Política de Certificación

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	1
Fecha edición:	22/04/2021
Fichero:	PC_SV_ES_v1.r3.docx

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 22/04/2021	Nombre: Albert Borrás Fecha: 22/04/2021	Nombre: Mario Hernández Fecha: 23/04/2021

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	AGB	22/04/2021

Índice

1. Introducción

1.1. Presentación

Este documento declara las prácticas de certificación de firma electrónica de Uanataca El Salvador, S.A. de CV, en adelante "*UANATACA*".

Los certificados electrónicos de firma electrónica certificada que se emiten son los siguientes:

- **De Persona Natural**
  - Certificado de persona natural ciudadano en QSCD
  - Certificado de persona natural perteneciente a empresa u organización en QSCD
  - Certificado de persona natural profesional en QSCD
  - Certificado de persona natural funcionario público en QSCD

- **De Persona Natural Representante**
  - Certificado de Persona Natural Representante de Persona Natural en QSCD
  - Certificado de Persona Natural Representante de Persona Jurídica en QSCD

- **De Sello Electrónico**
  - Certificado de Sello Electrónico en QSCD

- **De Facturación Electrónica**
  - Certificado de Facturación Electrónica de Persona Jurídica en QSCD
  - Certificado de Facturación Electrónica de Persona Natural en QSCD

- **De Dispositivos**
  - Certificado de Sello de Tiempo Electrónico
  - Certificado de VA-OCSP

Los certificados electrónicos de firma electrónica simple que se emiten son los siguientes:

- **De Facturación Electrónica**
  - Certificado de Facturación Electrónica en P12

1.2. Nombre del documento e identificación

Este documento es la "Política de Certificación de UANATACA".

1.2.1. Identificadores de certificados

UANATACA ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

Certificados electrónicos de firma electrónica certificada:

Número OID	Tipo de certificados
	Persona Natural
1.3.6.1.4.1.56489.3.1.1	Certificado de persona natural ciudadano en QSCD
1.3.6.1.4.1.56489.3.1.1	Certificado de persona natural perteneciente a empresa u organización en QSCD
1.3.6.1.4.1.56489.3.1.1	Certificado de persona natural profesional en QSCD
1.3.6.1.4.1.56489.3.1.1	Certificado de persona natural funcionario público en QSCD
	Persona Natural Representante
1.3.6.1.4.1.56489.3.2.1	Certificado de Persona Natural Representante de Persona Natural en QSCD
1.3.6.1.4.1.56489.3.2.1	Certificado de Persona Natural Representante de Persona Jurídica en QSCD
	Sello Electrónico
1.3.6.1.4.1.56489.3.3.1	Certificado de Sello Electrónico en QSCD
	Facturación Electrónica
1.3.6.1.4.1.56489.3.6.1	Certificado de Facturación Electrónica de Persona Jurídica en QSCD
1.3.6.1.4.1.56489.3.6.1	Certificado de Facturación Electrónica de Persona

	Natural en QSCD
	Dispositivos
1.3.6.1.4.1.56489.3.4.1	Certificado de Sello de Tiempo Electrónico
1.3.6.1.4.1.56489.3.5.1	Certificado de VA-OCSP

Certificados electrónicos de firma electrónica simple

Número OID	Tipo de certificados
	Facturación Electrónica
1.3.6.1.4.1.56489.2.3.1	Certificado de Facturación Electrónica en P12

En caso de contradicción entre la Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en la Declaración de Prácticas.

1.3. Participantes en los servicios de certificación

1.3.1. Proveedor de Servicios de certificación

El Proveedor de Servicios electrónicos de certificación es la persona natural o jurídica, que expide y gestiona certificados para entidades finales, empleando una Entidad de Certificación, o presta otros servicios relacionados con la firma electrónica.

UANATACA es un Proveedor de Servicios electrónicos de certificación, que actúa de acuerdo con la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento, Decreto 534 de Ley de Acceso a la Información Pública así como las normas técnicas del ETSI aplicables a la expedición y gestión de certificados principalmente, EN 319 401, EN 319 411-1 y EN 319 411-2, y los mejores estándares internacionales, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, UANATACA ha establecido una jerarquía de entidades de certificación:

1.3.1.1. AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave público ha sido auto firmado.

Datos de identificación:

CN:	AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR
Huella digital:	09 d7 55 ab cb 51 d9 a9 50 05 10 6c cf bf 30 dc 8b 87 2f 2b
Válido desde:	martes, 8 de septiembre de 2020
Válido hasta:	viernes, 8 de septiembre de 2045
Longitud de clave RSA:	4.096 bits

1.3.1.2. UANATACA EL SALVADOR CA1

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR.

Datos de identificación:

CN:	UANATACA EL SALVADOR CA1
Huella digital:	4c b8 7a 21 53 aa f4 84 ff 96 f5 5b 63 cc 28 d0 b0 f2 b2 aa
Válido desde:	miércoles, 14 de abril de 2021
Válido hasta:	domingo, 13 de abril de 2036
Longitud de clave RSA:	4.096 bits

1.3.2. Autoridad de Registro

Una Autoridad de Registro de UANATACA es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado.
- Gestionar la generación de claves y la emisión del certificado
- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

Podrán actuar como RA de UANATACA:

- Cualquier entidad autorizada por UANATACA.
- UANATACA directamente.

UANATACA formalizará contractualmente las relaciones entre ella misma y cada una de las entidades que actúen como Autoridad de Registro de UANATACA.

La entidad que actúe como Autoridad de Registro de UANATACA podrá autorizar a una o varias personas como Operador de la RA para operar con el sistema de emisión de certificados de UANATACA en nombre de la Autoridad de Registro.

La Autoridad de Registro podrá delegar las funciones de identificación de los suscriptores y/o firmantes, previo acuerdo de colaboración en el que se acepte la delegación de estas funciones. UANATACA deberá autorizar de manera expresa dicho acuerdo de colaboración.

