POLÍTICA DE CERTIFICACIÓN

Índice

1. Introducción

Este documento contiene la información esencial en relación con el servicio de certificación de los proveedores de servicios de confianza acreditados en El Salvador. El Ministerio de Economía en su calidad de autoridad de control y vigilancia a cargo de la Unidad de Firma Electrónica, es quien acredita a los proveedores de servicios de confianza, implementando la Infraestructura de Clave Pública (PKI) raíz país.

1.1 Presentación general del documento

La presente Política de Certificación (PC) de Proveedores de Servicios de Certificación, se ajusta a las disposiciones contenidas en la Declaración de Prácticas de Certificación (DPC) y las complementa; así como con los usos legales, exigencias técnicas y de seguridad requeridos para la emisión y revocación de Proveedores de Servicios de Certificación acreditados en El Salvador.

1.2 Nombre del documento e identificación

Este documento se denomina Política de Certificados de Proveedores de Servicios de Certificación, el cual contiene la siguiente información que podrá ser consultada en la página web, de acuerdo a la siguiente información:

Nombre del documento	*POLITICA DE CERTIFICACIÓN* *Certificado de Proveedores de Servicios de Confianza*
Descripción	*Los certificados de proveedores de servicios de certificación acreditan a las organizaciones que brindarán servicios dentro de El Salvador.*
Identificador OID	1.3.6.1.4.1.50377.1.1.1
Versión	1.0
Fecha de emisión	*08/09/2020*
Ubicación	*https://normativa.firmaelectronica.economia.gob.sv/dpc/*

1.3 Identificación de los tipos de certificado

Cada OID es particular y se emplea para identificar diferentes tipos, políticas y versiones de los certificados emitidos. Los certificados de proveedor de servicios de certificación emitidos por la Unidad de Firma Electrónica tienen asignados los siguientes identificadores de objeto (OID) dependiendo del tipo de contenedor criptográfico:

OIDS Ministerio de Economía de El Salvador	Descripción	Política	OIDs ETSI
1.3.6.1.4.1.50377	MINISTERIO DE ECONOMÍA DE EL SALVADOR		
1.3.6.1.4.1.50377.1.	Políticas de Certificados – Raíz		
1.3.6.1.4.1.50377.1.1.	Políticas de Certificados – CA Subordinada		
1.3.6.1.4.1.50377.1.1.1	Certificado de CA Subordinada en dispositivo cualificado		
1.3.6.1.4.1.50377.2.	Declaración de Prácticas de Certificación		
1.3.6.1.4.1.50377.2.1.	Declaración de Prácticas de Certificación – El Salvador		
1.3.6.1.4.1.50377.2.1.1	Declaración de Prácticas de Certificación CA Raíz MINEC		

1.4 Administración de la Política de Proveedores de Servicios de Certificación

La Política de Proveedores de Servicios de Certificación a través de la Unidad de Firma Electrónica y su Autoridad de Políticas es la encargada de su elaboración, actualización, registro y mantenimiento.

1.4.1 Organización responsable

UNIDAD DE FIRMA ELECTRÓNICA DEL MINISTERIO DE ECONOMÍA

ALAMEDA JUAN PABLO II, CALLE GUADALUPE, EDIFICIO C-2 TERCER NIVEL, CENTRO DE GOBIERNO

SAN SALVADOR, EL SALVADOR

1.4.2 Contacto

Para cualquier consulta, diríjanse a:

UNIDAD DE FIRMA ELECTRÓNICA DEL MINISTERIO DE ECONOMÍA
ALAMEDA JUAN PABLO II, CALLE GUADALUPE, EDIFICIO C-2 SEGUNDO NIVEL , CENTRO DE GOBIERNO
SAN SALVADOR, EL SALVADOR
ING. OSCAR HUMBERTO CRUZ GUARDADO
JEFE UNIDAD DE FIRMA ELECTRÓNICA
TELÉFONO: +503 2590 5640
EMAIL: FIRMA.ELECTRONICA@ECONOMIA.GOB.SV

1.4.3 Procedimiento para emisión de la política

La Política de Certificados para proveedores de servicios de certificación, es administrada y emitida por la Unidad de Firma Electrónica del Ministerio de Economía.

1.4.4 Publicidad

La política de proveedores de servicios de certificación es accesible al público a través de la página https://normativa.firmaelectronica.economia.gob.sv/dpc/ . Las modificaciones a esta política, que fueren aprobadas, se publicarán de forma inmediata.

1.5 Entidades y personas participantes

Los certificados de autoridad de certificación acreditada como proveedores de servicios de certificación son emitidos a las personas jurídicas, públicas o privadas nacionales o extranjeras que cumplan con los requisitos establecidos en las leyes competentes que operan en el país.

