentra la sede de negocios del emisor.

OrganizationName Emisor (requerido)

El campo organizationName (O=) es requerido y contiene el nombre de la organización del Emisor (o su abreviatura), marca comercial u otra identificación significativa de la CA, que identifica con precisión a la CA. El campo no debe contener una denominación genérica, como "Raíz" o "CA1".

CommonName Emisor (opcional)

Si el campo *commonName* (CN =) del Emisor está presente, debe contener un nombre que identifica con precisión la CA emisora.

Los siguientes atributos de nombre deberán ser utilizados para completar el Sujeto en los Certificados emitidos bajo esta CPS

subjectAlternativeName (requerido)

La extensión *subjectAlternativeName* es requerida y contiene al menos una entrada. Cada entrada es o bien un *dNSName* que contiene el Nombre de Dominio Completamente Calificado o una *iPAddress* contiene la dirección IP de un servidor. La CA de E-Sign confirma que el Solicitante controla el Nombre de Dominio Completamente Calificado (FQDN) o la dirección IP o se le ha concedido el derecho de uso por parte del Titular del Nombre de Dominio o del cesionario de la dirección IP, según corresponda. Los FQDN comodines están permitidos.

CountryName (opcional)

Si está presente, el componente *countryName* (C =), será el código de país de dos letras ISO 3166-1. Si está presente, la CA de E-Sign verificará el país asociado con el Sujeto, de conformidad con la sección respectiva.

OrganizationName (opcional)

Si el campo *organizationName* (O =) está presente, el campo contiene el nombre o DBA del Sujeto y los campos de dirección requeridos contienen una ubicación del Sujeto, según sean verificadas de conformidad con la sección respectiva del manual de la PKI.

Si el Sujeto es una persona física, debido a que los atributos de nombres del Sujeto para los individuos (por ejemplo, *givenName* y apellidos), no están ampliamente soportados por el software de aplicación, la CA puede utilizar el campo *organizationName* para comunicar el nombre o DBA del sujeto (ver 3.2.2.1 Verificación de Solicitante Individual).

Si los campos incluyen discrepancias que la CA considera de menor importancia, tales como las variaciones comunes y abreviaturas, la CA deberá documentar la discrepancia y deberá utilizar abreviaturas aceptadas a nivel local al abreviar el nombre de organización (por ejemplo, si el registro oficial muestra "Nombre de la Empresa Sociedad Anónima", la CA puede incluir "Nombre de la Empresa, S.A."). El campo *organizationName* puede incluir un DBA verificada o nombre comercial del Sujeto.

Si el campo `organizationName` está presente, entonces `localityName`, `stateOrProvinceName` (si procede), y `CountryName` también deberán ser requeridos y `streetAddress` y `postalCode` son opcionales. Si `organizationName` está ausente, entonces el Certificado no deberá contener los atributos `streetAddress`, `localityName`, `stateOrProvinceName`, o `postalCode`. La CA puede incluir el campo `CountryName` del Sujeto sin incluir otra Información de Identidad del Sujeto de conformidad con los requisitos anteriores para `CountryName`.

OrganizationalUnitName (opcional)

El componente `organizationalUnitName` (OU=), cuando está presente, puede contener información que no ha sido verificada por la CA. Metadatos como los caracteres '.', '-', y ' ' (es decir, el espacio), y/o cualquier otra indicación de que el valor está ausente, incompleto o no es aplicable, no deben ser utilizadas.

E-Sign implementa un proceso que impide que un atributo OU incluya un nombre, DBA, nombre comercial, marca registrada, dirección, localización, o texto de otra índole que se refiera a una persona natural o jurídica específica, a menos que E-Sign haya verificado esta información de acuerdo con la sección 3.2.2 y el Certificado también contenga los atributos `subject:organizationName`, `subject:localityName` y `subject:CountryName`, también verificados de acuerdo con la sección respectiva del manual de PKI.

Cuando un valor OU es enviado de una Solicitud, el valor está sujeto a una búsqueda de varias listas de alto riesgo según la sección del manual de la PKI por solicitudes de Alto Riesgo. Si se encuentra una coincidencia, el valor es revisado por la RA para asegurarse de que es preciso y no engañoso. Si el valor OU identifica el nombre de una persona jurídica, el valor es verificado de acuerdo con la sección respectiva de la PKI, Verificación de la Identidad del Sujeto compuesta por Nombre de País y otra Información de Identidad.

commonName (opcional)

El componente `commonName` (CN=) está discontinuado (desaconsejado, pero no prohibido). Si está presente, `commonName` contiene una única dirección IP o el un Nombre de Dominio Completamente Calificado que es también uno de los valores contenidos en la extensión `subjectAlternativeName` del Certificado.

domainComponent (opcional)

El componente domainComponent (dc=) es opcional. Si está presente, domainComponent contiene todos los componentes del Nombre de Dominio Registrado del sujeto en secuencia ordenada, con el componente más importante, el más cercano a la raíz del espacio de nombres, escrito al final.

