PO02 DECLARACIÓN DE LAS PRÁCTICAS DE CERTIFICACIÓN

1 INFORMACIÓN DEL DOCUMENTO

HISTORIA DEL DOCUMENTO			
Nombre del documento:	PO02 Declaración de las Prácticas de Certificación		
Generado por:	Osvaldo Martínez Burgos		
Revisado por	Rafael Pérez López	**Fecha de creación:**	04/03/2022
Aprobado por:	Rafael Pérez López	**Fecha de aprobación:**	11/05/2022
Oficializado por:	Comité de Riesgos y Seguridad	**Entrada en vigencia:**	13/05/2022

CONTROL DE VERSIONES				
Versión:	**Fecha de Publicación:**	**Preparado/ Actualizado por:**	**Aprobado por:**	**Descripción:**
1.0	04/03/2022	**Osvaldo Martínez**	Rafael Pérez	Creación
1.1	13/03/2023	**Nicolás Borbarán**	Rafael Pérez	Incorporación del procedimiento de enrolamiento de firma electrónica avanzada con token en domicilio del solicitante. Actualización URL de la página web.

CONTENIDO

2 INTRODUCCIÓN

2.1 PRESENTACIÓN

El presente documento constituye el Estatuto de Prácticas de Certificación (Certificate Practice Statement) del servicio de certificación de e-Digital PKI, al cual se hará referencia mediante el acrónimo de su denominación en inglés CPS.

2.2 IDENTIFICACIÓN

El presente documento se denomina “Declaración de las prácticas de Certificación” y puede localizarse en la siguiente URL: https://signapis.com/pdf/declaracion_practicas.pdf.

2.3 COMUNIDAD DE USUARIOS Y APLICACIONES

Los certificados de Firma Electrónica Avanzada (FEA) permiten que las personas puedan firmar electrónicamente. Identifica al usuario o titular de forma única y podrá utilizarse para firma electrónica mediante certificados digitales X.509 v3 emitidos bajo la Política de Firma Electrónica Avanzada. Este certificado permitirá firmar solo ajustándose a lo establecido en la ley 19.799 y su reglamento.

El usuario o Titular de un certificado de Firma Electrónica Avanzada de e-Digital PKI podrá ser cualquier persona natural, siempre que aplique a los criterios establecidos en la presente Práctica de Certificación (CPS), la Ley 19.799 y su reglamento especificado en el Decreto 181.

Los certificados FEA podrán ser utilizados por usuarios o titulares para realizar actos, celebrar contratos y expedir cualquier documento, exceptuando las no aplicaciones que se mencionen en el artículo 6° de la Ley 19.799.

2.3.1 FIRMA Y NO REPUDIO

El receptor de un mensaje o documento firmado con el certificado puede usar la clave pública del emisor para verificar que este último ha usado su clave privada para firmar el mensaje o documento. Esto permite confirmar frente a un tercero, la identidad del emisor del mensaje o documento y la no alteración de este.

El mensaje o documento firmado puede corresponder a una transacción y documento electrónico con validez legal según la legislación vigente, en especial la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación.

2.3.2 INTEGRIDAD

El uso de los servicios de certificados y de Firma Electrónica Avanzada permite asegurar al receptor de un mensaje o documento, que no ha sido alterado entre el envío y la recepción.

a) Autoridad Certificadora (AC)

e-Digital PKI actúa como Prestadora de Servicios de Certificación (PSC) y al emitir un certificado, relaciona una determinada clave pública y privada con un usuario o titular concreto. A su vez los desvincula al revocar dicho certificado, de conformidad con los términos de esta CPS.

b) Autoridad de Registro (AR)

Corresponde a una entidad intermedia entre la AC y los titulares, encargándose de la detección, comercialización y administración de las solicitudes de certificación. Siendo su principal función, comprobar fehacientemente la identidad del solicitante en conformidad con el Artículo Nº12 letra e) de la Ley Nº19.799, registrando los antecedentes del solicitante para establecer los atributos del certificado.

La AC podrá valerse de una o varias Autoridades de Registro (AR) (siempre personal interno de e-Digital PKI), quienes deberán llevar a cabo el proceso de comprobar fehacientemente la identidad del Solicitante.

c) Titular

El usuario o Titular del certificado será la persona que utiliza bajo su exclusivo control un certificado de firma electrónica - Art. 2, letra h) Ley 19.799.

d) Solicitante

Solicitante será la persona que comparece personalmente ante la Autoridad Certificadora permitiendo la comprobación fehaciente de su identidad para la emisión del certificado, previa solicitud vía formulario web, según lo dispuesto en la CP, CPS y Ley Nº19.799.

e) Tercera persona que confía

Persona que recibe cualquier instrumento firmado por un titular utilizando su certificado de Firma Electrónica Avanzada y decide voluntariamente confiar en este.

f) Tipo de Certificado

El tipo certificado que se ofrecen dentro del ámbito de esta CPS están definidos en la CP disponible en la URL: https://signapis.com/pdf/politica_certificados.pdf. La CP regula la aplicabilidad del certificado en relación con una comunidad de usuarios, algunos usos y restricciones determinados con requerimientos de seguridad comunes.

g) Limitaciones de uso

Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que éstos vayan cambiando.

No se permite un uso del certificado contrario a:

- La normativa chilena y a los convenios internacionales ratificados por el Estado Chileno.
- Lo establecido en esta CPS, en la Política de Certificación y en los contratos de suscripción de FEA que se firmen entre la entidad Prestadora de Servicios de Certificación (PSC) e-Digital PKI y el titular.

Los certificados de e-Digital PKI no podrán ser alterados, deberán utilizarse tal y como son suministrados por la AC.

2.4 DETALLES DE CONTACTO

Oficina	Badajoz 100 Oficina 1519, Las Condes, Santiago, Chile
e-mail	contacto@signapis.com
Teléfono	(+56) 2 2248 1264
Horario atención	Días hábiles de lunes a viernes entre 09:00 y 17:00 horas

3 CONSIDERACIONES GENERALES

3.1 OBLIGACIONES

3.1.1 OBLIGACIONES DEL PSC

Obligaciones de e-Digital PKI como prestadora de servicios de certificación son todas aquellas obligaciones impuestas por la presente CPS:

a) Asegurar conformidad de sus procesos y actividades con las prácticas de certificación definidas en este documento y las respectiva CP.

b) Emitir certificados haciendo uso de tecnologías y criptografía que permitan un adecuado proceso de certificación.

c) Apoyar la emisión de certificados con las tecnologías que permitan el resguardo de las llaves privadas de los titulares de e-Digital PKI.

d) Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley Nº 19.628, sobre Protección de la Vida Privada.

e) Utilizar mecanismos de comprobación fehaciente de la identidad del solicitante y garantizar una identificación fidedigna.

f) Almacenar la información obtenida del proceso de enrolamiento (ficha de registro, impresión huella dactilar, fotografía del titular y fotocopia de cedula de identidad por ambos lados) en un sistema de custodia documental manual y copia digitalizada.

