firmaschile

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

CPS (Certification Practice Statement)

14-Octubre-2022
Versión 1.01

Tabla de Contenido

1 Definiciones y Acrónimos

1.1 Definiciones

Para efectos del documento de Prácticas de Certificación, las expresiones que se indican a continuación tienen el alcance y/o significado que se expresa en cada caso:

- **Prestador de Servicios de Certificación:** Es aquella Autoridad que en conformidad con la legislación vigente emite certificados de firma electrónica.
- **Autoridad de Registro:** Es firmaschile quien actuando personalmente o representada a través de un mandatario o a través de medios informáticos automatizados, realiza la comprobación de la identidad de los solicitantes de certificados.
- **Autoridad Acreditadora:** Es la Autoridad Pública que asegura que los Prestadores de Servicios de Certificación operan de acuerdo con la normativa vigente aplicable, acreditándolos e incluyéndolos en un listado público de PSC acreditadas.
- **Certificado:** Certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica
- **Certificado raíz:** Certificado cuyo suscriptor es eMudhra y pertenece a la jerarquía que eMudhra presenta como Prestador de Servicios de Certificación.
- **Clave:** Secuencia de símbolos.
- **Datos de creación de firma:** Son datos únicos que el suscriptor utiliza para crear la Firma electrónica y que se encuentran inequívocamente unidos a la clave pública contenida en el certificado de firma electrónica.
- **Clave Pública:** Son los datos que se utilizan para verificar la Firma electrónica y que se encuentran inequívocamente unidos a los datos de creación de firma.
- **Declaración de Prácticas de Certificación:** Declaración de firmaschile, respecto a aquellas prácticas, a nivel de sistemas y de personal, que dan seguridad y confianza a los certificados y servicios provistos por firmaschile.
- **eMudhra:** firmaschile es la representante en Chile de la PSC eMudhra
- **Firma electrónica:** Aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría (esto último en caso de firmas digitales o avanzadas).
- **Listas de Revocación de Certificados:** Registro de acceso público de certificados, en el que quedará constancia de los certificados que han perdido su vigencia por haber sido revocados.
- **Número de serie de Certificado:** Valor entero y único que está asociado inequívocamente con un certificado expedido por firmaschile.
- **Online Certificate Status Protocol:** Protocolo informático que permite la comprobación del estado de un certificado en el momento en que éste es utilizado.
- **Política de Certificación:** Es el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad en particular y/o clase de aplicación con requerimientos de seguridad comunes. Es el documento que complementa la Declaración de Prácticas de Certificación, estableciendo las condiciones de uso y los procedimientos seguidos por firmaschile para emitir Certificados.
- **SHA-1: Secure Hash Algorithm** (algoritmo hash seguro). Desarrollado por el NIST (National Institute for Standars and Technology de Estados Unidos). El algoritmo consiste en tomar mensajes de menos de 2^{64} bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un

mismo resumen es teóricamente nula. Por este motivo se usa para asegurar la Integridad de los documentos durante el proceso de Firma electrónica.

- **SHA-2: Secure Hash Algorithm** (algoritmo hash seguro). Desarrollado por el NIST. El algoritmo consiste en tomar mensajes de menos de 2^{64} bits y generar un resumen de 256 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es teóricamente nula. Por este motivo se usa para asegurar la Integridad de los documentos durante el proceso de Firma electrónica.
- **Solicitante:** Persona que solicita la emisión de un certificado de firma electrónica, dando cumplimiento a las exigencias establecidas en la Ley y en la Declaración de Prácticas de Certificación.
- **Suscriptor:** Es la persona cuya identidad personal ha quedado vinculada a los datos de creación de firma, a través de una clave pública certificada por el Prestador de Servicios de Certificación firmaschile.
- **Terceras partes que confían:** Aquellas personas que voluntariamente depositan su confianza en un certificado de firmaschile, comprobando la validez y vigencia del certificado según lo descrito en esta Declaración de Prácticas de Certificación y en las Políticas de Certificación asociadas a cada tipo de certificado.
- **X.509:** Estándar desarrollado por la UIT (Union Internacional de Telecomunicaciones), que define el formato electrónico básico para certificados electrónicos.

1.2 Acrónimos

- AA: Autoridad Acreditadora
- AC: Autoridad Certificadora
- ACR: Autoridad Certificadora Raíz
- AFIS: Automated Fingerprint Identification System
- AR: Autoridad de Registro
- CA: Certification Authority
- CP: Certificate Policy
- CP: Políticas de Certificado de Firma Electrónica
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- EA: Autoridad Acreditadora
- EC: Autoridad de Certificación
- ER: Autoridad de Registro
- FIPS: Federal Information Processing Standard
- HSM: Hardware Security Module
- IANA: Internet Assigned Number Authority
- IETF: Internet Engineering Task Force
- ITU: international Telecommunication Union
- KEY USAGE: En este contexto es el uso que se da al Certificado
- NIST: Instituto Nacional de Estándares y Tecnología
- OCSP: On-line Certificate Status Protocol
- OID: Object Identifier
- PKCS#10: Certification Request Syntax Specification
- PSC: Prestador de Servicios de Certificación

- PIN: personal Identification Number
- PKI: Public Key Infrastructure
- RA: Registration Authority
- RSA: Algoritmo de Encriptación
- SII: Servicio de Impuestos Internos
- UIT: Unión Internacional de Telecomunicaciones
- X.500: Serie de estándares computacionales

2 Introducción

En el siguiente documento se presenta la Declaración de Prácticas de Certificación (CPS, por su sigla en inglés *Certification Practice Statement*) de firmaschile para los certificados de firma electrónica. Éstas son una descripción de los procedimientos o prácticas que firmaschile declara convenir en la prestación de sus servicios de certificación, cuando emite y gestiona certificados de firma electrónica, en su calidad de Prestador de Servicios de Certificación (PSC). Además, se incluyen las normas a seguir por quienes comprueban la identidad de los solicitantes de certificados de firma electrónica (Autoridad de Registro).

Es así como la presente Declaración de Prácticas de Certificación (CPS) detalla las normas y condiciones de los servicios de certificación de firma electrónica que presta firmaschile y que están relacionadas con la gestión del ciclo de vida de los certificados de firma, en particular lo relativo a la información utilizada en la emisión, la verificación de los certificados y de su firma, las condiciones asociadas a la solicitud, emisión, uso, suspensión y la revocación de dichos certificados. También se describen las medidas de seguridad técnica y organizativa, los perfiles y los mecanismos de información que permiten verificar y administrar la vigencia de los certificados, así como la forma en que se asegura que el proceso de certificación es llevado a cabo en un ambiente seguro capaz de brindar total confianza a la comunidad que interactúa en torno a la firma electrónica.

3 Sobre las Prácticas de Certificación

Las prácticas de certificación aquí descritas establecen y configuran el ciclo de vida de los certificados de firma electrónica que provee firmaschile.

3.1 Alcance

El alcance de esta Declaración de Prácticas de Certificación (CPS) detalla las normas y condiciones de los servicios de certificación que presta firmaschile para la emisión de sus certificados de firma electrónica.

3.2 Referencias

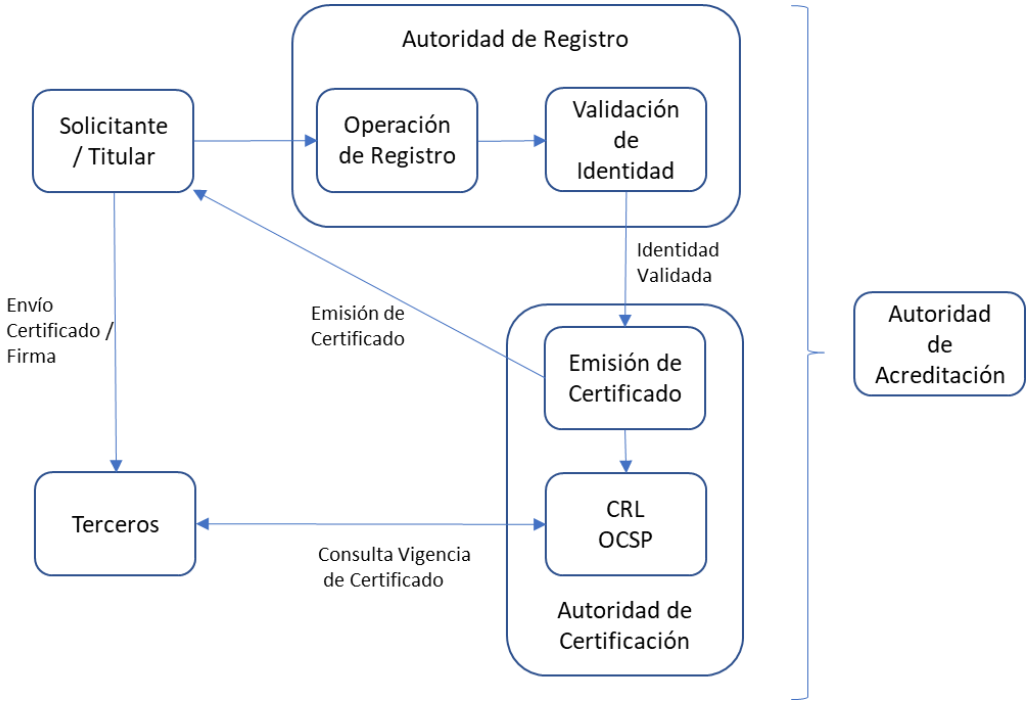
La presente Declaración de Prácticas de Certificación se ha generado siguiendo las especificaciones del documento RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” propuesto por Network Working Group para este tipo de documentos.