1.5.1 Autoridad de Certificación (AC)

La Autoridad de Certificación raíz de El Salvador es la entidad responsable de emitir y gestionar certificados, garantizar la autenticidad y veracidad de los datos recogidos en el certificado digital expedido, a las autoridades de certificación acreditadas como proveedores de servicios de certificación.

La AC además, emite los certificados digitales de conformidad con los términos establecidos en esta Política de Certificados (PC) y en la Declaración de Prácticas de Certificación (DPC) y garantiza la autenticidad y veracidad de los datos recogidos en el certificado digital expedido.

AC Raíz: Autoridad de Certificación de primer nivel. Esta AC sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la generación del certificado autofirmado; de certificados de AC subordinada y periódicamente para la generación de la lista de certificados revocados de Autoridad de Certificación Raíz ARL.

AC Subordinada: Autoridad de Certificación Subordinada acreditada como proveedor de servicios de certificación. Su función es la emisión de certificados de usuario final a personas naturales, personas naturales empleados públicos, persona natural representante, sello electrónico, sello de tiempo, autoridades de validación y otros que se pudieran establecer a futuro.

1.5.2 Autoridades de Registro (AR)

Las Autoridades de Registro son las entidades delegadas por el proveedor de servicio de certificación para la identificación y autenticación de los solicitantes de certificados, con el fin de receptar y procesar solicitudes de certificados digitales, requiriendo la emisión de los certificados a la AC Raíz de El Salvador.

1.5.3 Solicitante

El solicitante es aquella persona jurídica, pública o privada nacional o extranjera que cumpla con los requisitos establecidos en las leyes competentes que operan en el país.

1.5.4 Suscriptor

El suscriptor es aquella persona jurídica, pública o privada nacional o extranjera a quien se ha emitido un certificado de CA Subordinada por parte de la Unidad de Firma Electrónica.

1.6 Ámbito de aplicación de los certificados

1.6.1 Tiempo de validez de los certificados

Los certificados digitales de proveedores de servicios de certificación tendrán una validez de hasta quince (15) años.

1.6.2 Uso apropiado de los certificados

El certificado de proveedor de servicios de certificación emitido bajo esta política será utilizado solamente durante su período de vigencia, para dar cumplimiento a las funciones que le son propias y legítimas, y puede ser utilizado para los siguientes propósitos:

1.6.2.1 Firma de certificados de usuario final

Los certificados de usuario final generados podrán ser firmados a partir de cada una de los PSC o TSA acreditados en El Salvador de acuerdo a sus políticas y declaraciones de prácticas de certificación.

1.6.2.2 Firma de CRL

Los certificados de usuario final generados a partir de un proveedor de servicios de certificación firmarán la lista de certificados revocados CRL.

1.7 Límites de uso de los certificados

Los certificados autoridad de certificación serán utilizados para actuar como Autoridad de Certificación Subordinada de los PSC o TSA, firmando otros certificados de clave pública de entidad final y listas de certificados revocados (CRL).

1.8 Usos prohibidos de los certificados

La realización de operaciones no autorizadas según esta política de certificados, eximirá al Ministerio de Economía de cualquier responsabilidad por este uso prohibido, en consecuencia:

- Está prohibido utilizar el certificado para usos distintos a los estipulados en los numerales correspondientes a: ***Uso apropiado de los certificados*** especificados en el numeral **1.6.2** y ***Límites de uso de los certificados*** numeral **1.7** de la presente Política de Certificado.
- No está permitido el uso de certificados que puedan ocasionar daños personales o medioambientales.
- Se prohíbe toda acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente Política de Certificado.

1.9 Exención de responsabilidad

La Autoridad de Certificación Raíz de El Salvador quedará exenta de responsabilidad por daños y perjuicios cuando el usuario exceda los límites de uso indicados para este tipo de certificados.

1.10 Definiciones

En el desarrollo de la presente Política de Certificados los términos empleados y sus correspondientes definiciones son los siguientes:

Auditoría: Procedimiento utilizado para comprobar la eficiencia de los controles establecidos a la operación de la Entidad, en la prevención y detección de fraudes o mediante la realización de exámenes a aplicaciones concretas, que garanticen la fiabilidad e integridad de sus actividades.

Autenticación: Proceso electrónico mediante el cual se verifica la identidad de un proveedor de servicios de confianza, solicitante o suscriptor de un certificado emitido como Autoridad de Certificación.

Autoridad de Certificación (AC): Entidad encargada de emitir y revocar certificados digitales utilizados en firma electrónica y cuya clave pública está incluida en éstos.

Autoridad de Registro (AR): Entidad encargada de receptar las solicitudes de certificados, identificar y autenticar la información de los solicitantes de certificados, aprobar o rechazar las solicitudes de certificados, revocar o suspender certificados en determinadas circunstancias, y aprobar o rechazar las solicitudes para renovar o volver a introducir sus solicitudes de certificados.