Frente al Titular:

a) Notificar al Titular de la emisión de su certificado.
b) Notificar al Titular de la revocación de su certificado.
c) Mantener actualizados los registros de certificados vigentes y certificados revocados, en concordancia con la ley 19799.
d) Revocar certificados que no cumplan con declaraciones de esta CPS o de la CP.

Frente a la tercera parte interesada que confía:

a) Cumplir de manera sustancial con el contenido de esta CPS.
b) Poner a disposición de los usuarios los certificados que componen la(s) cadena(s) de confianza de e-Digital PKI.

3.1.2 OBLIGACIONES DE LA AR

La AR asumirá las siguientes obligaciones de las cuales será responsable:

a) Comprobar fehacientemente la identidad del Solicitante, conforme a los procedimientos que se establece en esta CPS y en las Políticas de Certificación, utilizando cualquiera de los medios admitidos en derecho, que para los certificados de FEA es la comparecencia personal y directa del solicitante.

b) Mantener y garantizar, de conformidad con el artículo 12 letra b) de la Ley Nº19.799, la existencia de un registro con los antecedentes proporcionados por el titular para efectos de certificación durante a lo menos durante seis años desde la emisión inicial de los certificados, y no podrá utilizarlos para otros fines. En lo restante se aplicarán las disposiciones de la ley N.º 19.628, sobre Protección de la Vida Privada.

c) Almacenar de forma segura la documentación aportada, tanto para el proceso de emisión del certificado, como para el proceso de revocación.

d) Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta CPS.

e) Aplicar medidas de seguridad adecuada y suficiente para salvaguardar la llave privada del titular, al momento de generación del certificado.

f) En caso de realizar una visita a las dependencias del solicitante, debe garantizar el registro y comprobación fehaciente de identidad, la seguridad y protección de los medios de enrolamiento y la entrega del dispositivo criptográfico token FIPS 140-2 nivel 3 al Titular.

g) Luego de importar el certificado en el dispositivo criptográfico token FIPS 140-2 Nivel 3, asignado al Titular, debe eliminar el certificado en el notebook del operador de la Autoridad de Registro.

La AR deberá disponer a la PSC del expedito acceso a los antecedentes, archivos y procedimientos relacionados al enrolamiento y entrega de los certificados, para una eventual investigación o sospecha de infracción de la CPS y/o de las Políticas de Certificación.

3.1.3 OBLIGACIONES DEL SOLICITANTE

Los solicitantes de certificados de firma electrónica avanzada de e-Digital PKI quedan obligados a presentarse presencialmente ante la Autoridad de Registro (AR), proporcionar sus datos de identidad personal y brindar declaraciones exactas y completas.

3.1.4 OBLIGACIONES DEL TITULAR

a) Conservar y utilizar correctamente el certificado.

b) Custodiar el certificado, tomando las precauciones necesarias para evitar la pérdida de su dispositivo criptográfico, de sus claves privadas o la mala utilización o uso no autorizado del mismo.

c) Proteger diligentemente la contraseña del certificado y el PIN Secreto del dispositivo criptográfico (token FIPS 140-2 Nivel 3) que cumpla con los estándares establecidos para la emisión de dicho certificado.

d) Solicitar la revocación del certificado cuando se cumpla alguno de los supuestos previstos en el epígrafe titulado “REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS” de la presente CPS en su numeral 5.3.

e) No revelar la clave privada ni el código de activación del certificado.

f) Asegurarse de que toda la información contenida en el certificado es correcta y en conformidad al Art. 24 de la Ley 19.799 y notificar inmediatamente a la AR o PSC, según corresponda.

g) Informar inmediatamente a la AR o el PSC acerca de cualquier situación que pueda afectar a la validez del certificado.

h) Realizar un debido y correcto uso del certificado, según se desprende de esta CPS y de las Políticas de Certificación. Será responsabilidad del Titular el uso indebido que éste haga del Certificado de Firma Electrónica Avanzada, según lo indicado en el Art. 24 de la Ley 19799.

i) Cualquier otra obligación que exija la ley 19.799, en esta CPS o de la CP.

3.1.5 OBLIGACIONES DE LOS PROVEEDORES

Las empresas proveedoras de servicios deberán cumplir con las políticas de seguridad de la información, mantener un procedimiento para el tratamiento de riesgos y contratos que aseguren la oportuna entrega de servicios con e-Digital PKI.

3.1.6 OBLIGACIONES DE LAS TERCERAS PARTES INTERESADAS

Las terceras partes interesadas que pretendan confiar y usar los certificados emitidos por el PSC deberán verificar la validez de las firmas emitidas por los Titulares.
Toda persona puede confiar en una firma electrónica emitida mediante un certificado de e-Digital PKI, debiendo tener las siguientes consideraciones:

a) Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad de la firma y en particular, si ha verificado que el certificado usado para firmar poseía una cadena de confianza.
b) Si la parte que confía confirmó si la firma estaba en entredicho o había sido revocada, según el punto 5.3 de esta CPS.
c) Si la parte que confía confirmó las políticas y procedimientos que rigen la actividad con relación a las firmas generadas mediante certificados emitidos por e-Digital PKI, que se especifican en esta CPS y en las CP disponibles públicamente en las URL https://signapis.com/pdf/declaracion_practicas.pdf y https://signapis.com/pdf/politica_certificados.pdf, respectivamente.

En el supuesto de que los usuarios o terceras partes interesadas, no realicen la verificación de los certificados a través del OCSP (Estado de un certificado en línea) o la CRL (Lista de certificados revocados), el PSC no se hace responsable del uso y confianza que hagan de estos certificados.

3.2 RESPONSABILIDAD

3.2.1 RESPONSABILIDAD DEL PSC

La PSC no será responsable de los daños derivados de errores u omisiones de las obligaciones por parte del titular.

El PSC no será responsable de la incorrecta utilización de los certificados ni de cualquier daño indirecto que pueda resultar de su mal uso.

Previa acción a cualquier emisión de certificado, el PSC no será responsable por el retraso o la no ejecución de cualquiera de las obligaciones de esta CPS a consecuencia de un acto de fuerza mayor, caso fortuito o en general, cualquier circunstancia que la PSC no pueda poseer control razonable, como por ejemplo: Desastres naturales, guerra, estado de sitio, alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico, de comunicación o básico, virus informáticos, estado de emergencia sanitaria, pandemias, endemia, estados de excepción y/o catástrofes en general.

