INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA:

ESTRUCTURA, CERTIFICADOS Y

LISTAS DE CERTIFICADOS REVOCADOS

CONTROL DE VERSIONES

VERSIÓN (EDICIÓN)	MOTIVO DEL CAMBIO	PUBLICACIÓN
1.1	Creación	Abril 2008
1.2	Modificaciones en los campos: punto de distribución de CRL, acceso a la información de autoridad OCSP y Políticas del certificado.	Julio 2008
2	Clasificación de la norma	Enero 2011

ÍNDICE

<table>
<tr><th colspan="6">TRÁMITE</th></tr>
<tr><td colspan="6">1.DIRECTORIO</td></tr>
<tr><td colspan="3">NOMBRE</td><td colspan="3">CARGO SUSCERTE</td></tr>
<tr><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td colspan="3">2. GRUPO DE TRABAJO: General</td><td colspan="3">3. COMISIÓN ESPECIAL:</td></tr>
<tr><td colspan="3">COORDINADOR:</td><td colspan="3"></td></tr>
<tr><td colspan="3">MIEMBROS PERMANENTES:</td><td colspan="3">CARGO:</td></tr>
<tr><td>NOMBRE</td><td>UNIDAD</td><td>CARGO</td><td colspan="3"></td></tr>
<tr><td></td><td></td><td></td><td colspan="3"></td></tr>
<tr><td></td><td></td><td></td><td colspan="3">4. ESPECIALISTA(S) INVITADO(S):</td></tr>
<tr><td></td><td></td><td></td><td>NOMBRE</td><td>ENTIDAD</td><td>CARGO</td></tr>
<tr><td></td><td></td><td></td><td></td><td>SUSCERTE</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">OBSERVACIONES</td><td colspan="3">RESPONSABLE DE LA EDICIÓN</td></tr>
<tr><td colspan="3" rowspan="3"></td><td colspan="3">COORDINADOR:

FECHA: FIRMA:</td></tr>
<tr><td colspan="3">SUPERINTENDENTE:

FECHA: FIRMA:</td></tr>
<tr><td colspan="3">APROBACIÓN APLICACIÓN EN:

FECHA: FIRMA:</td></tr>
</table>

1. OBJETO Y CAMPO DE APLICACIÓN

Esta norma describe la estructura de los identificadores de objeto para la Infraestructura Nacional de Certificación Electrónica (joint-iso-itu-t (2) country (16) ve (862)), que se utilizan para los campos de los Certificados Electrónicos, las Declaraciones de Prácticas de Certificación de los Proveedores de Servicios de Certificación, en las Listas de Certificados Revocados, entre otros.

2. REFERENCIAS NORMATIVAS

2.1. Decreto con Fuerza de Ley 1.204 Sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE). (Febrero 2001)

2.2. Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas. (Diciembre 2004)

2.3. Providencia Administrativa Nº 016 de SUSCERTE. (Febrero 2007).

2.4. ITU-T Rec. X.509 V.3 Tecnología de la Información. Interconexión de Sistemas abiertos – El Directorio : Marcos para certificados de claves públicas y atributos. (2000).

2.5. RFC 3280 Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile. (2002).

2.6. RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. (2002).

3. DEFINICIONES Y TERMINOLOGÍAS

A los efectos de esta norma se establecen las siguientes definiciones y terminologías:

CERTIFICADO ELECTRÓNICO	Mensaje de datos proporcionado por un Proveedor de Servicios de Certificación (PSC) que le atribuye certeza y validez a la firma electrónica.
IDENTIFICADOR DE OBJETO	Valor universal único asociado a un objeto para identificarlo inequívocamente.
LISTA DE CERTIFICADOS REVOCADOS	Documento mantenido y publicado por una Autoridad de Certificación (AC) que enumera los certificados revocados por ella.

4. SÍMBOLOS Y ABREVIATURAS

A los efectos de esta norma se establecen los siguientes símbolos y abreviaturas:

AC	Autoridad de Certificación.
AR	Autoridad de Registro.
ASN.1	Abstract Syntax Notation One – Notación de Sintaxis Abstracta Uno.
DPC	Declaración de Prácticas de Certificación.
HSM	Hardware Security Module. (Módulo de Seguridad de Hardware)
ITU-T	International Telecommunications Union-Telecommunications. (Unión Internacional de Telecomunicaciones.)
LCR	Lista de Certificados Revocados.

LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas.
OID	Identificador de Objeto.
PC	Política de Certificados.
PSC	Proveedor de Servicios de Certificación.
RBV	República Bolivariana de Venezuela.
RPLSMDFE	Reglamento Parcial de Ley Sobre Mensajes de Datos y Firmas Electrónicas.
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.

