ANEXO IV

INFRAESTRUCTURA DE FIRMA DIGITAL REPÚBLICA ARGENTINA

LEY N° 25.506

PERFILES DE LOS CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS REVOCADOS

SECRETARÍA DE INNOVACIÓN PÚBLICA

JEFATURA DE GABINETE DE MINISTROS

ANEXO IV

1 - Estructura básica

1.1 – Conceptos generales

La Autoridad de Aplicación adhiere a la especificación ITU X.509 "*Information Technology – Open Systems Interconnection – The Directory: Public- Key and Atribute Certificate Frameworks*", en todos los aspectos relacionados con el formato, codificación, contenidos e interpretación de los certificados digitales y las Listas de Certificados Revocados.

1.2 - Notación

Para la interpretación del presente documento deben tenerse en cuenta las siguientes consideraciones:

a) OBLIGATORIO, indicado por los términos "debe", "requerido", u "obligatorio".

b) RECOMENDADO, donde es altamente aconsejable que los Certificadores Licenciados operen de dicho modo, indicado por los términos "debería" o "recomendado".

c) OPCIONAL, donde los Certificadores Licenciados pueden optar por las alternativas que consideren más convenientes, indicado por los términos "opcional" o "puede".

d) NO PERMITIDO, indicado por los términos "no debe" o "no permitido".

2 - Perfil de certificados digitales

2.1 - Formato

El formato de certificados X.509 v3 permite la utilización de una amplia variedad de opciones; por esta razón, es conveniente definir un perfil único para los certificados, especificando los campos a completar para integrar la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA.

En lo referente a los certificados digitales se adhiere al contenido de los documentos:

- RFC 3739 *"Internet X.509 Public Key Infrastructure Qualified Certificates Profile".*
- RFC 5280 *"Internet X.509 Public Key Infrastructure Certificate and Certificate RevocationList (CRL) Profile".*

En lo referente a las consultas en línea del estado de los certificados, se adhiere particularmente al siguiente documento:

- RFC 6960 "*X.509 Internet Public Key Infrastructure On Line Certificate Status Protocol – OCSP"*

Para una completa implementación de esta especificación se recomienda la consulta de los formatos y definiciones especificadas en los referidos documentos.

Salvo mención explícita, las siguientes especificaciones deben ser aplicadas tanto a los certificados emitidos a personas humanas, jurídicas o aplicaciones, como a aquellos que identifican al Certificador o Prestador de Servicios de Certificación.

2.2 - Campos de los Certificados

Los siguientes campos DEBEN encontrarse presentes en los certificados:

- Versión (*version*).
- Número de Serie (*serialNumber*).
- Algoritmo de Firma (*signature algorithm*).
- Nombre Distintivo del Emisor (*issuer*).
- Validez (Desde, Hasta) (*validity* (*notBefore*, *notAfter*)).
- Nombre Distintivo del Suscriptor (*subject*).
- Clave Pública del Suscriptor (*subjectPublicKeyInfo*).

NO DEBEN estar presentes los siguientes campos porque corresponden a la versión 2 de la especificación X.509:

- Identificador único del Emisor (*issuerUniqueID*).
- Identificador único del Suscriptor (*subjectUniqueID*).

2.2.1 – Versión (*Version*)

El campo *"version"* describe la versión del certificado. DEBE tener el valor DOS (2) (correspondiente a versión 3).

2.2.2 – Número de Serie (*Serial Number*)

El campo *"serialNumber"* contiene un número asignado por el Certificador a cada certificado. Este número DEBE ser único para cada certificado emitido por cada Autoridad Certificante del Certificador.

2.2.3 – Algoritmo de Firma (*Signature Algorithm*)

El campo *"Signature Algorithm"* DEBE contener el identificador de objeto (OID) del algoritmo y, si fueran necesarios, los parámetros asociados usados por el

Certificador para firmar el certificado. Este identificador DEBE ser alguno de los definidos en el [RFC 4055] "*Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*" para RSA, [RFC 5480] "*Elliptic Curve Cryptography Subject Public Key Information*" para curvas elípticas o [RFC 5758] "*Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA*" para DSA y ECDSA.

2.2.4 – Nombre Distintivo del Emisor (*Issuer*)

El campo *"issuer"* DEBE identificar a la organización responsable de la emisión del certificado, mediante la utilización de un subconjunto de los siguientes atributos:

- Código de país (OID 2.5.4.6: *countryName*).
- Nombre de la organización (OID 2.5.4.10: *organizationName*).
- Nombre de la provincia (OID 2.5.4.8: *stateOrProvinceName*).
- Nombre de la localidad (OID 2.5.4.7: *localityName*).
- Número de serie (OID 2.5.4.5: *serialNumber*).
- Nombre común (OID 2.5.4.3: *commonName*).