Será responsabilidad del Titular disponer de todos los elementos técnicos necesarios para el normal funcionamiento y uso de del Certificado.

El PSC no será responsable del contenido de los documentos suscritos electrónicamente mediante cualquier certificado.

El PSC se compromete a mantener vigente y disponer un seguro de responsabilidad civil que cubra el valor mínimo exigido por el Art. 14, inciso 4 de la Ley 19.799.

3.2.2 RESPONSABILIDAD DE LA AR

La AR responderá de las funciones que le correspondan conforme a esta CPS y, en especial, asumirá toda la responsabilidad por la correcta comprobación fehaciente de la identidad del solicitante, con las mismas limitaciones que se establecen en el apartado 3.1.2 de esta CPS con relación al PSC.

3.2.3 RESPONSABILIDAD DEL SOLICITANTE

El solicitante responderá a las actividades que le correspondan ejecutar conforme a esta CPS y, en especial, asumirá toda la responsabilidad por la correcta entrega, en plazo y forma, de información y documentación solicitada durante la comprobación fehaciente de su identidad, además de presentarse presencialmente ante la AR, con las mismas limitaciones que se establecen en el apartado 3.1.3 de esta CPS con relación al PSC.

El solicitante, en caso de solicitar el enrolamiento en su domicilio, debe entregar una dirección válida para coordinar la visita del operador de la Autoridad de Registro a sus dependencias.

3.2.4 RESPONSABILIDAD DEL TITULAR

El Titular es responsable de custodiar el Certificado, tomando las precauciones razonables para evitar su pérdida, modificación o uso no autorizado y garantizar su seguridad, así como la del procedimiento para el cual se emiten, especialmente cuidando de no divulgar las claves privadas, especialmente si existe la posibilidad de extravío, hurto o sustracción indebida.

3.2.5 RESPONSABILIDAD FINANCIERA

Las responsabilidades que afectan la operación de e-Digital PKI están establecidas y limitadas a lo establecido en el artículo 14 de la Ley 19.799.

3.3 INTERPRETACIÓN Y EJECUCIÓN

3.3.1 LEY APLICABLE

e-Digital PKI cumple con las obligaciones establecidas por la Entidad Acreditadora a los requerimientos de la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación” – EA-103 Versión 2.4 establecida por la Entidad Acreditadora. Vigente a lo establecido en la Ley 19.799 de 2002, ley 19.799 de 2007, el Decreto 181 de 2002, modificación del Decreto 181 de 2012, y a cualquier otro reglamento que modifique o complemente alguna de las leyes o decretos anteriores.

3.3.2 SUBROGACIÓN, NOVACIÓN Y NOTIFICACIONES

El PSC se reserva el derecho de transmitir en el futuro todas las obligaciones y derechos que se deriven de esta CPS a un tercero para que éste continúe prestando el servicio de certificación. "En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y deberán, de no existir oposición de estos últimos, 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, 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." Esta CPS seguirá siendo el documento que regule las relaciones entre las partes mientras no se cree un nuevo documento por escrito.

El PSC podrá modificar cualquiera de las cláusulas de la presente CPS en los términos previstos en esta CPS, "siempre que no afecte derechos del titular (consumidor) en relación con la Ley 19.496 y Ley 1.968. Este caso se puede presentar en caso de perder la acreditación, según causas del Artículo 19, letra b) de la Ley 19.799".

3.3.3 TASAS DE REGISTRO POR LA EXPEDICIÓN Y RENOVACIÓN DE CERTIFICADOS

El costo por la emisión o renovación de los certificados serán puestas a disposición de los solicitantes, usuarios o titulares por el PSC, la cual podrá establecer promociones especiales, ofertas o similares que modifiquen las tarifas previamente establecidas.

3.4 PUBLICACIÓN Y DEPÓSITO DE LA CPS

El contenido de esta CPS, así como de toda la información que se publique, estará disponible a título informativo en la dirección de URL: https://signapis.com/pdf/declaracion_practicas.pdf y los originales en las oficinas del PSC.

3.5 SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

La seguridad de los equipos es resultado del análisis de las medidas de seguridad que mantiene nuestros proveedores de servicios en respuesta a la probabilidad e impacto de amenazas producto de omisiones o brechas de seguridad, según lo dispuesto en los requisitos de seguridad dispuestos en los dominios PS01 al PS07, que determinan los niveles de seguridad que dispone el PSC.

3.6 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

3.6.1 CONFIDENCIALIDAD DE LAS CLAVES DE FIRMA ELECTRÓNICA AVANZADA

El Operador AR, entregará un dispositivo criptográfico solicitará al Titular la creación de su clave propietaria del certificado, así como un PIN Secreto para el dispositivo criptográfico token FIPS 140-2 Nivel 3, quedando

a total control y administración de su Firma Electrónica. En caso de dudas se entregará el soporte y asistencia por el operador de la AR.

3.6.2 CONFIDENCIALIDAD EN LA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN

La información de los titulares de certificados es de carácter confidencial (Art. 23 párrafo 2° de la ley 19.799), por lo tanto, estos datos e información serán tratados por e-Digital PKI de acuerdo con las obligaciones según lo dispuesto por Artículo 12 b) de la ley N.°19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma.

3.6.3 PROTECCIÓN DE DATOS

La información de los titulares de certificados es de carácter confidencial (Art. 23 párrafo 2° de la ley 19.799), e-Digital PKI de acuerdo con las obligaciones y lo dispuesto por Artículo 12 b) de la ley N.°19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma, donde se estipula que la PSC debe mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley N.º 19.628, sobre Protección de la Vida Privada y lo relativo al Titular en su rol de consumidor, las disposiciones de la ley N.º 19.496, Sobre Protección a los Derechos de los Consumidores.

3.6.4 TIPOS DE INFORMACIÓN QUE DEBE MANTENERSE CONFIDENCIAL Y PRIVADA

e-Digital PKI no utilizará la información de los titulares para otros fines que los exclusivos y relacionados con sus actividades de certificación, ni compartirá esta información con terceros.

En relacionado a lo anterior, como política general, e-Digital PKI no entrega información personal de sus clientes.

Sin perjuicio de lo anterior, los certificados emitidos por e-Digital PKI contienen información de identificación del titular, y el contenido del certificado está definido en la Ley N.º 19.799.