3.3 Visión General del Sistema

Los servicios de certificados de firma electrónica de firmaschile, están insertos en una infraestructura en que se relacionan distintas Autoridades, entidades y personas. Básicamente existen 5 tipos de intervinientes o participantes:

- Autoridad Certificadora (EC) o Prestador de Servicios de Certificación (PSC) o Certification Authority (CA),
- Autoridad de Registro (AR) o Register Authority (RA),
- Solicitante / Titulares,
- Terceras partes que confían en los certificados y
- Autoridad de Acreditación (AA) o Autoridad Acreditadora (EA)

La siguiente figura muestra dicha relación:



En la figura la Autoridad de Registro es firmaschile y la Autoridad de Certificación es eMudhra. firmaschile es la representante en Chile de la empresa eMudhra.

Las prácticas y políticas de la AR de firmaschile son publicadas en la página web de la empresa. Cabe destacar que la AR de firmaschile tiene un convenio establecido con la CA de la empresa eMudhra. Las políticas y prácticasde esta última empresa también se publican en la página web de firmaschile para su consulta.

3.3.1 Comunidad de usuarios

La AR de firmaschile comparte la definición de la comunidad de usuarios declarada en las prácticas de certificación de la CA de firmaschile, siendo:

- **Solicitante:** Son las personas que concurren a firmaschile a solicitar un certificado de firma electrónica, completan el formulario de solicitud y proveen todos los antecedentes que exige la ley, la CPS y la CP para comprobar su identidad.
- **Suscriptores:** Son las personas titulares de los datos de creación de firma a quienes le corresponde o está asociada la clave pública informada en los certificados de firma electrónica. Los suscriptores son personas naturales.
- **Autoridad de Registro**: La recepción y procesamiento de las solicitudes de certificados es realizada por la Autoridad de Registro (ER / RA) de firmaschile, sea que lo haga directamente o a través de un mandatario especialmente designado para tal objeto. La Autoridad de Registro debe realizar la comprobación de la identidad de los solicitantes de certificados de firma electrónica. En caso de que sea un tercero el que actúe, en calidad de mandatario de firmaschile, como Autoridad de Registro, la actividad deberá desarrollarla dando pleno cumplimiento al contrato de mandato y a esta Declaración de Prácticas de Certificación. La comunicación entre la AR de firmaschile y su CA permite una comunicación ininterrumpida para el proceso de solicitud, consulta de estado y revocación de los certificados.
- **Prestador de Servicios de Certificación (PSC)**: Es la Autoridad prestadora de los servicios de certificación de firma electrónica, de conformidad a la ley, en particular, a lo previsto en la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma, que en este caso es firmaschile.
- **Tercera parte que confía**: Es el receptor de un certificado de firma electrónica. Normalmente, junto con el certificado este tercero recibe un documento electrónico que se encuentra suscrito con la firma electrónica del suscriptor. La parte que confía debe contar con mecanismos que le permitan validar si se trata de un certificado auténtico y si este certificado se encontraba vigente en el momento en que se produjo la suscripción documental.
- **Autoridad Acreditadora:** El Servicio de Impuestos Internos en su Resolución Exenta N° 09 del 15 de febrero de 2001 establece normas que regulan el uso de la firma electrónica simple para el ámbito tributario, actuando como Autoridad Acreditadora para estos fines e inscribiendo a las PSC en su lista de Autoridades acreditadas para efectos tributarios.

Los usuarios que utilicen los certificados emitidos por firmaschile, antes de solicitar dichos certificados, deben conocer y estar en conformidad con lo establecido en la CPS de firmaschile

y en la CP correspondiente al tipo de certificado.

3.3.2 Aplicabilidad de los certificados

Los Certificados emitidos por firmaschile se utilizarán únicamente conforme a la función y finalidad que tengan establecidos en la presente Declaración de Prácticas de Certificación (CPS) y en la Política de Certificación (CP).

3.3.3 Tipo y uso de los certificados

firmaschile emite certificados electrónicos y cuenta con un proceso de verificación a seguir.

Existe un nivel de seguridad, restricciones y requerimientos específicos respecto a las medidas tomadas para la verificación del suscriptor del certificado, mecanismos de emisión, revocación y utilización de los certificados.

El conjunto de normas que regulan la aplicabilidad de los certificados, en determinados ambientes y comunidades se denomina "Política de Certificados" o CP. firmaschile posee una política de certificado para los certificados electrónicos.

A continuación, se muestra un resumen de los certificados emitidos por firmaschile:

Tipo	Características generales	Usos típicos
Firma Electrónica	• Registro presencial o en línea. • Certificado para persona natural. • El medio de almacenamiento de la llave privada es elegido por el suscriptor del certificado. • Estas políticas de certificado han sido acreditadas por el SII	• e-mail firmado • Autenticación del suscriptor en sitios Web, como el del SII. • Factura electrónica. • Firmar documentos • Otros en que las partes elijan libremente confiar en estos certificados.

Tabla 1: Tipos de certificados

3.3.4 Limitaciones de Uso y Prohibiciones

Los Certificados de firma electrónica emitidos por firmaschile se utilizarán únicamente conforme a los usos y finalidades que tengan establecida en este documento y en las correspondientes Políticas de Certificación, y de acuerdo con la normativa chilena vigente y a los convenios internacionales ratificados por Chile. Cualquier uso diferente del autorizado por ley e indicado en estas prácticas está expresamente prohibido. En consecuencia, será responsabilidad del Suscriptor el uso no autorizado o indebido que éste haga del mismo.

Asimismo, queda expresamente prohibido alterar en cualquier forma los certificados emitidos por firmaschile, los que solo serán válidos en la forma suministrada por firmaschile.

4 Contenido de los Certificados

Este capítulo contiene especificaciones de los formatos y contenido de los certificados emitidos bajo la arquitectura señalada por estas CPS (campos, básicos y extensiones).

4.1 Composición del certificado raíz de eMudhra

Tabla 1: Composición del certificado Raíz de eMudhra

Versión	V3
Número de serie	Número CSPRNG único no secuencial y es mayor que cero: 79ed61337302cbcdb6a52
Algoritmo de firma	SHA-256 con cifrado RSA
Algoritmo hash de firma	SHA 256
Emisor: CN	CA Emisora Nombre común: emSign Trusted Root CA – C4
Emisor: O	CA Emisora Nombre de la organización: eMudhra Inc
Emisor: OU	CA Emisora Unidad de la Organización: emSign PKI
Emisor: C	CA Emisora País: US
Válido desde	Fecha expresada en formato UTC: Wed, Aug, 12, 2020 3:30:00 PM
Válido hasta	Fecha expresada en formato UTC: Sat, Aug 12, 2045 3:30:00 AM
Clave pública	RSA (2048 Bits)
Sujeto: CommonName	Nombre común de la CA raíz: emSign Trusted Root CA – C4
Sujeto: OrganizationName	Nombre legal de la organización de la CA: eMudhra Inc
Sujeto: OrganizationalUnitName	Información variable: emSign PKI
Sujeto: CountryName	País de la CA: US
Clave pública	RSA (2048 Bits)
Parámetros de Clave Pública	05 00
Uso de claves	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Identificador de clave del sujeto	160 bit hash (SHA-1) 973ec8090b2949dd67d17af3a7fface009c0b7a9
Restricciones básicas	Subject Type=CA, Restricción de longitud de trazado=None
Thrumprint	3b6f67fcdfc1701641c8d071518377901546a66