El contenido de este campo DEBE coincidir con el indicado en el campo del "*distinguishedName*" correspondiente al "*subject*" del certificado emitido por la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA.

Los contenidos y tipos de los atributos DEBEN respetar las mismas pautas establecidas en el punto 2.2.6 para el campo *"subject"* para certificados de Certificadores o Proveedores de Servicios de Firma Digital.

El atributo "*serialNumber*" DEBE estar presente.

El atributo "*organizationName"* DEBE estar presente.

El atributo "*countryName*" DEBE estar presente y DEBE representar el país en el cual se encuentra establecido el emisor, es decir, la REPÚBLICA ARGENTINA. Este atributo DEBE estar codificado según el estándar [ISO 3166].

2.2.5 – Validez (Desde, Hasta) (*Validity* (*notBefore, notAfter*))

El período de la validez del certificado es el intervalo de tiempo durante el cual el suscriptor se encuentra habilitado para utilizarlo.

El campo se representa como una secuencia de dos fechas:

- "*notBefore*": fecha en que el período de validez del certificado comienza.
- "*notAfter*": fecha en que el período de validez del certificado termina.

El período de validez de un certificado es el período de tiempo de *"notBefore"* a *"notAfter"* inclusive.

Se RECOMIENDAN los siguientes periodos de validez para certificados digitales, los cuales DEBEN ser especificados en la Política Única de Certificación:

- **CERTIFICADOS DE CERTIFICADOR**: DIEZ (10) años.
- **CERTIFICADOS DE APLICACIONES**: TRES (3) años.
- **CERTIFICADOS DE PERSONAS HUMANAS**: DOS (2) años.
- **CERTIFICADOS DE PERSONAS JURÍDICAS PÚBLICAS O PRIVADAS**: DOS (2) años.
- **CERTIFICADOS DE AUTORIDAD DE SELLO DE COMPETENCIA:** DOS (2) años.
- **CERTIFICADOS DE AUTORIDAD DE SELLO DE TIEMPO:** DOS (2) años.

Un Certificador NO DEBE emitir un certificado digital con vencimiento posterior al de su propio certificado.

2.2.6 – Nombre Distintivo del Suscriptor *(Subject)*

El campo *"subject"* identifica la entidad asociada a la clave pública guardada en el campo *"subjectPublicKeyInfo"*. DEBE contener un nombre distintivo del suscriptor. Dicho nombre DEBE ser único para cada suscriptor de certificado emitido por un Certificador durante todo el tiempo de vida del mismo.

La identidad del suscriptor DEBE quedar especificada utilizando los siguientes atributos:

- Código de país (OID 2.5.4.6: *countryName*).
- Nombre común (OID 2.5.4.3: *commonName*).
- Número de serie (OID 2.5.4.5: *serialNumber*).

Para los certificados de Certificadores Licenciados, los campos que integran el nombre distintivo del emisor (*issuer DN*) DEBEN coincidir con los campos correspondientes del nombre distintivo del suscriptor (*subject DN*), emitido a nombre del Certificador Licenciado por la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA.

Para certificados de proveedores de servicios de Firma Digital:

- "*commonName"*: DEBE corresponder al nombre del servicio prestado por el Certificador o al nombre de la unidad operativa responsable del servicio.
- "*organizationalUnitName*": en caso de existir PUEDE contener a las unidades operativas relacionadas con el servicio, pudiendo utilizarse varias instancias de este atributo de ser necesario.

- "*organizationName*": DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del servicio.
- "*serialNumber*": DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: ["código de identificación"] ["nro. de identificación"].

  El único valor posible para el campo ["código de identificación"] es "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.
- *"countryName":* DEBE estar presente y DEBE indicar el país en el cual está constituida la Persona Jurídica que brinda el servicio según el estándar IS0 3166.

Para los certificados de Personas Humanas:

- "*commonName*" (OID 2.5.4.3: Nombre común): DEBE estar presente y DEBE corresponder con el nombre que figura en el documento de identidad del suscriptor.
- "*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el tipo y número de identificación del titular, expresado como texto y respetando el siguiente formato y codificación: ["tipo de documento"] ["nro. de documento"]

  El valor posible para el campo [tipo de documento] es "CUIT" o "CUIL": Clave Única de Identificación Tributaria o Laboral (según corresponda).

  En el caso que el suscriptor sea extranjero:

"PA" [país]: Número de Pasaporte y código de país emisor. El atributo [país] DEBE estar codificado según el estándar [IS0 3166] de DOS (2) caracteres.