El certificado de firma electrónica avanzado contiene los siguientes campos obligatorios de información de los titulares:

a) RUT
b) Correo electrónico
c) Nombre del titular
d) Empresa emisora de certificado (PSC)
e) Datos de la acreditación de e-Digital PKI (Declaración del emisor)

3.6.5 TIPOS DE INFORMACIÓN QUE NO SE CONSIDERA CONFIDENCIAL NI PRIVADA

e-Digital PKI declara que los Certificados, la revocación de Certificados y la información contenida en ellos, no se consideran Información Confidencial/Privada. Asimismo, se establece que dicha información es tratada de conformidad con el artículo 12 b) de la ley 19.799.

De igual forma, la información contenida en la presente CPS y en la CP no será considerada confidencial ni privada, siendo de público acceso a través del sitio web de la PSC en las siguientes direcciones URL https://signapis.com/pdf/declaracion_practicas.pdf y https://signapis.com/pdf/politica_certificados.pdf, respectivamente.

3.7 DERECHOS DE PROPIEDAD INTELECTUAL

El PSC es titular de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva del PSC sin la autorización expresa por su parte. No obstante, no necesitará autorización del PSC para la reproducción del Certificado cuando la misma sea necesaria para la utilización del Certificado por parte del usuario legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta CPS.

4 IDENTIFICACIÓN Y AUTENTICACIÓN

4.1 REGISTRO INICIAL

El Solicitante deberá llenar el formulario dispuesto por el PSC en su página WEB para la solicitud del certificado. El ingreso de los datos solicitados en este formulario supondrá su consentimiento para ser registrado como solicitante de un certificado e-Digital PKI. La solicitud de este certificado no implicará en ningún caso su obtención de este si no llegan a cumplirse por parte del solicitante las cláusulas y condiciones establecidos en esta CPS o en la Política de Certificación para los certificados de Firma Electrónica Avanzada. En el mismo acto el solicitante proporcionará a la AR toda la información que necesite, bien para registrar al Solicitante como Titular, o con la finalidad de incluirla en el certificado, de acuerdo con los requisitos establecidos en esta CPS.

Existen dos opciones para validar fehacientemente la identidad del titular:

- **En Oficinas de Signapis**: El usuario completa el registro seleccionando la opción de “Enrolamiento presencial” y coordina con la Autoridad de Registro, según disponibilidad, una visita a las oficinas de Signapis y realiza el registro y comprobación fehaciente de identidad de manera presencial, en horario hábil de lunes a viernes entre 9:00 y 17:00 hrs.
- **En Domicilio del Solicitante**: El solicitante completa el registro seleccionando la opción “Enrolamiento en domicilio del solicitante” para realizar el registro y comprobación fehaciente de identidad en las dependencias del usuario y coordina la visita al domicilio señalado por el solicitante, con el operador de la Autoridad de Registro, acorde a la disponibilidad de su agenda. En el numeral 5.2. del documento se establece el detalle sobre la visita del operador de la Autoridad de Registro.

4.2 AUTENTICACIÓN DE LA IDENTIDAD DEL SOLICITANTE

Para que la AR pueda comprobar fehacientemente la identidad, el solicitante deberá estar presencialmente en las oficinas de Signapis o en el domicilio del solicitante, y acreditar todas las menciones básicas del certificado, para lo cual deberá presentar su Cédula Nacional de Identidad chilena vigente.

En el caso de la visita del operador de la Autoridad de Registro al domicilio del solicitante, el operador coordina con el solicitante la visita al lugar acordado. Para asistir a las dependencias del solicitante, el operador de la Autoridad de Registro utilizará un medio de transporte (público o privado) que dependerá de la distancia del trayecto.

Además, el operador de la Autoridad de Registro debe portar:

- Notebook de e-digital.
- Smartphone de e-digital.
- Módem propio (Conexión propia del operador de la Autoridad de Registro a internet).
- Dispositivo criptográfico token FIPS 140-2 nivel 3, donde está almacenada la llave privada y certificado del operador de la Autoridad de Registro (Certificado para acceder al software generador de certificados utilizado por Signapis, desde el Notebook de la Autoridad de Registro).
- Dispositivo criptográfico token FIPS 140-2 nivel 3, donde se almacenará la llave privada del titular y su certificado.
- Cámara fotográfica (no inteligente).
- Contrato impreso.
- Huellero (no captura datos biométricos).
- Lápiz.

4.3 CONFIRMACIÓN DE LA IDENTIDAD DEL SOLICITANTE

El operador de AR pedirá al solicitante que presente su Cédula de Identidad Chilena, original, vigente y en buen estado, con los datos de la CI se procederá a consultar la validación de los datos en el servicio de Registro Civil e Identificación, el solicitante deberá entregar todas las facilidades necesarias para la realizar las validaciones que correspondan, permitiendo comprobar fehacientemente su identificación.

4.4 ACEPTACIÓN DE LA SOLICITUD

Una vez superado el proceso de comprobación de solicitud de forma satisfactoria, siempre y cuando no existan circunstancias que de alguna manera afecten a la seguridad del servicio de certificación, la AR procederá a la aprobación de la solicitud.

4.5 RECHAZO DE LA SOLICITUD

Si la AR rechazara la solicitud del certificado (Información no corresponde al solicitante, cedula de identidad vencida, en mal estado o bloqueada o el solicitante es menor de 18 años o se encontrase interdicto), dicha

decisión será comunicada de forma inmediata al solicitante y a su vez, formalizada a través de correo electrónico. Si el rechazo es subsanable en forma, el solicitante deberá entregar los datos correctos para generar una nueva solicitud vía WEB.

4.6 ACEPTACIÓN DEL CERTIFICADO

La entrega del certificado, toma de fotografía del solicitante y de su Cédula de Identidad, firma e impresión de huella dactilar en el "Contrato de Suscripción de FEA" (este acto es manual y no se utilizan dispositivos tecnológicos), implicará la aceptación del certificado por parte del solicitante.

La aceptación del certificado deberá realizarse de forma expresa, por escrito y ante el operador de la AR.

Aceptando el Certificado, el solicitante confirma y asume la exactitud del contenido de este, con las consiguientes obligaciones que de ello se derive frente a la AR, la PSC o cualquier tercero que de buena fe confíe en el contenido del Certificado.

5 REQUERIMIENTOS OPERACIONALES

5.1 EMISIÓN DEL CERTIFICADO

Aprobada la solicitud por la AR y aceptado el certificado por el solicitante, la AR procederá a la emisión del certificado y entrega de este al Titular.

El Operador AR, proporcionará un dispositivo criptográfico token FIPS 140-2 nivel 3 y solicitará al Titular la creación de un PIN secreto para el token y una clave propietaria del certificado, quedando a total control y administración de su Firma Electrónica. En caso de dudas se entregará el soporte y asistencia por el operador de la AR.