5. PROCEDIMIENTO

5.1 Principio Básico

En esta norma se presenta la estructura de los OID para la Infraestructura Nacional de Certificación Electrónica, empleados para la distribución de los campos en los Certificados Electrónicos que pueden ser emitidos por los PSC, así como para las DPC y Listas de Certificados Revocados, entre otros.

5.2 Consideraciones Generales

5.2.1 Para la selección del modelo de la Infraestructura Nacional de Certificación Electrónica, se realizó un estudio de las diferentes topologías de Infraestructura de Claves Públicas, seleccionándose el modelo jerárquico con una Autoridad de Certificación Raíz única nacional de la cual dependen los Proveedores de Servicios de Certificación acreditados.

5.2.2 Este modelo de arquitectura jerárquica, debe ser adoptado por todo Proveedor de Servicios de Certificación (PSC) que desee solicitar su acreditación ante SUSCERTE.

5.2.3 En la Figura Nº 1 se establecen las relaciones de confianza basadas en la arquitectura jerárquica con una única raíz de la Infraestructura Nacional de Certificación Electrónica.

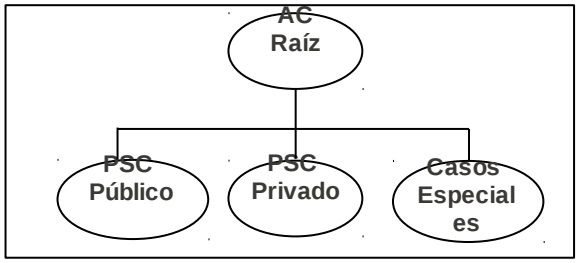

Fig. Nº 1. *Arquitectura Jerárquica subordinada*

5.2.4 La relación de confianza sólo se especifica en una dirección. La Autoridad de Certificación Raíz es quien emite los certificados a los PSC, quienes a su vez pueden emitir certificados a sus AC subordinadas y a sus signatarios, más no pueden emitir certificados a su AC superior.

5.2.5 SUSCERTE es el ente rector y responsable de la Infraestructura Nacional de Certificación Electrónica, a través de la Autoridad de Certificación raíz del Estado Venezolano.

5.2.6 En la arquitectura jerárquica de la Infraestructura Nacional de Certificación Electrónica, se permite que los PSC constituyan hasta dos niveles de AC subordinadas por debajo de la AC raíz.

5.2.7 No existe otra AC que pueda firmar el certificado de la AC raíz. Este es el único caso, en el que la AC raíz crea un certificado autofirmado. Luego ella firma con este certificado, los certificados electrónicos de las AC subordinadas de los PSC y la LCR de la AC raíz.

5.2.8 La AC raíz no emite certificados a los usuarios, sólo emite certificados a los PSC. Estos pueden emitir certificados a los signatarios o a otro nivel de AC subordinada, hasta un máximo de dos niveles.

5.2.9 La AC raíz establece las condiciones para los tipos de certificados que pueden emitir las AC de los PSC.

5.2.10 Cada PSC debe contar con una AC principal y AR's encargadas de atender a su comunidad de usuarios. De manera opcional, el PSC puede crear AC subordinadas de su AC principal.

5.2.11 Los PSC son responsables de la gestión (emisión, renovación, suspensión y revocación) de los certificados electrónicos de sus signatarios, mas no de los usos posteriores que estos le den a los certificados.

5.2.12 Los PSC pueden gestionar varios tipos de certificados, entre ellos:

a) Personas Naturales.
b) Personas Jurídicas.
c) Servidores y/o Aplicaciones.

5.2.13 Los certificados electrónicos se pueden renovar tantas veces como se requiera y la tecnología lo permita. Los tiempos de vida y tamaños mínimos requeridos para los pares de claves de dichos certificados, de acuerdo a su tipo se muestran en la Tabla Nº 1.

Tabla Nº 1. *Características para los certificados*

Tipo de Certificado	Dispositivo para Generación y Almacenamiento del par de claves	Duración máxima (años)	Tamaño Mínimo del par de claves (bits)
AC Raíz	Hardware (HSM)	20	4096
AC Principal de PSC		10	4096
AC Subordinada PSC		5	4096
Persona Natural	Software (guardados en discos)	1	1024
	Hardware (token criptográfico)	3	2048
Persona Jurídica	Hardware (token criptográfico)	3	2048
Servidor y/o Aplicaciones	Software (guardados en discos)	3	2048
	Hardware (HSM)	5	2048

5.3.14 SUSCERTE sigue el estándar ITU X.509 V3 en todos los aspectos relacionados con el formato, codificación, contenidos e interpretación de los certificados electrónicos y las listas de certificados revocados.