"EX" [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. El atributo [país] DEBE estar codificado según el estándar [IS0 3166] de DOS (2) caracteres.

- "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE indicar el país de nacimiento del suscriptor codificado según el estándar [ISO 3166].

Para los certificados de Personas Jurídicas Públicas o Privadas:

- "*commonName*" (OID 2.5.4.3: Nombre común): DEBE coincidir con la denominación de la Persona Jurídica Pública o Privada o con el nombre de la unidad operativa responsable del servicio.
- "*organizationalUnitName*" (OID 2.5.4.11: Nombre de la suborganización): PUEDE contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- "*organizationName*" (OID 2.5.4.10: Nombre de la organización): DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada.
- "serialNumber" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

  Los valores posibles para el campo [código de identificación] son:

a) "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

b) "ID" [país]: Número de identificación tributaria para Personas Jurídicas extranjeras. El atributo [país] DEBE estar codificado según el estándar [ISO 3166] de 2 caracteres.

- "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO 3166] de 2 (DOS) caracteres.

Para los certificados de Aplicaciones:

- "*commonName"*: (OID 2.5.4.3: Nombre común): DEBE corresponder al nombre de la aplicación, servicio o de la unidad operativa responsable del servicio.
- "*organizationalUnitName*" (OID 2.5.4.11: Nombre de la suborganización): DEBE contener a las unidades operativas relacionadas con el servicio, en caso de existir, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- *"organizationName"* (OID 2.5.4.10: Nombre de la organización): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del servicio o aplicación.
- "*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: ["código de identificación"]

["nro. de identificación"].

El valor posible para el campo ["código de identificación"] es "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

- "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país en el cual está constituida la Persona Jurídica. El atributo "*countryName*" DEBE estar codificado según el estándar [ISO 3166] de DOS (2) caracteres.

Para los certificados de Autoridad de Sello de Tiempo.

- *"commonName"* (OID 2.5.4.3: Nombre común): DEBE indicar el nombre del servicio.
- *"organizationalUnitName"* (OID 2.5.4.11: Nombre de la suborganización): PUEDE contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- "*organizationName*" (OID 2.5.4.10: Nombre de la organización): DEBE coincidir con la denominación de la Persona Jurídica Pública o Privada.
- "*serialNumber*" (OID 2.5.4.5: Nro de serie): DEBE estar presente y contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

  Los valores posibles para el campo [código de identificación] son:

  a) "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

  b) "ID" [país]: Número de identificación tributaria para Personas

Jurídicas extranjeras. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de DOS (2) caracteres.

- "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y representar el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

Para los Certificados de Autoridad de Sello de Competencia:

- "*commonName*" (OID 2.5.4.3: Nombre común): DEBE indicar el nombre de la Autoridad de Competencia.
- "*organizationName*" (OID 2.5.4.10: Nombre de la organización): DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada.
- "*organizationalUnitName*" (OID 2.5.4.11: Nombre de la suborganización): PUEDE contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- "*serialNumber*" (OID 2.5.4.5: Nro de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

  Los valores posibles para el campo [código de identificación] son: "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.
- "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

2.2.7 – Clave Pública del Suscriptor (*Subject Public Key Info*)

Este campo *"subjectPublicKeyInfo"* se utiliza para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. El identificador utilizado DEBE ser alguno de los definidos en [RFC 4055] para RSA, [RFC 5480] para curvas elípticas o [RFC 5758] para DSA y ECDSA.

2.3 - Extensiones de un Certificado

Las siguientes extensiones DEBEN encontrarse presentes en todos los certificados:

- Restricciones Básicas (*BasicConstraint*).
- Uso de Claves (*KeyUsage*).
- Puntos de Distribución de la Lista de Certificados Revocados (*CRLDistributionPoint*).
- Políticas Únicas de Certificación (*CertificatePolicies*).
- Identificador de la Clave de la Autoridad Certificante (*AuthorityKeyIdentifier*).
- Nombres Alternativos del Suscriptor (*SubjectAlternativeName*).

La extensión "Identificador de la Clave del Suscriptor" (*SubjectKeyIdentifier*) DEBE estar presente en todos los certificados de Autoridad Certificante, de persona humana y de persona jurídica pública o privada.

La extensión "Nombre Alternativo del Suscriptor" (*SubjectAlternativeName*) DEBE estar presente en todos los certificados de persona humana y persona jurídica y PUEDE estar presente en los de aplicaciones.

2.3.1 – Identificador de la Clave de la Autoridad Certificante (*Authority Key Identifier*)

La extensión *"authorityKeyIdentifier"* proporciona un medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo, en los casos en que el emisor tiene múltiples claves de firma.