Tabla 2: Certificado CA Subordinada (Issuer / Intermediate) de eMudhra

Versión	V3
Número de serie	Número CSPRNG único no secuencial y es mayor que cero. 00d3bd62369dc109de
Algoritmo de firma	SHA-256 con cifrado RSA
Algoritmo hash de firma	SHA-256
Emisor: CN	CA emisora Nombre común: emSign Trusted Root CA – C4
Emisor: O	CA emisora Nombre de la organización: eMudhra Inc
Emisor: OU	CA emisora Unidad de la Organización: emSign PKI
Emisor: C	CA emisora País> US
Válido desde	Fecha expresada en formato UTC Fri, Sep 16, 2022 7:01:19 AM
Válido hasta	Fecha expresada en formato UTC Tue, Sep 15, 2037 3:29:59 PM
Sujeto: CommonName	Nombre común de CA: emSign Trusted Issuing CA – C4
Sujeto: OrganizationName	Nombre legal de la organización de CA: eMudhra Inc
Sujeto: CountryName	País de CA: US
Clave pública	RSA (2048 Bits)
Parámetros de Clave Pública	05 00
Identificador de clave de la autoridad	973ec8090b2949dd67d17af3a7fface009cob7a9
Identificador de clave del sujeto	d2d49b1a340bcca5bb9abb6cacfed1a7c518951
Directivas de certificado	Certificate Policy: Policy identifier=All issuance policies Policy Qualifier id=CPS Qualifier: http://repository.emsign.com
Acceso a la información de la autoridad	Método Acceso=OCSP (1.3.6.1.5.5.7.48.1), Nombre alternativo: URL=http://ocsp.emsign.com Método Acceso=Certification Authority Issuer (1.3.6.1.5.5.7.48.2), Nombre alternativo: URL=https://repository.emsign.com/certs/TrustedRootCAC4.crt
Puntos de distribución de CRL	URL=http://crl.emsign.com/?TrustedRootCAC4.crl
Uso de claves	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints	Tipo de sujeto=CA, Restricción de longitud de trazado=0
Thumbprint	a3473ef1175a491ac20582701f676591900be9d3

4.2 Información del Certificado Electrónico

Los certificados de firma electrónica emitidos por firmaschile están en conformidad con el formato X.509v3 definido en ITU-T X.509v3 y las recomendaciones de la IETF RFC-3280.

Tabla 3: Composición del Certificado Electrónico (Ejemplo)

Version	V3
Número de serie	Número CSPRNG único no secuencial y es mayor que cero. 0a4b50ec02608c83
Algoritmo de firma	SHA-256 con cifrado RSA
Algoritmo hash de firma	SHA-256
Emisor: CN	Emisor CA Nombre común: emSign Trusted Issuing CA-C4
Emisor: O	Emisor CA Nombre de la organización: emSign PKI
Emisor: C	Emisor País de CA: US
Válido desde	Fecha expresada en formato UTC Fri, Nov 04, 2022 6:28:52 PM
Válido hasta	Fecha expresada en formato UTC Sat, Nov 04, 2023 6:28:52 PM
Clave pública	RSA (2048 Bits)
Sujeto: CommonName	Nombre común: Nombre Sujeto
Sujeto: GivenName	Nombre (Opcional si se proporciona el nombre de la organización)
Sujeto: Surname	Apellido (Opcional si se proporciona el nombre de la organización)
Sujeto: StreetAddress	Dirección
Sujeto: LocalityName	Localidad
Sujeto: StateOrProvinceName	Región
Sujeto: CountryName	País CL
Sujeto: EmailAddress	Dirección de correo electrónico
Clave Pública	RSA (2048 bits)
Parámetros de Cave Pública	05 00
Nombre alternativo del emisor	otherName: type-id = OID 1.3.6.1.4.1.8321.2 value = 77.156.373-2 (RUT de firmaschile) 1.3.6.1.4.1.8321.2=16 0a 37 37 31 35 36 33 37 33 2d 32
Nombre alternativo del sujeto	otherName: type-id = OID 1.3.6.1.4.1.8321.1 value = RUT del titular 1.3.6.1.4.1.8321.1=16 0a 31 33 30 36 38 39 38 39 2d 32
Uso de claves	Firma Electrónica, No Repudio (c0)
Directivas de certificado	Certificate Policy: Policy identifier=All issuance policies Policy Qualifier id=CPS Qualifier: http://repository.emsign.com
Identificador de clave del sujeto	845953ae93e982832fd9778f641c66e624962189
Identificador de clave de la autoridad	e24edaef757ed26bf3d28828e1f465053beea68f
Restricciones básicas	Subject Type=End Entity, Path Length Constraint=None
Acceso a la información de la autoridad	Método Acceso=OCSP (1.3.6.1.5.5.7.48.1), Nombre alternativo: URL=http://ocsp.emsign.com Método Acceso=Certification Authority Issuer (1.3.6.1.5.5.7.48.2), Nombre alternativo: URL=https://repository.emsign.com/certs/TrustedIssuingCAC4.crt

Puntos de Distribución de CRL	CRL URL = http://crl.emsign.com/?TrustedIssuingCAC4.crl
Thumbprint	6867ef8a812c843a7037b538058cdaf7a6e454e4

5 Requerimientos Generales

5.1 Obligaciones

firmaschile, en su calidad de prestador de servicios de certificación de firma electrónica, se obliga a realizar lassiguientes actividades en la prestación de sus servicios:

1. Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicadas a los usuarios de manera sencilla y en idioma castellano.
2. Contar con un registro fidedigno de los antecedentes proporcionados por los solicitantes de los certificados de firma electrónica al momento de comprobarse su identidad.
3. Comprobar la identidad del solicitante de los certificados de firma electrónica.
4. Mantener un registro de acceso público de certificados, en el que quede constancia de los emitidos y los que queden sin efecto, sea por revocación o suspensión de estos.
5. Tratar los datos personales recolectados con ocasión de la actividad de certificación dando cumplimiento a lo dispuesto las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada.
6. En el caso de cesar voluntariamente en su actividad, comunicarlo previamente a los titulares de los certificados de firma emitidos y, en caso de no existir oposición de los titulares, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, deja sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia.
7. Publicar en el home del sitio web de firmaschile las resoluciones de la Autoridad Acreditadora que la afecten.
8. Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Autoridad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que dará a los datos de los certificados, especificando, de ser el caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto.
9. Indicar a la Autoridad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento concursal de liquidación o que se encuentre en cesación de pagos.
10. Cumplir con las demás obligaciones legales establecidas en el país.
11. Ejecutar la actividad de certificación de conformidad a lo dispuesto en esta Declaración de Prácticas de Certificación (CPS).
12. Emitir los certificados de firma electrónica con mecanismos tecnológicos y criptográficos que garanticen que el proceso de certificación es realizado adecuadamente y que cumplen con los requisitos establecidos por la Autoridad

Acreditadora.

13. Revocar los certificados de firma electrónica en los cuales se vea comprometida la confianza respecto a la veracidad de su contenido.

5.2 Obligaciones de la AC Raíz (ACR)

El certificado raíz de eMudhra permite firmar certificados de distintas comunidades. Es así como eMudhra, apartir de su certificado raíz, genera la jerarquía de confianza para distintas comunidades, cada una de ellas encargadas de emitir certificados específicos de firma. Así es como a partir de la ACR, eMudhra genera un conjunto de AC intermedias, cada una de las cuales posee su propia vigencia.

En el caso que el certificado de eMudhra sea vulnerado durante su vigencia, eMudhra procederá a su revocación inmediata. Cuando se reemplazan estos certificados, se generan nuevos certificados, pertenecientes a una estructura jerárquica completamente nueva, cumpliendo con todas las formalidades de generación de llaves definidas para cada nueva autoridad certificadora intermedia.

Las autoridades certificadoras intermedias reemplazadas dejan de firmar certificados nuevos desde el momento de su revocación.

Las claves de las autoridades certificadoras reemplazadas siguen generando listas de revocación y respondiendo a consultas OCSP, por lo que todos los certificados firmados por estas autoridades certificadoras podrán cumplir su período de vigencia antes de que expire el certificado de alguna autoridad certificadora presente en su cadena de certificación.

5.3 Obligaciones de la Autoridad de Registro (AR/RA) y la Autoridad de Certificación (AC/CA)

firmaschile, para el desarrollo de la actividad de certificación de firma electrónica, desarrolla actividades que son propias de una autoridad certificadora de firma y otras que son propias de las autoridades de registro. Así, realiza actividades tales como: aprobar o rechazar solicitudes de certificados de firma electrónica; emitir y publicar los certificados de firma electrónica emitidos; proveer su llave pública de manera segura a terceros, de modo que ellos puedan verificar la validez de los certificados que firmaschile ha emitido, así como informar la revocación de dicha llave; proveer información del estado de los certificados emitidos así como de la lista de revocación; proveer la infraestructura necesaria para proveer los servicios de firma electrónica, procedimientos, seguridad física y personal adecuado para llevar a cabo las funciones asociadas a la certificación; y, en general cumplir las obligaciones legales, reglamentarias y las que emanan de esta CPS.

Las actividades que desarrolla en su calidad de autoridad certificadora (AC) las ejecuta personalmente por eMudhra y no son delegables en ninguna circunstancia. Por su parte, las actividades que desarrolla en su calidad de Autoridad de Registro, las realiza en forma personal o representada.

firmaschile no representa a ninguna AC distinta a la AC de eMudhra.

