DOCUMENTO TÉCNICO

DIVISIÓN INFORMÁTICA

Comprobante Fiscal Electrónico (e-Factura)

v. 1.1

Julio de 2012

CÓDIGO: T-5.020.00.000-001

[Página expresamente dejada en blanco]

Tabla de Contenido

1. Introducción

En el marco del proyecto de Comprobante Fiscal Electrónico (e-Factura), se describen en este documento los aspectos técnicos, en base al marco conceptual del mismo y las definiciones funcionales.

2. Objeto

El objeto es disponer de un documento base con la especificación de las decisiones y lineamientos técnicos respecto al “Proyecto de Comprobante Fiscal Electrónico (e-Factura)”, que las empresas deberán implementar en sus sistemas para incorporarse a este régimen.

3. Alcance

El alcance es el marco técnico, desde la postulación del sujeto pasivo hasta su operación dentro del régimen de facturación electrónica.

4. Público Objetivo

Empresas interesadas en el proyecto de “Comprobante Fiscal Electrónico (e-Factura)”.

5. Estructura de este documento

En las diferentes secciones de este documento se describen las decisiones funcionales y técnicas más relevantes que deberán tener en cuenta los sujetos pasivos para incorporarse al régimen de factura electrónica.

Al final del documento principal, previo a los anexos se incluye un Glosario y Referencias Electrónicas.

En el Anexo A se especifican las definiciones de esquema xml (xsd) que complementan este documento.

En el Anexo B se define sello digital y la autorización para emisión (CAE).

En el Anexo C se describe sintéticamente el mecanismo de PKI para firma digital / electrónica.

En el Anexo D se describe la estructura de un certificado digital / electrónico.

En el Anexo E se describe el código de barras bidimensional: QR-Code.

6. Síntesis de las decisiones funcionales y técnicas más relevantes

Se sintetizan a continuación los aspectos más generales que hacen al marco de los comprobantes fiscales electrónicos.

- Para incorporarse al régimen de Comprobantes Fiscales Electrónicos (CFE) las empresas deben cumplir con un proceso de "Postulación, Certificación y Resolución por parte de DGI".
- Las empresas incorporadas a este régimen se obligan a emitir CFE para los tipos de documentos autorizados de acuerdo a la Resolución antedicha.
- Esta autorización habilita a solicitar una constancia de autorización de emisión (CAE) para cada tipo de CFE a emitir.
- Los CFE se deberán firmar utilizando Firma Electrónica Avanzada.
- El control de los CFE emitidos, a realizarse por parte de DGI, se hará de forma asincrónica. En una situación de régimen ([1]) la información a DGI debe enviarse al momento de emitir el CFE y previo al envío del mismo al receptor. No se requiere autorización online para facturar.
- Las empresas incorporadas a este régimen deberán cumplir los formatos y mecanismos mínimos de intercambio entre emisor y receptor definidos por DGI.
- La representación impresa del CFE deberá incorporar un código de barras bidimensional: QR-Code.

7. Postulación, Certificación y Resolución para ser emisor electrónico

La postulación al régimen de las empresas implica que cumplan con los requisitos y condiciones establecidas, para los tipos de CFE que solicita emitir.

Los postulantes deben conocer toda la normativa e instructivos publicados en la Web y estar en situación de operar con el sistema. Esto implica:

- Contar con un Certificado Electrónico Reconocido de persona jurídica emitido por una entidad de certificación autorizada, bajo el esquema de PKI Uruguay.
- Software para la emisión de los CFE.
- Equipamiento y procedimientos necesarios.

Luego de aceptada la postulación la empresa debe cumplir las pruebas necesarias para poder ser emisor y receptor electrónico. Este proceso de certificación implica realizar:

- Pruebas de envío de CFE y reporte diario correspondiente, con un conjunto de datos asignados por DGI.
- Pruebas de simulación.
- Prueba de envío de CFE con adenda.
- Pruebas de intercambio de información.
- Declaración de cumplimiento de requisitos técnicos.

[1] No contingencia.

A su vez DGI dejará a disposición un sitio de pruebas que las empresas podrán utilizar en todo momento.

