POLÍTICA DE CERTIFICACIÓN

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	1
Fecha edición:	18/03/2024
Fichero:	PSC-3-PC_CER_UCO_v1.r1
Código	PSC-3-

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 18/03/2024	Nombre: Fabiola Ortega Fecha: 20/4/2024	Nombre: Elias Barzallo Fecha: 08/8/2024

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	Alejandro Grande	18/03/2024

Índice

1. Introducción

1.1. Presentación

Este documento constituye la Política de Certificación (PC) para la emisión de certificados digitales de Uanataca Colombia SAS, en adelante "UANATACA COLOMBIA"., de conformidad con la Ley 527 de 1999, Decreto Ley 019 de 2012 y demás normas y decretos reglamentarios aplicables a la prestación de servicios de certificación digital. Así como de los requisitos contenidos en la *CEA-3.0-07 Criterios Específicos De Acreditación Entidades De Certificación Digital* –vigente y establecido por el Organismo Nacional de Acreditación de Colombia – ONAC para la prestación de servicios de certificación digital.

Los certificados digitales en relación con las firmas electrónicas o digitales que se emiten serán conforme a lo siguiente:

- **De Persona natural:** El certificado digital de persona natural sirve para identificar a una persona natural, que permite su uso y firma para realizar todo tipo de trámites como Persona Natural sin vinculación a ninguna empresa o entidad.
    - Certificado de Persona Natural en tarjeta o token
    - Certificado de Persona Natural en HSM centralizado
- **De Profesional titulado:** Son certificados que permiten identificar al suscriptor y su título profesional y le permite al Suscriptor firmar en su propio nombre e interés.
    - Certificado Profesional titulado en tarjeta o token
    - Certificado de Profesional titulado en HSM centralizado
- **De Persona Natural - Miembro de Empresa u organización**: Son certificados que permiten identificar al Suscriptor y firmante, este último también podrá firmar como Persona Natural vinculada a una empresa o entidad (persona jurídica), ya sea como empleado, asociado, colaborador, cliente, etc.
    - Certificado de persona natural miembro de Empresa en tarjeta o token

- Certificado de persona natural miembro de Empresa en HSM Centralizado

- **De Representante:** Son certificados que permiten identificar y firmar como Persona Natural vinculada a una empresa o entidad (Persona Jurídica), como su representante legal. Por lo que el titular del certificado se identifica no únicamente como persona física, sino que añade su cualificación como representante legal o apoderado de la misma.

  - Certificado de Representante en tarjeta o token
  - Certificado de Representante en HSM centralizado

- **De Función Pública:** Son certificados emitidos a una Persona Natural vinculada al servicio de la Administración Pública y se identifica en su condición de funcionario público o de particular en ejercicio de una función pública. En concreto, el certificado identifica al funcionario público o de particular en ejercicio de una función pública, la identidad de la entidad pública y la vinculación que la persona natural tiene con esta. Solamente, otorgará a su titular las facultades que posee por el desempeño de sus competencias, de su trabajo o de los servicios prestados para la entidad pública correspondiente. Este certificado contiene en sus campos la referencia al cargo o puesto y al área o unidad de destino, pero no informa acerca de la existencia de poderes de representación.

  - Certificado de Función Pública en tarjeta o token
  - Certificado de Función Pública en HSM centralizado

- **De Persona jurídica – sello de empresa:** Se trata de un certificado digital emitido a favor de una Persona jurídica (entidad, empresa, etc.) y podrá ser utilizado en la identificación, autenticación y gestión concerniente dentro del giro normal de sus negocios.

  - Certificado de Persona Jurídica Sello Electrónico en tarjeta o token
  - Certificado de Persona Jurídica Sello Electrónico en HSM centralizado

- **De facturación electrónica:** Se trata de un certificado digital emitido a favor de una Persona jurídica (entidad, empresa, etc.) o natural para realizar la facturación electrónica atendiendo la necesidad de las empresas y/o personas naturales que buscan la seguridad del certificado para la emisión de las facturas electrónicas, entre otros documentos y podrá ser utilizado en la identificación, autenticación y gestión concerniente dentro del giro normal de sus negocios.

    - Certificado para Facturación Electrónica de Persona Natural en tarjeta o token.
    - Certificado para Facturación Electrónica de Persona Natural en HSM centralizado.
    - Certificado para Facturación Electrónica de Persona Jurídica en tarjeta o token
    - Certificado para Facturación Electrónica de Persona Jurídica en HSM centralizado.

- **De Sello de Tiempo:** 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. Certifica la fecha y hora exacta en las que se produjo la firma del documento tomando la referencia horaria en la República de Colombia.

    - Certificado de Estampado Cronológico (sello de tiempo)

1.2. Nombre del documento e identificación

Este documento es la "Política de Certificación de UANATACA" identificándose a los efectos bajo el ***OID 1.3.6.1.4.1.47286.201.0.2.***

Número OID	Tipo de certificados
1.3.6.1.4.1.47286.201.1.1	**Persona Natural**
1.3.6.1.4.1.47286.201.1.1.1	*Certificado de Persona Natural ciudadano en tarjeta o token*
1.3.6.1.4.1.47286. 201.1.1.2	*Certificado de Persona Natural ciudadano en HSM centralizado*
1.3.6.1.4.1.47286.201.1.2	**Profesional titulado**

1.3.6.1.4.1.47286.201.1.2.1	*Certificado de persona natural profesional titulado en tarjeta o token*
1.3.6.1.4.1.47286.201.1.2.2	*Certificado de persona natural profesional titulado en HSM centralizado*
1.3.6.1.4.1.47286.201.1.3	**Persona Natural - Miembro de Empresa u organización**
1.3.6.1.4.1.47286.201.1.3.1	*Certificado de Persona Natural miembro de Empresa u organización en tarjeta o token*
1.3.6.1.4.1.47286.201.1.3.2	*Certificado de Persona Natural miembro de Empresa u organización en HSM Centralizado*
1.3.6.1.4.1.47286.201.1.4	**Persona Natural Representante de Persona Jurídica**
1.3.6.1.4.1.47286.201.1.4.1	*Certificado de Persona Natural Representante de Persona Jurídica en tarjeta o token*
1.3.6.1.4.1.47286.201.1.4.2	*Certificado de Persona Natural Representante de Persona Jurídica en HSM centralizado*
1.3.6.1.4.1.47286.201.1.6	**De función Pública**
1.3.6.1.4.1.47286.201.1.6.1	*Certificado de Persona Natural Función Pública en tarjeta o token*
1.3.6.1.4.1.47286.201.1.6.2	*Certificado de Persona Natural Función Pública en HSM centralizado*
1.3.6.1.4.1.47286.201.1.7	**Persona Jurídica - Sello De Empresa**
1.3.6.1.4.1.47286.201.1.7.1	*Certificado de Sello Electrónico en tarjeta o token*
1.3.6.1.4.1.47286.201.1.7.2	*Certificado de Sello Electrónico en HSM Centralizado*
1.3.6.1.4.1.47286.201.1.8	**Persona Natural - Facturación Electrónica**
1.3.6.1.4.1.47286.201.1.8.1	*Certificado para Facturación Electrónica de Persona Natural en tarjeta o token*
1.3.6.1.4.1.47286.201.1.8.2	*Certificado para Facturación Electrónica de Persona Natural en HSM centralizado*
1.3.6.1.4.1.47286.201.1.9	**Persona Jurídica - Facturación Electrónica**
1.3.6.1.4.1.47286.201.1.9.1	*Certificado para Facturación Electrónica de Persona Jurídica en tarjeta o token*

1.3.6.1.4.1.47286.201.1.9.2	*Certificado para Facturación Electrónica de Persona Jurídica en HSM CENTRALIZADO*
1.3.6.1.4.1.47286.201.1.10	**Estampado Cronológico** *(De sello de Tiempo Electrónico)*

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.

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. Entidad de Certificación Digital

La Entidad de Certificación Digital o indistintamente el Proveedor de Servicios electrónicos de certificación es la persona autorizada y facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

UANATACA COLOMBIA en su papel de Entidad de Certificación Digital (ECD) abierta, es la persona jurídica privada que presta indistintamente en el país servicios y actividades inherentes a la certificación digital, que actúa de acuerdo con la legislación de Colombia, conformada por la Ley 527 de 1999, el Decreto Ley No. 019 de 2012, Decreto Único del Sector Comercio, Industria y Turismo – DURCSIT, 1074 de 2015, 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 319 412, y los mejores estándares internacionales, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

UANATACA COLOMBIA, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante el ONAC, a fin de lograr y mantener la acreditación correspondiente.

Asimismo, UANATACA COLOMBIA, en su papel de autoridad de certificación, emite y revoca los certificados, presta los servicios de comprobación de revocación mediante CRL (*Certificate Revocation List*) y OCSP (*Online Certificate Status Protocol*).

La jerarquía de certificación asociada de UANATACA COLOMBIA según se encuentra especificado en la Declaración de Prácticas de Certificación para la emisión de certificados.

1.3.1.1. UANATACA ROOT 2016

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave pública ha sido auto firmado. Su función es firmar el certificado de las otras CA pertenecientes a la Jerarquía de Certificación.

Asimismo, la CA Raíz de UANATACA podrá emitir certificados de otras CA Subordinadas del grupo y/o que sea de su interés, lo cual quedará reflejado en las correspondientes DPC de estas CA Subordinadas. Por tanto, UANATACA ROOT 2016 también podrá ser la CA Raíz de otras PKI del grupo y/o aquellas en las que persiga algún interés particular.

Datos de identificación:

CN:	UANATACA ROOT 2016
Huella digital:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 ad
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Lunes, 11 de marzo de 2041
Longitud de clave RSA:	4.096 bits

1.3.1.2. UANATACA CA1 2021

Se trata de la Autoridad de Certificación Subordinada (CA Sub) dentro de la jerarquía que emite los certificados a las entidades finales y los certificados de estampado cronológico (sellado de tiempo), y cuyo certificado de clave pública ha sido firmado digitalmente por UANATACA ROOT 2016.

Datos de identificación:

CN:	UANATACA CA1 2021
Huella digital:	a1 db ea 6c 10 7a a3 e8 1e 16 c9 af 8e 55 7f ed 3d 90 cf 98
Válido desde:	jueves, 3 de junio de 2021
Válido hasta:	sábado, 3 de junio de 2034
Longitud de clave RSA:	4.096 bits

1.3.1.3. UANATACA CA2 2021

Se trata de la entidad de certificación Subordinada (CA Sub) dentro de la jerarquía que emite los certificados a las entidades finales y los certificados de estampado cronológico (sellado de tiempo), y cuyo certificado de clave pública ha sido firmado digitalmente por UANATACA ROOT 2016.