5.3.1 Obligaciones de la Autoridad de Registro (AR):

- Comprobar la identidad de los solicitantes de los certificados de firma electrónica, de conformidad a lo dispuesto en esta CPS.
- Entregar a la Autoridad Certificadora (AC) los antecedentes exigidos por esta CPS que sirvieron de base para comprobar la identidad de los solicitantes de los certificados de firma electrónica.
- Custodiar los antecedentes que sirvieron de base para comprobar la identidad de los solicitantes de los certificados de firma electrónica mientras la AC no tome el control de éstos.
- Mantener los controles de seguridad física, de procedimiento y personales definidos para el desarrollo de la actividad de registro, de acuerdo con lo establecido en estas CPS y en la documentación de seguridad de firmaschile.
- Contar con la infraestructura requerida para prestar el servicio de certificación, conforme al nivel de calidad comprometido.

5.3.2 Obligaciones de la Autoridad Certificadora (AC):

- Hacer públicas las políticas y prácticas de certificación a que están sujetos los certificados de firma electrónica.
- Custodiar los datos de creación de firma con los cuales firmaschile suscribe los certificados de firma electrónica que comercializa de conformidad con las normas técnicas fijadas por la Autoridad Acreditadora.
- Contar con la infraestructura requerida para prestar el servicio de certificación, conforme al nivel de calidad comprometido y los requisitos y obligaciones que impone la ley.
- Generar y firmar los certificados de firma electrónica a partir de la información que le proporciona la Autoridad de Registro (AR).
- Entregar en la forma establecida en estas CPS los certificados de firma electrónica a los titulares.
- Procesar y reportar los requerimientos de revocación y suspensión de los certificados de firma electrónica.
- Proveer el estado de revocación de certificados a las partes interesadas.
- Mantener un registro de acceso público de los certificados de firma electrónica, en el que quedará constancia de los emitidos y los que han quedado sin efecto.

Para asegurar el cumplimiento de las obligaciones señaladas precedentemente, eMudhra ha definido:

- Prácticas de Certificación de firma electrónica.
- Controles respecto a la generación de llaves, que aseguran que ellas son generadas en una infraestructura segura (con múltiples sitios), con roles definidos y con un doble control (operadores de registro y validación).
- Algoritmos reconocidos por la industria para la generación de claves.

- Un largo de llave de al menos 2048 bits.
- Procedimientos para generación de llave de la AC ante expiración de esta, sin que ello implique interrupción de los servicios.
- Procedimientos para el respaldo, almacenamiento y recuperación de las llaves de la AC sólo por personal autorizado y en base al quórum que se ha definido para esta acción.
- Un canal seguro para la distribución de la llave pública de la AC que permita verificar a los terceros interesados, los certificados que eMudhra ha firmado.
- Que los certificados de firma estén asociados sólo al propósito para el cual han sido definidos.
- Que la llave privada no puede ser usada de manera posterior a su fecha de expiración.
- Que existe un procedimiento para el control del ciclo de vida de los elementos criptográficos.
- Que la entrega de los datos de creación de firma al titular no debe comprometer su seguridad.

5.4 Obligaciones del Solicitante

Los solicitantes de certificados de firma electrónica se encuentran obligados a:

- Conocer y aceptar esta CPS.
- Conocer y aceptar el propósito y alcance de los certificados de firma que le vaya a emitir firmaschile.
- Brindar a la Autoridad de Registro (AR) declaraciones exactas y completas respecto a su identidad personal y otras circunstancias objeto de certificación por parte de firmaschile.
- Notificar a firmaschile cualquier cambio en las declaraciones, respecto a su identidad personal u otras circunstancias objeto de certificación y que hayan sido proporcionadas a la Autoridad de Registro al momento de la comprobación de la identidad.
- Custodiar adecuadamente los datos de creación de firma del certificado de firma electrónica que firmaschile le emita, así como cualquier otro mecanismo de seguridad de funcionamiento delsistema de firma electrónica.
- Suscribir el contrato de prestación de servicios de certificación electrónica.
- Abonar la tarifa o precio establecido para el servicio solicitado.

5.5 Obligaciones del Suscriptor de la Llave

Las obligaciones del suscriptor del certificado de firma electrónica, incluidas en contrato de suscripción, se resumen en:

- Proteger y utilizar el certificado emitido para los fines con que ha sido solicitado; custodiando de manera adecuada dicho certificado, ya que éste corresponde a su identidad en el mundo digital, por ende, al igual que una Cédula de Identidad, el certificado emitido debe ser protegido de un uso no apropiado dado una pérdida, robo o hurto, informando de manera oportuna a firmaschile en caso de presentarse

algún inconveniente de seguridad de éste.

- Solicitar la revocación del certificado en caso de cumplirse condiciones tales como la pérdida del certificado o su dispositivo, la pérdida de la clave de acceso, la cesación del cargo en caso de ser certificados que se han asociado a un cargo específico, a solicitud del suscriptor del certificado, ante la no renovación del certificado o ante la necesidad de revocación de dicho certificado por parte de firmaschile.
- No revelar la clave privada ni el código de activación del certificado, la que es de exclusiva responsabilidad del suscriptor.
- Verificar y asegurar que la información contenida en el certificado es fidedigna e informar a firmaschile ante cualquier información incorrecta o inexacta detectada en dicho certificado o cambio que se haya generado respecto a la información originalmente entregada para la emisión de dicho certificado.
- Considerar sus responsabilidades legales y penales, en caso de una persona jurídica, derivadas de la representación de los titulares de dicha organización.
- Cualquiera otra obligación que derive de la Ley, el Reglamento, este documento o del certificado electrónico.

5.6 Obligaciones de los Usuarios

Los usuarios de los certificados de firma electrónica emitidos por firmaschile se obligan a aceptar las siguientes condiciones:

- Comprobar en firmaschile que el certificado en el que se pretende confiar se encuentra vigente (no ha sido revocado o suspendido o terminada su vigencia).
- Conocer y aceptar el propósito y alcance del certificado de firma electrónica, en que se pretende confiar.

5.7 Confianza en las Firmas y certificados

Las partes que confíen en las firmas emitidas por firmaschile deberán considerar:

- Que la operación que se pretende avalar con la firma está en el ámbito de esta última, no sólo en el uso de esta, sino en lo que determinan las normas legales y reglamentarias asociadas a la PSC y los distintos tipos de certificados emitidos.
- Que la parte que desea confiar ha tomado los resguardos de verificar la autenticidad de la firma en base a la llave pública de firmaschile
- Que la parte que desea confiar ha asegurado la validación de caducidad o revocación de la firma en cuestión en base a los servicios provisto por firmaschile.
- Que las partes que confían en los certificados han de:
    - Acotar la fiabilidad de los certificados emitidos, a los usos que se han definido para los mismos, en conformidad con lo definido en las extensiones de los certificados y la Política de Certificación pertinente.
    - Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
    - Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
    - Asumir su responsabilidad en la comprobación de la validez, revocación o

suspensión de los certificados en que confía.

- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

5.8 Obligaciones de los Repositorios

El repositorio público de firmaschile permite realizar distintas operaciones dependiendo del tipo de certificado con el que se esté trabajando. En este repositorio se llevará un registro actualizado de los certificados vigentes y revocados, estando dichas alternativas explicadas en el documento de políticas de cada tipo de certificado. En el caso de los certificados de firma electrónica, se contará con el acceso público a las prácticas y políticas del PSC, asociado a este tipo de certificado, así como del estado de un certificado en particular, ya sea por medio de una consulta al servicio en línea OCSP o a través de la listade revocación (CRL) publicada por firmaschile en su sitio web.

6 Responsabilidad del PSC

firmaschile solo será responsable de los daños y perjuicios que en el ejercicio de la actividad de certificaciónde firma electrónica ocasione y, en ningún caso será responsable del uso incorrecto, indebido o fraudulento de los certificados de firma electrónica emitidos ni de cualquier daño indirecto o imprevisto que resulte de su uso.

Se deja expresa constancia que, atendida la complejidad de los sistemas informáticos y el riesgo tecnológico que los mismos conllevan, no es posible garantizar que los sistemas operen libres de errores o inconsistencias, no obstante, el cuidado y la diligencia empleada por firmaschile. Por lo anterior, no otorga garantía alguna en relación con el posible compromiso en el futuro del sistema de claves asimétricas o cualquier otro riesgo no predecible de naturaleza similar. En todo caso, a fin propender a mitigar esta clase de riegos, firmaschile aplicará los procedimientos previstos en sus planes de contingencia.

Será responsabilidad de los usuarios adoptar las medidas de prevención usuales a la actividad computacional para evitar daños y perjuicios originados por el uso o incapacidad de uso de los certificados de firma electrónica.