También podrán ser Autoridades de Registro sujetas a esta Declaración de Prácticas de Certificación, las unidades designadas para esta función por los suscriptores de los certificados, como un departamento de personal, dado que disponen de los registros auténticos acerca de la vinculación de los firmantes con el suscriptor.

1.3.3. Entidades finales

Las entidades finales son las personas u organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados electrónicos, para los usos de autenticación y firma electrónica.

Serán entidades finales de los servicios de certificación de UANATACA las siguientes:

1. Suscriptores del servicio de certificación
2. Firmantes
3. Partes usuarias

1.3.3.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- Las empresas, entidades, corporaciones u organizaciones que los adquieren a UANATACA (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo, y se encuentran identificados en los certificados.
- Las personas naturales que adquieren los certificados para sí mismas, y se encuentran identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio – certificados de sello electrónico –, o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor – certificados de firma electrónica. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio electrónico de certificación es, por tanto, el cliente del Proveedor de Servicios de certificación, de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en las normas técnicas aplicables a la expedición de certificados electrónicos, en especial ETSI EN 319 411, secciones 5.4.2 y 6.3.4.e).

1.3.3.2. Firmantes

Los firmantes son las personas naturales que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma electrónica Certificada; siendo típicamente los empleados, representantes legales o voluntarios, así como otras personas vinculadas a los suscriptores; incluyendo las personas al servicio de la Administración, en los certificados de funcionario público.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación inequívoco, así como todos aquellos datos exigidos por la ley, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por el Proveedor de Servicios electrónicos de certificación, por lo que las personas naturales identificadas en los correspondientes certificados son las únicas responsables de su protección y deberían considerar las implicaciones de perder una clave privada.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la autenticación, también se emplea el término más genérico de "Persona natural identificada en el certificado", siempre con pleno respeto al cumplimiento de la regulación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.3.3.3. Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas electrónicas y certificados electrónicos.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en la declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en la página web de la Autoridad de Certificación.

1.3.4. Proveedor de Servicios de Infraestructura de Clave Pública

"Uanataca El Salvador, S.A. de CV" y "Uanataca, S.A." han suscrito un contrato de prestación de servicios de tecnología en el que Uanataca, S.A., proveerá la infraestructura de clave pública (PKI) que sustenta el servicio de certificación de Uanataca El Salvador, S.A. de CV. Así mismo Uanataca, S.A., pone a disposición de Uanataca El Salvador, S.A. de CV el personal técnico necesario para correcto desempeño de las funciones fiables propias de un Proveedor de Servicios de Certificación.

Dicho lo cual, Uanataca, S.A., se configura como el proveedor de servicios de Infraestructura para servicios de certificación, provee sus servicios tecnológicos a Uanataca El Salvador, S.A. de CV, para que éste pueda llevar a cabo los servicios inherentes a un Proveedor de Servicios de Certificación, garantizando en todo momento la continuidad de los servicios en las condiciones y bajo los requisitos exigidos por la normativa.

Asimismo, se informa que Uanataca, S.A., es un Proveedor de Servicios de Certificación cuya PKI se somete a auditorías anuales para la evaluación de la conformidad de prestadores de servicios de certificación de acuerdo con la normativa aplicable, bajo las normas:

a. ISO/IEC 17065:2012
b. ETSI EN 319 403
c. ETSI EN 319 421
d. ETSI EN 319 401
e. ETSI EN 319 411-2
f. ETSI EN 319 411-1

Asimismo, la PKI de Uanataca, S.A., se somete a auditorías anuales bajo los estándares de seguridad:

a. ISO 9001:2015
b. ISO/IEC 27001:2014

1.4. Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1. Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, disponibles en el web https://web.uanataca.com/sv/

1.4.1.1. Certificado de Persona natural en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.1.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma, es un certificado de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de certificación, y permite la generación de la “firma electrónica certificada”, es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.

b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.4.1.2. Certificado de persona natural perteneciente a empresa u organización en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.1.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado emitido en dispositivo seguro de creación de firma, es un certificado de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una entidad, empresa u organización descrita en el campo “O” (Organization), y permite la generación de la “firma electrónica certificada” es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.4.1.3. Certificado de Persona Natural Profesional en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.1.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma, es un certificado de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una entidad habilitante descrita en el campo “O” (Organization), y permite la generación de la “firma electrónica certificada” es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.4.1.4. Certificado de persona natural funcionario público en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.1.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma, es un certificado de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una Institución descrita en el campo “O” (Organization), y permite la generación de la “firma electrónica certificada” es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.4.1.5. Certificado de Persona Natural Representante de Persona Natural en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.2.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de representante emitido en dispositivo seguro de creación de firma, es un certificado de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una persona natural en el campo “O” (Organization), y permite la generación de la “firma electrónica certificada” es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.4.1.6. Certificado de Persona Natural Representante de Persona Jurídica en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.2.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de representante emitido en dispositivo seguro de creación de firma, es un certificado de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una persona jurídica, entidad u organización en el campo “O” (Organization), y permite la generación de la “firma electrónica certificada” es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.4.1.7. Certificado de Sello Electrónico en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.3.1. Es un certificado que se emite de acuerdo con la política de certificación QCP-l-qscd con el OID 0.4.0.194112.1.3. Este certificado de sello electrónico emitido en dispositivo seguro de creación de firma, es un certificado de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad del responsable del sello y de la entidad vinculada, incluidos en el certificado.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

1.4.1.8. Certificado de Facturación Electrónica de Persona Jurídica en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.6.1. Es un certificado que se emite de acuerdo con la política de certificación QCP-l-qscd con el OID 0.4.0.194112.1.3. Este certificado de facturación electrónica emitido en dispositivo seguro de creación de firma, es un certificado de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de facturación electrónica en dispositivo seguro de creación de firma garantizan la identidad del responsable del certificado y de la entidad vinculada, incluidos en el mismo.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionarlo, identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

Este certificado solo podrá ser utilizado para la facturación electrónica de la entidad suscriptora identificada en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos de conformidad con la normativa aplicable.