Otros atributos del Sujeto

Los atributos opcionales, cuando están presentes en el campo del sujeto, deben contener información que haya sido verificada por la CA. Metadatos como los caracteres '.', '-', y ' ' (es decir, el espacio), y/o cualquier otra indicación que el valor está ausente, incompleto o no es aplicable, no deberán ser utilizados.

E-Sign no incluirá Nombres de Dominio Totalmente Calificados en los atributos del Sujeto, excepto como se especifica para subjectAlternativeName y CommonName arriba.

Necesidad de que los Nombres sean Significativos

Los certificados de suscriptor de usuario final Class 2 y Class 3 contienen nombres con semántica comúnmente entendida que permite la determinación de la identidad de la persona u organización que es el Sujeto del Certificado.

Los certificados de CA de E-Sign contienen nombres con semántica comúnmente conocida que permiten la determinación de la identidad de la CA que es el Sujeto del Certificado.

Anonimato o Seudónimos de los Suscriptores

La identidad de Suscriptores individuales de certificados Class 1 no es autenticada. Los suscriptores de certificados Class 1 pueden usar seudónimos. A menos que sea requerido por una ley o solicitado por una autoridad del Estado o del Gobierno para proteger la identidad de algunos suscriptores usuarios finales (p. ej.,

menores, o información sensible de empleados de gobierno), no es permitido que suscriptores de Certificados Class 2 y Class 3 puedan utilizar seudónimos (nombres que no sean el verdadero nombre personal de un Suscriptor o de organización).

Reglas de Interpretación de Diversas Formas de Nombre

Ninguna estipulación.

Unicidad de los Nombres

E-Sign se asegura de que los Nombres Distinguidos del Sujeto de los Suscriptores son únicos en el dominio de una CA específica a través de componentes automatizados del proceso de enrolamiento de Suscriptor. Es posible que un suscriptor pueda tener dos o más certificados con el mismo Nombre Distinguido del Sujeto.

Reconocimiento, Autenticación, y el Rol de las Marcas Comerciales

Los Solicitantes de Certificados tienen prohibido el uso en sus Solicitudes de Certificados de nombres que infrinjan los Derechos de Propiedad Intelectual de otros. E-Sign, sin embargo, no verifica si un Solicitante de Certificados tiene Derechos de Propiedad Intelectual en el nombre que aparece en la Solicitud de Certificado ni arbitra, media o resuelve disputa alguna respecto de propiedad de un nombre de dominio, marca registrada o marca de servicio. E-Sign tiene la facultad, sin responsabilidad alguna hacia cualquier Solicitante de Certificado, para rechazar o suspender cualquier Solicitud de Certificado debido a tal disputa.

Validación de Identidad Inicial

Método para probar la posesión de la Llave Privada

El Solicitante del Certificado debe demostrar que legítimamente posee la llave privada que corresponde a la llave pública que será listada en el Certificado. El método para probar la posesión de una llave privada será PKCS # 10, otra demostración criptográficamente equivalente, u otro método aprobado por E-SIGN. Este requisito no es aplicado cuando un par de llaves es generado por una CA, en nombre de un Suscriptor, por ejemplo, cuando las llaves pre-generadas son colocadas en tarjetas inteligentes o en dispositivos criptográficos.

Autenticación de la Identidad de una Organización

Toda vez que un certificado contenga un nombre de organización, la identidad de la organización y otra información de enrolamiento proporcionada por Solicitantes de Certificado (a excepción de la Información No Verificada del Suscriptor) es confirmada, de conformidad con los procedimientos establecidos en los Planes de Validación documentados por E-Sign.

Deberes

Como mínimo E-Sign debe:

- Determinar que la organización existe mediante el uso de al menos un servicio o base de datos de prueba de identidad de tercera parte, o alternatively, la documentación organizacional emitida por o archivada ante un servicio público del territorio respectivo que confirme la existencia de la organización,
- Confirmar del Solicitante del Certificado por teléfono, correo electrónico, o un procedimiento comparable, cierta información sobre la organización, que la organización ha autorizado la Solicitud de Certificado, y que la persona que envía la Solicitud de Certificado en nombre del Solicitante de Certificado está autorizada para hacerlo. Cuando un certificado incluye el nombre de una persona como representante autorizado de la Organización, la filiación laboral de ese individuo y su autoridad para actuar en nombre de la Organización también deben ser confirmadas.