6.1 Responsabilidad Pecuniaria

La responsabilidad de firmaschile cualquiera sea la naturaleza de la acción o reclamo y salvo que medie dolo o culpa grave atribuible a ésta, quedará limitada como máximo al monto pagado por el certificado.

La actividad de certificación de firma electrónica se encuentra limitadas al ciclo de vida del certificado, esto es:

1. Solicitud del solicitante. Proveer todas las condiciones necesarias para que el solicitante de un certificado de firma electrónica pueda requerir y proporcionar toda la información necesaria para la emisión de este.

2. Registro del solicitante. Una vez que el prestador de servicios de certificación recibe la solicitud debe proceder a la aprobación de ésta, y para ello deberá comprobar los antecedentes que le han sido declarados, debiendo comprobar en la forma señalada en esta CPS y, especialmente la identidad del solicitante y que los datos de creación de firma son entregados realmente a quien solicitó el certificado de firma.

3. Firma y emisión del certificado. Una vez que se ha efectuado el registro del solicitante y se ha verificado la exactitud de los datos proporcionados, el prestador de servicios de certificación procede a emitir el certificado de firma electrónica, firmado por medio de la firma electrónica de la cual es titular.

4. Publicación y archivo. Una vez que el certificado de firma ha sido emitido y firmado por el prestador de servicios de certificación, hacerlo constar en el registro de acceso público.

5. Revocación y suspensión. Hacer cesar la vigencia del certificado, de manera temporal o definitiva, según sea el caso en la forma descrita en esta CPS.

6.2 Fuerza Mayor o Caso Fortuito

firmaschile no será responsable por daños, pérdidas o perjuicios que provengan de incumplimientos en el desarrollo de la actividad de certificación de firma electrónica y que sean atribuibles a circunstancias constitutivas de caso fortuito o fuerza mayor.

Las obligaciones de firmaschile afectadas por el caso fortuito o la fuerza mayor se suspenderán por el período de tiempo que dure el hecho que lo motivó.

Para los efectos de estas CPS, se entenderá por caso fortuito o fuerza mayor la definición del artículo 45 del Código Civil chileno, incluyendo, además, guerras, desastres naturales, paros, huelgas o suspensión de laborales del personal de firmaschile o de sus contratistas o subcontratistas, sin que esta enumeración sea taxativa.

6.3 Responsabilidad de la AC y AR

Aplica el régimen de responsabilidad establecido en 6.1, no siendo pertinente diferenciar entre la responsabilidad de la AR y la AC.

6.4 Ley Aplicable y Resolución de Conflictos

6.4.1 Ley Aplicable

Esta CPS y las Prácticas de Certificación específicas para cada tipo de certificado se regirán e interpretarán de conformidad con la ley chilena.

6.4.2 Resolución de Conflictos.

Cualquier diferencia, dificultad, problema o controversia que pueda surgir entre firmaschile y los suscriptores o signatarios que suscriban él (los) respectivo(s) contrato(s) de certificación o con los terceros interesados que adhieran a las CPS de firmaschile con motivo de la validez,

eficacia, interpretación, nulidad, cumplimiento o incumplimiento de estas CPS o de la actividad de certificación de firma electrónica y que no pueda ser resuelta por acuerdo entre las partes, será sometida a la jurisdicción de los Tribunales Ordinarios de Justicia de la Ciudad de Santiago.

7 Publicación y Repositorios

firmaschile mantiene publicadas en su sitio web en www.firmaschile.cl, su Declaración de Prácticas de Acreditación (CPS) y la Política de Certificación (CP) de las AC que representa o tiene afiliación, firmaschile es la representante en Chile de la empresa eMudhra.

La información respecto al estado de vigencia y validez de los certificados emitidos por firmaschile, se encuentra también disponible en el sitio Web de firmaschile.

firmaschile y su PSC acreditada se obligan a mantener dicha información disponible para su acceso público, así como publicar la información consistentemente con las prácticas de confidencialidad estipuladas en este documento, así como de las leyes vigentes.

La información de validación del estado de los certificados de firma electrónica (vigente, revocado o suspendido) se mantiene permanentemente actualizada.

El registro de acceso público de certificados funciona bajo las siguientes

normas:

a. La información relativa a los certificados de firma electrónica es publicada, a través de sistemas automatizados, en el mismo momento en que éstos son emitidos.
b. La información relativa a la revocación de los certificados de firma electrónica es publicada dentro de un plazo que no puede exceder de 8 horas laborales (entre 9:00 y 18:00 horas), contada desde la solicitud de revocación realizada de conformidad con el procedimiento indicado en 10.6.3 de estas CPS.

7.1 Privacidad y Protección de los Datos Personales

La acreditación de eMudhra respecto a las Normativas de Privacidad y la Política de Privacidad de firmaschile se encuentran publicadas en el sitio web de firmaschile www.firmaschile.cl.

7.1.1 Tipos de Información a Proteger

De manera complementaria a lo dispuesto en las Políticas de Privacidad de firmaschile, la empresa protege especialmente la siguiente información:

7.1.1.1 Información propia de la operación de firmaschile y de sus llaves

- Las claves privadas de las Autoridades que componen a firmaschile.
- Toda información relativa a las operaciones que lleve a cabo firmaschile.
- Toda información relativa a los controles de seguridad y procedimientos de auditoría.
- Planes de continuidad de negocio y de emergencia.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.

- Toda la información clasificada como “CONFIDENCIAL”.

7.1.1.2 Información propia del suscriptor capturada durante el registro

Toda la información de carácter personal proporcionada a firmaschile durante el proceso de registro de los suscriptores de certificados.

7.1.2 Tipos de Información que puede ser entregada

firmaschile considera como información de acceso público y, consecuentemente se encuentra disponible al público en www.firmaschile.cl o en las oficinas de la empresa:

- La Declaración de Prácticas de Certificación y Políticas de Certificación de firmaschile.
- La contenida en el registro de acceso público de certificados de firma electrónica (OCSP)
- La lista de certificados revocados (CRL).
- Toda aquella información que no teniendo un estatuto de protección especial establecido en la ley sea clasificada por firmaschile como "PÚBLICA".

Pese a la calificación de la información como de acceso público, firmaschile se reserva el derecho de imponer medidas y controles de seguridad adecuados y proporcionales con el fin de asegurarla autenticidad e integridad de los documentos.

7.1.3 Entrega de Información sobre la Revocación del Certificado

La información relativa a la revocación de certificados se proporciona vía CRL por parte de firmaschile. Esta información también se encuentra disponible en el servidor de validación OCSP de firmaschile.

7.1.4 Entrega de Información en virtud de un Procedimiento Judicial y/o Administrativo.

Las obligaciones, prohibiciones y responsabilidades de custodia de información sujetas a secreto, reserva o confidencialidad de acuerdo con la ley y éstas CPS no regirán si media alguna disposición legal o resolución judicial que obligue a firmaschile a entregar al conocimiento de los Tribunales de Justicia, organismos, instituciones o Autoridades facultadas por la ley para solicitarlos y que actúen dentro del ámbito de sus atribuciones.

7.1.5 Entrega de Información a Petición del Titular

firmaschile entregará la información del titular del certificado que mantiene en sus registros previo ejercicio del derecho de acceso por éste, en la forma establecida en las Políticas de Privacidad de firmaschile.

7.1.6 Autoridades de certificación afiliadas a la AR

7.1.6.1 Publicación de Autoridades

La AR de firmaschile publica la lista de Autoridades de certificación a las cuales representa o tiene afiliación, para realizar las actividades de registro, como parte de este mismo documento. En particular la AR de firmaschile sólo representa o tiene afiliación para realizar las actividades de registro, con las AC indicadas en 7. Publicación y Repositorios de su CPS.

7.1.6.2 Publicación de CP y CPS

La AR de firmaschile publica en su página web los documentos CP y CPS vigentes de las

Autoridades de Certificación a las cuales representan o tienen afiliación para realizar las actividades de registro, y que están limitadas a las indicadas en 7. Publicación y Repositorios.

7.1.6.3 Publicación de certificaciones

La AR de firmaschile publica en su página web las Resoluciones de Acreditación correspondientes a las Autoridades de Certificación a las que se encuentra vinculada, y que están limitadas a las indicadas en 7. Publicación y Repositorios.

7.1.6.4 Publicación de un documento que acredite representación de la AC

La AR de firmaschile declara en su CPS, punto 7. Publicación y Repositorios, su vinculación con cada Autoridad de Certificación a la cual representa. Esta misma CPS, además es publicada en la página web de firmaschile, tal como se indica en el punto "7. Publicación y Repositorios ".