Esta extensión DEBE estar presente en todos los certificados y NO DEBE ser marcada como crítica.

2.3.2 – Identificador de la Clave del Suscriptor (*Subject Key Identifier*)

La extensión "*subjectKeyIdentifier*" proporciona un medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.

Esta extensión DEBE estar presente en todos los certificados de Autoridad Certificante y NO DEBE ser marcada como crítica.

2.3.3 – Uso de Claves (*Key Usage*)

La extensión *"keyUsage"* define el propósito (por ejemplo: cifrado, firma) de la clave contenida en el certificado. DEBE encontrarse presente. Esta extensión DEBE ser marcada como crítica.

Para certificados de Certificadores:

- El bit "*Certificate Signing*" DEBE tener valor UNO (1).
- El bit "*Off-line CRL Signing*" DEBE tener valor UNO (1).
- El bit *"crlSigning"* DEBE tener valor UNO (1).
- El resto de bits DEBEN tener valor CERO (0).

Para certificados de Personas Humanas, Jurídicas, Aplicaciones, Autoridades de Sello de Tiempo y Autoridades de Sello de Competencia:

- El bit *"digitalSignature"* DEBE tener valor UNO (1).
- El bit "*Non-Repudiation*" DEBE tener valor UNO (1).
- Los bits correspondientes a "*keyEncipherment*", "*dataEncipherment*", DEBEN tener el valor UNO (1). Los bits correspondientes a "*keyAgreement*" y "*encipherOnly*" o "*decipherOnly*" PUEDEN tener el valor UNO (1) en los certificados de personas humanas, jurídicas y de aplicaciones, teniendo en cuenta, para ambos casos, que la pérdida de control de la clave privada correspondiente impedirá descifrar los datos originales.
- Los bits "*crlSigning*" y "*CertSign*" DEBEN tener valor CERO (0).

2.3.4 – Políticas Únicas de Certificación (*Certificate Policies*)

El Certificador DEBE incluir el OID de su Política Única de Certificación que utilizará para la emisión de certificados. Ese OID es asignado por la DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS o quien la reemplace en el futuro. El documento digital que contiene la Política Única de Certificación DEBE ser declarado ante la Autoridad de Aplicación y la extensión *"CertificatePolicies"* DEBE declarar la URI donde el documento estará disponible.

El campo "*userNotice*" DEBE incluir la leyenda "certificado emitido por un Certificador Licenciado en el marco de la Ley Nº 25.506".

La extensión *"CertificatePolicies"* DEBE incluir toda la información sobre la Política Única de Certificación necesaria para la validación del certificado.

Esta extensión DEBE estar presente en todos los certificados.

2.3.5 – Nombres Alternativos del Suscriptor (*Subject Alternative Name*)

En los certificados de personas jurídicas públicas o privadas que no identifiquen a un servicio o aplicación DEBEN incluirse los datos identificatorios de la persona humana a cargo de la custodia de la clave privada. Los datos a incluir en la extensión DEBEN ser representados mediante la utilización de campos de tipo "*otherName*" y son los siguientes:

- Nombre y apellido: DEBE ser utilizado, DEBE contener el OID de "*commonName*" (OID 2.5.4.3: Nombre común) y DEBE respetar lo especificado para el atributo "*commonName*" de los certificados de personas humanas (ver punto 2.2.6)
- Tipo y número de documento: DEBE ser utilizado, DEBE contener el OID de "*serialNumber*" (OID 2.5.4.5: Nro. de serie) y DEBE respetar lo especificado para el atributo "*serialNumber*" de los certificados de personas humanas (ver punto 2.2.6).
- Posición o función del suscriptor: Cuando corresponda será utilizado para indicar la relación que lo vincula con la persona jurídica titular del certificado, DEBE contener el OID de "*title*" (OID 2.5.4.12: Cargo o título).

Adicionalmente, esta extensión "*SubjectAlternativeName*" permite asociar identidades adicionales al suscriptor de un certificado. Las opciones definidas incluyen una dirección de correo electrónico, un nombre DNS, una dirección IP

y un Identificador Uniforme de Recurso (URI).

Esta extensión debe utilizarse para consignar las direcciones de correo electrónico de los suscriptores en lugar del atributo "*email*" del campo "*subject*" sólo en los certificados de personas humanas.

2.3.6 – Restricciones Básicas (*Basic Constraints*)

La extensión *"BasicConstraints"* permite identificar si el suscriptor de un certificado es un Certificador e indica la longitud máxima de las rutas de certificación válidas que el certificado incluye.

Esta extensión DEBE estar presente en todos los certificados.