5.3.15 Los procedimientos para las solicitudes y emisiones de los pares de claves, se especificarán en la Declaración de Prácticas de Certificación (DPC) del PSC.

5.2.16 Los procedimientos en caso de pérdida, reemplazo o renovación de algún certificado, se establecerán en la DPC del PSC.

5.2.17 El usuario de los certificados debe conocer las políticas de uso de los certificados establecidas por el PSC, así como emplear los certificados electrónicos para la realización de actividades enmarcadas en las leyes venezolanas.

5.2.18 Los OID de la familia joint-iso-itu-t (2) country (16) ve (862), serán utilizados para la Infraestructura Nacional de Certificación Electrónica.

5.2.19 En Venezuela, SUSCERTE administra dichos OID para la Infraestructura Nacional de Certificación Electrónica. El esquema de distribución se muestra en el anexo Nº 1.

5.2.20 El perfil de la Lista de Certificados Revocados debe seguir la RFC 3280 .

5.3 Consideraciones Específicas

5.3.1 La nomenclatura que debe utilizarse para los campos de tipo nombre distinguido (DN – Distinguished Name) se presenta en la tabla Nº 2.

Tabla Nº 2 *Nomenclatura de tipo nombre distinguido usada en las tablas de estructura.*

Abreviatura	Significado	Corresponde a
CN	Common Name (nombre común)	Nombre de la persona natural o jurídica, servidor o aplicación
O	Organization Name (nombre de la organización)	Nombre de la organización relacionada con el CN
OU	Organizational Unit (unidad organizacional)	Nombre de la unidad organizacional relacionada con el CN
C	Country (país)	País
E	E-mail (correo electrónico)	Dirección de correo electrónico
L	Locality (localidad)	Localidad
ST	State (estado)	Estado o Provincia

5.3.2 La estructura de campos del certificado electrónico raíz se especifica en la Tabla Nº 3.

5.3.3 La estructura de campos del certificado electrónico de la AC principal del PSC se detalla en la Tabla Nº 4.

5.3.4 La estructura de campos del certificado electrónico de AC subordinada del PSC se detalla en la Tabla Nº 5.

5.3.5 La estructura de campos del certificado electrónico de personas naturales se presenta en la Tabla Nº 6.

5.3.6 La estructura de campos del certificado electrónico de personas jurídicas se especifica en la Tabla Nº 7.

5.3.7 La estructura de campos del certificado electrónico de servidores y/o aplicaciones se especifica en la Tabla Nº 8.

5.3.8 Las limitaciones de uso de cada tipo de certificado deben estar establecidas en su correspondiente política de certificados.

5.3.9 Los campos que deben presentarse en toda LCR se detallan en la tabla Nº 9.

5.3.10 Las extensiones de una LCR se especifican en la tabla Nº 10.

Tabla Nº 3. *Estructura de campos del Certificado Raíz.*

CAMPO DEL CERTIFICADO	Valor del Certificado Raíz
Versión	V3
Serial	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. Los algoritmos permitidos son SHA1 y SHA256 withRSAEncryption.
DATOS DEL EMISOR (DN)	
CN	Autoridad de Certificacion Raiz del Estado Venezolano
O	Sistema Nacional de Certificacion Electronica
OU	Superintendencia de Servicios de Certificacion Electronica
C	VE (País)
E	acraiz@suscerte.gob.ve
L	(Dirección)
ST	(Estado)
PERÍODO DE VALIDEZ (VALIDITY)	
No antes de: (Not Before)	Fecha en que el período de validez del certificado comienza
No después de: (Not After)	Fecha en que el período de validez del certificado termina
DATOS DEL TITULAR	
CN	Autoridad de Certificacion Raiz del Estado Venezolano
O	Sistema Nacional de Certificacion Electronica
OU	Superintendencia de Servicios de Certificación Electronica
C	VE (País)
E	acraiz@suscerte.gob.ve
L	(Dirección)
ST	(Estado)
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)	
Algoritmo de clave pública (Public Key Algorithm)	Algoritmo con el que se generó la Clave Pública (RSA)
Tamaño de clave pública	4096 bits