ARL (Authority Revocation List): Lista de certificados revocados emitida por la AC Raíz que contiene la lista de todos los certificados de AC Subordinada emitidos por la AC Raíz que hayan sido revocados o suspendidos y que aún no hayan expirado.

Cadena de confianza: También conocida como Jerarquía de Confianza, la constituyen las autoridades de certificación relacionadas por la confiabilidad en la emisión de certificados digitales entre diferentes niveles jerárquicos. En el caso salvadoreño serán todos los proveedores de servicios de confianza acreditados por la Unidad de Firma Electrónica.

Normas CEN EN 419 221: Parte de 2-5, según corresponda requisitos de seguridad para módulos criptográficos HSM.

Clave privada: Es la clave, de un par de claves, que es conocida solamente por el usuario o titular del certificado.

Clave pública: Es la clave, de un par de claves, que se conoce públicamente.

CRL (Certificate Revocation List): Lista de certificados que han sido revocados.

CSR (Certificate Signature Request): solicitud de firma de certificado, contiene la información de la petición del certificado.

ETSI: European Telecommunications Standards Institute, Instituto europeo de normas de telecomunicaciones.

ETSI EN 319 411 Part 1: Firma Electrónica e Infraestructuras, Requisitos de política y seguridad para proveedores de servicios de confianza que emiten certificados, Requerimientos Generales.

- sección 6.5.2 de ETSI EN 319 411-1 – Relacionada con módulos criptográficos.

ETSI EN 319 411 Part 2: Firma Electrónica e Infraestructuras, Requisitos de política y seguridad para proveedores de servicios de confianza que emiten certificados, Requerimientos para proveedores de servicios de confianza que emiten certificados cualificados.

ETSI EN 319 412-1: Firma Electrónica e Infraestructuras, Perfiles de Certificados, Visión general y estructuras de datos comunes.

FIPS: Federal Information Processing Standard, es un estándar de seguridad para la acreditación de módulos criptográficos.

FIPS 140-2 nivel 3: valida el cumplimiento de su estándar PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, bajo su programa de validación Cryptographic Module Validation Program (CMVP).

HSM (Hardware Security Module): Es un componente o dispositivo criptográfico utilizado para generar, almacenar y proteger claves criptográficas.

ISO: Organización Internacional de Normalización

ISO/IEC 19790 nivel 3: especifica los requerimientos de seguridad para un módulo criptográfico utilizado dentro de un sistema de seguridad que protege información sensible en sistemas informáticos y de telecomunicaciones.

OCSP (Online Certificate Status Protocol): Protocolo de consulta en línea de estado de certificados utilizado para comprobar el estado de un certificado digital en el momento en que es utilizado. Proporciona información actualizada y complementaria del listado de certificados revocados.

OID (Object Identifier): El Identificador de Objetos constituye el valor de una secuencia de componentes variables utilizado para nombrar a casi cualquier tipo de objeto en los certificados digitales, tales como los componentes de los nombres distintivos DN, DPC, PC, etc.

PKCS (Public Key Cryptography Standard): Estándares de criptografía de claves públicas.

PKCS#10: Estándar de criptografía de clave pública utilizado para procesar la petición de un certificado y solicitar la generación de una clave.

PKI (Public Key Infrastructure): Infraestructura de Clave Pública es el conjunto de elementos informáticos (hardware y software), políticas y procedimientos necesarios para brindar servicios de certificación digital.

Política de certificados: Documento que complementa la Declaración de Prácticas de Certificación y que contiene un conjunto de reglas que norman las condiciones de uso y los procedimientos seguidos por la Unidad de Firma Electrónica de MINEC para la emisión de certificados, determinando la aplicabilidad de un certificado de Autoridad de Certificación.

RFC (Request for comments): Publicaciones de *Internet Engineering Task Force* que en forma de memorandos contienen protocolos y procedimientos para regular el funcionamiento de Internet.

Sellado de tiempo: Anotación firmada electrónicamente y agregada a un mensaje de datos mediante procedimientos criptográficos en la que consta como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación, basándose en la RFC 3161 Internet *X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*.

X.509: Estándar desarrollado por la UIT-T para infraestructuras de clave pública que especifica entre otros temas, los formatos estándar para certificados de claves públicas y para la implementación de listas de certificados revocados.