La empresa obtendrá la autorización como emisor electrónico, luego de haber concluido con todos los pasos incluidos en la Postulación y Certificación y que el Director General de Rentas de la DGI dicte resolución al respecto.

8. Obtención de la Autorización para emisión de CFE

El emisor electrónico está habilitado para solicitar por cada tipo de CFE una constancia de autorización para emisión (CAE), la cual tiene asociado un rango de numeración para ese tipo de CFE.

La autorización para emisión tiene entre otro datos: el número de autorización para emisión, serie y rango autorizado, tipo de CFE, vencimiento y firma electrónica avanzada de DGI.

Para ver el detalle de la estructura del CAE referirse al "**Anexo B** - Autorización de Emisión y Sello digital".

9. Generación de firma electrónica avanzada para CFE

Elementos utilizados en la generación de firma electrónica avanzada:

- Documento a firmar, en este caso un CFE.
- Certificado Electrónico Reconocido (CER) de persona jurídica, emitido por una Autoridad de Certificados (CA) acreditada, y su correspondiente clave privada.
- Algoritmos de criptografía de hash ([2]) y clave pública para firma electrónica avanzada.
- Especificaciones de conversión de la firma electrónica avanzada a Base 64.

10. Autenticación del emisor e Integridad de los documentos electrónicos

Se describe a continuación los elementos técnicos involucrados, y que cualidades desde el punto de vista de la seguridad de la información están involucradas y cuales no, y como se logran los atributos de seguridad requeridos.

10.1. Firma electrónica avanzada

La firma digital o electrónica, se basa en la teoría de clave pública y privada (PKI), y confía en el uso de certificados digitales. En particular, para la firma electrónica avanzada, estos certificados son emitidos por una CA acreditada, denominados por tanto Certificados Electrónicos Reconocidos (CER).

[2] Algoritmo matemático de función dispersa muy sensible a la variación de la entrada, y "casi" inyectiva. "Casi" en el sentido que presenta muy pocas colisiones o muy difíciles de encontrar.

Firma Electrónica Avanzada ([3]), es la firma electrónica que cumple los siguientes requisitos:

1. Requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;
2. ser creada por medios que el firmante pueda mantener bajo su exclusivo control;
3. ser susceptible de verificación por terceros;
4. estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detectable; y
5. haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma.

Para régimen de CFE, se utilizarán Certificados Electrónicos Reconocidos de persona jurídica emitidos por una CA perteneciente a la PKI-Uruguay.

Mientras no esté operativo el "Registro de Prestadores de Servicios de Certificación", según la ley 18.600 de 2009, se utilizarán los certificados de persona jurídica ("Política de Certificación – Empresa" [5]) expedidos por "El Correo Uruguayo" (Administración Nacional de Correos del Uruguay) a su RUC.

10.2. Autenticación / Autoría de la firma e Integridad del CFE

La persona jurídica está autenticada por su Certificado Electrónico Reconocido y el acceso a su clave privada. Es por tanto responsable absoluta de su firma electrónica avanzada, de igual manera que lo es una persona física de su firma ológrafa.

Tanto la DGI como el receptor de la factura, pueden estar seguros que la firma fue realizada con la clave privada que corresponde unívocamente a la persona jurídica propietaria del mismo, y esto se garantiza por el Certificado Electrónico Reconocido, otorgado por una Entidad/Autoridad Certificadora de la PKI Uruguay.

Además el sistema de facturación de la empresa emisora, debería tomar los recaudos correspondientes de seguridad para hacer que el acceso a la clave privada correspondiente al certificado digital de la persona jurídica cuente con los requerimientos de seguridad pertinentes, es decir, ser auditable y garantizar el acceso únicamente a personas autorizadas para ello.

Con la firma electrónica avanzada, además de asegurar la identidad y el "no repudio" del Emisor, se garantiza la integridad del CFE.

A los efectos de garantizar otros atributos requeridos de seguridad de la información como la confidencialidad y el no repudio del receptor, deben implementarse con otros mecanismos, como el cifrado y el protocolo de envío del CFE. (Ver "11 - Transmisión de los CFE a DGI" y "Implementar el intercambio de CFE entre emisor y receptor").