CAMPO DEL CERTIFICADO	Valor del Certificado Raíz
EXTENSIONES	
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe contener el atributo CA. CA: True y longitud del path = 2
Nombre alternativo del emisor (Issuer Alternative Name)	
DNSName	Nombre del DNS (suscerte.gob.ve)
OtherName Nº de Identif. OID 2.16.862.2.2	RIF-G-20004036-0
Identificador de clave del titular (Subject Key Identifier)	Medio para identificar certificados que contienen una clave pública particular, facilita la construcción de rutas de certificación (hash)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado
key id	Identificador de la clave
issuer	Contiene todos los datos del emisor
serial	Número serial
Uso de claves (Key usage)	Define el propósito de la clave del certificado. Se debe definir como valor crítico: Firma electrónica del certificado y firma de LCR
Nombre alternativo del titular (Subject Alternative Name)	
DNSName	Nombre del DNS (suscerte.gob.ve)
Other Name	Other Name
Punto de distribución de LCR (CRL Distribution Point)	Indica como se obtiene la información de LCR con SHA1 URI:http://www.suscerte.gob.ve/lcr/certificado-raiz-sha1crlder.crl con SHA256 URI:http://www.suscerte.gob.ve/lcr/certificado-raiz-sha256crlder.crl URI:ldap://acraiz.suscerte.gob.ve
Acceso a la Autoridad de Información (Authority Information Access)	OCSP, URI:http://ocsp.suscerte.gob.ve
Política de Certificados (Certificate Policies)	Incluye toda la información sobre la Política necesaria para la validación del certificado. (Lugar en internet desde donde se descargue la DPC y PC). URL:http://www.suscerte.gob.ve/dpc

Tabla Nº 4. *Estructura de campos del Certificado de la AC Principal PSC.*

CAMPO DEL CERTIFICADO	Valor del Certificado de la AC principal del PSC
Versión	V3
Serial	Identificador único del certifificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma (Signature)	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. Los algoritmos permitidos son SHA1 y SHA256 withRSAEncryption.
DATOS DEL EMISOR	
CN	Autoridad de Certificacion Raiz del Estado Venezolano
O	Sistema Nacional de Certificacion Electronica
OU	Superintendencia de Servicios de Certificacion Electronica
C	VE (País)
E	acraiz@suscerte.gob.ve
L	(Dirección)
ST	(Estado)
PERÍODO DE VALIDEZ (VALIDITY)	
No antes de: (Not Before)	Fecha en que el período de validez del certificado comienza
No después de: (Not After)	Fecha en que el período de validez del certificado termina
DATOS DEL TITULAR	
CN	Identificación del Proveedor de Servicios de Certificacion
O	Sistema Nacional de Certificacion Electronica
OU	Nombre o razón social tal cual aparezca en el documento constitutivo
C	País
E	(correo electronico)
L	(Dirección)
ST	(Estado)
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)	
Algoritmo de clave pública (Public Key Algorithm)	Algoritmo con el que se generó la Clave Pública (RSA)
Tamaño de clave pública	4096 bits

CAMPO DEL CERTIFICADO	Valor del Certificado de la AC principal del PSC
EXTENSIONES	
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe contener el atributo CA. CA: True y longitud del path = 1
Nombre alternativo del emisor (Issuer Alternative Name)	
DNSName	Nombre del DNS (suscerte.gob.ve)
Other Name	Other Name
Nº de Identificación OID 2.16.862.2.2	RIF-G-20004036-0
Identificador de clave del titular (Subject Key Identifier)	Medio para identificar certificados que contienen una clave pública particular, facilita la construcción de rutas de certificación (hash)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier).	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado
key id	Identificador de la clave
issuer	Contiene todos los datos del emisor
serial	Número serial
Uso de claves (Key usage)	Define el propósito de la clave del certificado. Debe especificar como valor crítico: Firma electrónica de certificados, Firma de LCR
Nombre alternativo del titular (Subject Alternative Name)	
DNS Name	(nombre de dominio del PSC registrado en nic.ve)
Other Name	Other Name
OID 2.16.862.2.1	(Código de identificación del PSC acreditado asignado por SUSCERTE)
OID 2.16.862.2.2	RIF-(RIF del PSC) de acuerdo al Anexo Nº 1 de esta norma
Punto de distribución de LCR (CRL Distribution Point)	Indica como se obtiene la información de LCR. con SHA1 URI:http://www.suscerte.gob.ve/lcr/certificado-raiz-sha1crlder.crl con SHA256 URI:http://www.suscerte.gob.ve/lcr/certificado-raiz-sha256crlder.crl
Acceso a la Autoridad de Información (Authority Information Access)	(Enlace al servicio OCSP). Campo opcional URI:http://ocsp.suscerte.gob.ve
Política de Certificados (Certificate Policies)	Incluye toda la información sobre la Política necesaria para la validación del certificado. (Lugar en internet desde donde se descargue la DPC y PC). URL:http://www.suscerte.gob.ve/dpc