Para la emisión del certificado (sea en las oficinas comerciales de Signapis o en las dependencias del Titular con la visita del operador de la Autoridad de Registro), el operador de la Autoridad de Registro genera un CSR o Certificate Signing Request (petición de certificado) con la información personal del Titular (nombre completo, RUT, número de documento, correo, comuna, país) y, a su vez, genera el par de llaves en el dispositivo criptográfico token FIPS 140-2 nivel 3 (token) del Titular. En este dispositivo, el titular del certificado genera sus credenciales privadas para acceder al token, con la finalidad de mantener el control absoluto, que posteriormente será utilizado en el software de Signapis para la emisión del certificado. Para acceder a dicho software, el operador de la Autoridad de Registro ingresa con un certificado personal e intransferible, almacenado en un dispositivo criptográfico token FIPS 140-2 nivel 3 (token del operador de la Autoridad de Registro), con sus credenciales correspondientes. Una vez que ingresa al sistema, procede a emitir el certificado del Titular con el CSR generado en el paso anterior. Luego, importa el certificado del Titular al dispositivo criptográfico token FIPS 140-2 nivel 3 del Titular con las extensiones correspondientes y, además, el operador de la Autoridad de Registro elimina de su notebook la copia del certificado del Titular y el CSR generado previamente. Finalmente, el operador de la Autoridad de Registro entrega el dispositivo criptográfico token FIPS 140-2 nivel 3 correspondiente al Titular, con el certificado importado.

Por último, se debe registrar en el sistema de inventario interno, la salida del dispositivo criptográfico, registrando el número de serie de cada elemento y la información del registro del Titular que dio origen al certificado que fue entregado Ej: Fecha, Rut, Nombre.

La AR se reserva el derecho a negarse a emitir certificados cuando concurra cualquier causa justificada, según lo que indica esta CPS en al punto 4.5, por lo que no podrá exigirse responsabilidad alguna por este motivo.

5.2 PUBLICACIÓN DEL CERTIFICADO

Una vez aceptado el Certificado por parte del Titular y emitido el certificado, la AR procederá a la publicación de la llave pública, en el Registro de Acceso Público.

La publicación de los datos del Certificado en el Registro de Acceso Público significa que ha sido aceptado para los terceros usuarios de buena fe, que confíen en el certificado y puedan verificar las firmas realizadas con la llave privada.

5.3 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

La PSC e-Digital PKI dará igual tratamiento a los certificados revocados y a los certificados suspendidos. La diferencia entre ambos procedimientos se detalla en los numerales siguientes 5.3.1 y 5.3.2.

5.3.1 REVOCACIÓN DE CERTIFICADOS

La revocación de certificados es un mecanismo a utilizar ante el supuesto de que, por alguna causa establecida en la presente CPS, se deje de confiar en el certificado antes de la finalización de su período de validez originalmente previsto. Esta acción es irreversible y origina el cese permanente de los servicios de certificación.

5.3.2 SUSPENSIÓN DE CERTIFICADOS

La suspensión de certificados es otro mecanismo que puede ser utilizado ante supuestos similares a los de la revocación, pero que a diferencia de esta, es una acción reversible, es decir, que el certificado recuperará su fiabilidad o vigencia una vez finalizado el periodo de suspensión. El procedimiento para solicitar la suspensión de un certificado es el mismo que se describe en los numerales siguientes para la revocación de un certificado.

5.3.3 SUPUESTO DE REVOCACIÓN/SUSPENSIÓN

Los certificados deberán ser revocados/suspendidos cuando concurra cualquiera de las circunstancias siguientes:

a) Solicitud voluntaria del Titular.
b) Pérdida o inutilización por daños del soporte del certificado.
c) Fallecimiento del Titular o incapacidad sobreviviente, total o parcial.

d) Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquél sean transferidos a otro prestador de servicios.
e) Que el titular del certificado digital informe causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, uso de las claves privadas por persona distinta al titular o bien por cualesquiera otras circunstancias, incluidas las fortuitas.
f) Por incumplimiento por parte de la AR, PSC o el Titular de las obligaciones establecidas en esta CPS.
g) Por resolución judicial ejecutoriada, o por incumplimiento de las obligaciones del usuario establecidas en el artículo 24 de la ley 19.799.
h) Por la concurrencia de cualquier otra causa especificada en la presente CPS o establecida en la CP.

5.3.4 EFECTOS DE LA REVOCACIÓN/SUSPENSIÓN

El efecto de la revocación del certificado es la pérdida de fiabilidad de este, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación de un certificado impide el uso legítimo del mismo por parte del Titular.

La revocación del certificado por causa no imputable al Titular originará la emisión de un nuevo certificado a favor del Titular por el plazo equivalente al restante para concluir el periodo originario de validez del certificado revocado.

La suspensión del certificado tendrá el mismo efecto que la revocación mientras dure el periodo de suspensión, posterior de lo cual el certificado recuperará la condición de vigente.

La revocación/suspensión del certificado tendrá como consecuencia la publicación de este en la CRL. De igual forma, terceros que consulten en otros servicios de consulta en línea como OCSP o a través del sitio web de acceso público https://signapis.com/estado-de-certificado.html serán notificados del estado revocado.

5.3.5 PROCEDIMIENTO DE REVOCACIÓN/SUSPENSIÓN

Deberán solicitar la revocación/suspensión en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado 5.3.3 anterior:

a) El Titular del Certificado, así como la persona natural o jurídica representada por éste.
b) La AR, respecto a aquellos certificados en cuya emisión haya participado.
c) La persona jurídica que conste en el certificado.

En todo caso, el PSC podrá iniciar de oficio el procedimiento de revocación/suspensión de certificados, en cualquiera de los casos previstos en el apartado 5.3.3 anterior.

5.3.6 RECEPCIÓN DE SOLICITUDES DE REVOCACIÓN/SUSPENSIÓN

Solo el Titular podrá solicitar la revocación/suspensión de un certificado, para lo cual se establece el siguiente procedimiento:

a) El Titular deberá completar el formulario de Solicitud de Revocación/Suspensión disponible en el sitio web de acceso público en la URL https://signapis.com/revocar-o-suspender-certificado.html, indicando en el campo 'Motivo' si se trata de una solicitud de revocación o suspensión.

   El titular o usuario dispone de 48 horas desde su solicitud para presentarse ante e-Digital PKI, ya sea en dependencias de la PSC o mediante una visita del operador de AR en terreno, para ratificar su solicitud de Suspensión/Revocación. El Titular deberá presentar su Cédula de Identidad vigente y en buen estado para identificarse. El operador de AR le hará entrega del formulario de ratificación de revocación de certificado, en donde se debe señalar el motivo de revocación o suspensión, firmar y estampar huella dactilar (este acto es manual y no se utilizan dispositivos tecnológicos).

b) Mediante la presencia física del usuario en la AR, ratificando la revocación, se deberá comprobar fehacientemente la identidad del solicitante, previo a dar curso a la revocación del certificado. Si la causa es por fallecimiento del Titular, se validará la información a través de algún bureau. Cualquier otra forma no contemplada será resuelta por la AR o PSC.

c) El inicio del proceso de revocación se realizará en forma inmediata al ser recibida la solicitud y con la presencialidad del titular.