[3] Ley nro. 18.600 de 2009

10.3. Algoritmos y Protocolos de Firma

Para el régimen de CFE la DGI a optado por RSA – SHA1 como algoritmos de firma electrónica.

Los algoritmos utilizados en la generación de firma electrónica avanzada implementada con RSA + SHA1 son los siguientes:

SHA1, que es una función hash de un solo sentido tal que para cualquier entrada (< 2^64 bits) produce una salida compleja de 160 bits (*digest* o resumen).

RSA Private Encrypt: que utiliza la clave privada del emisor para cifrar el resumen (*digest*) del mensaje.

RSA Public Decrypt: que utiliza la clave pública del emisor para descifrar el resumen (*digest*) del mensaje.

Nota:
El Certificado con el que se firma debe estar vigente al momento de la firma y por lo tanto no haber caducado ni haber sido revocado.

10.4. Representación Impresa del CFE

En la representación impresa del CFE se deberá incluir el código de barras bidimensional: QR-Code correspondiente al sello digital de acuerdo a lo definido en el "**Anexo B** - Autorización de Emisión y Sello digital".

Para acceder a los detalles de la codificación QR referirse al "**Anexo E** - Codificación QR del sello digital en la representación impresa del CFE"

11. Trasmisión de los CFE a DGI

Existirán los siguientes mecanismos de envío de los CFE a DGI:

- Web Services seguros, utilizando WS-Security con cifrado.
- Upload seguro de archivo, utilizando cifrado del canal (SSL).

En caso que DGI lo entienda conveniente se podrán habilitar otros mecanismos de trasmisión.

Los envíos de los CFE a DGI se harán en Sobres (archivo xml) de acuerdo a la especificación: EnvioCFE (xsd) conteniendo uno o más CFE según la especificación: CFE (xsd).

El envío del Reporte Diario se hará de acuerdo a la especificación: reporte_diario_CFE (xsd).

La DGI acusará recibo de estos envíos. Referirse a la sección “12.8 Acuses de recibo por parte de DGI”

12. Funciones a incorporar en los sistemas de facturación

Una vez cumplido con el proceso de postulación y obtenida la autorización por parte de DGI para incorporarse al régimen de CFE, la empresa debe incorporar en sus aplicaciones las funcionalidades certificadas que le permitan operar de forma electrónica.

Todo CFE debe estar numerado en forma única y estar firmado - con firma electrónica avanzada. Se describen a continuación las principales funcionalidades requeridas para tal fin.

12.1. Incorporar el rango de numeración autorizado a su sistema de facturación

El emisor debe ingresar en su sistema de facturación la información correspondiente al CAE.

El CAE debería ser resguardado bajo las políticas y mecanismos de seguridad que preserven su integridad.

El sistema debe administrar el rango de numeración por tipo CFE.

12.2. Asignar número único a cada documento

El sistema del emisor debe asignar en forma única un número para cada CFE, utilizando para ello el rango autorizado por DGI para el tipo de CFE que corresponda. El mecanismo e implementación de la asignación del número al CFE deberá asegurar la unicidad en la numeración.

12.3. Generar documento en formato XML exigido por DGI

El emisor debe generar el CFE en formato XML de acuerdo al formato definido por DGI. Ver “**Anexo A** - Estructura del XML de los CFE (XSD) “.

12.4. Firmar el CFE completo

El emisor debe generar la firma electrónica avanzada sobre el CFE completo excluyendo adenda. Esta firma debe ser generada con un Certificado Electrónico Reconocido vigente y no revocado al momento de la firma.

12.5. Adecuar procedimiento de impresión de los CFE

El emisor debe adecuar sus procedimientos y formularios utilizados para la impresión, con el fin de generar la representación impresa especificada por DGI, incluyendo el código de barras bidimensional QR-Code, que contenga la información del sello digital.

La información incluida en la impresión del Sello digital puede consultarse en el "**Anexo B** - Autorización de Emisión y Sello digital".