7.1.6.5 Limitación de responsabilidades

Tal como se indica en 7. Publicación y Repositorios - firmaschile no representa a ninguna CA distinta a la propia CA de eMudhra. Dicho esto, tanto la AR como la AC de firmaschile declaran en sus CP y CPS, las limitaciones de responsabilidad para cubrir los temas de compensación y garantías ofrecidas a los usuarios por casos de suplantación de identidad ocasionados por las operaciones de la Autoridad de Registro o por las Autoridadesde Certificación

8 Identificación y Autenticación

La identificación de los solicitantes y titulares de certificados de firma electrónica se realiza de acuerdo con las normas y procedimientos contenidas en esta sección de las CPS, con independencia de que la actividad de registro sea realiza directamente por firmaschile o por un mandatario.

8.1 Registro Inicial

8.1.1 Registro de Nombres

De conformidad con la Resolución Exenta N° 09 del 15 de Febrero de 2001 del SII y la Ley 19.799, los certificados de firma electrónica deberán contener como menciones mínimas: El nombre del solicitante, su RUT y una dirección de correo electrónico.

El nombre corresponderá al nombre completo del solicitante en los términos consignados en su cédula de identidad (nombres y apellidos). Este deberá ser registrado por firmaschile, personalmente o a través de mandatario, en los términos definidos en el estándar X.509 y será incluido en el certificado en el campo Common Name (CN). Se considerará como válido, en el caso de los nombres, cualquiera que sea aceptado por el Servicio de Registro Civil e Identificación.

La dirección de correo electrónico será aquel que declare el solicitante al momento de realizarse la comprobación de su identidad y no resolverá disputa alguna relativa a la titularidad de los nombres, ni dominios de las direcciones de correo electrónico.

8.1.2 Verificación General

Todas las menciones incorporadas en los certificados de firma electrónica son comprobadas por firmaschile, de manera de asegurar que el nombre y el RUT, incluido en éstos se encuentre efectivamente agregado en idénticos términos a los consignados en la cédula de identidad del solicitante. Respecto a la dirección de correo electrónico o cualquier otra mención certificable, firmaschile se asegurará que se adicione en idénticos términos consignados en la solicitud del certificado o en la documentación acreditativa de la respectiva mención.

8.2 Reemisión de la Llave

No aplica. firmaschile no reemite las llaves de sus certificados una vez generados por sus titulares. De requerirse una reemisión, producto de una revocación o expiración de vigencia, ella se considerará como una nueva emisión, y por ende se seguirán los procedimientos de validación de identidad de las personas naturales para la emisión de sus certificados electrónicos, ello conforme al tipo de certificado a proporcionar.

8.3 Reemisión de la Llave luego de una Revocación

No aplica. firmaschile no reemite las llaves de sus certificados una vez generados por sus titulares. De requerirse una reemisión, producto de una revocación, ella se considerará como una nueva emisión, y por ende se seguirán los procedimientos de validación de identidad de las personas naturales para la emisión de sus certificados electrónicos, ello conforme al tipo de certificado a proporcionar.

8.4 Requerimiento de Revocación

La revocación es el mecanismo a través del cual firmaschile deja sin efecto de manera permanente un certificado de firma electrónica emitido por él, cesando permanentemente los efectos jurídicos del certificado conforme a los usos que le son propios impidiendo el uso legítimo del mismo.

Tendrá lugar cuando firmaschile constate alguna de las siguientes circunstancias:

a) Solicitud del titular del certificado (en caso de emisión a persona natural) o solicitud del representante legal actual de la empresa o del titular del certificado a revocar (en caso de que el certificado esté emitido para un cargo de dicha empresa).
b) Fallecimiento del titular.
c) Resolución judicial ejecutoriada.
d) Que el titular haya proporcionado al momento de solicitar el certificado información inexacta o incompleta.
e) Si el titular no actualiza los datos proporcionados a firmaschile al momento de solicitar el certificado.
f) Que el titular no custodie adecuadamente los mecanismos de seguridad de funcionamiento del sistema de certificación provistos por firmaschile, generando compromisos de su clave de suscriptor.

9 Requisitos Operacionales

9.1 Requisitos Generales

En este capítulo se describen los requisitos operativos de firmaschile, dentro de su prestación de servicios asociados a su PSC, los que están relacionados directamente con las CPS de la AC de eMudhra, la cual cuenta con los siguientes componentes de sistema:

- **Interfaces:** firmaschile, para su emisión de certificados, establece una relación entre la AC, la AR y el titular. Esta relación se inicia en la captura de los datos relevantes para la emisión del certificado de firma desde el solicitante, los cuales son comprobados por la Autoridad de Registro.De ser aprobada esta solicitud, ella se envía a través de un canal seguro a la Autoridad de Certificación, de manera de realizar la generación del par de llaves, así como la generación del certificado de firma, elementos a ser almacenados y controlados por el titular en su dispositivo.

  La comunicación entre la AR y la AC, con posterioridad a la generación de las llaves, sólo ocurre en el registro de las revocaciones y suspensiones, las que son ingresadas por el operador de validación y cuyo efecto es el modificar la CRL y el servicio OCSP.

- **Procesos de Auditoría:** La auditoría sobre la PSC de eMudhra, se realiza para garantizar el funcionamiento y seguridad, de acuerdo con las disposiciones contenidas en la Declaración de Prácticas de Certificación de la PSC de eMudhra. Para más información respecto a los procesos de auditoría, acreditación y certificación de eMudhra, ver punto ANEXO: ACREDITACIONES / DOCUMENTACION DE eMudhra.

- **Privacidad:** firmaschile mantiene un compromiso respecto al uso de los datos personales, el cual asegura la confidencialidad de los datos personales de los titulares que se faciliten en el sitio web www.firmaschile.cl, ya sea mediante el o los formularios establecidos para esos efectos o bien los que sean recogidos por el hecho mismo de navegar por la Web. firmaschile únicamente recolectará aquellos datos que han sido entregados voluntariamente por los usuarios, los que serán usados o tratados únicamente para los fines para los cuales dichos datos fueron proporcionados. firmaschile utiliza cookies y su política se encuentra publicada en el sitio web www.firmaschile.cl.

9.2 Manuales Operacionales

Para cumplir las labores de registro inicial, validación y emisión de certificados de firma, firmaschile cuenta con manuales operacionales los cuales guían a los operadores de registro y validación en las labores asociadas a su rol. Sin perjuicio de lo anterior existen múltiples sistemas que automatizan las funciones mencionadas.

En el capítulo 10, se procede a describir y detallar el proceso antes mencionado. Las especificaciones contenidas en estos puntos lo son, sin perjuicio de las estipulaciones previstas en cada una de las distintas Políticas de Certificación para los distintos tipos de certificados emitidos por firmaschile.

10 Solicitud de Certificado

10.1 Registro Inicial

El solicitante deberá completar el formulario de solicitud del Certificado que está a su disposición en la dirección de Internet: www.firmaschile.cl, indicar la vigencia del certificado, los datos del solicitante, además deberá aceptar las condiciones del servicio e ingresar los datos para la facturación.

Con el envío del formulario, el Solicitante proporciona a firmaschile toda la información y documentación que necesita, para registrarlo como Suscriptor e incluirla en el Certificado, de acuerdo con los requisitos establecidos en la CP correspondiente.

Si los datos son correctos el solicitante podrá continuar con el proceso, en caso contrario se le indicará los pasos a seguir.

Con la aceptación de la solicitud que se despliega en pantalla el solicitante deberá realizar el pago correspondiente al tipo de Certificado, mediante el botón de pago que se despliega en la misma pantalla.

El envío de los datos solicitados en este formulario y el abono de las tasas de registro supondrá su consentimiento para ser registrado como suscriptor de un certificado de firmaschile y la aceptación del contrato. El contrato del suscriptor establece las responsabilidades de la AR, de la AC y del suscriptor, para los casos de compromiso de las claves del suscriptor o casos de suplantación de identidad ocasionado por las operaciones de registro. Así mismo, el contrato establece los términos y condiciones aplicables a los certificados de conformidad con la legislación, incluyendo:

- Compromiso de la clave privada
- Uso indebido del certificado
- Cambios que se produzcan en la información que dio origen al certificado y obliguen a la revocación de este.
- Obligaciones y responsabilidades del suscriptor
- Obligaciones y responsabilidades de firmaschile
- Provisiones de garantía y responsabilidad, incluyendo limitaciones y exclusiones
- Vigencia y Término de Contrato.
- Resolución de conflictos.

La solicitud de este certificado no implicará en ningún caso su obtención si no se llegan a cumplir por parte del solicitante los requisitos establecidos en la CPS y en la CP de Certificado de Firma Electrónica Simple.

La solicitud de un certificado de firma electrónica para fines tributarios es un acto personal y

en tal sentido se reconoce que la usurpación de nombre es un delito que se sanciona penalmente por ejercicio ilegal de nombre y/o por estafa y otros engaños. Asimismo, declara que acepta las políticas de certificación de firmaschile y de uso de estos certificados por el Servicio de Impuestos Internos.