Tabla Nº 5. *Estructura de campos del Certificado de la AC Subordinada del PSC.*

CAMPO DEL CERTIFICADO	Valor del Certificado de la AC subordinada del PSC
Versión	V3
Serial	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma (Signature)	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. Los algoritmos permitidos son SHA1 y SHA256 withRSAEncryption.
DATOS DEL EMISOR	
CN	Identificación de la AC Principal del Proveedor de Servicios de Certificacion
O	Sistema Nacional de Certificacion Electronica
OU	Nombre o razón social tal cual aparezca en el documento constitutivo
C	País
E	(correo electronico)
L	(Dirección)
ST	(Estado)
PERÍODO DE VALIDEZ (VALIDITY)	
No antes de: (Not Before)	Fecha en que el período de validez del certificado comienza
No después de: (Not After)	Fecha en que el período de validez del certificado termina
DATOS DEL TITULAR	
CN	Identificación de la AC Subordinada del Proveedor de Servicios de Certificacion
O	Sistema Nacional de Certificacion Electronica
OU	Nombre o razón social tal cual aparezca en el documento constitutivo
C	País
E	(correo electronico)
L	(Dirección)
ST	(Estado)
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)	
Algoritmo de clave pública (Public Key Algorithm)	Algoritmo con el que se generó la Clave Pública (RSA)
Tamaño de clave pública	4096 bits

CAMPO DEL CERTIFICADO	Valor del Certificado de la AC subordinada del PSC
EXTENSIONES	
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe contener el atributo CA. CA: True y longitud del path = 1
Nombre alternativo del emisor (Issuer Alternative Name)	
DNSName	Nombre DNS del PSC (nic.ve)
Other Name	Other Name
Nº de Identificación OID 2.16.862.2.2	RIF-(RIF del PSC)
Identificador de clave del titular (Subject Key Identifier)	Medio para identificar certificados que contienen una clave pública particular, facilita la construcción de rutas de certificación (hash)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier).	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado
key id	Identificador de la clave
issuer	Contiene todos los datos del emisor
serial	Número serial
Uso de claves (Key usage)	Define el propósito de la clave del certificado. Debe especificar como valor crítico: Firma electrónica de certificados, Firma de LCR
Uso de claves Extendido (Extended Key Usage)	Esta extensión es opcional e indica uno o más propósitos para los que la clave pública del certificado puede ser utilizada
Nombre alternativo del titular (Subject Alternative Name)	
DNS Name	(nombre de dominio que identifica a la AC subordinada registrado en nic.ve)
Other Name	Other Name
OID 2.16.862.2.1	(Código de identificación del PSC acreditado asignado por SUSCERTE)
OID 2.16.862.2.2	RIF que identifica a la AC subordinada de acuerdo al Anexo Nº 1 de esta norma
Punto de distribución de LCR (CRL Distribution Point)	Indica como se obtiene la información de LCR con SHA1 y/o con SHA256 del PSC
Acceso a la Autoridad de Información (Authority Information Access)	Indica el servicio del OCSP del PSC. (Enlace al servicio OCSP del PSC). Campo opcional
Política de Certificados (Certificate Policies)	Incluye toda la información sobre la Política necesaria para la validación del certificado. (Lugar en internet desde donde se descargue la DPC y PC).

Tabla Nº 6. *Estructura de campos del Certificado de Personas Naturales.*

CAMPO DEL CERTIFICADO	Valor del Certificado de Persona Natural
Versión	V3
Serial	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma (Signature)	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. Los algoritmos permitidos son SHA1 y SHA256 withRSAEncryption.
DATOS DEL EMISOR (DN)	
CN	(Identificacion de la AC del Proveedor de Servicios de Certificacion que emite el certificado)
O	Sistema Nacional de Certificacion Electronica
OU	(Identificación del Proveedor de Servicios de Certificación)
C	VE (País)
E	(Correo electrónico del PSC)
L	(Dirección)
ST	(Estado)
PERÍODO DE VALIDEZ (VALIDITY)	
No antes de: (Not Before)	Fecha en que el período de validez del certificado comienza
No después de: (Not After)	Fecha en que el período de validez del certificado termina
DATOS DEL TITULAR	
CN	(Nombre de la persona)
O	(Organización) Campo opcional
OU	(Unidad Organizacional) Campo opcional
C	(País)
E	(correo electronico)
L	(Dirección) Campo opcional
ST	(Estado) Campo opcional
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)	
Algoritmo de clave pública (Public Key Algorithm)	Algoritmo con el que se generó la Clave Pública (RSA)
Tamaño de clave pública	2.048 ó 1.024 bits