Los certificados del Certificador DEBEN contener el atributo *"CA"* con valor "*TRUE"* y la extensión DEBE ser marcada como crítica. Los certificados de usuarios finales DEBEN contener el atributo "*Subject Type*" con valor "*End Entity*" y el atributo "*Path Length Constraint*" DEBE tener valor "*NONE"*.

2.3.7 – Uso de Claves Extendido (*Extended Key Usage*)

Esta extensión *"ExtendedKeyUsage"* indica uno o más propósitos para los que la clave pública del certificado puede ser utilizada, además o en lugar de los propósitos básicos indicados en la extensión *"KeyUsage"*.

Esta extensión DEBE ser utilizada al menos en los siguientes casos:

- Certificados para firma de respuestas OCSP DEBEN incluir el valor *"id-kp-OCSPSigning"* (1.3.6.1.5.5.7.3.9).
- Certificados para servicios de certificación digital de fecha y hora DEBEN incluir el valor *"id- kp-timeStamping"* (1.3.6.1.5.5.7.3.8).

No se restringe la utilización de otros propósitos que sean concordantes con lo

establecido en la extensión "*KeyUsage*".

2.3.8 – Puntos de Distribución de la Lista de Certificados Revocados (*CRL Distribution Point*)

La extensión *"CRLDistributionPoint"* indica cómo se obtiene la información de CRL. Esta extensión DEBE estar presente en todos los certificados que no sean autofirmados. Esta extensión NO DEBE ser crítica.

2.3.9 – CRL más reciente (*Freshest CRL*)

La extensión *"FreshestCRL"* indica cómo puede ser obtenida la "*delta CRL*".

En caso de que el Certificador utilice *delta CRL*, esta extensión DEBE estar presente. Esta extensión NO DEBE ser crítica.

2.3.10 – Información de Acceso de la Autoridad Certificante (*Authority Information Access*)

La extensión *"AuthorityInformationAccess"* DEBE ser utilizada para indicar cómo se accede a la información del servicio de OCSP. Esta extensión NO DEBE ser crítica.

2.3.11 – Declaración del Certificado Calificado (*Qualified Certificate Statement*)

La extensión "*QCStatement"* es utilizada para indicar el módulo criptográfico utilizado para la generación de las claves del suscriptor, debiendo contener uno de los siguientes OIDs:

- 2.16.32.1.10.1, cuando las claves sean generadas por software.
- 2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1.

- 2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2.
- 2.16.32.1.10.2.3, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3.

Para los Certificados de Autoridad de Sello de Competencia esta extensión DEBE estar presente con el valor 2.16.32.1.10.2.3 indicando que las claves se generaron en un dispositivo FIPS 140 (versión 2) nivel 3.

Para los certificados cuyas claves hayan sido generadas mediante el Servicio de Firma Digital con Custodia Centralizada de Claves Criptográficas esta extensión DEBE estar presente con el valor 2.16.32.1.10.2.3 indicando que las claves se generaron en un dispositivo FIPS 140 (versión 2) nivel 3.

Esta extensión DEBE estar marcada como no crítica y codificada en "*PKIX*", de acuerdo al RFC 3739.

2.3.12 - Otras extensiones

NO se DEBEN crear nuevas extensiones más allá de las definidas en el presente Anexo.

3 - Perfil de CRLs

3.1 - Formato

El formato de las Listas de Certificados Revocados X.509 permite la utilización de una amplia variedad de opciones; por esta razón, se hace necesario definir un perfil para las Listas de Certificados Revocados, especificando que opciones deben aparecer de manera obligatoria y cuáles no está permitido usar.

En lo referente a CRLs se adhiere al contenido del documento:

- RFC 5280 "*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*".

Para aquellos casos en que no se hace una mención explícita sobre un tema en particular, se recomienda utilizar lo establecido en el documento antes mencionado. Para una completa implementación de esta especificación se recomienda la consulta de los formatos y definiciones especificadas en dicho documento.

3.2 - Campos de una CRL

Los siguientes campos DEBEN encontrarse presentes en todas las CRLs:

- Versión (*version*).
- Algoritmo de Firma (*signature algorithm*).
- Nombre Distintivo del Emisor (*issuer*).
- Día y Hora de Vigencia (*thisUpdate*).
- Próxima Actualización (*nextUpdate*).
- Certificados Revocados (*revokedCertificates*) (sólo en caso de que existan certificados revocados).

3.2.1 – Versión (*Version*)

El campo *"version"* describe la versión de la CRL. DEBE tener el valor UNO (1) (correspondiente a Versión 2).