12.6. Implementar el intercambio de CFE entre emisor y receptor

El receptor electrónico debe acusar respuesta del envío de un CFE con un comprobante electrónico de recepción de envío, de acuerdo al schema XML (XSD) definido por DGI (ACKCFE_Partes.xsd).

Dicho acuse de recibo deberá además contener la firma electrónica avanzada del receptor.

12.7.Acuses de recibo por parte de DGI

La DGI acusará recibo tanto del Sobre conteniendo los CFE así como de cada uno de ellos. Los archivos xsd que definen la estructura de los xml correspondientes pueden consultarse en [6] así como la Cartilla descriptiva correspondiente.

Referencias Electrónicas

[1] Firma digital, archivos XML
http://www.w3.org/TR/xmldsig-core/

[2] Web Services Security:
http://www.oasis-open.org/specs/index.php#wss

[3] Código QR - Standard ISO 18.004
http://www.iso.org

[4] Parlamento – Ley Nro. 18.600
http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18600&Anchor=

[5] El Correo Uruguayo
http://www.correo.com.uy/index.asp?pagVal=210

[6] Estructura de los documentos XML (XSD) y Cartilla descriptiva correspondiente – Sitio Web de e-Factura.
https://www.efactura.dgi.gub.uy/principal/ampliacion-de-contenido/DocumentosDeInteres1?es

Glosario

AGESIC	Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.
CA	*Certification Authority*. Autoridad de certificación, en la que confían los usuarios de los sistemas de certificación, para la emisión y revocación de certificados.
CAE	Constancia de Autorización de Emisión de CFE.
CER	Certificado Electrónico Reconocido: certificado electrónico emitido por un prestador de servicios de certificación acreditado.
CFE	Comprobante Fiscal Electrónico.
DGI	Dirección General Impositiva.
PKI	*Public Key Infrastructure*. Infraestructura de clave pública.
PKI Uruguay	Infraestructura de Clave Pública para Uruguay.
QR Code	*Quick Response Code*– tipo de código de barras bidimensional.
RSA	Rivest, Shamir y Adleman. Algoritmo criptográfico de clave pública.
SHA1	*Secure Hash Algorithm*. Algoritmo criptográfico de *hash* seguro.
SSL	*Secure Sockets Layer*. Protocolo criptográfico utilizado para establecer conexiones seguras.
UCE	Unidad de Certificación Electrónica.
XML	*eXtensible Markup Language.* Lenguaje de marcas extensible.
XSD	*XML Schema Definition*. Definición de esquema para XML.

Anexo A

Definición de esquemas XML
(XSD)

Complementan la información referida en este documento las definiciones de esquema de los XML correspondientes en cada caso.

Los archivos XSD, que definen la estructura de los documentos xml utilizados para Comprobante Fiscal Electrónico, así como su cartilla descriptiva están publicados en [6]:

https://www.efactura.dgi.gub.uy/principal/ampliacion-de-contenido/DocumentosDeInteres1?es

Anexo B

Autorización de Emisión y Sello digital

Autorización de emisión de CFE (CAE)

La autorización de CFE a ser firmada con firma electrónica avanzada de DGI debe contener los siguientes datos, además de presentar sellado de tiempo (*timestamp*):

RUC Emisor	Corresponde al RUC del emisor electrónico que se le asigna el CAE.
Tipo CFE	Tipo de CFE que se autoriza.
Serie CFE	Serie de CFE que se autoriza.
Número Desde	Desde del rango autorizado para el CFE.
Número Hasta	Hasta del rango autorizado para el CFE.
Tipo Autorización	Código de autorización para emisor electrónico.
Número Autorización	Número asignado a la autorización.
Fecha Emisión	Fecha de emisión del CAE
Fecha Vencimiento	Fecha de vigencia de la documentación

Sello digital

Se especifica a continuación la composición del sello digital.

Link al Portal e-factura con los siguientes parámetros:

- Nº de RUC emisor
- Tipo de CFE
- Nº de comprobante (serie y Nº)
- Monto: (Remito “0”, Resguardo “A-C125” y resto “A-C130”)
- Fecha de la firma (dd/mm/yyyy)
- Código de seguridad del CFE (hash SHA-1)

El link tendrá la siguiente forma:

https://www.efactura.dgi.gub.uy/consultaQR/cfe?ruc,tipoCFE,serie,nroCFE,monto,fecha,hash

Se definió que el mismo sea utilizado únicamente en la representación impresa del CFE, y corresponde a la representación en Código de Barras Bidimensional.