5.3.7 DECISIÓN DE REVOCAR/SUSPENDER

Una vez recibida y autenticada la solicitud de revocación/suspensión, e-Digital PKI efectuará la revocación/suspensión efectiva del Certificado. La decisión de revocar/suspender un Certificado corresponde a la AR.

5.3.8 COMUNICACIÓN Y PUBLICACIÓN DE LA REVOCACIÓN/SUSPENSIÓN

La decisión de revocar/suspender el certificado será comunicada inmediatamente por el PSC al Titular y se enviará confirmación mediante e-mail.

Igualmente, se publicará la revocación/suspensión del certificado en la próxima actualización de la CRL, que ocurre cada 24 horas, y se encuentra disponible en la URL: https://signapis.com/lista-de-revocaciones.html.

La revocación/suspensión comenzará a producir efectos a partir de su publicación por parte del PSC, salvo que la causa de revocación sea el cese de la actividad del PSC, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

5.4 CADUCIDAD DE CERTIFICADOS

Los certificados caducarán por el transcurso del período operacional indicadas en las fechas de creación (NotBefore) y vigencia (NotAfter) del mismo. La caducidad producirá automáticamente la invalidez del

certificado, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación. La caducidad de un certificado impide el uso legítimo del mismo por parte del Titular.

5.5 RENOVACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN

Este procedimiento se establece para los casos en que el certificado vaya a caducar y el Titular simplemente desee utilizar un certificado con las mismas características que tenía el que venía utilizando válidamente hasta entonces.

En este caso, el PSC emitirá un nuevo certificado y se generarán nuevas claves. Es requerido llevar a cabo nuevamente el proceso de verificación y validación de la identidad del Titular, según lo establecido en la CP.

Los certificados emitidos por e-Digital PKI tienen un plazo de vigencia de uno, dos o tres años. Se podrá acudir a los trámites que se establecen en este documento para la renovación de los servicios de certificación de e-Digital PKI si ocurren las situaciones que a continuación se detallan.

5.5.1 REQUISITOS PREVIOS

Deberán concurrir los siguientes:

a) Que el Titular posea o hubiese poseído en el anterior periodo, un certificado emitido por e-Digital PKI.
b) Que el Titular desee la renovación del servicio de certificación y lo solicite en debido tiempo y forma, siguiendo el proceso 5.5.2 que se específica a tal efecto.
c) Que el PSC no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación del certificado.
d) Que el Titular se someta a los trámites correspondientes para la emisión de un certificado como cualquier otro Solicitante que solicita su certificado por primera vez.
e) Que la solicitud de renovación de servicios de prestación se refiere al mismo tipo de certificado emitido inicialmente.

5.5.2 CÓMO SOLICITAR LA RENOVACIÓN

El Titular que solicite la renovación de los servicios de certificación deberá hacerlo completando el formulario de Solicitud de Certificado disponible en el sitio web de acceso público en la URL: https://signapis.com/solicitud-de-certificado.html.

El Titular o usuario del certificado se someterá al régimen general de revisión de datos e identidad, bajo el mismo proceso utilizado para la emisión de nuevos certificados, permitiendo de esta manera a e-Digital PKI comprobar fehacientemente la identidad del Solicitante o Titular. El certificado cuya vigencia ha expirado no es necesario revocarlo, debido a que por restricciones de fecha no puede dar continuidad a su uso.

5.5.3 PROCEDIMIENTO DE RENOVACIÓN DE CERTIFICADOS

Cuando el PSC reciba la solicitud del Titular en debida forma, procederá con la revisión de los antecedentes e iniciara el proceso de validación, comprobando fehacientemente la identidad del solicitante.

Con la renovación de los servicios de certificación se entenderán que se mantienen los derechos, obligaciones y responsabilidades tanto de Titular como de PSC y AR, según se establece en los correspondientes contratos, la CPS y de las Políticas de Certificación aplicables.

5.6 NUEVA EMISIÓN DE CERTIFICADOS

Este procedimiento se establece para los casos en que el certificado de un Titular sea declarado revocado por la existencia de inexactitudes en el Certificado y se emite un nuevo certificado.

5.6.1 REQUISITOS PREVIOS

Se podrá acudir a los trámites que se establecen en este documento para la nueva emisión de certificados de e-Digital PKI si concurren a la vez los requisitos generales que a continuación se detallan:

a) La solicitud la debe llevar a cabo el Titular del antiguo certificado.
b) El origen de la solicitud debe basarse en la renovación del certificado por inexactitudes en el mismo.
c) La solicitud debe realizarse en debida forma, siguiendo las instrucciones y normas que e-Digital PKI específica a tal efecto.
d) La solicitud de una nueva emisión del certificado debe referirse al mismo tipo de certificado emitido inicialmente.

5.6.2 CÓMO SOLICITAR LA NUEVA EMISIÓN

El antiguo Titular que solicite la nueva emisión de los servicios de certificación deberá completar el formulario de Solicitud de Certificado disponible en el sitio web de acceso público en la URL: https://signapis.com/solicitud-de-certificado.html.

El Titular deberá manifestar en dicho formulario, bajo su responsabilidad, cuáles de los datos que constaban en su certificado ya revocado no son ciertos o han variado de alguna forma.

La AR revisará la validez formal de la solicitud de nueva emisión y enviará a la AC una solicitud para la creación de un nuevo certificado a nombre del Titular. A continuación, la propia AR PSC, realizará la validación de la identidad y de los datos del certificado que hayan variado, solicitando la presencia física del solicitante y requiriendo la exhibición de cuantos documentos originales considere necesarios.

Para la validación definitiva de los nuevos datos del certificado, y para la entrega de éste, se aplicará el mismo procedimiento que para la primera emisión.

5.6.3 PROCEDIMIENTO DE NUEVA EMISIÓN DE CERTIFICADOS

Una vez presentada la documentación necesaria, la AR examinará si procede o no la nueva emisión del certificado, distinguiendo tres supuestos:

a) Defectos subsanables en la presentación. En este caso, la AR deberá comunicar al titular que solicita la nueva emisión por error o defecto.

b) Defectos no subsanables en la presentación. En este caso, la AR deberá comunicar al Titular que solicita la nueva emisión, estas circunstancias, denegándole la posibilidad de nueva emisión del certificado.

c) La documentación presentada es la necesaria y concurren los requisitos exigibles. En este caso, la AR entregará al Titular el nuevo certificado, entendiéndose que se mantienen los derechos, obligaciones y responsabilidades tanto del Titular como de PSC y AR, según se establece en los correspondientes contratos, la CPS y de las Políticas de Certificación aplicables.