3.2.2 – Algoritmo de *Firma (signature algorithm)*

El campo *"signature algorithm"* DEBE contener el Identificador de Objeto (OID) de los algoritmos y, de ser necesarios, los parámetros asociados usados por el

Certificador para firmar la CRL. Este identificador DEBE ser alguno de los definidos en el [RFC 4055] para RSA, [RFC 5480] para curvas elípticas (en el caso de utilizarse) o [RFC 5758] para DSA y ECDSA.

3.2.3 – Nombre Distintivo del Emisor (*Issuer*)

El campo *"issuer"* identifica a la entidad que firma y emite la CRL. Los contenidos y tipos de los atributos DEBEN respetar las pautas establecidas para el campo *"issuer"* de un certificado.

3.2.4 – Día y Hora de Vigencia (*This Update*)

El campo *"ThisUpdate"* DEBE estar presente e indicar la fecha de emisión de la CRL. La fecha de revocación de un certificado de la lista no DEBE ser posterior a esta fecha. La CRL DEBE estar disponible para su consulta inmediatamente después de emitida.

3.2.5 – Próxima Actualización (*Next Update*)

El campo *"NextUpdate"* indica la fecha límite de emisión de la próxima CRL. Este campo DEBE estar presente en todas las CRL emitidas.

3.2.6 – Certificados Revocados (*Revoked Certificates*)

El campo *"RevokedCertificates"* contiene la Lista de Certificados Revocados indicando su número de serie y su fecha de revocación. Asimismo, DEBEN incluirse extensiones específicas para cada elemento de esta lista, de acuerdo a lo establecido a continuación.

3.3 - Extensiones de una CRL

3.3.1 – Identificación de Clave de la Autoridad Certificante (*Authority Key Identifier*)

La extensión *"AuthorityKeyIdentifier"* proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una CRL.

Esta extensión DEBE estar presente en todas las Listas de Certificados Revocados.

3.3.2 - Número de CRL (*CRL Number*)

La extensión *"CRLNumber"* contiene un número de secuencia creciente para una CRL y emisor dado. Esta extensión permite que los usuarios determinen fácilmente cuándo una CRL particular reemplaza a otra CRL.

Esta extensión DEBE estar incluida en todas las Listas de Certificados Revocados.

3.3.3 – Indicador de Delta CRL (*Delta CRL Indicator*)

La extensión *"DeltaCRLIndicator"* permite indicar que una CRL es una CRL incremental o "*delta CRL*".

El Certificador PUEDE utilizar "delta CRL". De existir esta extensión DEBE ser crítica.

3.3.4 – Punto de Distribución del Emisor (*Issuing Distribution Point*)

La extensión *"IssuingDistributionPoint"* identifica el punto de distribución y el alcance de una CRL particular. Indica, por ejemplo, si la CRL cubre solamente la revocación de certificados del suscriptor o de certificados del Certificador.

Si existiera esta extensión DEBE ser considerada como crítica.

3.3.5 – CRL más Reciente – Punto de Distribución de la Delta CRL (*Freshest CRL - Delta CRL Distribution Point*)

La extensión *"FreshestCRL"* indica dónde puede obtenerse la información de la "*CRL*" de una CRL completa.

Esta extensión NO DEBE ser utilizada en "*delta CRL*". Esta extensión NO DEBE ser crítica.

3.3.6 - Otras extensiones de CRLs

NO DEBEN crearse nuevas extensiones más allá de las definidas en [RFC 5280] y sus actualizaciones.

3.4 - Extensiones de un elemento de la Lista de Certificados Revocados (*Revoked Certificates*)

3.4.1 – Código de motivo (*Reason Code*)

La extensión *"ReasonCode"* indica la razón de revocación de un elemento de la CRL. Se RECOMIENDA incluir el motivo de revocación del certificado.

3.4.2 – Fecha de invalidez (*Invalidity Date*)

La extensión *"InvalidityDate"* indica la fecha en la cual se sabe o se sospecha que la clave privada fue comprometida o que el certificado pasó a ser inválido.

3.4.3 – Emisor del certificado (*Certificate Issuer*)

La extensión "*CertificateIssuer*" identifica al emisor del certificado asociado con una entrada en una CRL indirecta, es decir una CRL que tenga el indicador "*indirectCRL*" en su extensión "*IssuingDistributionPoint*".

Esta extensión DEBE ser crítica.

Se RECOMIENDA que las implementaciones reconozcan esta extensión.

3.4.4 - Otras extensiones de entradas de la Lista de Certificados Revocados

NO se RECOMIENDA la creación de nuevas extensiones más allá de las definidas en el presente Anexo.