Cuando un nombre de dominio o dirección de correo electrónico está incluido en el certificado, E-Sign autentifica el derecho de la Organización para utilizar ese nombre de dominio, ya sea como un nombre de dominio completamente calificado o un dominio de correo electrónico.

Otros procedimientos se llevan a cabo para tipos específicos de Certificados como se describe en la siguiente Tabla.

Tipo de Certificado				Procedimientos adicionales
Certificado Hardware	TLS	Protegido	por	E-SIGN verifica que el par de llaves se generan en hardware certificado FIPS 140
Certificados de Organización (OV) y de Validación de Dominio (DV)	de	Validación	de	Los procedimientos de E-Sign para emitir certificados OV y DV se realizan a través de los Planes de Validación respectivos.

Tabla 5 - Procedimientos Específicos de Autenticación

Verificación de Mecanismos de Auditoría de Información relevante

Frecuencia de Procesamiento del Registro

El sistema y los logs de auditoría de la CA son monitoreados continuamente para proporcionar alertas en tiempo real de sucesos de seguridad y operativos significativos. Además, E-Sign revisa mensualmente los registros de auditoría para detectar actividades sospechosas o inusuales en respuesta a las alertas generadas en base a irregularidades e incidentes en los sistemas de la CA y RA de E-Sign.

Periodo de Retención para el Registro de Auditoría

Los registros de auditoría se retienen en el lugar en el que se generan por lo menos durante 2 meses a contar desde su procesamiento y luego se archivan de acuerdo a la sección respectiva.

Protección de Registro de Auditoría

Los registros de auditoría están protegidos con un sistema de auditoría de registro electrónico que incluye mecanismos para proteger los archivos de registro contra accesos no autorizados, modificación, borrado u otras manipulaciones.

Procedimientos de Respaldo de los Registros de Auditoría

Respallos incrementales de registros de auditoría son creados a diario y los respaldos completos se hacen de forma semanal.

Sistema de Recolección de Auditoria (Interna vs. Externa)

Los datos de auditoria automatizados son generados y grabados a nivel de aplicación, red y sistema operativo. Los datos de auditoria manuales son registrados por el personal de E-Sign.

Notificación al Sujeto Causante del Evento

Cuando un evento es registrado por el sistema de recolección de auditoria, no se requiere la entrega de una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

Evaluación de Vulnerabilidades

Los eventos en el proceso de auditoria son registrados, en parte, para monitorear vulnerabilidades del sistema. Las EVSL (evaluaciones de vulnerabilidad de seguridad lógica) son ejecutadas, revisadas y analizadas después de examinar estos eventos monitoreados. Las EVSL están basadas en datos registrados automáticamente en tiempo real y son realizadas diaria, mensual y anualmente. Una EVSL anual será una entrada para una auditoria de cumplimiento anual.

Archivo de Registros

Los procedimientos de archivo de registros de la CA de E-Sign son realizados por E-SIGN de acuerdo a los procedimientos establecidos en esta CPS.

Tipos de Registros Archivados

E-Sign archiva:

- Todos los datos de auditoria recopilados en términos de la Sección respectiva.
- Información de la solicitud Certificado
- Documentación de respaldo a las solicitudes de certificados

- Información de ciclo de vida del certificado p. ej., información de solicitudes de revocación, regeneración de llaves y renovación

Periodo de Retención Para el Archivo

Los registros serán conservados durante al menos los plazos establecidos a continuación después de la fecha en que el Certificado expira o es revocado.

- Cinco (5) años para los Certificados Class 1,
- Diez (10) años y seis (6) meses para Certificados Class 2 y Class 3

Protección del Archivo

E-Sign protege el archivo para que sólo las Personas de Confianza autorizadas puedan obtener acceso al archivo. El archivo está protegido contra accesos, modificación, borrado u otras manipulaciones no autorizadas por el sistema de almacenamiento dentro de un Sistema de Confianza. Los medios que contienen los datos de archivo y las aplicaciones necesarias para procesar los datos de archivo serán mantenidos para asegurar que los datos de archivo pueden ser accedidos por el período de tiempo establecido en esta CPS.

Procedimientos de Respaldo del Archivo

E-Sign respalda incrementalmente los archivos electrónicos de su información de certificados emitidos a diario y ejecuta respaldos completos semanalmente. Las copias de los registros en papel serán mantenidos en una instalación segura fuera del sitio.

Requisitos de Sellado de Tiempo de los Registros

Los certificados, CRLs, y otras entradas de bases de datos de revocación deberán contener información de fecha y hora. Tal información de tiempo no necesita estar basada criptográficamente.