1.4.1.9. Certificado de Facturación Electrónica de Persona Natural en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.6.1. Es un certificado que se emite de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este

certificado de facturación electrónica emitido en dispositivo seguro de creación de firma, es un certificado de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de certificación, y permite la generación de la "firma electrónica certificada", es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

d. Firma digital (Digital Signature, para realizar la función de autenticación)
e. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
f. Key Encipherment

Este certificado solo podrá ser utilizado para la facturación electrónica del firmante identificado en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos de conformidad con la normativa aplicable.

1.4.1.10. Certificado de sello de tiempo electrónico

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.4.1, y se emite de acuerdo con la política de certificación QCP-l-qscd con el OID 0.4.0.194112.1.3.

Los certificados de sello de tiempo electrónico se tratan de certificados emitidos para la operación de autoridades de sellado de tiempo y hora, para la firma de los sellos de tiempo que éstas producen.

Estos certificados permiten la firma de los sellos de tiempo que se emiten, desde el momento que hayan obtenido un certificado de sello de tiempo electrónico válido y mientras éste se encuentre vigente.

La sincronización de los tiempos en UANATACA se realiza mediante un servicio servidor de tiempo NTP Stratum 3.

Este servidor, un Meinberg Lantime M300/GPS, con oscilador TCXO de alta estabilidad, receptor GPS, formado por una tarjeta GPS interna para sincronizarse simultáneamente con los satélites con los que tiene visibilidad en cada momento (entre 3 y 8), y protección anti-rayos.

1.4.1.11. Certificado de VA-OCSP

Este certificado dispone del OID 1.3.6.1.4.1.56489.3.5.1, y se emite de acuerdo con la política de certificación QCP-l-qscd con el OID 0.4.0.194112.1.3.

Los certificados de VA-OCSP son certificados emitidos para la operación de las Autoridades de Validación, respecto del servicio de validación de certificados mediante el protocolo OCSP (*Online Certificate Status Protocol*).

Estos certificados permiten la firma de las respuestas realizadas por el servidor de OCSP, a las peticiones de los usuarios para la verificación del estado de un certificado.

1.4.1.12. Certificado de Facturación electrónica en P12

Este certificado dispone del OID 1.3.6.1.4.1.56489.2.3.1. Estos certificados garantizan la identidad suscriptora vinculada, y en su caso la del responsable de gestionar el certificado identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital (Digital Signature, para realizar la función de autenticación)
b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c. Key Encipherment

Este certificado solo podrá ser utilizado para la facturación electrónica de la entidad suscriptora identificada en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos.

1.4.2. Límites y prohibiciones de uso de los certificados

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la regulación aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, disponibles en la web de UANATACA.

El empleo de los certificados electrónicos en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada

certificado, o los contratos con las entidades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a UANATACA, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

UANATACA no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de UANATACA emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

2. Identificación y autenticación

2.1. Registro inicial

2.1.1. Tipos de nombres

Todos los certificados contienen un nombre distintivo (DN o *distinguished name*) conforme al estándar X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la Persona natural identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*

Los nombres contenidos en los certificados son los siguientes.

2.1.1.1. Certificado de persona natural ciudadano en QSCD

Country Name (C)	País de residencia o nacionalidad del firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número de documento de identificación del firmante
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad del Firmante

2.1.1.2. Certificado de persona natural perteneciente a empresa u organización en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Nombre de la Empresa u Organización
Organizational Unit Name (OU)	Departamento al que pertenece el firmante o el tipo de vinculación con la Empresa
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante
Title	Título o puesto que la persona ocupa en la Empresa u Organización
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número de documento de identificación del firmante
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad a la que está vinculado el firmante

2.1.1.3. Certificado de persona natural profesional en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Nombre de la entidad habilitante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante
Title	Se especificará el título o especialidad del firmante.
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número de documento de identificación del firmante
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad de la entidad habilitante

2.1.1.4. Certificado de persona natural funcionario público en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organizational Unit Name (OU)	Departamento al que pertenece el firmante o el tipo de vinculación con la Institución
Organization Name (O)	Se especificará el nombre de la Institución
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante
Title	Se especificará el cargo o puesto que la persona ocupa en la Institución
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número de documento de identificación del firmante
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad solicitante del certificado

2.1.1.5. Certificado de Persona Natural Representante de Persona Natural en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Nombre de persona natural representada
Organization Identifier	Número de documento de identificación de la persona a quien representa
Title	REPRESENTANTE LEGAL
Surname	Apellidos del representante
Given Name	Nombre del representante
Serial Number	Número de documento de identificación del representante
Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad del Representante

2.1.1.6. Certificado de Persona Natural Representante de Persona Jurídica en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Nombre de la organización de la que el firmante es representante
Organization Identifier	Número oficial de identificación de la organización o entidad representada por el firmante
Title	REPRESENTANTE LEGAL
Surname	Apellidos del representante
Given Name	Nombre del representante
Serial Number	Número de documento de identificación del representante
Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad del Representante

2.1.1.7. Certificado de Sello Electrónico en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Denominación (nombre "oficial" de la organización o entidad)
Organizational Unit Name (OU)	Denominación (nombre "oficial" de la unidad) del solicitante del sello (Ej: Subdirección de explotación)
Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello
Surname	Apellidos del firmante responsable firmante del sello
Given Name	Nombre del firmante responsable firmante del sello
Serial Number	Número de documento de identificación del responsable firmante del sello
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad

2.1.1.8. Certificado de Facturación Electrónica de Persona Jurídica en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Denominación (nombre "oficial" de la organización o entidad)
Organizational Unit Name (OU)	Denominación (nombre "oficial" de la unidad) del solicitante del sello (Ej: Subdirección de explotación)
Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Description	Número de Registro de Contribuyente (NRC)
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad

2.1.1.9. Certificado de Facturación Electrónica de Persona Natural en QSCD

Country Name (C)	País de residencia o nacionalidad del firmante
Surname	Apellidos del firmante responsable firmante del sello
Given Name	Nombre del firmante responsable firmante del sello
Serial Number	Número de documento de identificación del responsable firmante del sello
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Description	Número de Registro de Contribuyente (NRC)
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad del Contribuyente

2.1.1.10. Certificado de sello de tiempo electrónico

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Locality Name (L)	Nombre de la LOCALIDAD donde resida el proveedor del servicio de certificación.
Organizational Unit Name (OU)	TSP-UNIDAD PRESTADOR
Organization Name (O)	NOMBRE ORGANIZACIÓN
Common Name (CN)	Sello de tiempo electrónico de [NOMBRE DEL PRESTADOR DE SERVICIO]
Organization Identifier (other name)	VATSV-[NIT DEL PRESTADOR DEL SERVICIO]”
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad del proveedor del servicio de certificación

2.1.1.11. Certificado de VA-OCSP

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Locality Name (L)	Nombre de la LOCALIDAD donde resida el titular del certificado. (No incluir información adicional al nombre de la localidad)
Organizational Unit Name (OU)	TSP-UNIDAD PRESTADOR
Organization Name (O)	NOMBRE ORGANIZACIÓN
Common Name (CN)	Autoridad de Validación de [NOMBRE DEL PRESTADOR DE SERVICIO]
Organization Identifier (other name)	VATSV-[NIT DEL PRESTADOR DEL SERVICIO]”
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad del proveedor del servicio de certificación

2.1.1.12. Certificado de Facturación Electrónica en P12

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Denominación (nombre "oficial" de la organización o entidad)
Organizational Unit Name (OU)	Denominación (nombre "oficial" de la unidad) del solicitante del sello (Ej: Subdirección de explotación)
Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello en formato ETSI EN 319412-1 (Ejemplo: "VATSV-[NIT-DE-LA-ENTIDAD]")
Surname	Apellidos del firmante responsable firmante del sello (como consta en el documento de identificación)
Given Name	Nombre del firmante responsable firmante del sello (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del responsable firmante del sello, codificado acorde a ETSI EN 319 412-1 ejemplo ("IDCSV-[DUI]" o "PASEC-[PASAPORTE]")
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Description	Número de Registro de Contribuyente (NRC)
Address	Dirección, Código Postal y Ciudad/Municipio/Localidad del contribuyente

2.1.2. Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

2.1.2.1. Emisión de certificados del set de pruebas y certificados de pruebas en general

En el caso que los datos indicados en el DN o Subject fueran ficticios (ej. "Test Organization", "Test Nombre", "Apellido1") o se indique expresamente palabras que denoten su invalidez (ej. "TEST", "PRUEBA" o "INVALIDO"), se considerará al certificado sin validez legal y por lo tanto sin responsabilidad alguna sobre UANATACA. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y permitir al ente regulador su evaluación.

2.1.3. Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad, empresa u organización, ni a un firmante. Así mismo, en ningún caso se emiten certificados anónimos.

2.1.4. Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” o “estado” será el del suscriptor del certificado.

Los certificados cuyos suscriptores sean personas jurídicas, entidades u organismos de la administración pública, muestran la relación entre estas y una Persona natural, con independencia de la nacionalidad de la Persona natural.

En el campo “número de serie” se incluye el Documento Único de Identidad (DUI), Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

2.1.5. Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del número del Número de Identificación Fiscal, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Documento Único de Identidad (DUI), Pasaporte u otro identificador legalmente válido de la Persona natural.

- Número de Identificación Tributaria (NIT) u otro identificador legalmente válido del suscriptor.
- Tipo de certificado (OID de identificador de política de certificación).

Como excepción se permite emitir un certificado cuando coincida NIT del suscriptor, DUI del firmante, Tipo de certificado, con un certificado activo, siempre que exista algún elemento diferenciador entre ambos, en los campos cargo (title) y/o departamento (Organizational Unit).

2.1.6. Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

No existirá ninguna obligación a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el Proveedor de Servicios de electrónicos de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro en el marco de los organismos competentes para la realización de un arbitraje en El Salvador a los que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte en el documento contractual que formaliza el servicio.

2.2. Validación inicial de la identidad

La identificación de los suscriptores se realiza mediante comparecencia personal ante el operador o personal autorizado de la Autoridad de Registro, cuya identidad resulta fijada en el momento de la firma del contrato entre UANATACA y el suscriptor, momento en el que se verifica la existencia del suscriptor mediante su documento oficial de identidad o las escrituras correspondientes, al igual que los poderes de actuación de la persona que presente como representante si fuese el caso. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

En el caso de personas naturales identificadas en certificados cuyo suscriptor sea una persona jurídica, sus identidades podrán validarse mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados siempre que aseguren que se han identificado presencialmente. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a UANATACA, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

2.2.1. Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor, en certificados de sello, o por el firmante, en certificados de firma.

2.2.2. Autenticación de la identidad de una organización, empresa o entidad mediante representante

Las personas naturales con capacidad de actuar en nombre de las personas jurídicas o entidades sin personalidad jurídica, públicas o privadas, que sean suscriptoras de certificados, podrán actuar como representantes de estas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la Persona natural y la organización de la que se trate, que exige su reconocimiento por UANATACA, la cual se realizará mediante el siguiente procedimiento presencial:

1. El representante del suscriptor se identificará mediante comparecencia personal ante un operador o persona autorizada de una Autoridad de Registro de UANATACA, acreditando el carácter y facultades que alegue poseer. Alternativamente, a los mismos efectos UANATACA podrá poner a disposición de los suscriptores un formulario en su página web para su cumplimentación previa.