1.11 Siglas

AR	autoridad de registro (Registration Authority)
ARL	Lista de Revocación de Autoridades (Authority Revocation List)
C	Nombre País (CountryName)
CA	Autoridad de Certificación (Certification Authority)
CN	Nombre Común (CommonName)
CPS	Declaración de Prácticas de Certificación (Certificate Practice Statement)
CRL	Lista de Certificados Revocados (Certificate Revocation List)
CSR	Solicitud de firma de certificado (Certificate Signing Request)
DUI	Documento Unico de Identidad (National ID Card in El Salvador)
FC	Firma Centralizada (Remote Digital Signature)
HSM	Dispositivo Módulo de Seguridad (Hardware Security Module)
ISO	Organización Internacional de Estandarización (International Organization for Standardization)
L	Localidad (LocalityName)
MINEC	Ministerio de Economía (Ministry of Economic)
NIT	Número de Identificación Tributaria (Salvadorian VAT Number)
NRC	Número de Registro de Contribuyente
O	Nombre de Organización (OrganizationName)
ocsp	Protocolo Online online certificate status protocol
OID	Identificador de Objetos (Object IDentifier)
OU	Nombre de Unidad Organizativa (OrganizationalUnitName)
PAS	Pasaporte (Passport)
PKCS	Estándar de Clave Pública (Public-Key Cryptography Standard)
PKI	Infraestructura de Clave Pública (Public Key Infrastructure)
PSC TSA	Proveedores de Servicios de Certificación (Certification Services Provider)
RA	Autoridad de Registro (Registration Authority)
SFC	Servidor de Firma Centralizada (Centralized Signature Server)
SHA	Algoritmo Seguro de Resumen (Secure Hash Algorithm)
ST	Nombre de Provincia o Estado (STateOrProvinceName)
TSA	Autoridad de Sellado de Tiempo (Time-Stamping Authority)
UO	Unidades Organizativas (Organizational Units)
UTC	Tiempo Universal Coordinado (Universal Time Coordinated)
v	Versión (Version)
VA	Autoridad de Validación (Validation Authority)
VAT	Impuesto al Valor Agregado (Value Added Tax)

1.12 Referencias a otros documentos

[RFC5280] RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Mayo 2008.

ETSI EN 319 411 Part 1	Firma Electrónica e Infraestructuras, Requisitos de política y seguridad para proveedores de servicios de confianza que emiten certificados, Requerimientos Generales.
ETSI EN 319 411 Part 2	Firma Electrónica e Infraestructuras, Requisitos de política y seguridad para proveedores de servicios de confianza que emiten certificados, Requerimientos para proveedores de servicios de confianza que emiten certificados cualificados.
ETSI EN 319 412-1	Firma Electrónica e Infraestructuras, Perfiles de Certificados, Visión general y estructuras de datos comunes.
[DECRETO133-2015]	Decreto No. 133. Ley de Firma Electrónica. Dada en el Salón Azul del Palacio Legislativo, en San Salvador, al 1 de octubre de 2015.
[DECRETO60-2016]	Decreto No. 60. Reglamento de la Ley de Firma Electrónica. Dado en Casa Presidencial, en San Salvador, al 10 de diciembre del 2016.

2. Publicación y registro de certificados

Las políticas de certificados estarán disponibles para suscriptores de acuerdo a las políticas que establezca la Unidad de Firma Electrónica de El Salvador.

Cualquier cambio o modificación en la Política de Certificados generará una nueva versión, debiendo publicarse dicho cambio, además de guardar y custodiar la versión anterior, toda vez que al amparo de esta última pudieron haberse originado derechos y obligaciones para los suscriptores y usuarios.

Es responsabilidad de la Unidad de Firma Electrónica la adopción de las medidas de seguridad necesarias para garantizar la integridad, autenticidad y disponibilidad de dicha información.

3. Identificación y autenticación

En esta sección se describen los procedimientos específicos y criterios aplicados por la Autoridad de Certificación al momento de autenticar la identidad del proveedor de servicios de confianza y aprobar la emisión del certificado de autoridad de certificación.

3.1 Nombres

De acuerdo a la presente política de certificados se establece la necesidad de la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado, para vincular la clave pública con su identidad.

Todos los certificados digitales de la jerarquía raíz en El Salvador deben contener información distintiva que permita identificar al emisor y al titular y/o suscriptor. Dicha información, debe estar especificada en los campos *IssuerDN (Issuer Distinguished Name)* y *SubjectDN (Subject Distinguished Name)*, de acuerdo a las especificaciones de la familia de estándares ISO/IEC 9594 (recomendación X.500 y X.501).

3.1.1 Tipos de nombres

Todos los certificados de PSC o TSA tienen una sección llamada *SubjectDN* cuyo objetivo es permitir identificar al suscriptor o titular del certificado, incluyendo un *Distinguished Name* (DN) caracterizado por un conjunto de atributos que conforman un nombre diferenciado, único e inequívoco para cada proveedor de servicios de certificación.

Atributo	Nombre en Inglés	Nombre	Descripción
C	Country	País	*Abreviatura del país del proveedor de servicio de certificación*
L	Locality	Localidad	*Nombre de la LOCALIDAD/(DEPARTAMENTO) donde resida la CA subordinada**
OU	Organizational Unit	Unidad organizativa	*Nombre de la Unidad Organizativa del PSC o TSA*
O	Organization	Organización	*Nombre de la Organización del PSC o TSA*
CN	Common Name	Nombre común	*Nombres y apellidos completos del suscriptor*
organizationId entifier	Organization Identifier	Identificador de la Organización	*NIT del proveedor de servicio de certificación*

**En el caso de El Salvador la localidad será municipio, departamento. Para el caso de extranjeros se revisará según sea el caso.*

Para incluir una dirección de correo electrónico (e-mail) de contacto del proveedor de servicio de certificación, dicha información se debe colocar en el campo rfc822Name de la extensión "SubjectAltName".