Datos de identificación:

CN:	UANATACA CA2 2021
Huella digital:	2d 35 17 27 f4 5b 01 2a a4 88 03 4b db 01 1c da 4f 61 a4 2e
Válido desde:	jueves, 3 de junio de 2021
Válido hasta:	sábado, 3 de junio de 2034
Longitud de clave RSA:	4.096 bits

1.3.2. Autoridad de Registro

La Autoridad de Registro (RA) son las encargadas de recibir las solicitudes relacionadas con certificación digital, para registrar las peticiones que hagan los solicitantes para

obtener un certificado, comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones, enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas.

Una Autoridad de Registro (RA) de UANATACA COLOMBIA 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.

Teniendo en cuenta las funciones de la RA, UANATACA COLOMBIA formalizará contractualmente las relaciones entre ella misma y cada una de las entidades que actúen como Autoridad de Registro de UANATACA COLOMBIA garantizando que las funciones de comprobación de veracidad, y corrección de datos que aportan los usuarios, así como el envío a una CA de las peticiones cumplen con los requisitos exigidos en la CEA-3.0-07 siendo responsable total de las actividades realizadas por terceros debido a que mantiene como función propia de UANATACA COLOMBIA

Podrán actuar como RA de UANATACA COLOMBIA:

- Cualquier entidad autorizada por UANATACA COLOMBIA.
- UANATACA COLOMBIA directamente.

La entidad que actúe como Autoridad de Registro de UANATACA COLOMBIA podrá autorizar a una o varias personas como Operador de la RA para operar con el sistema de emisión de certificados de UANATACA COLOMBIA 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 COLOMBIA deberá autorizar de manera expresa dicho acuerdo de colaboración.

También podrán ser Autoridades de Registro sujetas a esta Declaración de Prácticas de Certificación de UANATACA COLOMBIA, 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 COLOMBIA las siguientes:

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

1.3.3.1. Suscriptores del servicio de certificación

A la persona a cuyo nombre la Entidad de Certificación Digital UANATACA COLOMBIA expide un certificado digital, se le conoce como el suscriptor del servicio de certificación.

A los efectos, pueden ser las personas naturales, empresas, entidades, corporaciones u organizaciones (directamente o a través de un tercero) que desplegará su uso en el ámbito personal, corporativo empresarial u organizativo, entre otros usos, los cuales se encuentran debidamente identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio 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. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio de certificación digital es, por tanto, el cliente de la entidad de certificación digital (ECD), de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por la entidad de certificación digital, 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 digitales, en especial ETSI EN 319 411.

1.3.3.2. Firmantes

Los firmantes son las personas naturales que poseen de forma exclusiva las claves de firma para autenticación y/o firma digital; 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 función pública.

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 la Entidad de certificación digital, 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 digital según corresponda, 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 digital 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 digitales a través de certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, dicha comprobación, se realiza a través del acceso a las listas de revocación (CRL) o a

servicios de consulta en línea (OCSP) tal y como se establece, en esta 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

Los proveedores de Servicios de Infraestructura de Clave Pública son terceros que prestan su infraestructura y/o servicios tecnológicos a la Entidad de Certificación Digital (ECD) para el óptimo desarrollo de sus operaciones, a su vez, garantizan la continuidad del servicio a las entidades finales, suscriptores y firmantes durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Que entre "Uanataca Colombia SAS" 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 COLOMBIA.

Así mismo, Uanataca, S.A., pone a disposición de UANATACA COLOMBIA el personal técnico necesario para el correcto desempeño de las funciones fiables propias de una Entidad de Certificación Digital (ECD).

Dicho lo cual, Uanataca, S.A., se configura como el proveedor de servicios de Infraestructura para servicios de certificación y provee sus servicios tecnológicos a UANATACA COLOMBIA, para que éste pueda llevar a cabo los servicios inherentes como una Entidad de Certificación Digital (ECD), garantizando en todo momento la continuidad de los servicios en las condiciones y bajo los requisitos exigidos por la normativa.

En relación con lo anterior, se informa que Uanataca, S.A., a nivel internacional es un **Proveedor de Servicios de Certificación Europeo** (Entidad de Certificación Digital) 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

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

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

En razón a lo anterior, se indican los datos de identificación del proveedor de servicios de infraestructura tecnológica de clave pública para la provisión de los servicios y actividades de certificación digital por parte de UANATACA COLOMBIA.

Nombre (Razón Social): UANATACA SA
NIF (NIT): A66721499
Datos de Inscripción en Registro Mercantil (Número de matrícula de Cámara de Comercio Colombia): Registro Mercantil de Barcelona, Hoja B-482242 Tomo 45264 Folio 12
Consulta el Estado de vigencia en el Registro Mercantil (Estado activo en Cámara de Comercio de Colombia) en: https://sede.registradores.org/site/mercantil buscando por sociedad introduciendo el NIF A66721499
Domicilio social y correspondencia: Avenida Meridiana Núm. 350 P.3 Barcelona (08027)
Teléfono: (+34) 935 27 22 90
Email: info@uanataca.com
Web: https://web.uanataca.com/es/

1.4. Uso de los certificados

Los certificados emitidos por UANATACA podrán usarse en los términos establecidos en la Declaración de Prácticas de Certificación para la emisión de certificados, en la presente Política de Certificación y en lo establecido en la legislación vigente al respecto.

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/co/politicas-practicas

1.4.1.1. Certificado de Persona natural ciudadano en tarjeta o token

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.1.1**. Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, 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 la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Natural ante servicios y aplicaciones informáticas.
- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o Common Criteria EAL 2, de conformidad con lo establecido en la normativa nacional.

Garantiza únicamente la identidad de la persona natural firmante y permite la generación de la “firma digital” entendido como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma manuscrita, 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 ciudadano en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.1.2**. Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, 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 la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 19 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:

- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Natural ante servicios y aplicaciones informáticas.
- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o Common Criteria EAL 2, de conformidad con lo establecido en la normativa nacional.

Garantiza únicamente la identidad de la persona natural firmante y permite la generación de la "firma digital", es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma manuscrita, 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 titulado en tarjeta o token

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.2.1**. Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, 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 la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Natural como profesional titulado en el ámbito de su actividad ante servicios y aplicaciones informáticas.

- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o Common Criteria EAL 2, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad de la persona natural titular del certificado, así como su condición de profesional titulado (vinculación con un título profesional). Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual en el ámbito de su profesión permitiendo la generación de la "firma digital", es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma manuscrita, 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 profesional titulado en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.2.2**. Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2., 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 la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 19 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 19 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Natural como profesional titulado en el ámbito de su actividad ante servicios y aplicaciones informáticas.
- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 *Level* 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad de la persona natural titular del certificado, así como su condición de profesional titulado (vinculación con un título profesional). Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual en el ámbito de su profesión permitiendo la generación de la “firma digital”, es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma manuscrita, 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 miembro de empresa u organización en tarjeta o token

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.3.1.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado emitido en dispositivo seguro de creación de firma es un certificado de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:

- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Natural como miembro de una entidad o persona jurídica en el ámbito de su actividad.
- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y firmante, certificando la vinculación de la persona natural a una entidad, quien actúa como suscriptor y descrita en el campo "O" (Organization), con ocasión a la relación y/o funciones que, como empleado, asociado, colaborador, etc., ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual,

permitiendo la generación de la "firma digital" es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma manuscrita, 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 miembro de empresa u organización en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.3.2.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, 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 la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Natural como miembro de una entidad o persona jurídica en el ámbito de su actividad.

- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y firmante, certificando la vinculación de la persona natural a una entidad, quien actúa como suscriptor y descrita en el campo "O" (Organization), con ocasión a la relación y/o funciones que, como empleado, asociado, colaborador, etc., ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual, permitiendo la generación de la "firma digital" es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

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 persona natural representante de persona jurídica en tarjeta o token

Este certificado dispone del OID **1.3.6.1.4.1.47286.201.1.4.1.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado de representante de persona jurídica es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Natural como representante legal de una entidad o persona jurídica en el ámbito de su actividad.
- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

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 digital” es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma manuscrita, 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

1.4.1.8. Certificado de persona natural representante de persona jurídica en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.4.2.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado de representante de persona jurídica es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:

- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una persona natural como representante legal de una entidad o persona jurídica en el ámbito de su actividad.
- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

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 digital” es decir, un valor

numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma manuscrita, 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

1.4.1.9. Certificado de persona natural función pública en token o tarjeta

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.6.1.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2, lo cual se declara en el certificado. Este certificado de función pública es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Natural como funcionario público o particular que ejerce una función pública en el ámbito de su actividad.

- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una Institución descrita en el campo "O" (Organization) que pertenece a la administración pública, en virtud del rango de funcionario público y/o que presta una función de carácter público, permite la generación de la "firma digital" es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma manuscrita, 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

1.4.1.10. Certificado de persona natural función pública en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.6.2.** Es un certificado que se emite para la firma digital, de acuerdo con la política de certificación NCP+ con el OID

0.4.0.2042.1.2, lo cual se declara en el certificado. Este certificado de función pública es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Natural como funcionario público o particular que ejerce una función pública en el ámbito de su actividad.
- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una Institución descrita en el campo "O" (Organization) que pertenece a la administración pública, en virtud del rango de funcionario público y/o que presta una función de carácter público, permite la generación de la "firma digital" es decir, un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación conforme a los términos del numeral c del artículo segundo de la ley 527 de 1999.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma manuscrita, 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

1.4.1.11. Certificado de Sello Electrónico en tarjeta o token (Persona Jurídica)

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.7.1**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado de sello electrónico es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Jurídica en el ámbito de su actividad.
- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad de la entidad suscriptora vinculada. 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

1.4.1.12. Certificado de Sello Electrónico en HSM centralizado (Persona Jurídica)

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.7.2**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado de sello electrónico es emitido en un dispositivo seguro de creación de firma de acuerdo con lo establecido en la legislación de la República de Colombia, conformada por la Ley 527 de 1999, Decreto-ley 019 de 2012, decreto 333 de 2014, que reglamenta el artículo 160 de Decreto-ley 019 de 2012, el Decreto único reglamentario del Sector Comercio, Industria y Turismo No. 1074 de 2015, entre otros.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar a una Persona Jurídica en el ámbito de su actividad.
- **Firma Digital**: Las firmas digitales realizadas con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad de la entidad suscriptora vinculada. 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