Anexo C

FIRMA DIGITAL Y PKI

1. Firma electrónica avanzada

La firma digital o electrónica, se basa en la teoría de clave pública y privada (PKI), y confía en el uso de certificados digitales.

Para firmar Comprobantes Fiscales Electrónicos (CFE), se utilizarán Certificados Electrónicos Reconocidos de persona jurídica otorgados por una CA perteneciente a la PKI-Uruguay.

1.1. Cualidades de la Firma Electrónica Avanzada

Se describen a continuación las principales cualidades de la Firma Electrónica Avanzada, en general, compartidas con la firma digital en general.

1.1.1 Autenticación / Autoría de la firma

La persona jurídica está autenticada por su Certificado Electrónico Reconocido y el acceso a su clave privada. Es por tanto responsable absoluta de su firma electrónica avanzada, de igual manera que lo es una persona física de su firma ológrafa.

Tanto la DGI como el receptor de la factura, pueden estar seguros que la firma fue realizada con la clave privada que corresponde unívocamente a la persona jurídica propietaria del mismo, y esto se garantiza por el Certificado Electrónico Reconocido, otorgado por una Entidad/Autoridad Certificadora de la PKI Uruguay.

1.1.2 Integridad

La Firma Digital, y por tanto la Firma Electrónica Avanzada, asegura la integridad del documento/CFE. No puede alterarse ni agregando, ni modificando ni borrando datos. El resumen (*digest*) calculado con la función de *hash* involucra la información digital de la totalidad del CFE. Cualquier cambio alteraría el cálculo del mismo y violaría el control de integridad (no se verificaría la firma).

1.1.3 No Repudio del Emisor

Al estar el documento (CFE) firmado digitalmente (con firma electrónica avanzada), la persona jurídica propietaria del mismo no puede negar su autoría. Es la única responsable de su clave privada. Si el documento es verificado con la clave pública correspondiente, sólo alguien con acceso a la clave privada pudo haberlo firmado, y es en definitiva, responsabilidad de la persona jurídica, y por tanto de su/s titular/es.

1.1.4 Confidencialidad

La firma digital – así como la firma electrónica avanzada-, no asegura la confidencialidad del documento/ factura (ni de un mensaje).

Para lograr esto, deben utilizarse mecanismos de cifrado de datos.

1.1.5 No Repudio del Receptor

La firma digital – así como la firma electrónica avanzada - por sí sola, tampoco asegura la recepción del documento.

2. Mecanismo de clave pública: PKI

La firma digital o electrónica, se basa en la teoría de clave pública (PKI), y confía en el uso de certificados digitales / electrónicos y relaciones y propiedades matemáticas que se describen a continuación.

La clave pública y privada de la persona se relacionan matemáticamente en que una es "inversa" de la otra en el sentido de cifrado y descifrado. La clave pública descifra lo que se cifra con la clave privada y viceversa. La clave privada, como lo sugiere el nombre, es privada y secreta.

Si un usuario quiere firmar electrónicamente un documento/mensaje (M), se le aplica al mismo una función de hash ([4]) y se computa así un resumen o código (*Digest*) calculado a partir del documento (M). Ese *Digest*, que es una secuencia de bits, se cifra con la clave privada del emisor (PRV_K).

Se envía al receptor, de forma empaquetada (o ensobrada), el "Resumen" (*Digest*) cifrado, el documento M y el Certificado y la clave pública del emisor.

O sea:

Firma = Cifrar (H(M), PRV_K)
Se envía: El Documento, la Firma y el Certificado del Emisor (con su PUB_K).

Para descifrar:

El Receptor, descifra la Firma recibida con la clave pública del emisor PUB_K y obtiene D1 (D1 = H(M) por construcción).
A su vez, vuelve a computar con la función de Hash sobre el documento recibido el resumen o *digest* (D2).