2. El representante proporcionará la siguiente información y sus correspondientes soportes acreditativos:
    - Sus datos de identificación, como representante:
        - Nombre y apellidos
        - Lugar y fecha de nacimiento
        - Documento: DUI, Pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
    - Los datos de identificación del suscriptor al que representa:
        - Denominación o razón social.
        - Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.
        - Documento: NIT o documento acreditativo de la identificación fiscal de la entidad.
        - Documento: Documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.
    - Los datos relativos a la representación o la capacidad de actuación que ostenta:
        - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin) si resulta aplicable.
        - El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:

- TOTAL. Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.
- PARCIAL. Representación o capacidad parcial. Esta comprobación se podrá realizar mediante copia auténtica electrónica de la escritura notarial de apoderamiento, en los términos de la normativa notarial.

3. El operador o personal autorizado de la Autoridad de Registro de UANATACA comprobará la identidad del representante mediante la presentación del Documento Único de Identidad (DUI), Pasaporte u otro medio idóneo reconocido en derecho para su identificación, así como el contenido de la representación con la documentación.

4. El operador o personal autorizado de la Autoridad de Registro de UANATACA verificará la información suministrada para la autenticación y le devolverá la documentación original aportada.

5. Alternativamente, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar al operador o personal autorizado de la Autoridad de Registro por correo postal certificado, en cuyo caso los pasos 3 y 4 anteriores no serán precisos.

La prestación del servicio de certificación digital se formaliza mediante el oportuno contrato entre UANATACA y el suscriptor, debidamente representado.

2.2.3. Autenticación de la identidad de una Persona natural

Esta sección describe los métodos de comprobación de la identidad de una Persona natural identificada en un certificado.

2.2.3.1. En los certificados

La identidad de las personas naturales firmantes identificados en los certificados, se valida mediante la presentación de su documento oficial de identificación (Documento

Único de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación).

La información de identificación de las personas naturales identificadas en los certificados cuyo suscriptor sea una entidad con o sin personalidad jurídica, la información podrá ser validada comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, o bien con la documentación que esta haya suministrado sobre la Persona natural que identifica como firmante, asegurando la corrección de la información a certificar.

2.2.3.2. Validación de la Identidad

Para la solicitud de certificados, el operador o personal autorizado de la Autoridad de Registro valida la identidad del solicitante, para lo cual la Persona natural deberá comparecer personalmente y exhibir su Documento Único de Identidad (DUI), Pasaporte u otro medio idóneo reconocido en derecho para su identificación en el lugar destinado para el registro.

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica no se requiere la presencia física directa, debido a la relación ya acreditada entre la Persona natural y entidad, empresa u organización de derecho público o privado a la que está vinculada. Sin embargo, antes de la entrega de un certificado, la entidad, empresa u organización de derecho público o privado suscriptora, por medio de su responsable de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la Persona natural identificada en el certificado mediante su presencia física.

Durante este trámite se confirma rigurosamente la identidad de la Persona natural identificada en el certificado. Por este motivo, en todos los casos en que se expide un certificado se acredita ante un operador de registro la identidad de la Persona natural firmante.

La Autoridad de Registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

2.2.3.3. Vinculación de la Persona natural

La justificación documental de la vinculación de una Persona natural identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización…) de cada una de las personas públicas y privadas a las que están vinculadas.

2.2.4. Información de suscriptor no verificada

UANATACA no incluye ninguna información de suscriptor no verificada en los certificados.

2.2.5. Autenticación de la identidad de una RA y sus operadores

Para la constitución de una nueva Autoridad de Registro, se realizan las verificaciones necesarias para confirmar la existencia de la entidad u organización de la que se trate. Para ello, se podrá utilizar exhibición de documentos o utilizar sus propias fuentes de información.

Igualmente, UANATACA directamente o a través de su Autoridad de Registro, verifica y valida la identidad de los operadores de las Autoridades de Registro, para lo cual estas últimas envían a UANATACA la documentación de identificación correspondientes al nuevo operador, juntamente con su autorización para actuar como tal.

UANATACA se asegura que los operadores de la Autoridad de Registro reciben la formación suficiente para el desarrollo de sus funciones, lo cual verifica con la evaluación correspondiente. Dicha formación y evaluación puede ser ejecutada por la Autoridad de Registro previamente autorizada por UANATACA.

Para la prestación de los servicios, UANATACA se asegura de que los operadores de Autoridad de Registro acceden al sistema mediante autenticación fuerte con certificado digital.

2.3. Identificación y autenticación de solicitudes de renovación

2.3.1. Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, el operador o personal autorizado de la Autoridad de Registro se comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la Persona natural identificada en el certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son:

- El uso del código "CRE" o "ERC" relativo al certificado anterior, o de otros métodos de autenticación personal, que consiste en información que sólo conoce la Persona natural identificada en el certificado, y que le permite renovar de forma automática su certificado, siempre que no se haya superado el plazo máximo legalmente establecido.
- El empleo del certificado vigente para su renovación y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la Persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa.

2.3.2. Identificación y autenticación de la solicitud de renovación

Antes de renovar un certificado, el operador o personal autorizado de la Autoridad de Registro se comprobará que la información empleada en su día para verificar la identidad y los restantes datos del suscriptor y de la Persona natural identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.

- El certificado fue revocado por emisión no autorizada por la Persona natural identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la Persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa.

2.4. Identificación y autenticación de la solicitud de revocación, suspensión o reactivación

UANATACA o un operador o personal autorizado de la Autoridad de Registro autentica las peticiones e informes relativos a la revocación, suspensión o reactivación de un certificado, comprobando que provienen de una persona autorizada.