3.1.2 Necesidad de que los nombres sean significativos

El campo *SubjectDN* de todos los certificados digitales de la jerarquía de certificación debe permitir determinar sin ambigüedad la identidad del suscriptor, necesarios para la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado.

3.1.3 Anonimato o seudónimos en los nombres

De acuerdo a esta Política de Certificados no se admiten anonimatos o seudónimos para identificar el nombre de proveedor de servicios de certificación.

3.1.4 Reglas para la interpretación de diversas formas de nombre

Las reglas para interpretar los formatos de nombre *IssuerDN* y siguen lo señalado por la familia de estándares ISO/IEC 9594 (recomendación X.500). Así, la estructura de un DN *(DistinguishedName)* se define en el estándar ISO/IEC 9594-2 (recomendación ITU-T X.501), que es construida con los atributos definidos en el estándar ISO/IEC 9594-6 (recomendación ITU-T X.520). Los numerales 4.1.2.4 y 4.1.2.6 del RFC 5280, indican el conjunto de atributos obligatorios y opcionales que deben contener los campos *IssuerDN* y *SubjectDN*.

3.1.5 Unicidad de los nombres

Los nombres distintivos en los certificados de proveedores de servicios de certificación son únicos para cada autoridad de certificación. En cualquier caso, la Unidad de Firma Electrónica de MINEC utiliza mecanismos para evitar conflictos de nombres.

3.1.6 Validación inicial de la identidad

A este respecto, deberá cumplirse con lo establecido en el artículo 16 del Reglamento de la Ley de Firma Electrónica, sobre la información requerida para la acreditación para proveedor de servicios de certificación.

3.1.7 Método para probar la posesión de la clave privada

Los proveedores de servicios de certificación deben generar su propio par de claves y demostrar la posesión de su clave privada mediante el envío de un mensaje de prueba de posesión de clave privada, conforme a lo estipulado en el RFC4210, como por ejemplo un *Certificate Signing Request* (CSR) en formato PKCS#10, según lo estipulado en el RFC2986.

3.1.8 Autenticación de la identidad de PSC o TSA

El solicitante, para demostrar su identidad, debe proporcionar la siguiente información para acreditarse como proveedor de servicios de certificación, conforme a la normativa aplicable.

La información suministrada por el solicitante a través del formulario a la Autoridad de Registro, junto con la documentación de soporte, será revisada por el personal de la Unidad de Firma Electrónica encargado de acreditar a los proveedores de servicios de certificación de acuerdo a los procedimientos internos definidos por la Unidad de Firma Electrónica de MINEC.

3.1.9 Información de solicitante no verificada

En la solicitud del certificado de autoridad de certificación el solicitante debe proporcionar documentos y datos personales que lo identifiquen absolutamente, toda la información será verificada aún si no hace parte de la información incluida en el certificado digital del PSC o TSA. Se debe dejar constancia de la información no verificada.

Toda la información a incluirse en un certificado digital debe ser siempre verificada durante el proceso de autenticación de la identidad. Cualquier información que no haya sido verificada no debe incluirse en el certificado digital.

3.1.10 Validación de autoridad para efectuar la solicitud

La Unidad de Firma Electrónica debe validar el derecho que posee un solicitante para gestionar un certificado de autoridad de certificación (Art. 37, literal b; Art. 43). La solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado y con las atribuciones y los poderes de representación correspondientes.

3.1.11 Identificación y autenticación para solicitudes de revocación

El procedimiento para identificación y autenticación para generar la solicitud de revocación de un certificado de autoridad de certificación mediante un formulario.

4. Ciclo de vida de los certificados digitales: requisitos operacionales

El ciclo de vida de los certificados digitales para los PSC o TSA, bajo la jerarquía de CA raíz en El Salvador contempla: emisión, expiración, revocación y renovación de certificados digitales.

La Unidad de Firma Electrónica debe procesar solicitudes de emisión de certificados digitales para los PSC o TSA que hayan sido acreditados. La Unidad de Firma Electrónica deberá aceptar únicamente solicitudes de emisión y pedidos de revocación de certificados digitales a través del representante legal de la entidad, o apoderado debidamente autorizado por ésta.