CAMPO DEL CERTIFICADO	Valor del Certificado de Persona Natural
EXTENSIONES	
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe contener el atributo CA. CA: False
Nombre alternativo del emisor	
DNSName	Nombre el DNS del PSC (nic.ve)
otherName	
OID 2.16.862.2.1	Código de identificación del PSC acreditado asignado por SUSCERTE)
OID 2.16.862.2.2	(RIF del PSC) de acuerdo al Anexo Nº 1 de esta norma
Identificador de clave del titular (Subject Key Identifier)	Medio para identificar certificados que contienen una clave pública particular, facilita la construcción de rutas de certificación (hash)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier).	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado
key id	Identificador de la clave
issuer	Contiene todos los datos del emisor
serial	Número serial
Uso de claves (Key usage)	Define el propósito de la clave del certificado. Debe especificar como valor crítico: Firma electrónica y no repudio
Uso de claves Extendido (Extended Key Usage)	Esta extensión es opcional e indica uno o más propósitos para los que la clave pública del certificado puede ser utilizada
Nombre alternativo del titular (Subject Alternative Name)	
otherName	
OID 2.16.862.2.2	Documento de identificación del titular. CI o Pasaporte (de acuerdo al Anexo Nº 1 de esta norma)
Puntos de distribución de LCR (CRLDistributionPoint)	Indica como se obtiene la información de LCR con SHA1 y/o con SHA256 del PSC
Acceso a la Autoridad de Información (Authority Information Access)	Indica el servicio del OCSP del PSC. (Enlace al servicio OCSP del PSC). Campo opcional
Política de Certificados (Certificate Policies)	Incluye toda la información sobre la Política necesaria para la validación del certificado. (Lugar en internet desde donde se descargue la DPC y PC).

Tabla Nº 7. *Estructura de campos del Certificado de Personas Jurídicas.*

CAMPO DEL CERTIFICADO	Valor del Certificado de Persona Jurídica
Versión	V3
Serial	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma (Signature)	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. Los algoritmos permitidos son SHA1 y SHA256 withRSAEncryption.
DATOS DEL EMISOR	
CN	(Identificacion de la AC del Proveedor de Servicios de Certificacion que emite el certificado)
O	Sistema Nacional de Certificacion Electronica
OU	(Identificación del Proveedor de Servicios de Certificación)
C	VE (País)
E	(Correo electrónico del PSC)
L	(Dirección)
ST	(Estado)
PERÍODO DE VALIDEZ (VALIDITY)	
No antes de: (Not Before)	Fecha en que el período de validez del certificado comienza
No después de: (Not After)	Fecha en que el período de validez del certificado termina
DATOS DEL TITULAR	
CN	(Identificación de la persona jurídica tal cual aparece en el documento constitutivo)
O	(Nombre de la Organización)
OU	(Nombre de la Unidad Organizacional) Campo opcional
C	(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)	
Algoritmo de clave pública (Public Key Algorithm)	Algoritmo con el que se generó la Clave Pública (RSA)
Tamaño de clave pública	2.048 bits

CAMPO DEL CERTIFICADO	Valor del Certificado de Persona Jurídica
EXTENSIONES	
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe contener el atributo CA. CA: False
Nombre alternativo del emisor	
DNSName	Nombre del DNS de la AC que emite el certificado
otherName	
OID 2.16.862.2.1	Código de identificación del PSC acreditado asignado por SUSCERTE)
OID 2.16.862.2.2	(RIF del PSC)
Identificador de clave del titular (Subject Key Identifier)	Medio para identificar certificados que contienen una clave pública particular, facilita la construcción de rutas de certificación (hash)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier).	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado
key id	Identificador de la clave
issuer	Contiene todos los datos del emisor
serial	Número serial
Uso de claves (Key usage)	Define el propósito de la clave del certificado. Debe especificar como valor crítico: Firma electrónica y no repudio.
Uso de claves Extendido (Extended Key Usage)	Esta extensión es opcional e indica uno o más propósitos para los que la clave pública del certificado puede ser utilizada
Nombre alternativo del titular (Subject Alternative Name)	
otherName	
OID 2.16.862.2.2	Documento de identificación de la persona jurídica, de acuerdo a lo establecido en el Anexo Nº 1 de esta norma
Puntos de distribución de LCR (CRLDistributionPoint)	Indica como se obtiene la información de LCR con SHA1 y/o con SHA256 del PSC
Acceso a la Autoridad de Información (Authority Information Access)	Indica el servicio del OCSP del PSC. (Enlace al servicio OCSP del PSC). Campo opcional
Política de Certificados (Certificate Policies)	Incluye toda la información sobre la Política necesaria para la validación del certificado. (Lugar en internet desde donde se descargue la DPC y PC).