1.4.1.13. Certificado para facturación electrónica de persona natural en tarjeta o token

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.8.1**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado es exclusivo para facturación electrónica atendiendo a la necesidad de las personas naturales que buscan la seguridad del certificado para la emisión de facturas electrónicas. Certificado exclusivo para la firma digital de facturas electrónicas, notas crédito, notas débito, soportes de pago de nómina electrónica, notas de ajuste del documento soporte de pago de nómina electrónica y otros documentos producto de los procesos de las plataformas desatendidas de los proveedores tecnológicos aprobados por la DIAN, el sistema de facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad. Uso exclusivo para la facturación electrónica y otras actividades relacionadas de la persona natural suscriptora identificada en el certificado y, por tanto, cualquier otra operación no autorizada tendrá la consideración de usos indebidos.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar al facturador electrónico dentro del ámbito de su actividad, únicamente con el firmado digital de las facturas que este expida, en cumplimiento de sus obligaciones establecidas por el Decreto 2241 de 2015, por el cual se reglamentan las condiciones de expedición e interoperabilidad de la factura electrónica con fines de masificación y control fiscal.
- **Firma Digital**: Las firmas digitales realizadas para emisor de factura electrónica, notas débito, soporte de pago de nómina electrónica con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

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

1.4.1.14. Certificado para facturación electrónica de persona natural en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.8.2**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado es exclusivo para facturación electrónica atendiendo a la necesidad de las personas naturales que buscan la seguridad del certificado para la emisión de facturas electrónicas. Certificado exclusivo para la firma digital de facturas electrónicas, notas crédito, notas débito, soportes de pago de nómina electrónica, notas de ajuste del documento soporte de pago de nómina electrónica y otros documentos producto de los procesos de las plataformas desatendidas de los proveedores tecnológicos aprobados por la DIAN, el sistema de facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad. Uso exclusivo para la facturación electrónica y otras actividades relacionadas de la persona natural suscriptora identificada en el certificado y, por tanto, cualquier otra operación no autorizada tendrá la consideración de usos indebidos.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar al facturador electrónico dentro del ámbito de su actividad, únicamente con el firmado digital de las facturas que este expida, en cumplimiento de sus obligaciones establecidas por el Decreto 2241 de 2015, por el cual se reglamentan las condiciones de expedición e interoperabilidad de la factura electrónica con fines de masificación y control fiscal.

- **Firma Digital**: Las firmas digitales realizadas para emisor de factura electrónica, notas débito, soporte de pago de nómina electrónica con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

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

1.4.1.15. Certificado para facturación electrónica de persona jurídica en tarjeta o token

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.9.1**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado es exclusivo para facturación electrónica atendiendo a la necesidad de las personas jurídicas que buscan la seguridad del certificado para la emisión de facturas electrónicas. Certificado exclusivo para la firma digital de facturas electrónicas, notas crédito, notas débito, soportes de pago de nómina electrónica, notas de ajuste del documento soporte de pago de nómina electrónica y otros documentos producto de los procesos de las plataformas desatendidas de los proveedores tecnológicos aprobados por la DIAN, el sistema de facturación gratuita de la DIAN y la plataforma RADIAN, en

cumplimiento de los anexos técnicos emitidos por dicha entidad. Uso exclusivo para la facturación electrónica y otras actividades relacionadas de la entidad suscriptora citada identificada en el certificado y, por tanto, cualquier otra operación no autorizada tendrá la consideración de usos indebidos.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar al facturador electrónico dentro del ámbito de su actividad, únicamente con el firmado digital de las facturas que este expida, en cumplimiento de sus obligaciones establecidas por el Decreto 2241 de 2015, por el cual se reglamentan las condiciones de expedición e interoperabilidad de la factura electrónica con fines de masificación y control fiscal.
- **Firma Digital**: Las firmas digitales realizadas para emisor de factura electrónica, notas débito, soporte de pago de nómina electrónica con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio,

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

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

1.4.1.16. Certificado para facturación electrónica de persona jurídica en HSM centralizado

Este certificado dispone del **OID 1.3.6.1.4.1.47286.201.1.9.2**. Es un certificado que se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2. Este certificado es exclusivo para facturación electrónica atendiendo a la necesidad de las personas jurídicas que buscan la seguridad del certificado para la emisión de facturas electrónicas. Certificado exclusivo para la firma digital de facturas electrónicas, notas crédito, notas débito, soportes de pago de nómina electrónica, notas de ajuste del documento soporte de pago de nómina electrónica y otros documentos producto de los procesos de las plataformas desatendidas de los proveedores tecnológicos aprobados por la DIAN, el sistema de facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad. Uso exclusivo para la facturación electrónica y otras actividades relacionadas de la entidad suscriptora citada identificada en el certificado y, por tanto, cualquier otra operación no autorizada tendrá la consideración de usos indebidos.

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.

Pueden ser utilizados con los siguientes propósitos:
- **Autenticación de identidad**: El certificado puede utilizarse para identificar al facturador electrónico dentro del ámbito de su actividad, únicamente con el firmado digital de las facturas que este expida, en cumplimiento de sus obligaciones establecidas por el Decreto 2241 de 2015, por el cual se reglamentan las condiciones de expedición e interoperabilidad de la factura electrónica con fines de masificación y control fiscal.
- **Firma Digital**: Las firmas digitales realizadas para emisor de factura electrónica, notas débito, soporte de pago de nómina electrónica con este tipo de certificados ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio

Funciona con dispositivos seguros de creación de firma que ostenten como mínimo las certificaciones en estándares criptográficos FIPS 140-2 Level 3 o *Common Criteria* EAL 2, de conformidad con lo establecido en la normativa nacional.

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

1.4.2. 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.

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

Se puntualiza la prohibición de utilizar la certificación digital de manera que contravenga la ley, documentos relacionados con el servicio de certificación u ocasione mala reputación para la Entidad de Certificación Digital de UANATACA COLOMBIA. Lo que a su vez implica, que no debe monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica del ONAC y de la ECD UNATACA COLOMBIA; así como comprometer intencionadamente la seguridad de la Jerarquía del ONAC y la Entidad de Certificación

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 COLOMBIA.

El empleo de los certificados digitales en operaciones que contravienen esta Política de Certificación, la 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 COLOMBIA, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

UANATACA COLOMBIA 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 COLOMBIA 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 Política de Certificación, en la 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.509 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 campos de **DN** del titular del certificado referentes a Nombre y Apellidos y/o a nombre o razón social serán idénticos a los datos que consten en la cédula de Ciudadanía, Cédula de Extranjería o Pasaporte y/o en el Certificado de existencia y representación legal en Cámara de Comercio y/o Registro único Tributario (o documentos equivalentes)

Los nombres contenidos en los certificados son los siguientes:

2.1.1.1. Certificado de persona natural ciudadano en tarjeta o token

Country Name (C)	CO
Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del SUSCRIPTOR codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL SUSCRIPTOR
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

2.1.1.2. Certificado de persona natural ciudadano en HSM centralizado

Country Name (C)	CO
Surname	Apellidos del Suscriptor (como consta en el documento de identificación)

Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del SUSCRIPTOR codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL SUSCRIPTOR
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

2.1.1.3. Certificado de persona natural profesional titulado en tarjeta o token

Country Name (C)	**CO**
Organization Name (O)	Se especificará el nombre de la entidad habilitante (Emisor de la tarjeta profesional o entidad/institución educativa que otorga el título)
Title	Se especificará el título o especialidad del suscriptor y el número de profesional si dispone. (Ejemplo: ABOGADO - NUMERO DE PROFESIONAL)
Surname	Apellidos del suscriptor (como consta en el documento de identificación)
Given Name	Nombre del suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	Nombre y apellido del Suscriptor + Título (Ejemplo: "Given name" + "Surname" + "Title")
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

2.1.1.4. Certificado de persona natural profesional titulado en HSM centralizado

Country Name (C)	CO
Organization Name (O)	Se especificará el nombre de la entidad habilitante (Emisor de la tarjeta profesional o entidad/institución educativa que otorga el título)
Title	Se especificará el título o especialidad del suscriptor y el número de profesional si dispone. (Ejemplo: ABOGADO - NUMERO DE PROFESIONAL)
Surname	Apellidos del suscriptor (como consta en el documento de identificación)
Given Name	Nombre del suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	Nombre y apellido del Suscriptor + Título (Ejemplo: "Given name" + "Surname" + "Title")
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

2.1.1.5. Certificado de persona natural miembro de empresa u organización en tarjeta o token

Country Name (C)	CO
Organizational Unit Name (OU)	Se especificará el Departamento al que pertenece el Firmante o el tipo de vinculación con la Empresa
Organization Name (O)	Se especificará el nombre de la Empresa u Organización
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: "VATCO-00000")
Title	Se especificará el nombre del título o puesto que la persona ocupa en la Empresa u Organización
Surname	Apellidos del firmante (como consta en el documento de identificación)
Given Name	Nombre del firmante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo ("IDCCO-[CC]" o "PASCO-[PASAPORTE]")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad a la que está vinculado el firmante

2.1.1.6. Certificado de persona natural miembro de empresa u organización en HSM centralizado

Country Name (C)	CO
Organizational Unit Name (OU)	Se especificará el Departamento al que pertenece el Firmante o el tipo de vinculación con la Empresa
Organization Name (O)	Se especificará el nombre de la Empresa u Organización
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: "VATCO-00000")
Title	Se especificará el nombre del título o puesto que la persona ocupa en la Empresa u Organización
Surname	Apellidos del firmante (como consta en el documento de identificación)
Given Name	Nombre del firmante (como consta en el documento de identificación)

Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad a la que está vinculado el firmante

2.1.1.7. Certificado de persona natural representante de persona jurídica en tarjeta o token

Country Name (C)	CO
Organization Name (O)	Nombre de la organización de la que el firmante es representante
Organizational Unit Name (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
Title	REPRESENTANTE LEGAL
Surname	Apellidos del representante (como consta en el documento de identificación)
Given Name	Nombre del representante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la persona jurídica a la que está vinculado el firmante

2.1.1.8. Certificado de persona natural representante de persona jurídica en HSM centralizado

Country Name (C)	CO
Organization Name (O)	Nombre de la organización de la que el firmante es representante
Organizational Unit Name (OU)	Unidad de la Organización a la que está vinculado el firmante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
Title	REPRESENTANTE LEGAL
Surname	Apellidos del representante (como consta en el documento de identificación)