Si D1 = D2, entonces sabemos que por un lado el documento fue firmado por el dueño de PRV_K (y del Certificado enviado por el Emisor), o sea por el Emisor. Por otra parte,

[4] algoritmo matemático de función dispersa muy sensible a la variación de la entrada, y "casi" inyectiva. "Casi" en el sentido que presenta muy pocas colisiones o muy difíciles de encontrar.

gracias a la función de Hash, tenemos certeza sobre la integridad del documento y que no sufrió alteraciones posteriores a la firma.

Es decir:

D1 = Descifrar (Firma, PUB_K)
D2 = H(M), calculado por el receptor.
Si D1 = D2, entonces las PRV_K y PUB_K se corresponden matemáticamente y son de la persona 'dueña'/responsable del CER de PUB_K.

En particular, para la firma electrónica avanzada, se utilizarán Certificados Electrónicos Reconocidos (CER), los cuales son otorgados y firmados por una Entidad Certificadora acreditada bajo el esquema de PKI Uruguay, y por tanto podemos confiar que esa PUB_K corresponde a quien dice el Certificado (su dueño).

Anexo D

Estructura del Certificado Digital y Certificado Electrónico Reconocido

Según la legislación y normativa vigente para Uruguay

De acuerdo al art. 21 de la ley 18.600 de 2009, los certificados reconocidos tendrán el siguiente contenido:

A) La indicación de que se expiden como tales.

B) El código identificativo único del certificado.

C) La identificación del prestador de servicios de certificación acreditado que expide el certificado, indicando su nombre o razón social, su domicilio, su correo electrónico, su número de identificación fiscal y sus datos de identificación registral.

D) La firma electrónica avanzada del prestador de servicios de certificación acreditado que expide el certificado.

E) La identificación del firmante a través de sus nombres, apellidos y documento de identidad para las personas físicas o la razón social y número de identificación fiscal para las personas jurídicas. Se podrá consignar en el certificado cualquier otra circunstancia del titular en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.

F) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.

G) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

H) El comienzo y el fin del período de validez del certificado.

I) Los límites de uso del certificado, si se prevén.

La consignación en el certificado de cualquier otra información relativa al signatario requerirá su consentimiento expreso.

Según el estándar X.509

La estructura de un certificado digital X.509 v3 es la siguiente:

- Certificado
  - Versión
  - Número de serie
  - ID del algoritmo
  - Emisor
  - Validez
    - No antes de
    - No después de
  - Sujeto
  - Información de clave pública del sujeto
    - Algoritmo de clave pública
    - Clave pública del sujeto
  - Identificador único de emisor (opcional)
  - Identificador único de sujeto (opcional)
  - Extensiones (optional)
    - ...
- Algoritmo usado para firmar el certificado
- Firma digital del certificado

Certificado de Persona Jurídica

Son certificados emitidos para personas jurídicas que desean realizar transacciones electrónicas, ya sea desde servidores de manera automatizada o de forma manual y nominada.

Estos certificados de Firma Digital Empresa tienen las siguientes características:

Nominado: Certificado X.509 con clave RSA de 1024 bits de largo. Se podrá optar por incluir un nombre y documento de identidad al certificado lo cual lo identificará ante terceros dando trazabilidad hasta el solicitante.

Innominado: Certificado X.509 con clave RSA de 1024 bits de largo. Contendrá todos los datos de la empresa pero no incluirá información del solicitante. Pensado para sistemas automatizados.

Por más información http://www.correo.com.uy/index.asp?codPag=firmaDig

A modo de ejemplo, la extensión para 'Firma Digital – Empresa' publicada por "El Correo" es la siguiente:

Firma Digital - PERSONA JURÍDICA	
Campos X509v1	**Contenido**
1. Version	V3
2. Serial Number	No secuencial
3. Signature	sha1RSA
4. Issuer	CN = Correo Uruguayo - CA OU = SERVICIOS ELECTRONICOS O = ADMINISTRACION NACIONAL DE CORREOS C = UY
5. Validity	1 año
6. Subject	CN = Nombre de fantasía de la persona jurídica O = Nombre de registro de la persona jurídica OU = División o Unidad dentro de la persona jurídica OU = Subsecuentes OU podrán contener subdivisiones C = Código de país S = Departamento E = Correo electrónico SerialNumber = [RUC o BPS][Numero de registro]
7. Subject Public Key	RSA (1024 bits)
Campos X509v3	
1. Authority Key Identifier	Hash sobre la clave de la CA
2. Subject Key Identifier	Hash sobre la clave del sujeto
3. Key Usage	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
4. Private Key Usage Period	No se usará
5. Certificate Policies	OID = 1.3.6.1.4.1.31439.1.1.1.4 Valor = http://www.correo.com.uy/correocert/cps.pdf
6. Policy Mappings	No se usará
7. Subject Alternative Name	RFC822 = Correo electrónico otherName = Podrá contener la identificación de la persona física solicitante en el formato: [IDE o PAS][Numero de documento]/[NOMBRE COMPLETO]
8. Issuer Alternative Name	No se usará
9. Subject Directory Attributes	No se usará
10. Basic Constraints	Entidad final
11. Name Constraints	No se usará
12. Policy Constraints	No se usará
13. Extended key usage field	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
14. CRL Distribution Points	http://www.correo.com.uy/CorreoCert/anc.crl

Formatos de nombres

Los certificados emitidos por ANC contienen el *distinguished name* X.500 del emisor y del titular del certificado en los campos *"Issuer" y "Subject"* respectivamente.

El Subject para los certificados de Firma Digital – EMPRESA estará compuesto de los siguientes elementos: CN, O, OU, OU, C, S, E, serialNumber.

El atributo "CN" (commonName) contendrá el nombre de fantasía de la persona jurídica completo en mayúsculas.

El atributo "O" (organizationName) contendrá el nombre de registro de la persona jurídica completo en mayúsculas.

El atributo "OU" (organizationalUnitNames) contendrá el nombre de la unidad (división, área, sector, departamento, etc.) dentro de la organización.

Subsecuentes atributos "OU" (organizationalUnitNames) podrán existir y contener subdivisiones dentro de la unidad (división, área, sector, departamento, etc.).

El atributo "C" (countryName) tendrá el código de país y se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en PrintableString.

El atributo "S" (stateName) tendrá el nombre del departamento, estado o provincia de registro de la organización.

El atributo "E" (emailAddress) tendrá el correo electrónico y se codificará, en IA5String.

El atributo "SerialNumber" contendrá el tipo y número de registro de la persona jurídica. Este atributo concatenará un tipo de registro que será exclusivamente "RUC" para números de registro ante la Dirección General Impositiva o "BPS" para números de registro ante el Banco de Previsión Social, con el número de registro o documento.

Anexo E

Codificación QR del sello digital
en la representación impresa del CFE

Generación e impresión del código QR (Quick Response)

El código QR (ISO/IEC1800) es un código bidimensional con una matriz de propósito general diseñada para un escaneo rápido de la información. Se trata de un código de uso libre, ya que su fabricante ha optado por no ejercer derechos de licencia.

Las impresiones de los comprobantes fiscales deberán incluir un código QR, que será la implementación elegida para la representación del sello digital, utilizando UTF-8 para la codificación de los caracteres.

El uso de impresión térmica y papel térmico sólo será admitido en la emisión de e-tickets y sus notas de corrección. Otros CFEs pueden imprimirse en papel térmico bajo ciertas condiciones([5]) especificadas en [6] (Formato de CFE), de no ser así, la impresión de los restantes tipos de documentos deberá ser realizada con impresoras láser o de inyección de tinta.

Requisitos para la impresión:

En el ángulo inferior izquierdo del documento deberá tener impreso el QR-Code con los siguientes requisitos:

- Impresora con una resolución mayor o igual a 200 dpi.
- Color de impresión: negro.
- Tamaño mínimo de 22 x 22 mm con un margen de 3mm en los lados del sello.
- Tamaño máximo de 30 x 30 mm con un margen de 5mm en los lados del sello.

[5] Al momento de escribir este documento, la condición es que los mismos queden disponibles en el Sitio Web del emisor, por 5 años, posibilitando su reimpresión por parte del receptor.