Tabla Nº 8. *Estructura de campos del Certificado de Servidores.*

CAMPO DEL CERTIFICADO	Valor del Certificado de Servidor o Aplicación
Versión	V3
Serial	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma (Signature)	SHA256 withRSAEncryption
DATOS DEL EMISOR	
CN	(Identificacion de la AC del Proveedor de Servicios de Certificacion que emite el certificado)
O	Sistema Nacional de Certificacion Electronica
OU	(Identificación del Proveedor de Servicios de Certificación)
C	VE (País)
E	(Correo electrónico del PSC)
L	(Dirección)
ST	(Estado)
PERÍODO DE VALIDEZ (VALIDITY)	
No antes de: (Not Before)	Fecha en que el período de validez del certificado comienza
No después de: (Not After)	Fecha en que el período de validez del certificado termina
DATOS DEL TITULAR	
CN	(Identificación del servidor o aplicación)
O	(Nombre de la Organización)
OU	(Nombre de la Unidad Organizacional) Campo opcional
C	(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)	
Algoritmo de clave pública (Public Key Algorithm)	Algoritmo con el que se generó la Clave Pública (RSA)
Tamaño de clave pública	2.048 ó 1.024 bits

CAMPO DEL CERTIFICADO	Valor del Certificado de Servidor o Aplicación
EXTENSIONES	
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe contener el atributo CA. CA: False
Nombre alternativo del emisor	
DNSName	Nombre del DNS del emisor en nic.ve
otherName	
OID 2.16.862.2.1	Código de identificación del PSC acreditado asignado por SUSCERTE)
OID 2.16.862.2.2	(RIF del PSC)
Identificador de clave del titular	Medio para identificar certificados que contienen una clave pública particular, facilita la construcción de rutas de certificación (hash)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier).	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado
key id	Identificador de la clave
issuer	Contiene todos los datos del emisor
serial	Número serial
Uso de claves (Key usage)	Define el propósito de la clave del certificado. Debe especificar como valor crítico: Firma electrónica, no repudio y cifrado de datos.
Uso de claves Extendido (Extended Key Usage)	Esta extensión es opcional e indica uno o más propósitos para los que la clave pública del certificado puede ser utilizada. Campo opcional
Nombre alternativo del titular (Subject Alternative Name)	
dNSName	(nombre de dominio del PSC registrado en nic.ve)
otherName	
OID 2.16.862.2.2	Documento de identificación de la persona jurídica, de acuerdo a lo establecido en el Anexo Nº 1 de esta norma
Dirección IP	IP del servidor
DNS Primario	DNS
DNS Secundario	DNS (opcional)
Puntos de distribución de LCR (CRLDistributionPoint)	Indica como se obtiene la información de LCR con SHA1 y/o con SHA256 del PSC
Acceso a la Autoridad de Información (Authority Information Access)	Indica el servicio del OCSP del PSC. (Enlace al servicio OCSP del PSC). Campo opcional
Política de Certificados	Incluye toda la información sobre la Política necesaria para la validación

CAMPO DEL CERTIFICADO	Valor del Certificado de Servidor o Aplicación
(Certificate Policies)	del certificado. (Lugar en internet desde donde se descargue la DPC y PC).

Tabla Nº 9. *Perfil de Lista de Certificados Revocados.*

NOMBRE DEL CAMPO	VALOR
Versión (version)	Versión 2
Algoritmo de firma (signature)	OID del algoritmo y, de ser necesarios, los parámetros asociados usados por el certificador para firmar la LCR. SHA1 y SHA256 withRSAEncryption.
DATOS DEL EMISOR	
CN	Identificación de la Autoridad de Certificación que emite la lista
O	Sistema Nacional de Certificacion Electronica
OU	Nombre o razón social tal cual aparezca en el documento constitutivo
C	País
E	(correo electronico)
L	(Dirección)
ST	(Estado)
PERÍODO DE VALIDEZ (VALIDITY)	
Última actualización (Last Update)	Indica la fecha de emisión de LCR. La fecha de revocación de la lista no debe ser posterior a esta fecha, La LCR debe estar disponible para consulta, inmediatamente después de emitida
Próxima actualización (Next Update)	Indica la fecha límite de emisión de la próxima LCR
LISTA DE CERTIFICADOS REVOCADOS	
Certificados Revocados (revokedCertificates) (sólo para los casos en que existan certificados revocados)	Contiene la Lista de Certificados Revocados indicados por su número de serie y su fecha de revocación.