4 - Perfil de la consulta en línea del estado del certificado

4.1 - Formato

El formato de la consulta en línea del estado del certificado se realiza utilizando el Protocolo OCSP (*On-Line Certificate Status Protocol*). Esta consulta se utiliza para determinar el estado de un certificado digital como método alternativo a la Lista de Certificados Revocados. En esta sección se especifican los campos a utilizar, adhiriéndose al contenido de los documentos:

- RFC 5280 "*Internet X.509 Public Key Infrastructure Certificate and Certificate RevocationList (CRL) Profile*".
- RFC 6960 "*X.509 Internet Public Key Infrastructure On Line Certificate Status Protocol - OCSP*".

Para una completa implementación de esta especificación se recomienda la consulta de los formatos y definiciones especificados en dichos documentos.

4.2 - Consultas OCSP

Los siguientes datos DEBEN encontrarse presentes en las consultas:

- Versión (*version*).
- Requerimiento de servicio (*service request*).
- Identificador del certificado bajo consulta (*target certificate identifier*).
- Extensiones opcionales (*optionals extensions*), las cuales podrían ser procesadas por quien responde.

Al recibir la consulta OCSP, quien responde DEBE determinar:

- Si el formato de la consulta es adecuado.
- Si quien responde se encuentra habilitado para responder la consulta.
- Si la consulta contiene la información que necesita quien responde.

Si alguna de estas condiciones no se cumpliera, da lugar a un mensaje de error. De lo contrario se devuelve una respuesta.

4.3 – Respuestas OCSP

Todas las respuestas OCSP DEBEN ser firmadas digitalmente por la Autoridad Certificante perteneciente al Certificador Licenciado que emitió el certificado digital para el cual se hace la consulta o bien, por un certificado digital emitido por la Autoridad Certificante para tal fin.

Una respuesta OCSP DEBE considerar los siguientes datos:

- Versión de la sintaxis de respuesta.
- Identificador de quien responde.
- Fecha y hora en la que se genera la respuesta.
- Respuesta respecto al estado del certificado.
- Extensiones opcionales.
- Identificador (OID) único del algoritmo de firma.
- Firma de la respuesta.

La respuesta a una consulta OCSP consiste en:

- Identificador del certificado.
- Valor correspondiente al estado del certificado.
- Período de validez de la respuesta.

- Extensiones opcionales.

Se especifican las siguientes respuestas posibles para el valor correspondiente al estado del certificado:

- Válido (*good*), indicando una respuesta positiva a la consulta. Este valor indica que no existe un certificado digital con el número de serie contenido en la consulta, que haya sido revocado durante su vigencia.
- Revocado (*revoked*), indicando que el certificado ha sido revocado.
- Desconocido (*unknown*), indicando que quien responde no reconoce el número de serie incluido en la consulta, debido comúnmente a la inclusión de un emisor desconocido.

5 – Perfil de Sello de Competencia

5.1 – Formato

El formato de certificados X.509 v3 permite la utilización de una amplia variedad de opciones; por esta razón, es conveniente definir un perfil único para los sellos de competencia, especificando los campos a completar para integrar la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA.

En lo referente a los certificados digitales se adhiere al contenido de los documentos:

RFC 5755 "*An Internet Attribute Certificate Profile for Authorization*".

Para una completa implementación de esta especificación se recomienda la consulta de los formatos y definiciones especificadas en los referidos documentos.

5.2 – Campos de los certificados

Los siguientes campos DEBEN encontrarse en los certificados:

- Versión (*version*).
- Número de Serie (*serialNumber*).
- Algoritmo de Firma (*signature algorithm*).
- Nombre Distintivo del Emisor (*issuer*).
- Validez (Desde, Hasta) (*validity (notBefore, notAfter*)).
- Nombre Distintivo del Suscriptor (*holder)*.
- Competencia (*attributes*).

5.2.1 – Versión (*versión*)

El campo "*version"* describe la versión del sello de competencia. DEBE tener el valor 2 (correspondiente a la versión 3)

5.2.2 – Número de Serie (*Serial Number*)

El campo "*serialNumber"* contiene un número asignado por la Autoridad de Competencia a cada certificado. Dicho número DEBE ser único para cada certificado emitido por dicha Autoridad.

5.2.3. – Algoritmo de Firma (*Signature Algorithm*)

El campo "*signature algorithm*" DEBE contener el identificador de objeto (OID) del algoritmo y, si fueran necesarios, los parámetros asociados usados por la Autoridad de Competencia para firmar el certificado. Este identificador DEBE ser alguno de los definidos en el [RFC 4055] para RSA, [RFC 5480] para curvas elípticas o [RFC 5758] para DSA y ECDSA.

5.2.4. – Nombre Distintivo del Emisor (*issuer*)

El campo "*issuer*" DEBE identificar la organización responsable de la emisión del sello de competencia.