4.1 Solicitud de certificados

4.1.1 Persona apta para presentar una solicitud de certificado

La solicitud de un certificado de PSC o TSA debe ser hecha por el representante legal de la persona jurídica. En este caso, la titularidad del certificado y de los certificados digitales generados a partir de dicho certificado corresponderá a la autoridad de certificación acreditada como PSC o TSA. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

4.1.2 Presentación de una solicitud de certificado

Toda persona jurídica que desee obtener un certificado de firma electrónica emitido por la autoridad de certificación raíz en El Salvador, debe realizar la solicitud de certificado a través del formulario definido por la Unidad de Firma Electrónica.

4.1.3 Comprobación de solicitudes

El Oficial de Verificación y Registro deberá comprobar y validar la información y los documentos que son requeridos para solicitar los certificados de persona jurídica.

Para estos efectos el solicitante autoriza y faculta expresamente a la Unidad de Firma Electrónica para que verifique la información proporcionada con otras bases de datos públicas o privadas.

La Unidad de Firma Electrónica mantendrán un archivo con la información que respalde cada solicitud de inscripción realizada para la emisión de los certificados de PSC o TSA, por un periodo de mínimo diez (10) años.

4.1.4 Aprobación de la solicitud

Si el proceso de verificación y validación de la documentación e información entregada por el solicitante resulta exitosa, la Unidad de Firma Electrónica aprobará dicha solicitud y notificará al proveedor para continuar con el proceso de acreditación y emisión del certificado de autoridad de certificación.

4.1.5 Archivo de la solicitud

Se archivarán, notificando la causa, las solicitudes que no cumplan con los requerimientos, información y documentación solicitada por la Unidad de Firma Electrónica.

4.1.6 Registro de pago

El usuario cuya solicitud ha sido aprobada presentará el documento acreditativo de la constitución de la fianza y la liquidación de las tasas correspondientes a la acreditación de acuerdo a la Ley de Firma Electrónica y su Reglamento.

4.2 Emisión de certificados

4.2.1 Acciones de la AC durante la emisión del certificado

La Unidad de Firma Electrónica solo emite un certificado digital de PSC o TSA, si recibe una solicitud de emisión acompañada de un mensaje de prueba de posesión de clave privada, conforme a lo estipulado en el RFC4210, como una petición de firma de certificado (CSR) válido en formato PKCS#10, según lo indicado en la solicitud de certificado digital.

4.2.2 Notificación al suscriptor por parte de la AC de la emisión del certificado

La notificación de la emisión y entrega puede realizarse mediante medios telemáticos a través del envío del certificado al PSC o TSA.

4.2.3 Aceptación del certificado

La aceptación del certificado digital se da en el momento en el que titular del certificado expresa la aceptación de los términos y condiciones contenidos en la resolución de acreditación como PSC o TSA.

4.2.4 Publicación del certificado

Emitido el certificado de PSC o TSA por parte de la Unidad de Firma Electrónica, se procede a su publicación en el directorio de certificados. La clave pública del certificado es publicada en el sitio web de la Unidad de Firma Electrónica de lista de proveedores de servicios de certificación.

4.3 Par de claves y uso del certificado

4.3.1 Uso de la clave privada y del certificado por parte del suscriptor

El suscriptor podrá utilizar la clave privada y el certificado exclusivamente para los usos autorizados en esta política de certificación, luego de que el suscriptor haya aceptado los términos y condiciones de la misma.

4.3.2 Uso de la clave pública y del certificado por los terceros que confían

Los terceros que confían deben usar la clave pública contenida en el certificado para realizar las validaciones indicadas únicamente en las extensiones *KeyUsage (KU)* del certificado o en la presente política de Certificación

Los usuarios que confían deben verificar el estado del certificado utilizando los mecanismos establecidos en la DPC y en la presente PC.

4.4 Renovación de certificados

La renovación del certificado se produce cuando éste va a expirar, para esto el suscriptor deberá realizar el mismo procedimiento utilizado para solicitar un certificado de PSC o TSA.

4.5 Renovación de certificados con cambio de claves

No Aplica.

4.6 Modificación de certificados

4.6.1 Circunstancias para la modificación de un certificado

El certificado no puede ser modificado. Todas las modificaciones de certificados realizadas en el ámbito de esta PC se tratarán como una nueva emisión de certificado.

4.7 Revocación, suspensión y reactivación de certificados

La revocación de los certificados es un mecanismo que se utiliza cuando existe la pérdida de fiabilidad de los mismos, ocasionando el cese de su operatividad e impidiendo su uso legítimo.

En la Declaración de Prácticas de Certificación se especifican las razones por las cuales se puede revocar o suspender un certificado digital, los medios para efectuarlas, el procedimiento, y el tiempo que se tarda en procesar y resolver la suspensión o revocación.

La revocación de un certificado tiene como principal efecto la terminación inmediata y anticipada del periodo de validez del mismo.

Los certificados revocados no podrán bajo ninguna circunstancia volver al estado activo.

La revocación de un certificado implica su publicación en la Lista de Certificados Revocados de Autoridad de Certificación (ARL) de acceso público.