La identificación de los suscriptores y/o firmantes en el proceso de revocación, suspensión o reactivación de certificados podrá ser realizada por:

- El suscriptor y/o firmante:
    - Identificándose y autenticándose mediante el uso del Código de Revocación (ERC o ERC) a través de la página web de UANATACA en horario 24x7.
    - Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la suspensión o revocación, a juicio de UANATACA y/o Autoridades de Registro.

- Las autoridades de registro de Uanataca: deberán identificar al firmante ante una petición de revocación, suspensión o reactivación según los propios medios que considere necesarios.

Cuando en horario de oficina el suscriptor desee iniciar una petición de revocación y existan dudas para su identificación, su certificado pasa a estado de suspensión.

3. Requisitos de operación del ciclo de vida de los certificados

3.1. Solicitud de emisión de certificado

3.1.1. Legitimación para solicitar la emisión

El solicitante del certificado, sea Persona natural o jurídica, debe firmar un contrato de prestación de servicios de certificación con UANATACA.

Asimismo, con anterioridad a la emisión y entrega de un certificado, debe existir una solicitud de certificados ya sea en el mismo contrato, en un documento específico de hoja de solicitud de certificados o ante la autoridad de registro.

Cuando el solicitante es una persona distinta al suscriptor, debe existir una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por dicho solicitante en nombre propio en el caso de certificados para Persona natural, o bien en nombre del suscriptor en el caso de que el suscriptor sea la por entidad, empresa u organización de derecho público o privado.

3.1.2. Procedimiento de alta y responsabilidades

UANATACA recibe solicitudes de certificados, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se instrumentan mediante un formulario en formato papel o electrónico, de manera individual o por lotes, o mediante la conexión con bases de datos externas, o a través de una capa de *Web Services* cuyo destinatario es UANATACA. En el caso de certificados cuyo suscriptor sea una entidad, empresa u organización de derecho público o privado que actúe como una Autoridad de Registro de UANATACA, podrá gestionar directamente las solicitudes accediendo a los sistemas informáticos de UANATACA y generar los certificados correspondientes para la propia entidad, empresa u organización o para sus miembros.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la Persona natural identificada en el certificado.También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la Persona natural identificada en el certificado.

3.2. Procesamiento de la solicitud de certificación

3.2.1. Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, UANATACA se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, UANATACA verifica la información proporcionada, según lo descrito en la DPC de UANATACA en su apartado 3.2

La documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 10 años desde la expiración del certificado, incluso en caso de pérdida anticipada de vigencia por revocación.

3.2.2. Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, UANATACA debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Autoridad de Certificación, de las Autoridades de Registro o de los suscriptores, UANATACA denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, la solicitud quedará denegada definitivamente.

Se notifica al solicitante la aprobación o denegación de la solicitud.

Podrá automatizarse los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

3.2.3. Plazo para resolver la solicitud

Las solicitudes de certificados se atienden por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

3.3. Emisión del certificado

3.3.1. Acciones de la CA durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, UANATACA:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.

- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo de las claves por parte del usuario, no pudiendo la propia UANATACA o sus Autoridades de Registro deducirlas o utilizarlas en ningún modo.

3.3.2. Notificación de la emisión al suscriptor

UANATACA notifica la emisión del certificado al suscriptor y/o a la Persona natural identificada en el certificado y el método de generación/descarga.

3.4. Entrega y aceptación del certificado

3.4.1. Responsabilidades de la CA

Durante este proceso, el operador o personal autorizado de la Autoridad de Registro UANATACA debe realizar las siguientes actuaciones:

- Acreditar definitivamente la identidad de la Persona natural identificada en el certificado, de acuerdo con lo establecido en la DPC en las secciones 2.2.2 y 2.2.3.
- Disponer del Contrato de Prestación de Servicios de Certificación debidamente firmado por el Suscriptor.
- Entregar la hoja de entrega y aceptación del certificado a la Persona natural identificada en el certificado con los siguientes contenidos mínimos:
    - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del Proveedor de Servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades.

- Información acerca del certificado.
- Reconocimiento, por parte del firmante, de recibir el certificado y/o los mecanismos para su generación/descarga y la aceptación de los citados elementos.
- Régimen de obligaciones del firmante.
- Responsabilidad del firmante.
- Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4 de la Declaración de Prácticas de Certificación.
- La fecha del acto de entrega y aceptación.

Toda esta información podrá incluirse en el propio Contrato de Prestación de Servicios de Certificación. Dicho lo cual, cuando se produzca la firma del Contrato Prestación de Servicios de Certificación por el Suscriptor, se entenderá perfeccionada la entrega y aceptación del certificado.

- Obtener la firma de la persona identificada en el certificado.

Las Autoridades de Registro son las encargadas de realizar estos procesos, debiendo registrar documentalmente los anteriores actos y conserva los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a UANATACA, así como los originales cuando UANATACA precise de acceso a los mismos.

3.4.2. Conducta que constituye aceptación del certificado

Cuando se haga entrega de la hoja de aceptación, la aceptación del certificado por la Persona natural identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación.

Cuando la generación y entrega del certificado se lleve a cabo a través del procedimiento automatizado definido por UANATACA, la aceptación del certificado por la Persona natural identificada en el mismo se produce mediante la firma del contrato de Prestación de Servicios de Certificación utilizando el propio certificado.

3.4.3. Publicación del certificado

UANATACA publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes y siempre que UANATACA disponga de la autorización de la Persona natural identificada en el certificado.

3.4.4. Notificación de la emisión a terceros

UANATACA no realiza ninguna notificación de la emisión a terceras entidades.

3.5. Uso del par de claves y del certificado

3.5.1. Uso por el firmante

UANATACA obliga a:

- Facilitar a UANATACA información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4
- Cuando el certificado funcione juntamente con un DCCF, reconocer su capacidad de producción de firmas electrónicas certificadas; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados.
- Comunicar a UANATACA, Autoridades de Registro y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2 de la DPC.