Given Name	Nombre del representante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la persona jurídica a la que está vinculado el firmante

2.1.1.9. Certificado de persona natural función pública en tarjeta o token

Country Name (C)	CO
Organizational Unit Name (OU) –	Se especificará el 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 institución a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
Title	Se especificará el cargo o puesto que la persona ocupa en la Institución
Surname	Apellidos del firmante (como consta en el documento de identificación)
Given Name	Nombre del firmante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la institución

2.1.1.10. Certificado de persona natural función pública en HSM centralizado

Country Name (C)	CO
Organizational Unit Name (OU) –	Se especificará el 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 institución a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: "VATCO-00000")
Title	Se especificará el cargo o puesto que la persona ocupa en la Institución
Surname	Apellidos del firmante (como consta en el documento de identificación)
Given Name	Nombre del firmante (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo ("IDCCO-[CC]" o "PASCO-[PASAPORTE]")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la institución

2.1.1.11. Certificado de Sello Electrónico en tarjeta o token

Country Name (C)	CO
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 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: "VATCO-00000")
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad

2.1.1.12. Certificado de Sello Electrónico en HSM centralizado

Country Name (C)	CO
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 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad

2.1.1.13. Certificado para facturación electrónica de persona natural en tarjeta o token

Country Name (C)	País de residencia o nacionalidad del Suscriptor
Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del Suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	Certificado de facturación electrónica de [Nombre del Suscriptor] (Ejemplo "Certificado de facturación electrónica de + [Given Name] + [Surname])
Description	Número de documento de identificación del Suscriptor + digito de verificación (sin puntos) (Ejemplo: [Núm. Documento de identificación del Suscriptor] + "digito de verificación").
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

2.1.1.14. Certificado para facturación electrónica de persona natural en HSM centralizado

Country Name (C)	País de residencia o nacionalidad del Suscriptor
Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
Serial Number	Número de documento de identificación del Suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
Common Name	Certificado de facturación electrónica de [Nombre del Suscriptor] (Ejemplo "Certificado de facturación electrónica de + [Given Name] + [Surname])
Description	Número de documento de identificación del Suscriptor + digito de verificación (sin puntos) (Ejemplo: [Núm. Documento de identificación del Suscriptor] + "digito de verificación").
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

2.1.1.15. Certificado para facturación electrónica de persona jurídica en tarjeta o token

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 (área en la empresa que hará uso del certificado (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: “VATCO-[NIT-DE-LA-ENTIDAD]”)
Common Name	Número de identificación empresa + digito de verificación (sin puntos) (Ejemplo: [Num. NIT de la entidad] + "digito de verificación").
Description	Certificado de facturación electrónica de [Nombre de la Organización] (Ejemplo "Certificado de facturación electrónica de + [Organization Name])
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

2.1.1.16. Certificado para facturación electrónica de persona jurídica en HSM centralizado

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 (área en la empresa que hará uso del certificado (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: "VATCO-[NIT-DE-LA-ENTIDAD]")
Common Name	Número de identificación empresa + digito de verificación (sin puntos) (Ejemplo: [Num. NIT de la entidad] + "digito de verificación").
Description	Certificado de facturación electrónica de [Nombre de la Organización] (Ejemplo "Certificado de facturación electrónica de + [Organization Name])
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad

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.

2.1.3. 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.

2.1.4. 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.

2.1.5. 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 número de identificación de la Cédula de Ciudadanía, Cédula de Extranjería Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

2.1.6. 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 documento de identidad y/o el Número de Identificación Fiscal, o equivalente, en el esquema de nombres, permitiendo distinguir entre dos identidades cuando exista algún problema de duplicidad 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:

- Cédula de Ciudadanía, Cédula de Extranjería, 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).
- El certificado anterior no conste como vigente.

Como excepción esta DPC permite emitir un certificado cuando coincida NIT del suscriptor, documento de identidad del suscriptor (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*).

2.1.7. 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, la Entidad de Certificación Digital se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres y no está obligada a tener evidencia de la posesión de marcas registradas antes de la emisión de los certificados.

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 la República de Colombia 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 o remota según la necesidad del usuario y las políticas de UANATACA COLOMBIA, cuya identidad resulta fijada en el momento de la firma del contrato entre UANATACA COLOMBIA y el suscriptor, momento en el que queda verificada fehacientemente la identidad del suscriptor mediante los procedimientos de reconocimiento establecidos, su documento nacional de identidad y/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 únicamente la consulta directa a los registros públicos correspondientes.

En el caso de personas naturales identificadas presencialmente, 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 COLOMBIA, 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.

El método de prueba de posesión de la clave privada para cada uno de los tipos de soporte en los que se pueden emitir los correspondientes certificados implica procesos criptográficos seguros que permiten la autenticación sin revelar la clave privada de la misma conforme con el numeral 6.1.2 de la Declaración de Practicas de Certificación de UANATACA COLOMBIA.

2.2.2. Validación de la Identidad

Para la solicitud de certificados los Operadores de Registro de UANATACA COLOMBIA verificarán la identidad del suscriptor a la que se le expide el certificado (véase la persona física o representante autorizado de la persona jurídica), así como cualquier atributo especifico de la persona física o jurídica con la que tenga relación o vinculación.

Para la verificación se procederá a través de un operador de registro o persona autorizada de la Autoridad de Registro, de acuerdo con los siguientes métodos:

a. De forma presencial por parte de la persona física o de un representante autorizado de la persona jurídica, quien deberá aportar la Cédula de Ciudadanía, Cédula de Extranjería, Pasaporte u otro medio idóneo reconocido en derecho para su identificación.
b. Por medio del procedimiento de identificación a distancia a través del sistema de validación de identificación remota de UANATACA COLOMBIA o utilizando otros métodos de identificación a distancia que cumplan las condiciones y requisitos de seguridad determinados por el ONAC.

2.2.3. Autenticación de la identidad de una persona jurídica(organización, empresa o entidad)

La Autoridad de registro verificará la información para poder autenticar la identidad de la persona jurídica, empresa o entidad (u otro tipo de entidad pública o privada) que desempeñe una actividad económica para la cual esté obligada a inscribirse en un registro de carácter fiscal o tributario identificada en el certificado digital mediante la siguiente documentación:

- Solicitud de Certificado de existencia y representación legal en Cámara de Comercio o documento equivalente, en los casos que sea aplicable; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.
- Solicitud de Registro Único Tributario o documento equivalente, en todos los casos; expedido en Colombia (por defecto) o en otro país.
- Si no se incluye en la documentación anterior, solicitud de un documento oficial adicional en el que conste una dirección completa actual de la empresa o entidad (por ejemplo, un Certificado de Residencia para Personas Naturales), en el caso de que el Suscriptor desee que figure en el certificado una dirección distinta

a las incluidas en el Certificado de existencia y representación legal en Cámara de Comercio y/o en el Registro Único Tributario o documentos equivalentes; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.
- Para aquellos casos en los que sea posible, consulta del número de identificación tributaria de la empresa o entidad en una base de datos online (en Colombia, para las empresas del tipo Persona Jurídica o Persona Natural, base de datos RUES), para verificar la existencia de la empresa o entidad y que se encuentra activa.

En el caso de 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 COLOMBIA, la cual se realizará mediante el siguiente procedimiento:

1. El representante del suscriptor deberá acreditar su identidad por uno de los métodos de identificación especificados en el apartado 3.2.2., de tal manera que:
   i. Si se identifica presencialmente ante un operador o persona autorizada de una Autoridad de Registro de UANATACA COLOMBIA:
      - Mostrando su documento nacional de identificación (la Cédula de Ciudadanía, Cédula de Extranjería, pasaporte u otro medio idóneo reconocido en derecho para su identificación).
      - Acreditando el carácter y facultades que alegue poseer.

   ii. Si se identifica electrónicamente a través del sistema de video identificación remota de UANATACA COLOMBIA:
      - Mostrando su documento nacional de identificación (la Cédula de Ciudadanía, Cédula de Extranjería, pasaporte u otro medio idóneo reconocido en derecho para su identificación).
      - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.
      - Acreditando el carácter y facultades que alegue poseer.

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: Cédula de Ciudadanía, Cédula de Extranjería, 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 COLOMBIA comprobará la identidad del representante actuando del siguiente modo:

- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
  - Documento de identidad aportado.
  - Documentación que acredite su representación.

- Cuando la identificación se haya realizado a través del método de identificación electrónica a través del sistema de validación de identificación remota de UANATACA COLOMBIA mediante:

- Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
- Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de validación de identificación remota.
- Revisión del cotejo producido por el sistema de validación de identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
- Revisión producida por el sistema de validación de identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.
- Documentación que acredite su representación.

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

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

La ECD se reserva el derecho de no emitir el certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

La Autoridad de Registro guardará la documentación relativa al sustento de la validación de la identidad de la empresa o entidad identificada en el certificado.

2.2.4. Autenticación de la identidad de una Persona natural

La autoridad de Registro verificará de forma fehaciente la identidad de la Persona Natural individual identificada en el certificado, y validará que el documento de identidad presentado sea aparentemente legítimo y que los datos contenidos en el mismo (país de expedición, tipo y número de documento de identidad, nombres y apellidos) son conformes a los datos de la solicitud. Asimismo, en los casos que sea aplicable, la RA verificará que el documento estaba vigente cuando se presentó. Está sección describe los métodos de comprobación de la identidad de la persona identificada en un certificado.

2.2.4.1. En los certificados

La identidad de las personas naturales suscriptoras (firmantes) identificados en los certificados, se valida a través de los métodos de identificación especificados en el apartado 3.2.2 de esta DPC, de tal manera que:

- (i) Si se identifica presencialmente ante un operador o persona autorizada de una Autoridad de Registro de UANATACA COLOMBIA:
  - Mostrando su Documento de Identidad (Cédula de Ciudadanía, Cédula de Extranjería, pasaporte u otro medio idóneo reconocido en derecho).

- (ii) Si se identifica electrónicamente a través del sistema de validación de identidad remota usado por UANATACA COLOMBIA, o sistemas aprobados previamente por UANATACA COLOMBIA que garanticen el reconocimiento de identidad del titular:
  - Mostrando su Documento de Identidad (Cédula de Ciudadanía, Cédula de Extranjería, pasaporte u otro medio idóneo reconocido en derecho).
  - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.

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.