4.7.1 Circunstancias para la revocación

Los certificados emitidos por la Autoridad de Certificación Raíz de El Salvador serán revocados bajo las siguientes circunstancias:

- Por exposición, puesta en peligro, uso indebido o compromiso de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Cuando la información contenida en el certificado digital no resulte correcta.
- Por el cese en la actividad como proveedor de servicios de certificación.

4.8 Servicios de información del estado del certificado

La Unidad de Firma Electrónica proporciona el servicio de validación de los certificados a través de las ARL publicadas en su página web.

- https://normativa.firmaelectronica.economia.gob.sv/dpc/

Para comprobar la última ARL se pueden consultar las siguientes direcciones web:

- http://crl1.firmaelectronica.economia.gob.sv/crl/arl_sv.crl
- http://crl2.firmaelectronica.economia.gob.sv/crl/arl_sv.crl

4.9 Finalización de la suscripción

La acreditación como PSC o TSA debe ser renovada anualmente ante la Unidad de Firma Electrónica del Ministerio de Economía, pero la validez del certificado como autoridad de certificación se rige de acuerdo a la vigencia del certificado.

5. Perfiles de certificado

5.1 Contenido del certificado

El contenido de los certificados de PSC o TSA es el siguiente:

Campo	Contenido	Obligatorio	Crítico
1. Basic estructure			
1.1. Version	"2" (equivalente a la v3)	Sí	
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí	
1.3. Signature Algorithm		Sí	
1.3.1 Identifier	1.2.840.113549.1.1.13		
1.3.2. Algorithm	Sha512WithRSAEncryption	Sí	
1.4. Issuer		Sí	
1.4.1. Country Name (C)	"SV"	Sí	
1.4.2. Locality Name (L)	"SAN SALVADOR"	Sí	
1.4.3. Organizational Unit (OU)	"UNIDAD DE FIRMA ELECTRONICA"	Sí	
1.4.4. Organization Name (O)	"MINISTERIO DE ECONOMIA"	Sí	
1.4.5. Common Name (CN)	"AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR"	Sí	
1.4.6. Organization Identifier (other name)	"VATSV-06140101140073"	Sí	
1.5. Validity	**(15 años)**	Sí	
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado (codificado en UTCTime)	Sí	
1.5.2. Not After	Fecha y hora de expiración del certificado (codificado en UTCTime) NotBefore + 15 años	Sí	
1.6. Subject		Sí	
1.6.1. Country Name	"SV"	Sí	

Campo	Contenido	Obligatorio	Crítico
1.6.2. Locality Name (L)	Nombre de la LOCALIDAD donde resida legalmente el proveedor del servicio de certificación. (No incluir información adicional al nombre de la localidad)	Sí	
1.6.3. Organizational Unit (OU)	UNIDAD ORGANIZATIVA CA SUBORDINADA	Sí	
1.6.4. Organization Name (O)	ORGANIZACIÓN CA SUBORDINADA	Sí	
1.6.5. Common Name (CN)	NOMBRE DE LA CA SUBORDINADA	Sí	
1.6.6. Organization Identifier (other name)	"VATSV-[NIT CA SUBORDINADA]"	Sí	
1.7. Subject Public Key Info		Sí	
1.7.1. AlgorithmIdentifier	1.2.840.113549.1.1.1		
1.7.1.1. Algorithm	RSA encryption	Sí	
1.7.1.2. Parameters	No aplicable	No	
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 4096 bits	Sí	
2. Extensions			
2.1. Authority Key Identifier		Sí	No
2.1.1. KeyIdentifier	Identificador de la clave del emisor	Sí	
2.2. Subject Key Identifier		Sí	No
2.2.1. KeyIdentifier	Identificador de la clave del subject	Sí	
2.3. Key Usage		Sí	Sí
2.3.1. Digital Signature	No seleccionado "0"		
2.3.2. Content commintment	No seleccionado "0"		

Campo	Contenido	Obligatorio	Crítico
2.3.3. Key Encipherment	No seleccionado "0"		
2.3.4. Data Encipherment	No seleccionado. "0"		
2.3.5. Key Agreement	No seleccionado. "0"		
2.3.6. Key Certificate Signature	Seleccionado "1"	Sí	
2.3.7. CRL Signature	Seleccionado "1"	Sí	
2.3.8. Encipher Only	No seleccionado. "0"		
2.3.9. Decipher Only	No seleccionado. "0"		
2.4. Certificate Policies		Si	No
2.4.1. Policy Information		Sí	
2.4.1.1. Policy Identifier	1.3.6.1.4.1. 50377.1.1.1	Sí	
2.4.1.2. Policy Qualifiers		Sí	
2.4.1.1.1. CPS URI	URL donde se encuentra la DPC. (https://normativa.firmaelectronica.economia.gob.sv/dpc/)	Sí	
2.4.1.1.2. User Notice/Explicit text	Certificado de la autoridad subordinada proveedor de servicios de certificación	Sí	
2.4.2. Policy Information		No	
2.4.2.1. Policy Identifier		No	
2.5. Subject Alternative Names		No	No
2.5.1. rfc822Name	Email de la CA Subordinada (Ej. info@ca-subordinada.sv)	No	
2.6. cRLDistributionPoint		Sí	Sí