UANATACA obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un Proveedor de Servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de Proveedor de Servicios de certificación ni en ningún otro caso.

3.5.2. Uso por el subscriptor

3.5.2.1. Obligaciones del suscriptor del certificado

UANATACA obliga contractualmente al suscriptor a:

- Facilitar a la Autoridad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4 de la Declaración de Practicas de Certificación.
- Comunicar a UANATACA, Autoridades de Registro y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
    - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas naturales identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de las mismas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de UANATACA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del Proveedor de Servicios de certificación de UANATACA.

3.5.2.2. Responsabilidad civil del suscriptor de certificado

UANATACA obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.

- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un Proveedor de Servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de Proveedor de Servicios de certificación ni en ningún otro caso.

3.5.3. Uso por el tercero que confía en certificados

3.5.3.1. Obligaciones del tercero que confía en certificados

UANATACA informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas, producidas en un dispositivo seguro de creación de firma (DSCF) tienen la consideración legal de firmas electrónicas certificadas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.

- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de UANATACA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la UANATACA.

3.5.3.2. Responsabilidad civil del tercero que confía en certificados

UANATACA informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

3.6. Renovación de certificados

La renovación de los certificados exige la renovación de claves, por lo que debe atenderse a lo establecido en la sección 3.7 de la Declaración de Practicas de Certificación de UANATACA.

3.7. Renovación de claves y certificados

3.7.1. Causas de renovación de claves y certificados

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación.

Se consideran al menos dos posibilidades para la renovación de certificados:

- Proceso de renovación presencial, que se efectuará del mismo modo que la emisión de un nuevo certificado.
- Proceso de renovación online (a través de internet), que se detalla a continuación.

3.7.2. Procedimiento de renovación online de certificados

3.7.2.1. Circunstancias para la renovación online

Solamente se podrá proceder a la renovación online del certificado si se cumplen las condiciones siguientes:

- La Autoridad de Registro y/o UANATACA dispone del servicio de renovación online.
- El certificado con el que se firma la renovación esté vigente, es decir, no haya caducado, no esté revocado ni suspendido.

3.7.2.2. Quién puede solicitar la renovación online de un certificado

Cualquier firmante podrá pedir la renovación online de su certificado si se cumplen las circunstancias descritas en el punto anterior.

El firmante podrá formalizar su solicitud accediendo al servicio de renovación online de certificados en la página web de UANATACA.

3.7.2.3. Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, UANATACA aprobará la solicitud de renovación del certificado y proceder a su emisión y entrega.

UANATACA notifica al solicitante la aprobación o denegación de la solicitud.

UANATACA podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

3.7.2.4. Tramitación de las peticiones de renovación online

La solicitud de una renovación del certificado se realizará de acuerdo con lo siguiente:

- Cuando el certificado digital de un usuario esté próximo a caducar, UANATACA podrá enviar una o más notificaciones distribuidas en el tiempo, invitándole a su renovación.
- El firmante se conectará al servicio de renovación de la página web de UANATACA y procederá a la solicitud de renovación.
- El firmante firmará la renovación de su certificado válido.
- Se procederá a la generación del nuevo par de claves y generación e importación del certificado, respetando los siguientes condicionantes:
    - Protege la confidencialidad e integridad de los datos de registro de que dispone.
    - Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
    - Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
    - Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
    - Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
    - Indica la fecha y la hora en que se expidió un certificado.
    - Garantiza el control exclusivo del usuario sobre sus propias claves, no pudiendo la propia UANATACA o sus Autoridades de Registro deducirlas o utilizarlas.

3.7.2.5. Notificación de la emisión del certificado renovado

UANATACA notifica la emisión del certificado al suscriptor y a la Persona natural identificada en el certificado.

3.7.2.6. Conducta que constituye aceptación del certificado renovado

El certificado se considerará aceptado al firmar electrónicamente la renovación.

3.7.2.7. Publicación del certificado renovado

UANATACA publica el certificado renovado en el Depósito a que se refiere la sección 2.1 de la DPC, con los controles de seguridad pertinentes.

3.7.2.8. Notificación de la emisión a terceros

UANATACA no realiza notificación alguna de la emisión a terceras entidades.

3.8. Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 3.1, 3.2, 3.3 y 3.4 de la DPC.

3.9. Revocación, suspensión o reactivación de certificados

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible. Sólo los certificados de entidad final podrán ser suspendidos.

La reactivación de un certificado supone su paso de estado suspendido a estado activo.

3.9.1. Causas de revocación de certificados

Un certificado será revocado cuando concurre alguna de las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:
   a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
   b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
   c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

2) Circunstancias que afectan a la seguridad de la clave o del certificado:
   a) Compromiso de la clave privada, de la infraestructura o de los sistemas del Proveedor de Servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
   b) Infracción, por UANATACA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la Declaración de Prácticas de Certificación.
   c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
   d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
   e) El uso irregular del certificado por la Persona natural identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.

3) Circunstancias que afectan al suscriptor o a la Persona natural identificada en el certificado:
   a) Finalización de la relación jurídica de prestación de servicios entre UANATACA y el suscriptor.
   b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la Persona natural identificada en el certificado.
   c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.

e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.

f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.

g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 2.4 de la DPC.