10.2 Autenticación de la Identidad del Suscriptor

Para acreditar las circunstancias que garantizará el Certificado en la fase definitiva se requerirá la presentación de la siguiente información

- Número de la cédula de identidad chilena vigente del suscriptor
- Número de serie o de documento de la cédula de identidad

10.3 Aceptación y Rechazo de la Solicitud

Una vez recibida la solicitud y la información, la AR debe proceder al proceso de verificación de la información proporcionada, previo a la aceptación de esta.

En concreto, la AR confirmará:

a) La información entregada por el solicitante y que figurará en el Certificado.
b) Que se haya entregado la documentación requerida y que ésta se ajuste a lo solicitado.
c) La comprobación de la cédula a través de la serie, vigencia, bloqueo, y eventualmente, otras preguntas personales, se realiza mediante consulta a un bureau de información.
d) Cualquier otra información que se incluye en el Certificado, a no ser que en este se indique expresamente la ausencia de la verificación correspondiente.

10.3.1 Aceptación de la Solicitud

De no haber circunstancias que de alguna manera afecten a la seguridad del servicio de certificación y siempre que la identidad del solicitante sea válida, la AR procederá a la aprobación de la solicitud.

10.3.2 Rechazo de la Solicitud

Si la AR decidiese rechazar la solicitud del Certificado, comunicará a través de correo electrónico la decisión, con indicación de los motivos que la provocaron. En caso de que los defectos encontrados sean subsanables, se le otorgará al solicitante del certificado un plazo de veinticuatro horas para llevar a cabo la subsanación, transcurrido el cual la AR procederá a confirmar o a revocar su decisión de manera definitiva.

10.3.3 Emisión de Certificados

Realizada la validación de pago y datos personales entregados, se le informa al Solicitante por e-mail el ID y Password necesarios para generar y descargar el certificado en un computador vía web.

10.3.4 información no verificada del suscriptor o titular

firmaschile no incluye en sus certificados información no verificada del titular, siendo la única excepción la que corresponde a la dirección de correo electrónico del suscriptor. En este caso, firmaschile al momento del registro, solicita suscriptor o el titular comprobar que la dirección

de correo electrónico que se incluirá en el certificado es la que efectivamente desea incluir. firmaschile no comprueba ni la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento; siendo todo ello responsabilidad del solicitante. A pesar de lo dicho, si la dirección no es válida o correcta, el suscriptor o el titular no recibirá el mail de instalación del certificado, por lo cual no existe riesgo de registrar de manera errada este dato en el certificado; ello debido a que sólo el titular o suscriptor tendrán el acceso al mail de instalación, el número de solicitud y el pin de instalación generado durante la operación del registro. Cualquiera de estos elementos que no se posea, no permitirá la generación e instalación del certificado.

10.4 Uso del par de claves y del certificado

El suscriptor sólo puede utilizar los datos de creación de firma y el certificado de firma electrónica para los usos autorizados en este instrumento y de acuerdo con lo establecido en los campos “Key Usage” y “Extended Key Usage” del certificado.

Tras la expiración o revocación del certificado, el suscriptor debe cesar en el uso de los datos de creación de firma.

Todo uso del certificado fuera del ámbito o uso autorizado indicado en éste es de exclusiva responsabilidad del titular y representan usos ilegítimos.

10.5 Renovación de claves

La renovación de claves implica necesariamente la emisión de un nuevo certificado de firma electrónica. Las claves no son recuperables.

10.6 Revocación de Certificado

Las alternativas disponibles para suspender o revocar cada tipo de certificado están disponibles en las políticas de certificación correspondientes.

10.6.1 Circunstancias de Revocación

Aplica lo dispuesto en 10.6.3

10.6.2 Solicitud de Revocación

Aplica lo dispuesto en 10.6.3

10.6.3 Descripción de Procedimiento de Revocación

La revocación de certificados puede ser solicitada por el titular, en caso persona natural, la AC que emitió el certificado, un juez en su aplicación de la Ley o un tercero con elementos fundantes adecuados.firmaschile realiza la validación de identidad de las personas naturales para la revocación de sus certificados electrónicos, siendo ello de tres formas:

- **En forma presencial en oficinas de firmaschile:** En ella se entregarán los antecedentes que comprueben la identidad del suscriptor o titular, mencionando también los motivos de la revocación. Esta información se registra a través de un

documento que incluye la fotocopia de la cédula de identidad, y un documento manuscrito que indique los motivos de la solicitud de revocación. Todo esto debe ser firmado por el mismo titular o suscriptor.

- **Un correo electrónico:** Se debe indicar la solicitud de revocación, señalando los motivos de dicha **solicitud**, e incluyendo una copia de la cédula de identidad, por ambos lados. Se debe incluir en ella los motivos de revocación, incluyendo la firma del titular. Esta información debe ser enviada a la casilla de correo electrónico revocaciones@firmaschile.cl. En caso de ser necesario, se le solicitará al suscriptor o titular, el número de serie que identifique el certificado a revocar, dada la posibilidad de que él tenga más de un certificado emitido a su nombre.
- **Juez, EC y/o tercero:** Ante un oficio oficial de un juez de la República, en aplicación de la Ley; o la AC de firmaschile o un tercero que demuestre el no cumplimiento de estas CPS por parte del suscriptor.

10.6.4 Solicitantes

Los habilitados para realizar la revocación de los certificados son:

- El titular o suscriptor de su propio certificado
- Tribunales de Justicia, organismos, instituciones o Autoridades facultadas por la ley, que tengan la potestad para solicitar la revocación de un certificado.
- La AC que emite el certificado
- Un tercero que tenga pruebas que demuestre el no cumplimiento de estas CPS por parte del suscriptor.

10.6.5 Aprobación o rechazo de la solicitud

Una vez que el Operador de Validación ha recibido la solicitud de revocación, éste la aprobará, sólo si el solicitante de la revocación corresponde a alguno de los descritos en 10.6.4, y si se ha provisto de toda la información solicitada para la revocación del certificado, según lo descrito en 10.6.3. En caso de no cumplirse alguno de los puntos antes mencionados, se procederá al rechazo de la solicitud de revocación.

10.6.6 Ejecución de la revocación

El Operador de Validación, una vez validada la correcta entrega por parte del solicitante, de la información requerida para la solicitud de revocación, procederá a la revocación del certificado, acción que se verá reflejada inmediatamente en el servicio OCSP provisto por firmaschile; mientras que el cambio del estado del certificado en la CRL será actualizado en las próximas 24 horas.

El plazo transcurrido entre la recepción de la solicitud y su procesamiento no podrá ser superior a 8 horas, considerando lunes a viernes de 9:00 a 18:00 horas. Una vez recibida la solicitud, el tiempo de actualización de los servicios OCSP será inmediato a partir de revocado el certificado y de a lo más 24 horas para la actualización de la lista CRL.

10.6.7 Tiempo de procesamiento

Desde que la AR de firmaschile recepciona la solicitud de revocación de un certificado, el tiempo comprometido para su procesamiento, será de acuerdo con lo declarado en 10.6.6 de estas CPS.

10.7 Listado de Certificados Revocados

firmaschile publicará una nueva CRL en su repositorio en intervalos de 24 horas, aunque no se hayan producido modificaciones en la misma (cambios de estado de certificados) durante dicho periodo.

10.8 Servicios de comprobación de estado de certificados.

firmaschile cuenta con dos servicios para la comprobación de los certificados, el primero es la CRL o lista de revocación, la que se actualiza tal como se indica en 10.7; la segunda es el servicio OCSP, el cual entrega el estado actual de un certificado.

10.9 Finalización de la suscripción.

La suscripción finaliza con el término de vigencia de un certificado o la revocación de este.

11 Derechos de Propiedad Intelectual e Industrial

La prestación de los servicios de certificación de firma electrónica en ningún caso otorga a los partícipes de la comunidad descritos en 3.3.1 de estas CPS derecho de propiedad intelectual o industrial alguno. Así, firmaschile retiene todos sus derechos de propiedad intelectual e industrial sobre las obras creadas, desarrolladas o modificadas. Ningún derecho de propiedad intelectual o industrial preexistente o que se adquiera o licencie a o por firmaschile, se entenderá conferido a los miembros de la comunidad antes citada.

Salvo acuerdo previo, específico y por escrito en contrario celebrado con algún miembro de la comunidad descrita en 3.3.1 de estas CPS, ninguno de ellos puede publicar o usar logotipos, marcas, marcas registradas, incluso marcas de servicio y patentes, nombres, redacciones, imágenes, símbolos o palabras de firmaschile.