El contenido de este campo DEBE coincidir con el indicado en el campo del "*distinguishedName*" correspondiente al "*subject*" del certificado emitido de la Autoridad de Competencia que fuera emitido por la Autoridad Certificante del Certificador Licenciado.

5.2.5 – Validez (Desde, Hasta) *(attrCertValidityPeriod (notBefore, notAfter))*

El período de la validez es el intervalo de tiempo durante el cual el sello de competencia se considera válido. Este intervalo dependerá de la validez del atributo correspondiente.

El campo se representa como una secuencia de dos fechas:

"notBefore": fecha en que el período de validez del certificado comienza.

"notAfter": fecha en que el período de validez del certificado termina.

El periodo de validez de un certificado es el período de tiempo desde "*notBefore*" hasta "*notAfter*" inclusive.

Una autoridad de competencia NO DEBE emitir un certificado con vencimiento posterior al de su propio certificado.

5.2.6 – Nombre Distintivo del Titular (*holder*)

El campo "*subjet*" identifica la entidad asociada a la competencia contenida en el certificado. DEBE contener un nombre distintivo del titular. Dicho nombre DEBE ser único para cada titular de certificado emitido por una autoridad de competencia durante todo el tiempo de vida del mismo.

La identidad del suscriptor DEBE quedar especificada utilizando los siguientes atributos:

- Nombre común (OID 2.5.4.3: *commonName*).
- Número de serie (OID 2.5.4.5: *serialNumber*)

Para certificados de personas jurídicas:

"*commonName*": DEBE corresponder al nombre de la Persona Jurídica Pública o Privada.

"*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: ["código de identificación"] [nro. de identificación].

El único valor posible para el campo [código de identificación] es "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

Para los certificados de Personas Humanas:

"*commonName*": DEBE estar presente y DEBE corresponder al nombre de que figura en el documento de identidad del suscriptor.

"serialNumber" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el tipo y número de identificación del titular, expresado como texto y respetando el siguiente formato y codificación: ["tipo de documento"] [nro. de documento].

El único valor posible para el campo [tipo de documento] es "CUIT" o "CUIL": Clave Única de Identificación Tributaria o Laboral, según corresponda.

5.2.7 – Competencia (*attributes*)

Este campo contiene las competencias asociadas al titular, que se está certificando. Pueden tratarse de competencias profesionales, relaciones laborales o similar.

6 - Algoritmos criptográficos

Los algoritmos utilizados DEBEN ser los especificados en el [RFC 4055] para RSA, [RFC 5480] para curvas elípticas o [RFC 5758] para DSA y ECDSA o los que, en su defecto, determine la Autoridad de Aplicación.

Todos los certificados DEBEN respetar las siguientes longitudes mínimas de claves para los algoritmos de firma:

- **Para certificados de Certificador o de información de estado de certificados**:

CUATRO MIL NOVENTA Y SEIS (4096) bits si se utiliza RSA o DSA y TRESCIENTOS OCHENTA Y CUATRO (384) bits en caso de ECDSA.

- **Para certificados utilizados en servicios relacionados con la Firma Digital**:

DOS MIL CUARENTA Y OCHO (2048) bits si se utiliza RSA o DSA y DOSCIENTOS VEINTICUATRO (224) bits en caso de ECDSA.

- **Para certificados de Oficiales de Registro**:

DOS MIL CUARENTA Y OCHO (2048) bits si se utiliza RSA o DSA y DOSCIENTOS VEINTICUATRO (224) bits en caso de ECDSA.

- **Para certificados de suscriptores (personas humanas o jurídicas):**

DOS MIL CUARENTA Y OCHO (2048) bits si se utiliza RSA o DSA y DOSCIENTOS

VEINTICUATRO (224) bits en caso de ECDSA.

7 – Correspondencia con estándares

A continuación, se establece un paralelo entre las definiciones incluidas en esta especificación y los ítems respectivos definidos en los documentos [RFC 4055], [RFC 5480], [RFC 5758], [RFC 5280], [RFC 3739], [ISO/IEC 9594-8] y la Ley Nº 25.506, incluyéndose referencias a cada uno de ellos.

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Hoja Adicional de Firmas
Anexo

Número: IF-2021-61068229-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Jueves 8 de Julio de 2021

Referencia: ANEXO IV: PERFILES DE LOS CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS REVOCADOS

El documento fue importado por el sistema GEDO con un total de 31 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.07.08 11:01:33 -03:00

Luis Mariano PAPAGNI
Subsecretario
Subsecretaría de Innovación Administrativa
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2021.07.08 11:01:34 -03:00