Tabla Nº 10. *Extensiones de Lista de Certificados Revocados.*

Extensión	Valor
Identificación de clave de la Autoridad Certificadora (Authority Key Identifier)	Proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una LCR.
Nombre alternativo del emisor. (Issuer Alternative Name)	
DNSName	Nombre del DNS del emisor en nic.ve
Othername	
Número de LCR (CRL Number)	Número de Identificación de la LCR
Indicador de Delta LCR (Delta CRL Indicator)	Indica que una LCR es una LCR incremental o “Delta LCR”. Campo opcional y de presentarse debe ser crítico.
Punto de distribución del emisor. (Issuing Distribution Point)	Identifica el punto de distribución y el alcance de una LCR particular. Campo opcional, Si existiera, este campo debe ser crítico. Ejemplo: indica si la LCR cubre la revocación de certificados del signatario solamente, certificados del certificador solamente, etc.
LCR más reciente – Punto de distribución de la Delta LCR (Freshest CRL – Delta CRL Distribution Point)	Indica donde puede obtenerse la información de la “LCR” de una LCR completa. Esta extensión no debe ser utilizada en “Delta LCR” y no debe ser crítica

6. ANEXOS

6.1 Anexo Nº 1 OID para la Infraestructura Nacional de Certificación Electrónica

6.1.1 SUSCERTE administra el nodo de los OID de la rama ISO de la Unión Internacional de Telecomunicaciones (UIT) de la siguiente familia: **joint-iso-itu-t(2) country(16) ve(862),** para la identificación unívoca de los elementos dentro de la Infraestructura Nacional de Certificación Electrónica.

A continuación se explica la asignación:

6.1.2 La raíz del nodo OID es **joint-iso-itu-t(2) country(16) ve(862),** correspondiente a Venezuela, y se utiliza para la asignación de los OID requeridos en la Infraestructura Nacional de Certificación Electrónica.

6.1.3 La primera rama **joint-iso-itu-t(2) country(16) ve(862) (1)** está asignada a la documentación de la Declaración de Prácticas de Certificación y Políticas de Certificados de la Autoridad de Administración (AC) Raíz gestionada por SUSCERTE, el rango de OID correpondiente es desde **joint-iso-itu-t(2) country(16) ve(862) (1)** hasta **joint-iso-itu-t(2) country(16) ve(862) (1)....(n).**

6.1.4 La segunda rama **joint-iso-itu-t(2) country(16) ve(862) (2)** está asignada a los Campos de Certificados Electrónicos. El rango de acción es desde **joint-iso-itu-t(2) country(16) ve(862) (2)** hasta **joint-iso-itu-t(2) country(16) ve(862) (2)....(n)**.

- Si un Proveedor de Servicios de Certificación (PSC) requiere definir un campo adicional no estándar, debe ser solicitado a SUSCERTE para su aprobación y asignación de su OID respectivo.

- El OID **joint-iso-itu-t(2) country(16) ve(862) (2) (1)** corresponde al campo de identificación del código del PSC acreditado asignado por SUSCERTE.

6.1.5 El OID **joint-iso-itu-t(2) country(16) ve(862) (2) (2)** corresponde a los números de documentos de identificación de los PSC y titulares de los certificados de la siguiente forma:

- Persona Natural - Nacionales:
  CI – (V) – Nº de la cédula de identidad
- Persona Natural – Extranjero, el XX es el código del país:
  PA - (XX) – Nº del pasaporte
- Persona Jurídica – Nacionales:
  RIF- (G) – Nº del Rif (Del sector Gobierno)
  RIF- (J) – Nº del Rif (Del sector Privado)
- Persona Jurídica – Extranjero, el XX es el código del país:
  EX- (XX) – Nº de documento.

6.1.6 Desde la rama **joint-iso-itu-t(2) country(16) ve(862) 3** hasta la **joint-iso-itu-t(2) country(16) ve(862) 10,** está reservada para la identificación de futuros documentos que considere necesario SUSCERTE.

6.1.7 Desde la rama **joint-iso-itu-t(2) country(16) ve(862) 11** hasta la **joint-iso-itu-t(2) country(16) ve(862) n,** está reservada para los documentos de Declaración de Prácticas de Certificación y políticas de Certificados de los Proveedores de Servicios de Certificación acreditados. La designación corresponderá a una previa solicitud hecha por el PSC acreditado ante SUSCERTE.

6.2 Anexo Nº 2 Distribución de los OID para la Infraestructura Nacional de Certificación Electrónica