2.2.4.2. Validación de la Identidad

Para la solicitud de certificados, el operador o personal autorizado de la Autoridad de Registro de UANATACA comprobará la identidad de la persona física identificada en la solicitud del certificado, actuando del siguiente modo:

- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
  - Documento de identidad aportado.

- Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de UANATACA COLOMBIA mediante:
  - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
  - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota.
  - Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
  - Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.

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 o siguiendo el procedimiento de validación de identidad establecido por UANATACA COLOMBIA.

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 los datos y atributos a incluir en el certificado, guardando documentación o consulta acreditativa de la validez de estos.

2.2.4.3. 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.

2.2.5. Información de suscriptor no verificada

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

2.2.6. 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 COLOMBIA 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 COLOMBIA la documentación de identificación correspondientes al nuevo operador, juntamente con su autorización para actuar como tal.

UANATACA COLOMBIA 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 COLOMBIA.

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

En ese sentido, UANATACA COLOMBIA conservará como propias las funciones de comprobación de veracidad, y corrección de los datos que aportan los usuarios, así como el envío a una CA de las peticiones que cumplen los requisitos exigidos por la Entidad de Certificación Digital.

2.3. Identificación y autenticación de solicitudes de renovación

2.3.1. Validación para la renovación rutinaria de certificados

La renovación se entenderá como la emisión de un nuevo certificado digital, por lo cual implica el registro de una nueva solicitud, la cual estará sujeta a validación de identidad por parte de la autoridad de registro según lo especificado en la sección 3.2., con la respectiva generación de un nuevo par de claves.

La ECD UANATACA COLOMBIA notificará con al menos treinta (30) días calendario de anticipación a sus suscriptores y/o firmantes la terminación de la vigencia de su certificado digital. Esta notificación podrá realizarse por correo electrónico a la dirección proporcionada por el suscriptor o por cualquier otro medio idóneo de comunicación cuando UANATACA COLOMBIA lo considere pertinente.

Sin embargo, no es obligación de UANATACA COLOMBIA garantizar la efectividad de la notificación sobre la terminación de la vigencia de su certificado o confirmar la recepción de esta, pues es una obligación del Suscriptor y/o firmante conocer la vigencia de su certificado digital y adelantar los trámites pertinentes ante UANATACA COLOMBIA para la emisión del certificado

Los casos en los que se requiera un nuevo certificado digital con cambio de claves, por expiración, próxima expiración o revocación de un certificado, se tratan como una nueva emisión de certificado, realizándose la misma validación de identidad que se hizo inicialmente para el primer certificado digital, según lo especificado en la sección 3.2. de la Declaración de Practicas de Certificación.

2.4. Modificación del certificado

Durante el ciclo de vida de un certificado, no se tiene prevista la modificación/actualización de los campos contenidos en el certificado. Si se requiere un cambio en los datos del certificado emitido, será necesario revocar el certificado y emitir uno nuevo con las modificaciones correspondientes, registrando adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2. de la Declaración de Practicas de Certificación.

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

UANATACA COLOMBIA 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 de manera online mediante el uso del Código de Revocación (CRE o ERC) a través de la página web de UANATACA COLOMBIA 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 COLOMBIA y/o Autoridades de Registro.

- Las autoridades de registro de UANATACA COLOMBIA: 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

Están autorizados para solicitar la emisión de un certificado digital cualquier persona mayor de edad en plena capacidad de asumir las obligaciones y responsabilidades inherentes a la posesión y uso del certificado y que sustente correctamente la información requerida por 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 entidad, empresa u organización de derecho público o privado.

El solicitante del certificado indistintamente del método de identificación empleado por UANATACA COLOMBIA, sea persona natural o jurídica, debe firmar un contrato de prestación de servicios de certificación con UANATACA COLOMBIA.

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.

3.1.2. Procedimiento de alta y responsabilidades

UANATACA COLOMBIA 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 COLOMBIA. 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 COLOMBIA, podrá gestionar directamente las solicitudes accediendo a los sistemas informáticos de UANATACA COLOMBIA 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, de acuerdo con lo establecido en la sección 2.2.4. 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 COLOMBIA se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, UANATACA COLOMBIA verifica la información proporcionada, verificando los aspectos descritos en la sección 2.2.

La documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el periodo que establezca la legislación vigente cuando sea aplicable y hasta por un plazo máximo 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

Tras realizar la identificación de la persona de manera presencial o a distancia, siguiendo las políticas y procedimientos de UANATACA COLOMBIA, se procederá a su verificación. En caso de que los datos se verifiquen correctamente, UANATACA COLOMBIA debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Siempre que lo considere oportuno, el operador de registro podrá solicitar la subsanación de la información inicialmente proporcionada por el solicitante en su solicitud, necesaria para la correcta validación y aprobación del servicio. En caso de que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, la solicitud quedará denegada definitivamente.

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 COLOMBIA denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

Igualmente, se declinará una solicitud de un servicio de certificación digital, si el mismo no se encuentra en el alcance de la acreditación que le fue otorgado por ONAC.

Asimismo, de conformidad con el numeral 10.11.3.7 de la CEA-3.0-07 el operador de registro de la RA podrá declinar la aceptación de una solicitud cuando existan razones fundamentadas y demostradas, por ejemplo, la participación del solicitante y/o suscriptor en actividades ilegales, o temas relacionados con el suscriptor.

En atención a criterios de imparcialidad y no discriminación dentro de la Autoridad de Registro se dejará un registro interno en la aplicación (CMS) de la RA a efectos de evidenciar que quien realiza la función de la revisión de la solicitud (Operador de Registro) ha emitido una recomendación documentada positiva para que se tenga en cuenta en la decisión sobre la certificación, siendo el Operador de Decisión quien deberá tomar la decisión final sobre la emisión del certificado.

De otra parte, cuando se emita una recomendación documentada negativa será obligatorio para el Operador de Registro justificar y registrar esta debido a que no satisface algún requisito establecido en este documento, en la Política de Certificación correspondiente o en las normas o leyes vigentes aplicables.

En el caso de no otorgar la certificación digital, la autoridad de registro, a quien corresponda, enviará un correo electrónico al Solicitante y al Suscriptor notificando las razones de la decisión de no emitir el certificado.

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. Las solicitudes se mantienen activas hasta su aprobación o rechazo.

3.3. Emisión del certificado

3.3.1. Acciones de la ECD 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 COLOMBIA:

- Protege la confidencialidad e integridad de los datos de registro de que dispone provenientes tanto de la identificación realizada de manera presencial como de la realizada a distancia.
- 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 COLOMBIA o sus Autoridades de Registro deducirlas o utilizarlas en ningún modo.

3.3.2. Notificación de la emisión al suscriptor

UANATACA COLOMBIA 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

UANATACA COLOMBIA, pondrá a disposición de las partes relevantes los certificados emitidos por la CA a través de los medios y procedimientos indicados al efecto según corresponda.

3.4.1. Responsabilidades de la ECD

UANATACA COLOMBIA suministra al interesado la documentación formal de los servicios de certificación digital que adquirió, de forma que indique claramente el contenido del certificado digital o las características del servicio adquirido como lo establece esta Declaración de Prácticas de Certificación y Política de certificación respectivamente.

Las Autoridades de Registro, durante este proceso, el operador o personal autorizado de la Autoridad de Registro UANATACA COLOMBIA debe realizar las siguientes actuaciones:

- Independientemente del método de identificación realizado por UANATACA COLOMBIA se deberá acreditar definitivamente la identidad de la Persona natural identificada en el certificado, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.4. de la Declaración de Practicas de Certificación.
- 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.

  - ❖ Nombre y dirección de la ECD
  - ❖ Nombre y dirección del Suscriptor
  - ❖ Fecha de expiración de los servicios de certificación digital.

- Alcance de los servicios de certificación digital
- Información básica acerca del uso del certificado, incluyendo especialmente información acerca de la Entidad de Certificación Digital 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.
- La fecha del acto de entrega y aceptación. Fecha en la que se otorga el servicio de certificación digital (esta fecha no debe ser anterior a la fecha en la cual se tomó la decisión sobre la certificación digital) o fecha de activación del servicio.

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.

En ese sentido, se registrará documentalmente los anteriores actos y conservará los citados documentos originales (hojas de entrega y aceptación) según corresponda, remitiendo copia electrónica a UANATACA COLOMBIA, así como los originales cuando UANATACA COLOMBIA precise de acceso a los mismos.

3.4.2. Conducta que constituye aceptación del certificado

Indistintamente del método de identificación utilizado para la emisión del certificado cuando se haga entrega de la hoja de aceptación en formato digital o físico según corresponda, dicha 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 COLOMBIA, 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 COLOMBIA publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes, siempre con la autorización de la persona natural identificada en el certificado mediante la firma del contrato.

3.4.4. Notificación de la emisión a terceros

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

3.5. Uso del par de claves y del certificado

Los certificados y las respectivas claves podrán ser utilizados según lo estipulado en la Declaración de Prácticas de Certificación y este documento.

3.5.1. Uso por el firmante

UANATACA COLOMBIA obliga a:

- Facilitar a UANATACA COLOMBIA información completa y adecuada, conforme a los requisitos de esta Política 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 dispositivo seguro de creación de firmas, reconocer su capacidad de producción de firmas digitales 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, de acuerdo con lo establecido en las secciones 6.1, 6.2, 6.3 de la DPC.
- Comunicar a UANATACA COLOMBIA, 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 COLOMBIA 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 una Entidad de Certificación Digital, 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 (entidad de certificación digital) ni en ningún otro caso.

3.5.2. Uso por el subscriptor

3.5.2.1. Obligaciones del suscriptor del certificado

UANATACA COLOMBIA obliga contractualmente al suscriptor a:

- Facilitar a la Autoridad de Certificación información completa y adecuada, conforme a los requisitos de esta Política 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 COLOMBIA, 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 de la Entidad de certificación digital de UANATACA COLOMBIA.
- No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por la ECD o la RA de la revocación de este, o una vez expirado el plazo de validez del certificado.
- Informar a la mayor brevedad la existencia de alguna causa de revocación señaladas en los numerales 4.9.1 conforme al 4.9.4 de la Declaración de Prácticas de Certificación.

3.5.2.2. Responsabilidad civil del suscriptor de certificado

UANATACA COLOMBIA obliga contractualmente al suscriptor a responsabilizarse por:

- 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 una Entidad de Certificación Digital (ECD), 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 Entidad de Certificación Digital ni en ningún otro caso.