5.7 TÉRMINO DE LA PSC POR CESE VOLUNTARIO O CANCELACIÓN

Se podrán dar por terminadas las actividades de certificación de la PSC por cese voluntario en su actividad o por cancelación de la inscripción en el registro de prestadores acreditados por la Entidad Acreditadora, según indican incisos c) y h), respectivamente, del Artículo 12 de la Ley Nº19.799.

En orden a causar el menor daño posible tanto en los Titulares como a los Usuarios del sistema de certificación ante el hipotético término de la PSC se establecen las siguientes medidas:

a) Comunicar el término de las actividades de la PSC mediante el envío de un correo electrónico o una notificación mediante correo ordinario certificado dirigido a todos los titulares o usuario cuyos certificados permanezcan en vigor y la publicación de un anuncio en dos diarios de alcance nacional. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

b) Establecer, cuando ello fuera posible, un acuerdo con otro prestador de servicios con la intención de traspasar todas sus obligaciones y derechos dentro del sistema de certificación con la intención de continuar el servicio. Si se produce la subrogación, a la cual el titular o usuario da su consentimiento de manera expresa, esta CPS seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito.

c) Proceder, en caso de no haberse podido llevar a cabo transferencia de derechos y obligaciones a otro PSC, a la revocación de todos los certificados una vez transcurrido el plazo de dos meses desde la comunicación.

d) Indemnizar adecuadamente a aquellos titulares o usuarios que lo soliciten cuando sus certificados sean revocados con anterioridad al plazo previsto de vigencia, pactándose como tope para la indemnización el coste efectivo del servicio, descontando a prorrata el coste por los días transcurridos desde el inicio del contrato hasta la fecha de resolución, o la emisión de un nuevo certificado en la otra PSC que tomo la responsabilidad, con un periodo de vigencia hasta la fecha de vigencia del certificado original.

e) Cualquier otra obligación que venga impuesta por la ley 19.799.

6 CONTROLES DE PROCEDIMIENTO, PERSONAL Y FÍSICOS

6.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

e-Digital PKI ha establecido una Estructura Organizacional de Seguridad que contempla la definición de funciones específicas en el ámbito de la seguridad, que da pie al Comité de Seguridad de la Información.

6.2 PROCEDIMIENTOS DE DIFUSIÓN INTERNA

e-Digital PKI comunica la información relevante definida por el Sistema de Gestión de Seguridad de la Información, a las personas de la organización, a través de mecanismos que aseguran la capacitación permanente de las distintas políticas y procedimientos que le atañan.

6.3 RESPONSABILIDAD SOBRE LOS ACTIVOS

e-Digital PKI mantiene un inventario de activos el cual es revisado periódicamente y que se encuentra en el archivo “Inventario de Activos”.

La Gerencia de e-Digital PKI es el propietario de sus activos y debe entregar los recursos necesarios para gestionarlos y así proveer productos y soluciones de Firma Electrónica (Certificados Digitales) de forma segura y eficiente a sus clientes.

6.4 AUDITORÍAS

Con el fin de velar por el correcto uso de los recursos de su propiedad, e-Digital PKI se reserva el derecho de auditar en cualquier momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos.

En referencia a las revisiones de la seguridad de la información, se considera revisiones independientes evaluaciones del cumplimiento de las políticas y normas de seguridad y evidencia que compruebe del cumplimiento.

7 CONTROLES DE SEGURIDAD TÉCNICA

Con el objeto de reforzar la seguridad técnica, el PSC dispone de un reglamento interno de funcionamiento que regula todos estos aspectos, el cual es entregado a los empleados de e-Digital PKI al momento de firmar su contrato.

Los requerimientos básicos de seguridad que ha de observar el PSC son los siguientes:

a) El software y la información del PSC correrá en una estación de trabajo dedicada a tal fin, con las providencias y medidas necesarias para protegerlo contra ataques de la red interna y por sobre todo de la red externa.
b) La clave de firma del PSC tendrá una longitud de 2048 bits.
c) Al menos una copia de los Backups del equipo del PSC deberá ser respaldados en medios externos al PSC.

7.1 RIESGOS

e-Digital PKI realiza la gestión de riesgos a través de su Política de Gestión de riesgos que se detalla en el requisito PS01.

7.2 PLAN DE SEGURIDAD

El Plan de Seguridad permite trabajar en el transcurso del año en aquellos ámbitos de acción establecidos, con el objetivo de proveer protección a los recursos de información, según lo definido en PS02 Política de Seguridad de Información de la organización.

7.3 PLAN DE ADMINISTRACIÓN DE LLAVES

En el documento PS06 Plan de Administración de Llaves se definen las acciones sobre las llaves criptográficas de e-Digital PKI, con el fin de resguardarlas y administrarlas durante su ciclo de vida.

7.4 MANTENCIÓN DE LA INFRAESTRUCTURA

e-Digital PKI cuenta con servicios de infraestructura contratados a un proveedor que cumple con los requisitos mínimos exigidos por la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación” publicados por la Entidad Acreditadora del ministerio de Economía en su versión vigente.

7.5 CONTROL DE ACCESO

En e-Digital PKI el control de acceso a la información es de alta importancia, por lo que se regula en base a lo establecido en la “Política de Control de Accesos” ubicada en la Carpeta “00_Documentos_Relacionados”.

8 PERFILES DE CERTIFICADOS Y REGISTRO DE ACCESO PÚBLICO

8.1 CONTENIDO DEL CERTIFICADO

Los certificados de la CA de e-Digital PKI están basados en la estructura x509 v3.

8.2 TIPOS DE NOMBRES

La estructura x509 v3 contiene los datos expresados en notación DN (Distinguished Name), donde un DN se compone a su vez de diversos campos. Los DN correspondientes al campo SUJETO y ASUNTO de e-Digital PKI consiste en los elementos que se especifican en el cuadro siguiente:

Atributo	Valor
País (C)	CL
Organización (O)	e-Digital PKI
Unidad Organizacional (OU)	77423125-0
Localidad (L)	Santiago
Dirección de correo electrónico (E)	contacto@signapis.com
Nombre Común (CN)	Autoridad Certificadora Firma Electrónica Avanzada Signapis

En el caso de los datos del titular, los certificados también contienen los datos expresados en notación DN (Distinguished Name) en los campos del SUJETO y ASUNTO, ambos contienen los elementos que se especifican en el cuadro siguiente:

Atributo	Valor
País (P)	Código del País del domicilio del Titular, p.e. CL
Organización (O)	Persona Natural
Unidad Organizacional (OU)	RUT del Titular, p.e. 12345678-9
Localidad (L)	Ciudad del domicilio del Titular, p.e. Santiago
Nombre Común (CN)	Nombre del Titular, p.e. PNombre SNombre PApellido SApellido
Dirección de correo electrónico (E)	Dirección de correo del Titular, p.e. nombre@dominio.com
Limitaciones	Contiene los límites establecidos por la AC en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero.