Campo	Contenido	Obligatorio	Crítico
2.6.1. distributionPoint	URL donde se encuentra la ARL (CRL de la CA Raíz) Ej. http://firmaelectronica.minec.gob.sv/crl/arl_minec.crl	Sí	
2.6.2. distributionPoint	URL alterna donde se encuentra la ARL (CRL de la CA Raíz) Ej. http://crl2.firmaelectronica.minec.gob.sv/crl/arl_minec.crl	No	
2.7. Basic Constraints		Sí	Sí
2.7.1. Subject type	CA (VERDADERO)	Sí	
2.7.2 Path Length Constraints	Ninguno	Sí	

CRL de PSC o TSA

CRL (CA SUBORDINADAS)	
Componente	**Valor**
Campos de CRL X.509 v2 (tbsCertList)	
version	"1" (equivalente a la v2)
signature	
algorithm	sha256withRSAEncryption
issuer	
countryName (C)	"SV"
localityName (L)	Nombre de la LOCALIDAD/(DEPARTAMENTO) donde resida el proveedor del servicio de certificación. (No incluir información adicional al nombre de la localidad)
organizationalUnitName (OU)	UNIDAD ORGANIZATIVA CA SUBORDINADA
organizationName (O)	ORGANIZACIÓN CA SUBORDINADA
commonName (CN)	NOMBRE DE LA CA SUBORDINADA
otherName	"VATSV-[NIT _PROVEEDOR]"
thisUpdate	Fecha y hora de emisión de la CRL, codificado en UTCTime
nextUpdate	thisUpdate + 1 día, codificado en UTCTime

CRL (CA SUBORDINADAS)	
Componente	**Valor**
Certificados revocados en CRL X.509 v2 (revokedCertificates)[1]	
userCertificate	Valor del campo serialNumber del certificado revocado
revocationDate	Fecha y hora de revocación del certificado, codificado en UTCTime
crlEntryExtensions	
reasonCode	Motivo de revocación del certificado (uno de los valores): unspecified; keyCompromise; keyCompromise; affiliationChanged; superseded; cessationOfOperation; certificateHold; privilegeWithdrawn; aACompromise
Extensiones de CRL X.509 v2 (crlExtensions)	
authorityKeyIdentifier	
keyIdentifier	Valor en extensión subjectKeyIdentifier del certificado de CA Subordinada
cRLNumber	Número entero secuencial (valor inicial: 00)

5.1.1 Número de versión

Se debe utilizar el estándar x.509 versión 3.

5.1.2 Extensiones del certificado

Las extensiones incluidas en los certificados digitales de PSC o TSA de acuerdo a numeral 5.1 Contenido del certificado.

5.1.3 Identificadores de objeto del algoritmo

Los certificados digitales de PSC o TSA utilizan los siguientes algoritmos:

- SHA512 con cifrado RSA
  - Notación ASN.1 → OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
  - Notación numérica → OID = 1.2.840.113549.1.1.13
  - Nombre: sha512WithRSAEncryption.

5.1.4 Formatos de nombre

Se debe respetar la forma de nombres de acuerdo a la familia de estándares ISO/IEC 9594

[1] Lista de entradas, una por cada certificado revocado, cada una de ellas con los 3 componentes indicados.

(recomendación X.500) para *DistinguishedName* como se especifica en el numeral 3.1.1 Tipos de Nombres.

5.1.5 Restricciones de nombre

Los PSC o TSA pueden establecer restricciones de nombre como se indica en el estándar RFC 5280.

5.1.6 Objeto identificador de la Política de Certificados

Los PSC o TSA utilizarán la estructura de OID definida por la Unidad de Firma electrónica, podrán también declarar, de forma adicional, los OID de aquellas políticas de línea base a las que se adhieran a efectos de interoperabilidad, como ETSI EN 319 411-1.

5.1.7 Sintaxis y semántica de los calificadores de la política

La extensión de los certificados referente a los calificadores de la Política de Certificados contiene la siguiente información:

- *CertificatePolicy*: Contiene la Política de Certificados de PSC o TSA.

5.2 Perfil de la CRL

5.2.1 Número de versión

Se debe implementar al menos el perfil de CRL en su versión 2 (X.509 v2) en conformidad con lo especificado en el RFC 5280 "PKIX Certificate and CRL Profile".

5.2.2 CRL y extensiones

De conformidad a lo descrito 5.1 Contenido del Certificado relacionado con el perfil de CRL de PSC o TSA.