3.5.3. Uso por el tercero que confía en certificados

Los terceros de buena fe sólo pueden depositar su confianza en los certificados para aquello que establece esta Política de Certificación, la DPC y la normativa aplicable. En ese sentido, pueden realizar operaciones de clave pública de manera satisfactoria confiando en el certificado emitido por la cadena de confianza.

Así mismo, deben tener a precaución y asumir la responsabilidad de verificar el estado del certificado utilizando los medios y servicios ofrecidos por UANATACA COLOMBIA y que se establecen en este documento y correspondiente DPC.

3.5.3.1. Obligaciones del tercero que confía en certificados

UANATACA COLOMBIA 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 vigencia, validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados,

lo cual, incluirá comprobar que los certificados no han expirado ni han sido revocados (mediante consulta de la CRL o del servicio OCSP).

- 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
- Reconoce que las firmas generadas en un dispositivo seguro de creación de firma tienen la consideración legal de firmas digitales; 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 COLOMBIA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de UANATACA COLOMBIA.
- Notificar a UANATACA COLOMBIA cualquier situación irregular con respecto al servicio prestado por la Entidad de Certificación Digital (ECD).

3.5.3.2. Responsabilidad civil del tercero que confía en certificados

UANATACA COLOMBIA 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

UANATACA COLOMBIA notificará con al menos treinta (30) días calendario de anticipación a sus suscriptores y/o firmantes la terminación de la vigencia de su certificado digital. Esta notificación podrá realizarse por correo electrónico a la dirección proporcionada por el suscriptor o por cualquier otro medio idóneo de comunicación cuando UANATACA COLOMBIA lo considere pertinente.

No obstante, es de resaltar que no constituye una obligación para UANATACA COLOMBIA garantizar la efectividad de la notificación sobre la terminación de la vigencia de su certificado o confirmar la recepción de esta, pues es una obligación de Suscriptor y/o firmante conocer la vigencia de su certificado digital y adelantar los trámites pertinentes ante UANATACA COLOMBIA para la emisión de su nuevo certificado.

La renovación se entenderá como la emisión de un nuevo certificado digital, por lo cual implica el registro de una nueva solicitud, la cual estará sujeta a la validación de identidad por parte de la autoridad de registro, y la generación de un nuevo par de claves.

3.7. Modificación de certificados

UANATACA COLOMBIA no atiende requerimientos de modificación de certificados digitales.

Los casos en los que se requiera modificar algún dato en un certificado digital (actualización de la información contenida en un certificado) se tratan como una revocación de certificado y una nueva emisión de certificado, con cambio de claves.

3.8. 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.

3.8.1. Causas de revocación de certificados

Un certificado será revocado o cancelado ya sea por solicitud del suscriptor, o cuando la ECD conoce, tiene indicios o confirmación de alguna de las siguientes situaciones conforme al numeral 10.11.5.1 de la CEA-3.0-07:

a) Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
b) Por muerte o incapacidad sobrevenida del suscriptor.
c) Por liquidación de la persona jurídica representada que consta en el servicio de certificación digital.
d) Por la confirmación de que alguna información o hecho contenido en el certificado digital es falso.
e) Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
f) Por orden judicial o de entidad administrativa competente.
g) Por pérdida, inutilización del certificado digital que haya sido informado a la ECD.
h) Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato
i) Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la confiabilidad del servicio.
j) Por el manejo indebido por parte del suscriptor del certificado digital.
k) Por el incumplimiento del suscriptor o de la persona jurídica que representa o la que está vinculado a través del Contrato del Servicio de Certificación Digital proporcionado por la ECD,

A continuación, a efectos meramente orientativos, se describen algunas circunstancias específicas derivadas de las causales anteriormente citadas, de manera que si concurre alguna de las siguientes circunstancias se revocará o cancelará el certificado digital conforme a los términos indicados en esta DPC.

3.8.1.1. 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 falso o incorrecto.
c) Descubrimiento de que alguno de los datos contenidos en el certificado es falso o incorrecto.
d) Liquidación de la persona jurídica que consta en el certificado y/o bien cese del desempeño de la actividad económica para la cual estaba obligada a inscribirse en un registro de carácter fiscal o tributario, por la persona natural que consta en el certificado como empresa o entidad.

3.8.1.2 Circunstancias que afectan a la seguridad de la clave privada o del certificado:

a) Compromiso de la clave privada, de la infraestructura o de los sistemas de la ECD que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
b) Infracción, por UANATACA COLOMBIA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación o en la Política de certificación correspondiente.
c) Compromiso o sospecha de compromiso de la seguridad de la clave privada 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.
f) Cualquier causa que induzca a creer razonablemente que el servicio de certificación haya sido comprometido, poniendo en duda la confiabilidad del certificado digital.
g) En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de la clave privada o el certificado no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

3.8.1.3 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 COLOMBIA 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 de este.

d) Infracción por el suscriptor, la entidad que se encuentra vinculado al 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, total o parcial, o el fallecimiento del suscriptor 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 3.4. de la Declaración de Prácticas de Certificación.

3.8.1.4 Otras circunstancias:

a) Por resolución judicial o administrativa que lo ordene.
b) La terminación del servicio de certificación de la Entidad de Certificación Digital UANATACA COLOMBIA
c) Cualquier otra causa lícita especificada en la presente DPC o en la PC que corresponda, entre ellas, el uso del certificado que sea dañino y continuado para UANATACA COLOMBIA. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
    1. La naturaleza y el número de quejas recibidas.
    2. La identidad de las entidades que presentan las quejas.
    3. La legislación relevante vigente en cada momento.
    4. La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

3.8.2. Causas de suspensión de un certificado

Los certificados de UANATACA COLOMBIA 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.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, UANATACA COLOMBIA tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

3.8.3. 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.

3.8.4. Quién puede solicitar la revocación, suspensión o reactivación

Pueden solicitar la revocación, suspensión o reactivación de un certificado de acuerdo con esta Política de Certificación, Declaración de Prácticas de certificación los siguientes:

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

3.8.5. Procedimientos de solicitud de revocación, suspensión o reactivación

La entidad que precise revocación, suspensión o reactivación un certificado puede solicitarlo directamente a UANATACA COLOMBIA o a la Autoridad de Registro del suscriptor o realizarlo él mismo a través del servicio online disponible en la página web de UANATACA COLOMBIA. 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 COLOMBIA, de acuerdo con los requisitos establecidos en la sección 2.4 de la DPC antes 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/co/

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 COLOMBIA.

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 COLOMBIA.

3.8.6. 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.

3.8.7. 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 COLOMBIA o en su caso de la Autoridad de Registro. Si se realiza a través del servicio online, será inmediata.

3.8.8. 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.

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la CRL o del servicio OCSP.

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 COLOMBIA o del servicio OCSP.

Las Listas de Revocación de Certificados se publican en el Depósito de la Entidad de Certificación, así como en los certificados emitidos, en sus respectivas extensiones CRL Distribution Points y *Authority Information Access* y en las direcciones web de acceso a ambos sistemas en línea así:

UANATACA COLOMBIA CA1 2021

- http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
- http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

UANATACA COLOMBIA CA2 2021

- http://crl1.uanataca.com/public/pki/crl/2021CA2sub.crl
- http://crl2.uanataca.com/public/pki/crl/2021CA2sub.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/

3.8.9. Frecuencia de emisión de listas de revocación de certificados (CRLs) y (ARLs)

UANATACA COLOMBIA emite una CRL al menos cada 24 horas.

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

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

La Lista de revocación de Autoridades de Certificación (ARLs) se actualizará cada 180 días.

3.8.10. Plazo máximo de publicación de LRCs

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

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

UANATACA COLOMBIA tiene disponibles dos sistemas en línea de verificación del estado de los certificados, uno mediante comprobación de revocación por CRL y otro por OCSP, ambos gratuitos y sin restricciones de acceso.

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de UANATACA COLOMBIA, que se encuentra disponible las 24 horas de los 7 días de la semana en el web https://www.uanataca.com/co/

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

- *Autoridad de Certificación Raíz (UANATACA ROOT 2016):*
  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *Autoridad de Certificación Subordinada (UANATACA CA1 2021):*

  - http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl

- *Autoridad de Certificación Subordinada (UANATACA CA2 2021):*

  - http://crl1.uanataca.com/public/pki/crl/2021CA2sub.crl
  - http://crl2.uanataca.com/public/pki/crl/2021CA2sub.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 COLOMBIA suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

3.8.12. 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.

3.8.13. 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 COLOMBIA, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

3.8.14. Período máximo de un certificado digital en estado suspendido

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

3.10. Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Política de Certificación.

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 COLOMBIA.

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 COLOMBIA https://www.uanataca.com

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 de certificados, CRL y respuestas OCSP es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública en certificados 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., conforme a los siguientes estandares: - RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. - ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

4.2.2. Perfil de OCSP

El certificado OCSP de la CA Subordinada de la ECD es coherente con lo dispuesto en los siguientes estándares: - RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

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
DPC	Declaración de Prácticas de Certificación
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DSCF	Dispositivo Seguro de Creación de Firma
ECD	Entidad de Certificaicón Digital
SSCD	Secure Signature Creation Device. Dispositivo Seguro de Creación de Firma
FIPS	Federal Information Processing Standard Publication
HSM	Hardware Security Module
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
ONAC	Organismo Nacional de Acreditación de Colombia
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

6. Perfiles de Certificados

6.1. Certificado de persona natural ciudadano en tarjeta o token

	TOKEN o TARJETA
De PN Ciudadano	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
1.6.3. Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
1.6.4. Serial Number	Número de documento de identificación del SUSCRIPTOR codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.5. Common Name	NOMBRE Y APELLIDOS DEL SUSCRIPTOR
1.6.7. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	

2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado "1"
2.3.2. Content commintment	Seleccionado "1"
2.3.3. Key Encipherment	Seleccionado "1"
2.3.4. Data Encipherment	No seleccionado. "0"
2.3.5. Key Agreement	No seleccionado. "0"
2.3.6. Key Certificate Signature	No seleccionado. "0"
2.3.7. CRL Signature	No seleccionado. "0"
2.3.8. Encipher Only	No seleccionado. "0"
2.3.9. Decipher Only	No seleccionado. "0"
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.1.1
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de persona natural ciudadano en tarjeta o token
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.1.1
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.1.1
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.1.1
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	

2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-calssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.2. Certificado de persona natural ciudadano en HSM centralizado

	en HSM CENTRALIZADO
De PN Ciudadano	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA

1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
1.6.3. Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
1.6.4. Serial Number	Número de documento de identificación del Suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.5. Common Name	NOMBRE Y APELLIDOS DEL SUSCRIPTOR
1.6.7. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.1.2
2.4.1.1. Qualifier Type	User Notice Text

2.4.1.1. Qualifier	Certificado de persona natural ciudadano en HSM CENTRALIZADO
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.1.2
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.1.2
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.1.2
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	

2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.3. Certificado de persona natural profesional titulado en tarjeta o token

	en TARJETA o TOKEN
De PN Profesional	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organization Name (O)	Se especificará el nombre de la entidad habilitante (Emisor de la tarjeta profesional o entidad/institución educativa que otorga el título)
1.6.3. Title	Se especificará el título o especialidad del suscriptor y el número de profesional si dispone. (Ejemplo: ABOGADO - NUMERO DE PROFESIONAL)
1.6.4. Surname	Apellidos del suscriptor (como consta en el documento de identificación)
1.6.5. Given Name	Nombre del suscriptor (como consta en el documento de identificación)
1.6.6. Serial Number	Número de documento de identificación del suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)

1.6.7. Common Name	Nombre y apellido del Suscriptor + Título (Ejemplo: "Given name" + "Surname" + "Title"
1.6.8. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.2.1
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de persona natural profesional titulado en tarjeta o token
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.2.1
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.2.1
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.2.1
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co

2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.4. Certificado de persona natural profesional titulado en HSM centralizado

	en HSM CENTRALIZADO
De PN Profesional	Autenticación y Firma
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organization Name (O)	Se especificará el nombre de la entidad habilitante (Emisor de la tarjeta profesional o entidad/institución educativa que otorga el título)
1.6.3. Title	Se especificará el título o especialidad del suscriptor y el número de profesional si dispone. (Ejemplo: ABOGADO - NUMERO DE PROFESIONAL)
1.6.4. Surname	Apellidos del suscriptor (como consta en el documento de identificación)
1.6.5. Given Name	Nombre del suscriptor (como consta en el documento de identificación)
1.6.6. Serial Number	Número de documento de identificación del suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.7. Common Name	Nombre y apellido del Suscriptor + Título (Ejemplo: "Given name" + "Surname" + "Title"
1.6.8. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits

2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado "1"
2.3.2. Content commintment	Seleccionado "1"
2.3.3. Key Encipherment	Seleccionado "1"
2.3.4. Data Encipherment	No seleccionado. "0"
2.3.5. Key Agreement	No seleccionado. "0"
2.3.6. Key Certificate Signature	No seleccionado. "0"
2.3.7. CRL Signature	No seleccionado. "0"
2.3.8. Encipher Only	No seleccionado. "0"
2.3.9. Decipher Only	No seleccionado. "0"
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.2.2
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de persona natural profesional titulado en HSM centralizado
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.2.2
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.2.2
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.2.2
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	

2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.5. Certificado de persona natural miembro de empresa u organización en tarjeta o token

	EN TARJETA o TOKEN
De PN Perteneciente	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.

1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organizational Unit Name (OU)	Se especificará el Departamento al que pertenece el Firmante o el tipo de vinculación con la Empresa
1.6.3. Organization Name (O)	Se especificará el nombre de la Empresa u Organización
1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
1.6.5. Title	Se especificará el nombre del título o puesto que la persona ocupa en la Empresa u Organización
1.6.7. Surname	Apellidos del firmante (como consta en el documento de identificación)
1.6.8. Given Name	Nombre del firmante (como consta en el documento de identificación)
1.6.9. Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.10. Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
1.6.11. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad a la que está vinculado el firmante
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”

2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.3.1
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de persona natural miembro de empresa u organización en tarjeta o token
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.3.1
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.3.1
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.3.1
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	

2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.6. Certificado de persona natural miembro de empresa u organización en HSM centralizado

	en HSM CENTRALIZADO
De PN Perteneciente	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organizational Unit Name (OU)	Se especificará el Departamento al que pertenece el Firmante o el tipo de vinculación con la Empresa
1.6.3. Organization Name (O)	Se especificará el nombre de la Empresa u Organización

1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: "VATCO-00000")
1.6.5. Title	Se especificará el nombre del título o puesto que la persona ocupa en la Empresa u Organización
1.6.7. Surname	Apellidos del firmante (como consta en el documento de identificación)
1.6.8. Given Name	Nombre del firmante (como consta en el documento de identificación)
1.6.9. Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo ("IDCCO-[CC]" o "PASCO-[PASAPORTE]")
1.6.10. Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
1.6.11. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad a la que está vinculado el firmante
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado "1"
2.3.2. Content commintment	Seleccionado "1"
2.3.3. Key Encipherment	Seleccionado "1"
2.3.4. Data Encipherment	No seleccionado. "0"
2.3.5. Key Agreement	No seleccionado. "0"
2.3.6. Key Certificate Signature	No seleccionado. "0"
2.3.7. CRL Signature	No seleccionado. "0"
2.3.8. Encipher Only	No seleccionado. "0"
2.3.9. Decipher Only	No seleccionado. "0"
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.3.2
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de persona natural miembro de empresa u organización en HSM centralizado
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.3.2
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas

2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.3.2
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.3.2
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.7. Certificado de persona natural representante de persona jurídica en tarjeta o token

	en TARJETA o TOKEN
De PN Representante de Persona Jurídica	Autenticación y Firma
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organization Name (O)	Nombre de la organización de la que el firmante es representante
1.6.3. Organizational Unit Name (OU)	Unidad de la Organización a la que está vinculado el firmante
1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
1.6.5. Title	REPRESENTANTE LEGAL
1.6.6. Surname	Apellidos del representante (como consta en el documento de identificación)
1.6.8. Given Name	Nombre del representante (como consta en el documento de identificación)
1.6.9. Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.10. Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
1.6.11. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la persona jurídica a la que está vinculado el firmante
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption

1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.4.1
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de persona natural representante de persona jurídica en tarjeta o token
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.4.1
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.4.1
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.4.1
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	

2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-calssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE
2.10. Subject Directory Attributes	
2.10.1 OID 1.3.6.1.4.1.47286.10.1	Nivel de apoderamiento
2.10.2 OID 1.3.6.1.4.1.47286.10.2	Documento de presentación

6.8. Certificado de persona natural representante de persona jurídica en HSM centralizado

	en HSM CENTRALIZADO
De PN Representante de Persona Jurídica	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11

1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organization Name (O)	Nombre de la organización de la que el firmante es representante
1.6.3. Organizational Unit Name (OU)	Unidad de la Organización a la que está vinculado el firmante
1.6.4. Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
1.6.5. Title	REPRESENTANTE LEGAL
1.6.6. Surname	Apellidos del representante (como consta en el documento de identificación)
1.6.8. Given Name	Nombre del representante (como consta en el documento de identificación)
1.6.9. Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.10. Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
1.6.11. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la persona jurídica a la que está vinculado el firmante
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”

2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.4.2
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de persona natural representante de persona jurídica en HSM centralizado
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.4.2
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.4.2
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.4.2
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)

2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-calssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE
2.10. Subject Directory Attributes	
2.10.1 OID 1.3.6.1.4.1.47286.10.1	Nivel de apoderamiento
2.10.2 OID 1.3.6.1.4.1.47286.10.2	Documento de presentación

6.9. Certificado de persona natural función pública en tarjeta o token

	en TARJETA o TOKEN
De PN Función Pública	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)

1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organizational Unit Name (OU)	Se especificará el Departamento al que pertenece el firmante o el tipo de vinculación con la Institución
1.6.3. Organization Name (O)	Se especificará el nombre de la Institución
1.6.4. Organization Identifier	Número oficial de identificación de la institución a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
1.6.5. Title	Se especificará el cargo o puesto que la persona ocupa en la Institución
1.6.6. Surname	Apellidos del firmante (como consta en el documento de identificación)
1.6.7. Given Name	Nombre del firmante (como consta en el documento de identificación)
1.6.8. Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.9. Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
1.6.10. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la institución
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.6.1

2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de persona natural función pública en tarjeta o token
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.6.1
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.6.1
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.6.1
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	id-ad-ocsp
2.8.1.1.2. Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	http://ocsp2.uanataca.com/public/pki/ocsp/

2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.10. Certificado de persona natural función pública en HSM centralizado

	en HSM CENTRALIZADO
De PN Función Pública	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organizational Unit Name (OU)	Se especificará el Departamento al que pertenece el firmante o el tipo de vinculación con la Institución
1.6.3. Organization Name (O)	Se especificará el nombre de la Institución
1.6.4. Organization Identifier	Número oficial de identificación de la institución a la que está vinculado el firmante, en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
1.6.5. Title	Se especificará el cargo o puesto que la persona ocupa en la Institución
1.6.6. Surname	Apellidos del firmante (como consta en el documento de identificación)
1.6.7. Given Name	Nombre del firmante (como consta en el documento de identificación)
1.6.8. Serial Number	Número de documento de identificación del firmante codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.9. Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE

1.6.10. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la institución
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.6.2
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de persona natural función pública en HSM centralizado
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.6.2
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.6.2
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.6.2
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co

2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Se especificará el correo electrónico de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	id-ad-ocsp
2.8.1.1.2. Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.11. Certificado de Sello Electrónico en tarjeta o token

	en TARJETA o TOKEN
De Sello electrónico	Autenticación y Firma
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organization Name (O)	Denominación (nombre “oficial” de la organización o entidad)
1.6.3. Organizational Unit Name (OU)	Denominación (nombre “oficial” de la unidad) del solicitante del sello (Ej: Subdirección de explotación)
1.6.4. Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
1.6.5. Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
1.6.6. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	

2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.7.1
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de sello electrónico en tarjeta o token
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.7.1
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.7.1
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.7.1
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Correo electrónico de contacto de la entidad u organización suscriptora del sello
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com

2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.12. Certificado de Sello Electrónico en HSM centralizado

	en HSM CENTRALIZADO
De Sello electrónico	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021

1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	CO
1.6.2. Organization Name (O)	Denominación (nombre “oficial” de la organización o entidad)
1.6.3. Organizational Unit Name (OU)	Denominación (nombre “oficial” de la unidad) del solicitante del sello (Ej: Subdirección de explotación)
1.6.4. Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello en formato ETSI EN 319412-1 "VAT" + "CO" + "-" + <NIT de la entidad suscriptora> (Ejemplo: “VATCO-00000”)
1.6.5. Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
1.6.6. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.7.2

2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de sello electrónico en HSM centralizado
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.7.2
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.7.2
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.7.2
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Correo electrónico de contacto de la entidad u organización suscriptora del sello
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/