8.3 SINGULARIDAD DE LOS NOMBRE

e-Digital PKI garantiza que los DN del Sujeto son únicos dentro del dominio de una AR específica a través de elementos del proceso de inscripción del Titular.

8.4 PERFIL DE CERTIFICADO DE LA POLÍTICA DE FIRMA ELECTRÓNICA AVANZADA

PERFIL DE CERTIFICADO DE POLÍTICA DE FIRMA ELECTRÓNICA AVANZADA		
Nombre del Campo	**Descripción**	**Valor**

PERFIL DE CERTIFICADO DE POLÍTICA DE FIRMA ELECTRÓNICA AVANZADA		
Versión	Versión del certificado X.509	3
DN del Sujeto	Country (C)	Código del País del domicilio del Titular, p.e. CL
	Locality Name (L)	Ciudad del domicilio del Titular, p.e. Santiago
	Organization Name (O)	Persona Natural
	Organization Unit (OU)	RUN del Titular, p.e. 12345678-9
	Common Name (CN)	Nombre del Titular, p.e. PNombre SNombre PApellido SApellido
	E-mail (E)	Dirección de correo del Titular, p.e. PNombre123@dominio.com
DN del Emisor	Country (C)	CL
	Locality Name (L)	Santiago
	Organization Name (O)	E-Digital PKI
	Organization Unit (OU)	77423125-0
	Common Name (CN)	Autoridad Certificadora Firma Electrónica Avanzada Signapis
	E-mail (E)	contacto@signapis.com
Número de Serie	Serial Number Es el Identificador del Certificado con Valor único dado por DN Emisor	0x00000000000000000000000000000000000000000 Generado aleatoriamente por la AC un número irrepetible
Período de validez	Valid From (Validez a partir de la Fecha)	dd-mm-aaaa hh:mm:ss CLST donde: dd= día; mm=mes; aaaa=año; hh=hora;mm=min; ss=seg.
	Valid Until (Validez hasta la Fecha)	dd-dd-aaaa hh:mm:ss CLST
Largo de llave	Key Size	2048 bits
Clave pública	Public Key	00 00 00 00 00 00 00 00 00 00 00 00 00 00 (...)
Algoritmo de Firma	Signature Algorithm	SHA256withRSA
Fingerprint	Huella del Certificado: SHA1: p.e. CC A1 F1 F4 E6 BB F6 C4 E6 7A E7 73 92 F5 A9 7F 31 5C 13 74	

a.

8.5 CARACTERÍSTICAS DEL CERTIFICADO

Los certificados podrán ser emitidos en los tipos de soportes autorizados y validados por la PSC de acuerdo con las Políticas de Certificación, token FIPS 140-2 nivel 3, que serán proporcionados por e-Digital PKI al momento del enrolamiento por el operador de AR en presencia del Titular, en dependencias de la PSC o mediante una visita a terreno.

8.6 LISTAS DE CERTIFICADOS EMITIDOS POR E-DIGITAL PKI

Los certificados una vez emitidos, su parte publica estará disponible para consultar su estado en el sitio web de acceso público en la siguiente url: https://signapis.com/estado-de-certificado.html.

La PSC publicará cada 24 una CRL actualizada con la lista de certificados revocados. Esta operación será realizada por personal autorizado a partir de los ficheros generados por el PSC y el listado de certificados revocados (CRL) estará a disposición de los usuarios en la página web de acceso público del PSC en la siguiente URL: https://signapis.com/lista-de-revocaciones.html.

9 ESPECIFICACIONES DE ADMINISTRACIÓN DE LA POLÍTICA

9.1 PROCEDIMIENTO DE MODIFICACIÓN DE LA CPS Y DE LAS CP

El PSC podrá modificar las estipulaciones de la presente CPS y de su CP específicas, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación y siempre que toda modificación se justifique desde el punto de vista jurídico, técnico y comercial.

Tanto las modificaciones a las CPS y CP, serán publicadas en régimen de vigencia, una vez sean aprobadas por la Entidad Acreditadora del Ministerio de Economía.

9.2 PROCEDIMIENTO DE PUBLICACIÓN DE LAS MODIFICACIONES

El PSC podrá modificar las estipulaciones de la presente CPS y de su CP específicas, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación y no se afecten los derechos del consumidor según la ley 19.496 y, siempre y cuando, toda modificación se justifique desde el punto de vista jurídico, técnico y comercial.

Las modificaciones efectuadas sobre la CPS o las CP se darán a conocer a los interesados, en la página web de acceso público del PSC https://signapis.com/modificaciones-politicas.html.

A estos efectos, en dicha página web, se hará una referencia expresa y fácilmente localizable a la existencia de dicha modificación, durante un período de treinta días.

De igual modo, se procederá a sustituir la versión anterior de la CPS o de las CP por la nueva.

En la página Web del PSC se incluirá un listado de control de las sucesivas versiones que sobre la CPS o las CP puedan originarse, desde que se podrá tener acceso tanto a la versión actual y operativa como a las versiones anteriores con una antigüedad no superior a un año.

9.3 PROCEDIMIENTO DE NOTIFICACIÓN DE LAS PUBLICACIONES

En caso de que las modificaciones efectuadas en la CPS o en las Políticas de Certificación incidan directamente en los derechos y obligaciones de los Titulares y/o Solicitantes, así como cuando dichas modificaciones alteren la operatividad de los certificados por parte de los usuarios, deberán notificarse dichas modificaciones a los Titulares y/o Solicitantes con un período de antelación de quince días a la aplicación de los cambios efectuados. El transcurso de dicho período sin que medie comunicación escrita por parte del Titular y/o Solicitante, en contra de las citadas modificaciones implicará su aceptación. La no aceptación de las modificaciones de esta CPS o de las Políticas de Certificación realizadas por el PSC, tendrá como consecuencia el término de la relación comercial con el Titular/Solicitante. Se considerará como medio eficaz para la realización de notificaciones el correo electrónico y enviado a la dirección proporcionada por el Titular y/o Solicitante.

10 REFERENCIAS

ETSI TS 102 042

**** FIN DEL DOCUMENTO ****