Los documentos definidos cómo públicos pueden ser reproducidos respetando las restricciones indicadas en cada documento:

- Políticas de privacidad
- Políticas de certificados
- Prácticas de certificación

12 Detalle de los contactos y administración de la PSC

Cualquier consulta respecto a las normas contenidas en este documento, puede ser realizada en la siguiente dirección:

- **Nombre**: firmaschile
- **Dirección de e-mail**: contacto@firmaschile.cl
- **Número telefónico**: +562 2306 6170

ANEXO: ACREDITACIONES / DOCUMENTACION DE eMudhra

1. ROOT CA Certificate: http://repository.emsign.com/certs/TrustedRootCAC4.crt
2. ROOT CA CRL URL: http://crl.emsign.com/?TrustedRootCAC4.crl
3. ROOT OCSP URL: http://ocsp.emsign.com
4. Issuing CA Certificate: http://repository.emsign.com/certs/TrustedIssuingCAC4.crt
5. Issuing CA CRL URL: http://crl.emsign.com/?TrustedIssuingCAC4.crl
6. Issuing CA OCSP URL: http://ocsp.emsign.com
7. emSign Repository _ eMudhra: https://repository.emsign.com/index.jsp
8. CPS-v1.0 / OID: 1.3.6.1.4.1.50977.1.0.1.1: https://repository.emsign.com
9. Privacy Policy _ eMudhra: https://www.eMudhra.com/privacy-policy.jsp

10. eMudhra Limited - EU GDPR:

11. Certificate of Appraisal eMudhra CMMI Level5

CMMI Institute

Univate Solutions
Innovation Unleashed

Certificate of Appraisal

Organization

eMudhra Limited

Organization Unit

Product Development Center

Organization Unit has been appraised at

CMMI DEV /5 SM

Exp. 2022-12-03 / Appraisal #4884

Date of Result: 3rd December, 2019

Appraisal Expiration Date: 3rd December, 2022

Lead Appraiser

Rajarshi Kumar Das

Appraisal Method Used: SCAMPI Ver. 1.3 A

CMMI Model Used: CMMI DEV Version 1.3

CEO, Univate Solutions Pvt. Ltd.

CMMI Institute Partner

12. BQSR -HIPAA eMudhra Consumer Services Limited

13. eMudhra Limited-27001-2013 QEC

QEC CERTIFICATION

CERTIFICATION

Information Security Management System

Certificate of Approval

This is to certify that the ISMS of

eMudhra Limited

OFFICE - #56, 3rd Floor, Sai Arcade, Outer Ring Road, Devarabeesanahalli, Bangalore - 560103.
SITE 1: No, 23, 24, 1st & 2nd floor, Above ICICI Bank, Bellandur Village, Varthur Hobli, Bangalore - 560103.
SITE 2: 270, First Floor, V.M.G. Srivasan Complex, Saradha College Main Road, Swarnapuri, Salem, Tamil Nadu - 636016.

Has been assessed and found to meet the requirements of

ISO/IEC 27001:2013

This certificate is valid for the following scope of operations

Statement of Applicability: Date: 05/10/2019,
Ref. Doc: EML/ISMS/SOA_01, Issue Level: 01

FUNCTIONING AS CERTIFYING AUTHORITY, PROVIDING E-SIGN SERVICE, DEVELOPMENT & DELIVERY OF SOFTWARE/ SOLUTIONS/ SERVICES IN PUBLIC KEY INFRASTRUCTURE (PKI), IDENTITY & AUTHENTICATION PLATFORMS AND DATA ANALYTICS.

CERTIFICATION

Authorised by:

R N Cooke
Director

Date of Certificate Issue: 06 May 2020
Certificate Valid Until: 05 May 2023

Recertification audit before 05 April 2023. Certified since 06 May 2020.
This certificate is the property of SN Registrars (Holdings) Limited and remains valid subject to satisfactory annual Surveillance audits.

SN Registrars (Holdings) Limited
Registration House, 22b Church Street,
Rushden, Northamptonshire,
NN10 9YT, UK
Tel: +44 (0) 1933 383261
Email: enquiries@qec.co.uk
Web: www.qec.co.uk
Company Number: 07659067

Certificate Number: QEC 43709165/71/I Rev: 001

IAF

CERTIFICATION ISO/IEC 27001 Trading name of SN Registrars (Holdings) Ltd

UKAS MANAGEMENT SYSTEMS 8327

14. eMudhra Limited - 27018-2014

ISO/IEC 27018:2014

Certificate of Compliance

UNIVERSAL REGISTRARS

EMUDHRA LIMITED

Location 1: #56, 3rd Floor, Sai Arcade, Outer Ring Road, Devarabeesanahalli, Bangalore - 560103.
Location 2: No. 23, 24, 1st & 2nd floor, Above ICICI Bank, Bellandur Village, Varthur Hobli, Bangalore - 560103.
Location 3: 270, First Floor, V.M.G. Srivasan Complex, Saradha college main road, Swarnapuri, Salem, Tamil Nadu 636016.

has implemented techniques in line with Information Technology - Security Techniques Code of Practice for Protection of Personally Identifiable Information System

System Certification
ISO/IEC 27018:2014

ISO/IEC 27018:2014

For the following scope:
Functioning as certifying authority, providing e-sign service, development & delivery of software/ solutions/ services in public key infrastructure (PKI), identity & authentication platforms and data analytics.

Certificate number: 26971
This certificate is valid from 03-Feb-2022 until 02-Feb-2025.
And remains valid subject to satisfactory surveillance audits
On or before 3-Feb-2023 and 2-Feb-2024.
Re-certification audit due on 3-Feb-2025.

.....
Certification Manager

UNIVERSAL REGISTRARS
www.universalregistrars.com

This certificate can be verified at the above URL.
The certificate remains the property of Universal Registrars, to whom it must be returned on request. Lack of fulfillment of certification terms and conditions at all times, may render this certificate invalid.

15. Adobe Approved Trust List Members, Acrobat

Last updated on Apr 26, 2022 | Also Applies to Adobe Acrobat Sign, R...

The Adobe Approved Trust List (AATL) is a program that enables millions of people around the world to sign documents in Adobe Document Cloud solutions using the world's most trusted digital signing certificates. The certificate authorities (CAs) and trust service providers (TSPs) on this list issue digital signing certificates and timestamp services that can be used to comply with legal and regulatory requirements around the world, including the EU eIDAS regulation. Adobe's digital signatures also work with every accredited provider offering qualified trust services listed in the European Union Trust List (EUTL).

Get your digital certificates or timestamp service from one of the providers below, and start signing documents securely with Adobe Acrobat Reader DC, Acrobat DC, or Adobe Acrobat Sign.

Current AATL Members

Country/Region Code	Headquarters Location	Company Name	Company Logo	Cloud Signature Consortium TSP*
AE	Abu Dhabi, United Arab Emirates	DigitalTrust	DIGITALTRUST	
AE	Abu Dhabi, United Arab Emirates	Telecommunications and Digital Government Regulatory Authority (TDRA)	TDRA	
AE	Dubai, United Arab Emirates	Dubai Electronic Security Center	DUBAI ELECTRONIC SECURITY CENTER	

HK	Hong Kong SAR of China	Hongkong Post	
ID	Indonesia	Vida	
IL	Israel	ComSign	
IN	India	CCA India	
IN	India	eMudhra	
IT	Italy	Actalis	
IT	Italy	InfoCert	
IT	Italy	Intesa IBM	
IT	Italy	Intesi Group	
IT	Italy	IPZS	
IT	Italy	Namirial	

16. eMudhra WebTrust for CA - Audit Report & Management Assertion

Tel: +603 2616 2888
Fax: +603 2616 2829
www.bdo.my

Level 8
BDO @ Menara CenTARa
360 Jalan Tuanku Abdul Rahman
50100 Kuala Lumpur
Malaysia

INDEPENDENT ASSURANCE REPORT

To the management of eMudhra Technologies Limited ("emSign PKI"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on emSign PKI management's assertion that for its Certification Authority (CA) operations at Bangalore and Salem, India throughout the period 1 June 2020 to 31 May 2021 for its CAs as enumerated in Appendix A, emSign PKI has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in applicable versions of its Certification Practice Statements in Appendix B
- maintained effective controls to provide reasonable assurance that emSign PKI provides its services in accordance with applicable versions of its Certification Practice Statements as enumerated in Appendix B
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by emSign PKI); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.

emSign PKI does not escrow its CA keys, does not provide integrated circuit card lifecycle management and certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

BDO Consulting Sdn Bhd (269105-W), a Malaysian Limited Liability Company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

Certification authority's responsibilities

emSign PKI's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

(1) obtaining an understanding of emSign PKI's key and certificate lifecycle management business practices and its control over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
(3) testing and evaluating the operating effectiveness of controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at emSign PKI and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, emSign PKI's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, throughout the period 1 June 2020 to 31 May 2021, emSign PKI management's assertion, as referred to above is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.

This report does not include any representation as to the quality of emSign PKI's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2, nor the suitability of any emSign PKI's services for any customer's intended purpose.

Use of the WebTrust seal

emSign PKI's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

BDO Consulting Sdn. Bhd.

BDO Consulting Sdn. Bhd.
Kuala Lumpur, Malaysia
27 August 2021