2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-calssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.13. Certificado para facturación electrónica de persona natural en tarjeta o token

	en TOKEN o TARJETA
De Facturación Electrónica de Persona Natural	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	País de residencia o nacionalidad del Suscriptor
1.6.2. Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
1.6.3. Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
1.6.4. Serial Number	Número de documento de identificación del Suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.5. Common Name	Certificado de facturación electrónica de [Nombre del Suscriptor] (Ejemplo "Certificado de facturación electrónica de + [Given Name] + [Surname])
1.6.6. Description	Número de documento de identificación del Suscriptor + digito de verificación (sin puntos) (Ejemplo: [Núm. Documento de identificación del Suscriptor] + "digito de verificación").
1.6.7. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor

1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.8.1
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado para facturación electrónica de persona natural en tarjeta o token
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.8.1
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.8.1
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.8.1
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None

2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Correo electrónico de contacto de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.14. Certificado para facturación electrónica de persona natural en HSM centralizado

	en HSM CENTRALIZADO
De Facturación Electrónica de Persona Natural	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	País de residencia o nacionalidad del Suscriptor
1.6.2. Surname	Apellidos del Suscriptor (como consta en el documento de identificación)
1.6.3. Given Name	Nombre del Suscriptor (como consta en el documento de identificación)
1.6.4. Serial Number	Número de documento de identificación del Suscriptor codificado acorde a ETSI EN 319 412-1 ejemplo (“IDCCO-[CC]” o “PASCO-[PASAPORTE]”)
1.6.5. Common Name	Certificado de facturación electrónica de [Nombre del Suscriptor] (Ejemplo "Certificado de facturación electrónica de + [Given Name] + [Surname])
1.6.6. Description	Número de documento de identificación del Suscriptor + digito de verificación (sin puntos) (Ejemplo: [Núm. Documento de identificación del Suscriptor] + "digito de verificación").
1.6.7. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del Suscriptor
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits

2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado "1"
2.3.2. Content commintment	Seleccionado "1"
2.3.3. Key Encipherment	Seleccionado "1"
2.3.4. Data Encipherment	No seleccionado. "0"
2.3.5. Key Agreement	No seleccionado. "0"
2.3.6. Key Certificate Signature	No seleccionado. "0"
2.3.7. CRL Signature	No seleccionado. "0"
2.3.8. Encipher Only	No seleccionado. "0"
2.3.9. Decipher Only	No seleccionado. "0"
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.8.2
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado para facturación electrónica de persona natural en HSM centralizado
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.8.2
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.8.2
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.8.2
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	

2.5.1. rfc822Name	Correo electrónico de contacto de la persona natural
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.15. Certificado para facturación electrónica de persona jurídica en tarjeta o token

	en TARJETA o TOKEN
De Facturación Electrónica de Persona Jurídica	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona

1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
1.6.2. Organization Name (O)	Denominación (nombre “oficial” de la organización o entidad)
1.6.3. Organizational Unit Name (OU)	Denominación (nombre “oficial” de la unidad) del solicitante del sello (área en la empresa que hará uso del certificado (Ej: Subdirección de explotación)
1.6.4. 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: “VATCO-[NIT-DE-LA-ENTIDAD]”)
1.6.5. Serial Number	Número de identificación empresa + digito de verificación (sin puntos) (Ejemplo: [Num. NIT de la entidad] + "digito de verificación").
1.6.6. Common Name	Certificado de facturación electrónica de [Nombre de la Organización] (Ejemplo "Certificado de facturación electrónica de + [Organization Name])
1.6.7. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”

2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.9.1
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado para facturación electrónica de persona jurídica en tarjeta o token
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.9.1
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.9.1
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.9.1
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Correo electrónico de contacto de la entidad u organización suscriptora del sello
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/

2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.16. Certificado para facturación electrónica de persona jurídica en HSM centralizado

	en HSM CENTRALIZADO
De Facturación Electrónica de Persona Jurídica	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	ES
1.4.2. Locality Name (L)	Barcelona
1.4.3. Organizational Unit (OU)	TSP-UANATACA
1.4.4. Organization Name (O)	UANATACA S.A.
1.4.5. Common Name (CN)	UANATACA CA1 2021
1.4.6. Organization Identifier (other name)	VATES-A66721499
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
1.6.2. Organization Name (O)	Denominación (nombre “oficial” de la organización o entidad)
1.6.3. Organizational Unit Name (OU)	Denominación (nombre “oficial” de la unidad) del solicitante del sello (área en la empresa que hará uso del certificado (Ej: Subdirección de explotación)
1.6.4. 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: “VATCO-[NIT-DE-LA-ENTIDAD]”)
1.6.5. Serial Number	Número de identificación empresa + digito de verificación (sin puntos) (Ejemplo: [Num. NIT de la entidad] + "digito de verificación").

1.6.6. Common Name	Certificado de facturación electrónica de [Nombre de la Organización] (Ejemplo "Certificado de facturación electrónica de + [Organization Name])
1.6.7. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización o entidad
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	Seleccionado “1”
2.3.3. Key Encipherment	Seleccionado “1”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.9.2
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado para facturación electrónica de persona jurídica en HSM centralizado
2.4.1.2 Certificate Policy Id	1.3.6.1.4.1.47286.201.1.9.2
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.9.2
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	1.3.6.1.4.1.47286.201.1.9.2
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co

2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	
2.5.1. rfc822Name	Correo electrónico de contacto de la entidad u organización suscriptora del sello
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)
2.7. cRLDistributionPoint	
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.9. Basic Constraints	
2.9.1. cA	FALSE

6.17. Certificado para sello electrónico de tiempo

De Sello de Tiempo Electrónico	**Autenticación y Firma**
1. Basic estructure	
1.1. Version	"2"
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.
1.3. Signature Algorithm	1.2.840.113549.1.1.11
1.3.1. Algorithm	SHA-256 with RSA Signature
1.3.2. Parameters	No aplicable
1.4. Issuer	
1.4.1. Country Name (C)	CO
1.4.2. Locality Name (L)	Bogotá D.C
1.4.3. Organizational Unit (OU)	TSP-UANATACA CO
1.4.4. Organization Name (O)	UANATACA COLOMBIA SAS
1.4.5. Common Name (CN)	UANATACA CO CA1
1.4.6. Organization Identifier (other name)	NITCO-901671447-5
1.5. Validity	(hasta 2 años)
1.5.1. Not Before	Fecha y hora de inicio de validez del certificado codificado en UTCTime
1.5.2. Not After	Fecha y hora de expiración del certificado codificado en UTCTime NotBefore + 2 años
1.6. Subject	
1.6.1. Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada (CO)
1.6.2. Locality Name (L)	Nombre de la LOCALIDAD donde resida el proveedor del servicio de certificación. (No incluir información adicional al nombre de la localidad)
1.6.3. Organizational Unit Name (OU)	TSP-UNIDAD DEL PRESTADOR
1.6.4. Organization Name (O)	NOMBRE ORGANIZACIÓN
1.6.5. Common Name (CN)	Estampado cronológico de [NOMBRE DEL PRESTADOR DE SERVICIO]
1.6.6. Organization Identifier	VATCO-[NIT DEL PRESTADOR DEL SERVICIO]
1.6.7. Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio del proveedor del servicio de certificación
1.7. Subject Public Key Info	
1.7.1. AlgorithmIdentifier	
1.7.1.1. Algorithm	RSA encryption
1.7.1.2. Parameters	No aplicable
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits
2. Extensions	
2.1. Authority Key Identifier	Identificador de la clave del emisor
2.1.1. KeyIdentifier	
2.2. Subject Key Identifier	Identificador de la clave del firmante
2.2.1. KeyIdentifier	

2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado “1”
2.3.2. Content commintment	No seleccionado. “0”
2.3.3. Key Encipherment	No seleccionado. “0”
2.3.4. Data Encipherment	No seleccionado. “0”
2.3.5. Key Agreement	No seleccionado. “0”
2.3.6. Key Certificate Signature	No seleccionado. “0”
2.3.7. CRL Signature	No seleccionado. “0”
2.3.8. Encipher Only	No seleccionado. “0”
2.3.9. Decipher Only	No seleccionado. “0”
2.4. Certificate Policies	
2.4.1.1. Certificate Policy Id	OID 1.3.6.1.4.1.47286.201.1.10
2.4.1.1. Qualifier Type	User Notice Text
2.4.1.1. Qualifier	Certificado de Estampado Cronológico (sello de tiempo electrónico)
2.4.1.2 Certificate Policy Id	OID 1.3.6.1.4.1.47286.201.1.10
2.4.1.2 Qualifier Type	CPS URI
2.4.1.2 Qualifier	https://web.uanataca.com/co/politicas-practicas
2.4.1.3. Certificate Policy Id	OID 1.3.6.1.4.1.47286.201.1.10
2.4.1.3. Qualifier Type	User Notice Text
2.4.1.3. Qualifier	XX-ECD-XXX
2.4.1.4. Certificate Policy Id	OID 1.3.6.1.4.1.47286.201.1.10
2.4.1.4. Qualifier Type	User Notice Text
2.4.1.4. Qualifier	Uanataca Colombia SAS CALLE 93 B 12 28 OF 203 204 Bogotá, Colombia info@uanataca.co
2.4.1.5 Certificate Policy Id	0.4.0.2042.1.2
2.4.1.5 Qualifier Type	None
2.4.1.5 Qualifier	
2.5. Subject Alternative Names	0.4.0.2042.1.2
2.5.1. rfc822Name	Correo electrónico de contacto de la entidad u organización suscriptora del certificado
2.5.bis Issuer Alternative Names	
2.5.1.bis Issuer alternative name	info@uanataca.com
2.6. Extended Key Usage	
2.6.1. TimeStamping	Presente (1.3.6.1.5.5.7.3.8)
2.7. cRLDistributionPoint	

2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl
2.8. Authority Info Acces	
2.8.1. Access Description	
2.8.1.1. Acces Method	id-ad-ocsp
2.8.1.1.1 Acces Location	http://ocsp1.uanataca.com/public/pki/ocsp/
2.8.1.1.2. Acces Location	http://ocsp2.uanataca.com/public/pki/ocsp/
2.8.2. Access Description	
2.8.2.1. Acces Method	id-ad-caIssuers
2.8.2.1.1 Acces Location	http://web.uanataca.com/co/certificados-ca
2.10. Basic Constraints	
2.10.1. cA	FALSE