4) Otras circunstancias:

a) La terminación del servicio de certificación de la Entidad de Certificación de UANATACA.

b) El uso del certificado que sea dañino y continuado para UANATACA. En este caso, se considera que un uso es dañino en función de los siguientes criterios:

- La naturaleza y el número de quejas recibidas.
- La identidad de las entidades que presentan las quejas.
- La legislación relevante vigente en cada momento.
- La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

3.9.2. Causas de suspensión de un certificado

Los certificados de UANATACA pueden ser suspendidos a partir de las siguientes causas:

- Cuando así sea solicitado por el suscriptor o la Persona natural identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al suscriptor o la Persona natural identificada en el certificado.
- La falta de uso del certificado durante un periodo prolongado de tiempo, conocido previamente.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, UANATACA tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

3.9.3. Causas de reactivación de un certificado

Los certificados de UANATACA pueden ser reactivados a partir de las siguientes causas:

- Cuando el certificado se encuentre en un estado de suspendido.
- Cuando así sea solicitado por el suscriptor o la Persona natural identificada en el certificado.

3.9.4. Quién puede solicitar la revocación, suspensión o reactivación

Pueden solicitar la revocación, suspensión o reactivación de un certificado:

- La persona identificada en el certificado.
- El suscriptor del certificado por medio responsable del servicio de certificación.

3.9.5. Procedimientos de solicitud de revocación, suspensión o reactivación

La entidad que precise revocación, suspensión o reactivación un certificado puede solicitarlo directamente a UANATACA o a la Autoridad de Registro del suscriptor o realizarlo él mismo a través del servicio online disponible en la página web de UANATACA. La solicitud de revocación, suspensión o reactivación deberá incorporar la siguiente información:

- Fecha de solicitud de la revocación, suspensión o reactivación.
- Identidad del suscriptor.
- Nombre y título de la persona que pide la revocación, suspensión o reactivación.
- Información de contacto de la persona que pide la revocación, suspensión o reactivación.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, por UANATACA, de acuerdo con los requisitos establecidos en la sección 2.4 de la DPCantes de proceder a la revocación, suspensión o reactivación.

El servicio de revocación, suspensión o reactivación se encuentra en la página web de UANATACA en la dirección: https://web.uanataca.com/sv.

En caso de que el destinatario de una solicitud de revocación, suspensión o reactivación por parte de una Persona natural identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a UANATACA.

La solicitud de revocación, suspensión o reactivación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la Persona natural identificada en el certificado, acerca del cambio de estado del certificado.

Tanto el servicio de gestión de revocación, suspensión o reactivación como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de UANATACA.

3.9.6. Plazo temporal de solicitud de revocación, suspensión o reactivación

Las solicitudes de revocación, suspensión o reactivación se remitirán de forma inmediata en cuanto se tenga conocimiento.

3.9.7. Plazo temporal de procesamiento de la solicitud de revocación, suspensión o reactivación

La revocación, suspensión o reactivación se producirá inmediatamente cuando sea recibida. Si se realiza a través de un operador, se ejecutará dentro del horario ordinario de operación de UANATACA o en su caso de la Autoridad de Registro. Si se realiza a través del servicio online, será inmediata.

3.9.8. Obligación de consulta de información de revocación o suspensión de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de UANATACA.

Las Listas de Revocación de Certificados se publican en el Depósito de la Entidad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- http://crl1.uanataca.com/public/pki/crl/CA1subordinada_SV.crl
- http://crl2.uanataca.com/public/pki/crl/CA1subordinada_SV.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

3.9.9. Frecuencia de emisión de listas de revocación de certificados (LRCs)

UANATACA emite una LRC al menos cada 24 horas.

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

3.9.10. Plazo máximo de publicación de LRCs

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

3.9.11. Disponibilidad de servicios de comprobación en línea de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de UANATACA, que se encuentra disponible las 24 horas de los 7 días de la semana en el web:

- http://www.uanataca.com/public/download/tsp_certificates/subordinate1_sv.crt

Para comprobar la última CRL emitida en cada CA se debe descargar:

- *Autoridad de Certificación Raíz (AUTORIDAD DE CERTIFICACIÓN RAIZ EL SALVADOR):*
  - http://crl1.firmaelectronica.minec.gob.sv/crl/arl_minec.crl
  - http://crl2.firmaelectronica.minec.gob.sv/crl/arl_minec.crl

- *Autoridad de Certificación Intermedia 1 (UANATACA EL SALVADOR CA1):*
  - http://crl1.uanataca.com/public/pki/crl/CA1subordinada_sv.crl
  - http://crl2.uanataca.com/public/pki/crl/CA1subordinada_sv.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de UANATACA, ésta deberá realizar sus mejores esfuerzos por asegurar

que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

UANATACA suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

3.9.12. Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

3.9.13. Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de UANATACA es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de UANATACA, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

3.9.14. Período máximo de un certificado digital en estado suspendido

El plazo máximo de un certificado digital en estado suspendido es indefinido hasta su caducidad.

4. Perfiles de certificados y listas de certificados revocados

4.1. Perfil de certificado

Todos los certificados emitidos bajo esta política cumplen con el estándar X.509 versión 3 y el RFC 3739 y los diferentes perfiles descritos en la norma EN 319 412.
La documentación relativa a los perfiles de la norma EN 319 412 puede solicitarse a UANATACA.

4.1.1. Número de versión

UANATACA emite certificados X.509 Versión 3

4.1.2. Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la página web de UANATACA (https://web.uanataca.com/sv).

De esta forma se permite mantener unas versiones más estables de la Declaración de Prácticas de Certificación y desligarlos de los frecuentes ajustes en los perfiles.

4.1.3. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

4.1.4. Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

4.1.5. Restricción de los nombres

Los nombres contenidos en los certificados están restringidos a “Distinguished Names” X.500, que son únicos y no ambiguos.

4.1.6. Identificador de objeto (OID) de los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1 de la DPC.

4.2. Perfil de la lista de revocación de certificados

4.2.1. Número de versión

Las CRL emitidas por UANATACA son de la versión 2.

4.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960.

5. Anexo I - Acrónimos

AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
RA	Autoridad de Registro
CP	Certificate Policy
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DSCF	Dispositivo Seguro de Creación de Firma
SSCD	Secure Signature Creation Device. Dispositivo Seguro de Creación de Firma
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol