Resolución 0019 de febrero de 2016

Anexo Técnico 002 – Política de Firma de los Documentos XML de Facturación Electrónica – Versión 2

Contenido

17. Momento desde el cual será medido el tiempo al que se refiere el “Artículo 7.42

Control de Versiones

Fecha	Versión	Descripción
2016-02-24	1.0	Versión inicial.
2018-01-05	2.0	- Aclaraciones sobre el documento. - Ejemplificaciones. Actualización de la Resolución 0019-2016, adoptada mediante la Resolución 000001 de fecha: 05 de enero de 2018

1. Introducción

Este documento forma parte de los Anexos Técnicos de la resolución que desarrolla el Decreto 2242 de 2015, por el cual se reglamentan las condiciones de expedición e interoperabilidad de la factura electrónica con fines de masificación y control fiscal.

2. Consideraciones Generales.

El objetivo de esta Política define las principales características técnicas para la firma digital, que garantizan la seguridad, autenticidad y confiabilidad de todos los procesos que soporten la implementación de la factura electrónica en Colombia con fines de masificación y control fiscal, y los criterios comunes para el reconocimiento mutuo de firmas digitales basadas en certificados digitales, que garanticen la seguridad e interoperabilidad.

La Política de Firma está indicada y referenciada para todos los documentos electrónicos que componen el conjunto de documentos del negocio electrónico denominado Facturación Electrónica establecida por el Gobierno Nacional a cargo de la DIAN, mediante el Decreto 2242 de 2015. Para todos los documentos que componen la facturación electrónica la firma se hará mediante la inclusión de una etiqueta i.e. <Signature .../> — dentro del formato estándar de intercambio XML, el cual está localizado en la siguiente ruta:

XPath:

- /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature
- /fe:CreditNote/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature
- /fe:DebitNote/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature

La etiqueta contendrá los elementos que constituyen la implementación del estándar técnico XAdES, i.e. XML Advanced Electronic Signature asc; firma electrónica avanzada XML. Los elementos que componen los detalles se encuentran en el documento «Anexo Técnico 001 – Formatos de los Documentos XML de Facturación Electrónica».

La política de firma suministra la información que sobre la firma digital con destino al control fiscal de la DIAN, deberá aplicar el facturador electrónico como medida de ampliación del proceso de expedición de las facturas electrónicas. Se advierte que los

detalles de las técnicas informáticas de implementación no forman parte de esta política. Únicamente se incluyen las referencias a los estándares que describen las especificaciones técnicas sobre la implementación.

La política de firma suministra la información que sobre la firma digital debiera verificar el Adquirente, de acuerdo con lo previsto en el Artículo 5. Verificación y Rechazo de la factura electrónica, del decreto 2242 de 2015.

3. Referencias Normativas

Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Decreto reglamentario 1747 de 2000 por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

Resolución 36119 de 30 de diciembre de 2005 por la cual se autoriza una entidad de certificación cerrada el Superintendente de Industria y Comercio.

Ley 1341 de 2009 por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Decreto 2364 de 2012 por medio del cual se reglamenta el artículo 7 de la ley 527 de 1999 sobre la Firma Electrónica y se dictan otras disposiciones.

Decreto 19 de 2012 por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

Decreto 333 del 19 de febrero 2014 por el cual se reglamenta el artículo 160 del Decreto ley 9 de 2012, tiene por objeto definir el régimen de acreditación de las entidades de certificación, en desarrollo de lo previsto en dicho artículo.

Normativa de aplicación sobre factura electrónica:

Decreto 410 de 1971 por el que se expide el Código de Comercio y sus modificaciones.

Decreto 624 de 1989 de aprobación del Estatuto Tributario y sus modificaciones.

Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 962 de 2005 por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos y sus modificaciones.

Decreto 1929 de 2007 por el cual se reglamenta el artículo 616-1 del Estatuto Tributario.

Resolución 14465 de 2007 por medio de la cual se establecen las características y contenido técnico de la factura electrónica y de las notas crédito y otros aspectos relacionados con esta modalidad de facturación, y se adecúa el sistema técnico de control.

Ley 1231 de 2008 por la cual se unifica la factura como título valor como mecanismo de financiación para el micro, pequeño y mediano empresario, y se dictan otras disposiciones.

Decreto 3327 de 2009 por el cual se reglamente parcialmente la ley 1231 de 17 de julio de 2008 y se dictan otras disposiciones.

Decreto 2668 de 2010 por el cual se adiciona un parágrafo al artículo 2o del Decreto 1929 de 2007.

Decreto 2242 del 24 de noviembre de 2015 por el cual se reglamentan las condiciones de expedición e interoperabilidad de la factura electrónica con fines de masificación y control fiscal.

Especificaciones técnicas sobre la Firma Electrónica Avanzada:

ETSI TS 101 903, v.1.2.2. v 1.3.2. y 1.4.1. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).

ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infraestructures (SEI); XML format for signature policies.

ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infraestructures (ESI): Algorithms and Paremeters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infraestructures (SEI); Signature policies report.

ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infraestructures (SEI); Signature policy for extended business model.

ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infraestructures (SEI); ASN.1 format for signature policies.

IETF RFC 2560, X.509 Public Key Infrastructure Online Certificate Status-Protocol-OCSP

IETF RFC 3125, Electronic Signature Policies

IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

ITU-T Recommendation X.680 (1997): “Information technology – Abstract Syntax Notation One (ASN.1): Specification on basic notation”

4. Alcance de la Política de Firma

Este documento define la Política de Firma que detalla las condiciones generales para la validación de la factura electrónica y que deberán ser admitidas por todas las plataformas tecnológicas implicadas en el ciclo de facturación electrónica.

5. Política de Firma

5.1. Actores de la Firma

Facturador Electrónico:

Persona natural o jurídica comprendida en el ámbito del Decreto 2242 de 2015 y que como tal debe facturar electrónicamente en las condiciones establecidas en el mismo decreto. Para el ámbito de la firma electrónica son los ***firmantes*** vinculados a la persona natural o jurídica que ha cumplido la habilitación de los Artículos 10 y 11 del Decreto 2242 de 2015.

Adquirente:

En el ámbito de la facturación electrónica es el receptor de la factura electrónica quien debe cumplir con el Artículo 5 del Decreto 2242 de 2015.

Proveedor Tecnológico:

En el ámbito de la facturación electrónica podrá ser el ***firmante*** autorizado por el facturador electrónico a actuar en su nombre.

El término ***firmante*** se circunscribe a la definición dada en el Artículo 1.4 Decreto 2364 de 2012.

Entidades de Certificación Digital - ECD

En el ámbito de la factura electrónica es el tercero de confianza que tiene bajo su control la gestión de constatación, expedición, autenticación y registro histórico de los certificados digitales utilizados para las firmas digitales de las facturas electrónicas.

5.2. Formato de Firma

Se debe utilizar el estándar XMLDSig enveloped con formato XAdES-EPES según la especificación técnica ETSI TS 101 903, versión 1.2.2, versión 1.3.2 y versión 1.4.1 siendo obligatorio indicar la versión adoptada en las etiquetas XML, en las que se hace referencia al número de versión.

El formato XAdES de firma electrónica avanzada adoptado por la DIAN para el uso de firma digital corresponde a la Directiva XAdES-EPES, con el certificado digital y toda la cadena de certificación (desde el certificado raíz) incluida en los elementos «ds:X509Data» y «ds:Object», y la política de firma, es decir este documento, como un hiperenlace en el elemento «xades:SignaturePolicyIdentifier».

Se admiten como válidos los algoritmos de generación de hash, codificación en base64, firma, normalización y transformación definidos en el estándar XMLDSig.

5.3. Proceso de Firma

6. Algoritmo de Firma

El algoritmo de firma usado sobre el elemento «SignedInfo» (organizado previamente como establece el cánon) para la firma digital (que se adiciona al elemento «SignatureValue») de la factura electrónica puede ser cualquiera de los definidos en la especificación XML-Signature Syntax and Processing (http://www.w3.org/TR/xmldsig-core2/#sec-Algorithms) que actualmente son:

Recomendado RSAwithSHA1 http://www.w3.org/2000/09/xmldsig#rsa-sha1

Recomendado RSAwithSHA256 http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

Recomendado RSAwithSHA384 http://www.w3.org/2001/04/xmldsig-more#rsa-sha384

Recomendado RSAwithSHA512 http://www.w3.org/2001/04/xmldsig-more#rsa-sha512

7. Algoritmo de Organización de Datos según el Canon

El algoritmo para organizar los datos según el canon usado sobre el elemento «SignedInfo» para la firma digital (que se adiciona al elemento «SignatureValue») de la factura electrónica es “Canonical XML (omits comments)”. Para esto se debe usar el valor “http://www.w3.org/TR/2001/REC-xml-c14n-20010315” dentro del elemento «CanonicalizationMethod».

> NOTA: atienda lo dicho en la sección “8 Sobre el CANON de los documentos electrónicos y la validez de la firma digital”

```
<ds:CanonicalizationMethod
    Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
```

8. Ubicación de la Firma

La firma se ubicará dentro del documento electrónico en el XPath:

/fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent

/ds:Signature/ds:SignatureValue

en la ruta /Invoice/UBLExtensions/ExtensionContent/Signature como lo define el documento «ANEXO TÉCNICO – FORMATOS DE INTERCAMBIO DE LA FACTURACIÓN ELECTRÓNICA – Definición de los Esquemas y Perfiles XSD».

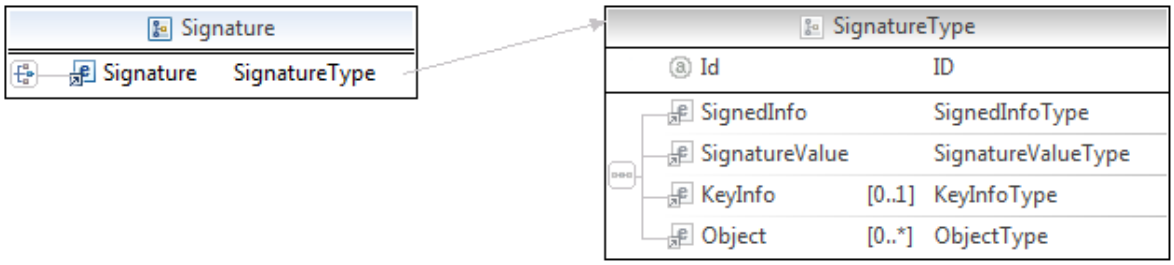

Figura 1. Estructura firma electrónica

9. Condiciones de la Firma

El facturador electrónico o el proveedor tecnológico expresamente autorizado por este para hacerlo deberá aplicar la firma digital sobre el documento completo, con un certificado digital vigente y no revocado al momento de la firma.

La firma se aplica a todos los elementos de la factura electrónica, los elementos contenidos dentro del elemento SignedProperties más la clave pública contenida en el elemento KeyInfo. Cada uno de estos se adiciona como referencia dentro del elemento SignedInfo.

<ds:SignedInfo>

…

<ds:Reference URI="">


```
                <ds:Transforms>
                        <ds:Transform

        Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                </ds:Transforms>
                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>Z4ZtpzPV5wz4pHSbxvX0Yiod+Dw=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#KeyInfo">
                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>WXYRuBvNqeIfwXNlZqRfGWfrl08=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties"
                URI="#SignedProperties">
                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>NRsf6F1vvGb8DJAeEAYVQF3kcDw=</ds:DigestValue>
        </ds:Reference>
        …
</ds:SignedInfo>
```

El certificado público requerido para validar la firma debe ser embebido dentro del XPath:

/fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent
/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate
en formato base64:

```
<ds:KeyInfo Id="KeyInfo">
        <ds:X509Data>

        <ds:X509Certificate>MIIFszCCBJugAwIBAgICJS4wDQYJKoZIhvcNAQEFBQAwgYwxC
zAJBgNVBAYTAkNPMR8wHQYDVQQHExZDYXJyZXJhIDkgMTYtMjEgQm9nb3RhMTIwMAYD
VQQKEylDZXJ0aWNhbWFyYSBTLkEuIEVudGlkYWQgZGUgQ2VydGlmaWNhY2lvbjEoMCYG
A1UEAxMfQ2VydGlmaWNhZG8gRW1wcmVzYXJpYWwgQ2xhc2UtQTAeFw0wNjAxMDMx
NjIxMDlaFw0wODAxMDMxNjIxMDlaMIHLMQswCQYDVQQGEwJDTzENMAsGA1UECBMER
```

C5DLjEPMA0GA1UEBxMGQm9nb3RhMUAwPgYDVQQKEzdEaXJlY2Npb24gZGUgSW1wdW
VzdG9zIHkgQWR1YW5hcyBOYWNpb25hbGVzIGRlIENvbG9tYmlhMRgwFgYDVQQLEw9Qc
m95ZWN0byBNVUlTQ0ExQDA+BgNVBAMTN0RpcmVjY2lvbiBkZSBJbXB1ZXN0b3MgeSBBZ
HVhbmFzIE5hY2lvbmFsZXMgZGUgQ29sb21iaWEwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMI
GJAoGBAIKPxSCoMIBOxjf87AlhSquNNQZgmPXQna5H2WqfxTot8G7e24hAquWZ7QRfwD
W6qIhSGZfffcRXVgGZfMLBzsciPXuMLjYCaepAF7zrCiaAJRft/RMZqngQaM8DdMoVaH1qO
MAqeLgHRdGjcSNCEN/Og2jSdutdnc/r+SToUUP9AgMBAAGjggJgMIICXDAlBgNVHRIEHjAch
hpodHRwOi8vd3d3LmNlcnRpY2FtYXJhLmNvbTAMBgNVHRMBAf8EAjAAMA4GA1UdDwEB
/wQEAwID+DATBgNVHSUEDDAKBggrBgEFBQcDAzARBglghkgBhvhCAQEEBAMCBaAwOAYJ
YIZIAYb4QgEDBCsWKWh0dHA6Ly93d3cuY2VydGljYW1hcmEuY29tL2NlcnRzL2NybC5waHA
/MBMGCWCGSAGG+EIBCAQGFgRodHRwMC0GCWCGSAGG+EIBDQQgFh5DZXJ0aWZpY2F
kbyBkZSBmaXJtYSBkZSBj82RpZ28wHQYDVR0OBBYEFADk16fCfpFySux+Fm19mFxJm3evMI
G5BgNVHSMEgbEwga6AFFN5H20Hz35AtxBO88ii2J1BLSshoYGSpIGPMIGMMQswCQYDVQ
QGEwJDTzEfMB0GA1UEBxMWQ2FycmVyYSA5IDE2LTIxIEJvZ290YTEyMDAGA1UEChMpQ2
VydGljYW1hcmEgUy5BLiBFbnRpZGFkIGRlIENlcnRpZmljYWNpb24xKDAmBgNVBAMTH0Nlc
nRpZmljYWRvIEVtcHJlc2FyaWFsIENsYXNlLUGCAQEwUQYDVR0gBEowSDBGBggrBgEEoVQK
MjA6MDgGCCsGAQUFBwIBFixodHRwOi8vd3d3LmNlcnRpY2FtYXJhLmNvbS9maXJtYV9jb2
RpZ28uaHRtbDBBBgNVHR8EOjA4MDagNKAyhjBodHRwOi8vd3d3LmNlcnRpY2FtYXJhLmNv
bS9jZXJ0cy9jZXJ0aWNhbWFyYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBAA93/J8l+t6KrKerp
8JC3vMwLykh8NnWpUdmUTDJacMY5E+vML23CxSmYifveByt4/s6s+hT/MHYm8khPNIJ4k3
qFRnnQgbgi4GOkRHqfcihF6cahBVO9lZ7Kud6tcTV+zchLmh0fy75QKzSLPEnb7pNdcr1cAYd
984DOgP7HxGBy7mxHUszUt3YCgKMbeuXg86L69ekVWUskydw/q/xLFvQwh/2RVjxdv5ydkr
s8d4+W9G1Z310bw8X3MFzhanG9t2COzjCECTqUCLjXx+Z9Jp79iuLkcwEMNP43kBrBQ94y8
xlLcy295z3EdTd+XHAJ+4dZk+N9mBYUPs4jeW56CM=<ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>

10. Identificador de la Política

10.1. Opción-1 Configuración del ***Identificador de Política*** para certificados digitales tipo ***sha-1***
xPath: /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SignaturePolicyIdentifier/xades:SignaturePolicyId/xades:SigPolicyId/xades:Identifier:=

10.1. Opción-1 Configuración del ***Identificador de Política*** para certificados digitales tipo ***sha-1***
Valor: https://facturaelectronica.dian.gov.co/politicadefirma/v2/politicadefirmav2.pdf
xPath: /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SignaturePolicyIdentifier/xades:SignaturePolicyId/xades:SigPolicyHash/ds:DigestMethod/@Algorithm:= **Valor:** http://www.w3.org/2000/09/xmldsig#sha1
xPath: /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SignaturePolicyIdentifier/xades:SignaturePolicyId/xades:SigPolicyId/xades:Description **Valor:** Política de firma para facturas electrónicas de la República de Colombia.

10.2. Opción-2 Configuración del ***Identificador de Política*** para certificados digitales tipo ***sha-2***
xPath: /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureP

10.2. Opción-2 Configuración del ***Identificador de Política*** para certificados digitales tipo ***sha-2***
roperties/xades:SignaturePolicyIdentifier/xades:SignaturePolicyId/xades:SigPolicyId/xades:Identifier:= **Valor del elemento:** https://facturaelectronica.dian.gov.co/politicadefirma/v2/politicadefirmav2.pdf
xPath: /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SignaturePolicyIdentifier/xades:SignaturePolicyId/xades:SigPolicyHash/ds:DigestMethod/@Algorithm:= **Valor del atributo:** http://www.w3.org/2001/04/xmlenc#sha512 Este valor depende del resumen criptográfico utilizado; vea la Regla-3
xPath: /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SignaturePolicyIdentifier/xades:SignaturePolicyId/xades:SigPolicyId/xades:Description **Valor del elemento:** "Política de firma para facturas electrónicas de la República de Colombia."
OBSERVACIÓN: **Si utiliza y aplica las definiciones de este documento para firmar digitalmente, entonces observe que el nombre del identificador ..**/xades:Identifier cambió, i.e. que existe una nueva Política de Firma

11. Hora de Firma

Se debe especificar en formato xsd:dateTime la fecha y hora en que reclama el firmante haber firmado la factura electrónica.

<xades:SigningTime>2009-07-14T13:28:00+02:00</xades:SigningTime>

NOTA: Es deber de los facturadores electrónicos que los sistemas computacionales que utilicen para el firmado de los documentos deberán estar sincronizados con el reloj de la súper intendencia de industria y comercio el cual determina la hora legal colombiana.

http://www.sic.gov.co/hora-legal-colombiana

12. Firmante

El elemento xades:SignerRole contiene uno y sólo uno de los siguientes atributos:

- "supplier" cuando la firma de la factura la realiza el Obligado a Facturar.
- "third party" cuando la firma la realiza un Proveedor Tecnológico que en su caso, actué en su nombre.

<xades:SignerRole>supplier</xades:SignerRole>

13. Ejemplo Firma

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<fe:Invoice xmlns:fe="http://www.dian.gov.co/contratos/facturaelectronica/v1"
xmlns:cac="urn:oasis:names:specification:ubl:schema:xsd:CommonAggregateComponents-2"
 xmlns:cbc="urn:oasis:names:specification:ubl:schema:xsd:CommonBasicComponents-2"
 xmlns:clm54217="urn:un:unece:uncefact:codelist:specification:54217:2001"
 xmlns:clm66411="urn:un:unece:uncefact:codelist:specification:66411:2001"
xmlns:clmIANAMIMEMediaType="urn:un:unece:uncefact:codelist:specification:IANAMIMEMediaType:2003"
xmlns:ext="urn:oasis:names:specification:ubl:schema:xsd:CommonExtensionComponents-2"
xmlns:qdt="urn:oasis:names:specification:ubl:schema:xsd:QualifiedDatatypes-2"
xmlns:sts="http://www.dian.gov.co/contratos/facturaelectronica/v1/Structures"
xmlns:udt="urn:un:unece:uncefact:data:specification:UnqualifiedDataTypesSchemaModule:2"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="
```


```
http://www.dian.gov.co/contratos/facturaelectronica/v1 http://000-24204z9.dian.loc:18016/micrositios/fac_electronica/documentos/XSD/r1/DIAN_UBL.xsd
">
 <ext:UBLExtensions>
  <ext:UBLExtension>
   <ext:ExtensionContent>
    <sts:DianExtensions>
     <sts:InvoiceControl>
      <sts:InvoiceAuthorization>000001</sts:InvoiceAuthorization>
      <sts:AuthorizationPeriod>
       <cbc:StartDate>2014-01-04</cbc:StartDate>
       <cbc:EndDate>2016-01-04</cbc:EndDate>
      </sts:AuthorizationPeriod>
      <sts:AuthorizedInvoices>
       <sts:Prefix>81</sts:Prefix>
       <sts:From>10007869</sts:From>
       <sts:To>19999999</sts:To>
      </sts:AuthorizedInvoices>
     </sts:InvoiceControl>
     <sts:InvoiceSource>
      <cbc:IdentificationCode listAgencyID="6"
            listAgencyName="United Nations Economic Commission for Europe"

listSchemeURI="urn:oasis:names:specification:ubl:codelist:gc:CountryIdentificationCode-2.0">
             CO
      </cbc:IdentificationCode>
     </sts:InvoiceSource>
     <sts:SoftwareProvider>
      <sts:ProviderID schemeAgencyID="195"
            schemeAgencyName="CO, DIAN (Dirección de Impuestos y Aduanas Nacionales)"
            schemeName="SoftwareMakerID"

schemeURI="http://www.dian.gov.co/contratos/facturaelectronica/v1/anexo_v1_0.html#SoftwareMakerID">
             700085380
      </sts:ProviderID>
```


```
    <sts:SoftwareID schemeAgencyID="195"
            schemeAgencyName="CO, DIAN (Dirección de Impuestos y Aduanas
Nacionales)"
            schemeName="SoftwareID"

schemeURI="http://www.dian.gov.co/contratos/facturaelectronica/v1/anexo_v1_0.html#
sofwareID">
             8bad2864-011e-4fa1-8bfe-843ab63a4bf2
     </sts:SoftwareID>
    </sts:SoftwareProvider>
    <sts:SoftwareSecurityCode
            schemeAgencyID="195"
            schemeAgencyName="CO, DIAN (Dirección de Impuestos y Aduanas Nacionales)"
            schemeName="SoftwareSecurityCode"

schemeURI="http://www.dian.gov.co/contratos/facturaelectronica/v1/anexo_v1_0.html#
SofwareSecurityCode">

54bf6b1cfe683bcaf1fe8b67e98e9facfb5d3ec011a9966327f6d2b5c368d59d76d811e40d
19f050e4a8ea0eaa0a0d42
    </sts:SoftwareSecurityCode>
   </sts:DianExtensions>
  </ext:ExtensionContent>
 </ext:UBLExtension>
 <ext:UBLExtension>
  <ext:ExtensionContent>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
           Id="xmldsig-e2f27048-53c6-4130-bf5e-5915089e9807">
    <ds:SignedInfo>
     <ds:CanonicalizationMethod  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
     <ds:Reference Id="xmldsig-e2f27048-53c6-4130-bf5e-5915089e9807-ref0" URI="">
      <ds:Transforms>
       <ds:Transform          Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
 <ds:DigestValue>nQoslfKNH9/a7YoLBXFYsyTkBJ8=</ds:DigestValue>
 </ds:Reference>
 <ds:Reference URI="#xmldsig-87d128b5-aa31-4f0b-8e45-3d9cfa0eec26-keyinfo">
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:DigestValue>0iE/FGZgLfbnV9DhUaDBBVPjn44=</ds:DigestValue>
 </ds:Reference>
 <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties"
        URI="#xmldsig-e2f27048-53c6-4130-bf5e-5915089e9807-signedprops">
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:DigestValue>4VZaJAZGvxifoGYetOYuOEuZUrE=</ds:DigestValue>
 </ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue Id="xmldsig-e2f27048-53c6-4130-bf5e-5915089e9807-sigvalue">
Ijd7mzeBj4NV/F+EyP7WQO13Bi1wLNFFyvQPmiXgcTQ9zBYtuTWNeUS+vk425vrA1ghgC8V
fpem9
ODzhe/gsV5R82Ya9Dp3Ek6SDIoJYsD1nFEaq5h1Gt56iMr+hPEvyvR6ddQl+n4sRhmLCKvKV3
Jge
L8MvAx6Bg+m8Z7sQVdbBjLE/4oSdN+jo8DpUQrPuKMg0ZRmMEBp4LGbljQE0esFLG0cHml
LeFEZH
</ds:SignatureValue>
<ds:KeyInfo Id="xmldsig-87d128b5-aa31-4f0b-8e45-3d9cfa0eec26-keyinfo">
 <ds:X509Data>
  <ds:X509Certificate>
MIIILDCCBhSgAwIBAgIIfq9P6xyRMBEwDQYJKoZIhvcNAQELBQAwgbQxIzAhBgkqhkiG9w0B
CQEW
FGluZm9AYW5kZXNzY2QuY29tLmNvMSMwIQYDVQQDExpDQSBBTkRFUyBTQ0QgUy5BLiB
DbGFzZSBJ
STEwMC4GA1UECxMnRGl2aXNpb24gZGUgY2VydGlmaWNhY2lvbiBlbnRpZGFkIGZpbmFsM
RMwEQYD
</ds:X509Certificate>
 </ds:X509Data>
</ds:KeyInfo>
<ds:Object>
 <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
        xmlns:xades141="http://uri.etsi.org/01903/v1.4.1#"
        Target="#xmldsig-e2f27048-53c6-4130-bf5e-5915089e9807">
  <xades:SignedProperties Id="xmldsig-e2f27048-53c6-4130-bf5e-5915089e9807-
signedprops">
```


```
<xades:SignedSignatureProperties>
 <xades:SigningTime>2015-09-04T20:06:27.100-05:00</xades:SigningTime>
 <xades:SigningCertificate>
  <xades:Cert>
   <xades:CertDigest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>2el6MfWvYsvEaa/TV513a7tVK0g=</ds:DigestValue>
   </xades:CertDigest>
   <xades:IssuerSerial>
    <ds:X509IssuerName>
C=CO,L=Bogota D.C.,O=Andes SCD.,OU=Division de certificacion entidad final,CN=Ficticious ECD Colombia Clase II,1.2.840.113549.1.9.1=#1614696e666f40616e6465737363642e636f6d2e636f
    </ds:X509IssuerName>
    <ds:X509SerialNumber>9128602840918470673</ds:X509SerialNumber>
   </xades:IssuerSerial>
  </xades:Cert>
  <xades:Cert>
   <xades:CertDigest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>YGJTXnOzmebG2Mc6A/QapNi1PRA=</ds:DigestValue>
   </xades:CertDigest>
   <xades:IssuerSerial>
    <ds:X509IssuerName>
C=CO,L=Bogota D.C.,O=Andes SCD,OU=Division de certificacion,CN=Sub CA Ficticious ECD Colombia
S.A.,1.2.840.113549.1.9.1=#1614696e666f40616e6465737363642e636f6d2e636f
    </ds:X509IssuerName>
    <ds:X509SerialNumber>7958418607150926283</ds:X509SerialNumber>
   </xades:IssuerSerial>
  </xades:Cert>
  <xades:Cert>
   <xades:CertDigest>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>6EVr7OINyc49AgvNkie19xul55c=</ds:DigestValue>
   </xades:CertDigest>
   <xades:IssuerSerial>
    <ds:X509IssuerName>
```

C=CO,L=Bogota D.C.,O=Andes SCD,OU=Division de certificacion,CN=ROOT CA Ficticious ECD Colombia S.A.,1.2.840.113549.1.9.1=#1614696e666f40616e6465737363642e636f6d2e636f

</ds:X509IssuerName>
<ds:X509SerialNumber>3248112716520923666</ds:X509SerialNumber>
</xades:IssuerSerial>
</xades:Cert>
</xades:SigningCertificate>
<xades:SignaturePolicyIdentifier>
<xades:SignaturePolicyId>
<xades:SigPolicyId>
<xades:Identifier>
http://www.facturae.es/politica_de_firma_formato_facturae/politica_de_firma_formato_facturae_v3_1.pdf
</xades:Identifier>
</xades:SigPolicyId>
<xades:SigPolicyHash>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>Ohixl6upD6av8N7pEvDABhEL6hM=</ds:DigestValue>
</xades:SigPolicyHash>
</xades:SignaturePolicyId>
</xades:SignaturePolicyIdentifier>
<xades:SignerRole>
<xades:ClaimedRoles>
<xades:ClaimedRole>supplier</xades:ClaimedRole>
</xades:ClaimedRoles>
</xades:SignerRole>
</xades:SignedSignatureProperties>
</xades:SignedProperties>
</xades:QualifyingProperties>
</ds:Object>
</ds:Signature>
</ext:ExtensionContent>
</ext:UBLExtension>
</ext:UBLExtensions>
<cbc:UBLVersionID>UBL 2.0</cbc:UBLVersionID>
<cbc:CustomizationID
schemeName="nombre archivo xsd"


```
schemeURI="http://www.dian.gov.co/contratos/facturaelectronica/v1/anexo_v1_0.html#
xsdFile">
  DIAN_UBL_v1_0_foc.xsd
 </cbc:CustomizationID>
 <cbc:ProfileID schemeName="Lista de perfiles UBL de la DIAN"

schemeURI="http://www.dian.gov.co/contratos/facturaelectronica/v1/anexo_v1_0.html#
profileList">
  Factura de Venta Contingencia - Transcripción
 </cbc:ProfileID>
 <cbc:ID>8110007869</cbc:ID>
 <cbc:UUID schemeAgencyID="195"
  schemeAgencyName="CO, DIAN (Dirección de Impuestos y Aduanas Nacionales)">
a1beaaef31a0c05e97b0c4f6fbc1902d66a93245
 </cbc:UUID>
 <cbc:IssueDate>2015-07-21</cbc:IssueDate>
 <cbc:IssueTime>00:00:00</cbc:IssueTime>
 <cbc:InvoiceTypeCode listAgencyID="195"
  listAgencyName="CO, DIAN (Dirección de Impuestos y Aduanas Nacionales)"
  listName="Lista de códigos por tipo de factura"

listURI="http://www.dian.gov.co/contratos/facturaelectronica/v1/anexo_v1_0.html#Invoi
ceTypeCodeList">
  2
 </cbc:InvoiceTypeCode>
 <cbc:Note>Set de pruebas =  fos0001_900373076 </cbc:Note>
 <cbc:DocumentCurrencyCode>COP</cbc:DocumentCurrencyCode>
 <fe:AccountingSupplierParty>
  <cbc:AdditionalAccountID>1</cbc:AdditionalAccountID>
  <fe:Party>
   <cac:PartyIdentification>
    <cbc:ID schemeAgencyID="195"
            schemeAgencyName="CO, DIAN (Dirección de Impuestos y Aduanas Nacionales)"
            schemeID="31"
            schemeName="NIT del contribuyente">
             900373076
           </cbc:ID>
```


```
</cac:PartyIdentification>
<cac:PartyName>
 <cbc:Name>PJ - 900373076 - Adquiriente FE</cbc:Name>
</cac:PartyName>
<fe:PhysicalLocation>
 <fe:Address>
  <cbc:CitySubdivisionName>Centro</cbc:CitySubdivisionName>
  <cbc:CityName>Velez</cbc:CityName>
  <cbc:CountrySubentity>Santander</cbc:CountrySubentity>
  <cac:AddressLine>
   <cbc:Line> carrera 8 Nº 6C - 89</cbc:Line>
  </cac:AddressLine>
  <cac:Country>
   <cbc:IdentificationCode>CO</cbc:IdentificationCode>
  </cac:Country>
 </fe:Address>
</fe:PhysicalLocation>
<fe:PartyTaxScheme>
 <cbc:TaxLevelCode listName="Régimen Común de IVA">2</cbc:TaxLevelCode>
 <cac:TaxScheme/>
</fe:PartyTaxScheme>
<fe:PartyLegalEntity>
 <cbc:RegistrationName>PJ - 900373076</cbc:RegistrationName>
</fe:PartyLegalEntity>
</fe:Party>
</fe:AccountingSupplierParty>
<fe:AccountingCustomerParty>
 <cbc:AdditionalAccountID>2</cbc:AdditionalAccountID>
 <fe:Party>
  <cac:PartyIdentification>
   <cbc:ID schemeAgencyID="195"
          schemeAgencyName="CO, DIAN (Dirección de Impuestos y Aduanas Nacionales)"
          schemeID="22"

schemeURI="http://www.dian.gov.co/contratos/facturaelectronica/v1/anexo_v1_0.html#
tipoDocIdentidad"
          schemeName="Número del Documento de Identidad del Adquiriente; código del
tipo en el atributo schemeID">
```


```
          8355990
         </cbc:ID>
 </cac:PartyIdentification>
 <fe:PhysicalLocation>
  <fe:Address>
   <cbc:Department>Tolima</cbc:Department>
   <cbc:CitySubdivisionName>Centro</cbc:CitySubdivisionName>
   <cbc:CityName>Guamo</cbc:CityName>
   <cbc:CountrySubentity>Tolima</cbc:CountrySubentity>
   <cac:AddressLine>
    <cbc:Line> carrera 8 Nº 6C - 39</cbc:Line>
   </cac:AddressLine>
   <cac:Country>
    <cbc:IdentificationCode>CO</cbc:IdentificationCode>
   </cac:Country>
  </fe:Address>
 </fe:PhysicalLocation>
 <fe:PartyTaxScheme>
  <cbc:TaxLevelCode>0</cbc:TaxLevelCode>
  <cac:TaxScheme/>
 </fe:PartyTaxScheme>
 <fe:Person>
  <cbc:FirstName>Primer-N</cbc:FirstName>
  <cbc:FamilyName>Apellido-8355990</cbc:FamilyName>
  <cbc:MiddleName>Segundo-N</cbc:MiddleName>
 </fe:Person>
</fe:Party>
</fe:AccountingCustomerParty>
<fe:TaxTotal>
 <cbc:TaxAmount currencyID="COP">1619504.64</cbc:TaxAmount>
 <cbc:TaxEvidenceIndicator>false</cbc:TaxEvidenceIndicator>
 <fe:TaxSubtotal>
  <cbc:TaxableAmount currencyID="COP">10121904</cbc:TaxableAmount>
  <cbc:TaxAmount currencyID="COP">1619504.64</cbc:TaxAmount>
  <cbc:Percent>16</cbc:Percent>
  <cac:TaxCategory>
   <cac:TaxScheme>
    <cbc:ID>01</cbc:ID>
```


```
  </cac:TaxScheme>
 </cac:TaxCategory>
</fe:TaxSubtotal>
</fe:TaxTotal>
<fe:TaxTotal>
 <cbc:TaxAmount currencyID="COP">419046.82</cbc:TaxAmount>
 <cbc:TaxEvidenceIndicator>false</cbc:TaxEvidenceIndicator>
 <fe:TaxSubtotal>
  <cbc:TaxableAmount currencyID="COP">10121904</cbc:TaxableAmount>
  <cbc:TaxAmount currencyID="COP">419046.82</cbc:TaxAmount>
  <cbc:Percent>4.14</cbc:Percent>
  <cac:TaxCategory>
   <cac:TaxScheme>
    <cbc:ID>03</cbc:ID>
   </cac:TaxScheme>
  </cac:TaxCategory>
 </fe:TaxSubtotal>
</fe:TaxTotal>
<fe:LegalMonetaryTotal>
 <cbc:LineExtensionAmount currencyID="COP">10121904</cbc:LineExtensionAmount>
 <cbc:TaxExclusiveAmount currencyID="COP">2038551.46</cbc:TaxExclusiveAmount>
 <cbc:PayableAmount currencyID="COP">12160455.46</cbc:PayableAmount>
</fe:LegalMonetaryTotal>
<fe:InvoiceLine>
 <cbc:ID>1</cbc:ID>
 <cbc:InvoicedQuantity>10</cbc:InvoicedQuantity>
 <cbc:LineExtensionAmount currencyID="COP">100</cbc:LineExtensionAmount>
 <fe:Item>
  <cbc:Description>Línea-1 8110007869 fos0001_900373076_8bad2_R000001-81-
26610</cbc:Description>
 </fe:Item>
 <fe:Price>
  <cbc:PriceAmount currencyID="COP">43256</cbc:PriceAmount>
 </fe:Price>
</fe:InvoiceLine>
<fe:InvoiceLine>
 <cbc:ID>2</cbc:ID>
 <cbc:InvoicedQuantity>10</cbc:InvoicedQuantity>
```


```
<cbc:LineExtensionAmount currencyID="COP">100</cbc:LineExtensionAmount>
<cac:TaxTotal>
 <cbc:TaxAmount currencyID="COP">20.14</cbc:TaxAmount>
 <cac:TaxSubtotal>
  <cbc:TaxAmount currencyID="COP">16</cbc:TaxAmount>
  <cbc:Percent>16</cbc:Percent>
  <cac:TaxCategory>
   <cac:TaxScheme>
    <cbc:ID>01</cbc:ID>
   </cac:TaxScheme>
  </cac:TaxCategory>
 </cac:TaxSubtotal>
 <cac:TaxSubtotal>
  <cbc:TaxAmount currencyID="COP">4.14</cbc:TaxAmount>
  <cbc:Percent>4.14</cbc:Percent>
  <cac:TaxCategory>
   <cac:TaxScheme>
    <cbc:ID>03</cbc:ID>
   </cac:TaxScheme>
  </cac:TaxCategory>
 </cac:TaxSubtotal>
</cac:TaxTotal>
<fe:Item>
 <cbc:Description>Línea-2 8110007869 fos0001_900373076_8bad2_R000001-81-
26610</cbc:Description>
</fe:Item>
<fe:Price>
 <cbc:PriceAmount currencyID="COP">10</cbc:PriceAmount>
</fe:Price>
</fe:InvoiceLine>
</fe:Invoice>
```

Vea la precisión hecha a la sección “Firmante”, aplicable al elemento /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SignerRole/xades:ClaimedRoles/xades:ClaimedRole

Y al cumplimiento del literal “d” del Artículo 3 del Decreto 2242-2015: el PT “…expresamente autorizado” por el OFE.

Vea la definición sobre el lapso del artículo 7 del decreto 2242-2015, aplicable al elemento /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SigningTime

14. Mecanismo de firma electrónica

El mecanismo de firma electrónica a que se refiere el artículo 7 de la Ley 527 de 1999 y el Decreto 2364 de 2012 será considerada en el negocio electrónico denominado Facturación Electrónica una vez sea reglamentada por la DIAN para tal efecto.

15. Certificado digital desde la vigencia de la circular 03-2016 de la ONAC

Este documento incluye los argumentos que deberán usarse como valores de los parámetros de:

- Los certificados digitales *con no repudio* previstos en el estándar RFC-5280, y que cumplan con la Ley de Comercio Electrónico de Colombia, que utilicen los facturadores ***electrónicos previstos*** en el Decreto 2242-2015 para firmar digitalmente los documentos desmaterializados del negocio de la Facturación Electrónica.
- Los atributos que resuelven las ambigüedades de los elementos que conforman los documentos desmaterializados del negocio de la Facturación Electrónica, precisando las características criptográficas empleadas para cumplir con la Ley de Comercio Electrónico de Colombia.

Referencia: URL https://es.wikipedia.org/wiki/SHA-2

Regla-1

Lapso de Validez del certificado digital	Expedido ANTES de octubre 1 de 2016 T00:00:00, y hasta la terminación de la vigencia
Signature Algorithm	Valores válidos dentro del certificado digital: Sha1WithRSAEncryption sha224WithRSAEncryption sha256WithRSAEncryption sha384WithRSAEncryption sha512WithRSAEncryption
X509v3 Key Usage: critical	Valores necesarios dentro del certificado digital: Digital Signature Non Repudiation

Descripción:

Estamos aplicando la reglamentación de la ONAC, URL http://onac.org.co/anexos/documentos/TRANSICIRCULARES/2016circulares/circular03-2016.pdf

Si el valor "Validity" del lapso de vigencia del certificado empezó antes de octubre 1 de 2016, la firma digital de la ***factura electrónica*** puede:

- Emplear certificados digitales que hayan sido generados con resúmenes criptográficos del tipo SHA1
- Que el fragmento SignedInfo al que se le aplicó el canon fue la entrada para calcular el resumen criptográfico que fue firmado digitalmente con << http://www.w3.org/2000/09/xmldsig#rsa-sha1 >>
- La aplicación del algoritmo de firma digital de las facturas electrónicas depende del lapso de vigencia dentro del cual debió haber sido generada y firmada, y del método de generación del certificado digital utilizado. No podrá existir una factura con fecha válida, i.e. /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SigningTime— diferente o por fuera del lapso de vigencia del certificado digital que se usó para calcular la firma-digital.

El no cumplimiento de estos valores deberá registrarse como una firma digital ***fallida*** para el documento electrónico, motivada en:

- Algoritmo de Firma del certificado digital (tipo SHA1) no previsto por la DIAN

Lapso de Validez del certificado digital	Expedido ANTES de octubre 1 de 2016 T00:00:00, y hasta la terminación de la vigencia
• Uso de la clave pública del certificado digital carece de los propósitos “firma digital” o “no repudio”. Pueden estar presentes ambos motivos.	
Si el lapso de validez inhabilita a /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SigningTime, entonces deberá registrarse como una firma digital ***fallida*** para el documento electrónico, motivada en: • Fecha de expedición del documento electrónico no corresponde con el lapso de vigencia del certificado digital. Este motivo puede ser concurrente con los descritos en la celda anterior.	

Regla-2

Lapso de Validez del certificado digital	Después de 30 de septiembre de 2016 T23:59:59
Signature Algorithm	Valores válidos dentro del certificado digital: sha256WithRSAEncryption sha384WithRSAEncryption sha512WithRSAEncryption
X509v3 Key Usage: critical	Valores necesarios dentro del certificado digital: Digital Signature Non Repudiation

Descripción:

Estamos aplicando la reglamentación de la ONAC, URL http://onac.org.co/anexos/documentos/TRANSICIRCULARES/2016circulares/circular03-2016.pdf

Si el valor "Validity" del lapso de vigencia del certificado empezó después del 30 de septiembre de 2016 T23:59:59, la firma digital de la ***factura electrónica*** tiene que:

- Emplear certificados digitales que hayan sido generados con resúmenes criptográficos del tipo SHA256; existen otras opciones como aparece en la lista << Signature Algorithm >>
- Que el resumen criptográfico que se aplicó al fragmento que fue firmado digitalmente corresponda con el << SignatureMethod >> empleado

El no cumplimiento de estos valores deberá registrarse como una firma digital ***fallida*** para el documento electrónico, motivada en:

- Algoritmo de Firma del certificado digital (tipo SHA2) no previsto por la DIAN
- Uso de la clave pública del certificado digital carece de los propósitos "firma digital" o "no repudio". Vea Anexo 2.

Pueden estar presentes ambos motivos.

Si el lapso de validez inhabilita a

/fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SigningTime, entonces deberá registrarse como una firma digital ***fallida*** para el documento electrónico, motivada en:

Lapso de Validez del certificado digital	Después de 30 de septiembre de 2016 T23:59:59
• Fecha de expedición del documento electrónico no corresponde con el lapso de vigencia del certificado digital. Este motivo puede ser concurrente con los descritos en la celda anterior.	

Regla-3

Algoritmo de firma digital aplicado a la factura electrónica dentro del documento electrónico UBL	Certificado digital expedido después de 30 de septiembre de 2016 T23:59:59
/fe:Invoice/ext:UBLExtensions/ext:UBLExtension[X]/ext:ExtensionContent/ds:Signature/ds:SignedInfo/ds:SignatureMethod/@Algorithm=	Algoritmo=RSAwithSHA256 Use: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 Algoritmo=RSAwithSHA384 Use: http://www.w3.org/2001/04/xmldsig-more#rsa-sha384 Algoritmo=RSAwithSHA512 Use: http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
Descripción: Estamos aplicando la reglamentación de la ONAC, URL http://onac.org.co/anexos/documentos/TRANSICIRCULARES/2016circulares/circular03-2016.pdf El algoritmo de *firma digital* aplicado a la facture electrónica no tiene correspondencia directa con el *resumen criptográfico* utilizado para obtener los fragmentos de la Regla-4, i.e. pueden usarse tamaños de	
Si el valor del ../ds:SignatureMethod/@Algorithm no corresponde con los valores paramétricos, entonces deberá registrarse como una firma digital ***fallida*** para el documento electrónico, motivada en: • Empleó un algoritmo de *firma digital* no previsto por la DIAN. Vea Anexo 2.	
Si el valor del ../ds:SignatureMethod/@Algorithm corresponde a	

Algoritmo de firma digital aplicado a la factura electrónica dentro del documento electrónico UBL	Certificado digital expedido después de 30 de septiembre de 2016 T23:59:59
http://www.w3.org/2000/09/xmldsig#rsa-sha1, entonces deberá registrarse como una firma digital ***fallida*** para el documento electrónico, motivada en: • Empleó un algoritmo de *firma digital* que está caducado según el reglamento de la Ley de Comercio Electrónico de Colombia. Vea Anexo 2.	

Regla-4

Algoritmos de resumen criptográfico aplicado a los fragmentos de la factura electrónica que se incluyen dentro del fragmento que se firma digitalmente	Certificado digital expedido después de 30 de septiembre de 2016 T23:59:59
/fe:Invoice/ext:UBLExtensions/ext:UBLExtension[X]/ext:ExtensionContent/ds:Signature/ds:SignedInfo/ds:Reference[1]/ds:DigestMethod/@Algorithm= /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[X]/ext:ExtensionContent/ds:Signature/ds:SignedInfo/ds:Reference[2]/ds:DigestMethod/@Algorithm= /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[X]/ext:ExtensionContent/ds:Signature/ds:SignedInfo/ds:Reference[3]/ds:DigestMethod/@Algorithm /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[X]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignaturePproperties/xades:SigningCertificate/xades:Cert[1]/xades:CertDigest/ds:DigestMethod/@Algorithm= /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignaturePproperties/xades:SigningCertificate/xades:Cert[2]/xades:CertDigest/ds:DigestMethod/@Algorithm= /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignaturePproperties/xades:SigningCertificate/xades:Cert[3]/xades:CertDigest/ds:DigestMethod/@Algorithm=	SHA256. Cadena de 256 bits. Use: http://www.w3.org/2001/04/xmlenc#sha256 SHA384. Cadena de 384 bits. Use: http://www.w3.org/2001/04/xmldsig-more#sha384 SHA512. Cadena de 512 bits. Use: http://www.w3.org/2001/04/xmlenc#sha512

Algoritmos de resumen criptográfico aplicado a los fragmentos de la factura electrónica que se incluyen dentro del fragmento que se firma digitalmente	Certificado digital expedido después de 30 de septiembre de 2016 T23:59:59
/fe:Invoice/ext:UBLExtensions/ext:UBLExtension[X]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignaturePproperties/xades:SignaturePolicyIdentifier/xades:SignaturePolicyId/xades:SigPolicyHash/ds:DigestMethod/@Algorithm=	

Descripción:

Estamos aplicando la reglamentación de la ONAC, URL

http://onac.org.co/anexos/documentos/TRANSICIRCULARES/2016circulares/circular03-2016.pdf

El algoritmo de resumen criptográfico utilizado para los fragmentos que intervienen y forman parte del elemento que se firma digitalmente no tiene correspondencia con el algoritmo de firma digital de la Regla-3.

Si el valor del ../ds:DigestMethod/@Algorithm no corresponde con los valores paramétricos, entonces deberá registrarse como una firma digital ***fallida*** para el documento electrónico, motivada en:

- Empleó un algoritmo de *resumen criptográfico* no previsto por la DIAN. Vea Anexo 2.

Si el valor del ../ds:DigestMethod/@Algorithm corresponde a http://www.w3.org/2000/09/xmldsig#sha1, entonces deberá registrarse como una firma digital ***fallida*** para el documento electrónico, motivada en:

- Empleó un algoritmo de *resumen criptográfico* que está caducado según el reglamento de la Ley de Comercio Electrónico de Colombia. Vea Anexo 2.

La vista de un certificado digital
Certificate: Data: Version: 3 (0x2) Serial Number: 5b:aa:82:68:12:65:0b:cc Signature Algorithm: sha256WithRSAEncryption Issuer: emailAddress=info@andesscd.com.co, CN=CA ANDES SCD S.A. Clase II, OU=Division de certificacion entidad final, O=Andes SCD., L=Bogota D.C., C=CO Validity Not Before: Sep 24 17:35:03 2016 GMT Not After : Sep 24 17:35:03 2019 GMT Subject: streetAddress=Calle Falsa No 12 34/emailAddress=persona_juridica_pruebas@empresaparapruebas.com, CN=Usuario de Pruebas/serialNumber=11111111/title=Persona Juridica, OU=Certificado de Persona Juridica emitido por Andes SCD Av. Carrera 45 No 103 - 34 OF 205, L=Bogota, ST=Cundinamarca, C=CO Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) Modulus (2048 bit): 00:9e:fa:a3:e7:ef:dc:90:e3:9a:f6:b9:24:83:32: 7e:2c:70:d1:b3:09:dc:26:3a:02:e9:0d:5f:0d:a8: 8f:7a:c7:90:77:f2:59:d8:6b:dc:3b:c3:b7:95:5f: 90:d9:be:14:66:dc:34:07:ba:45:c7:6d:87:3d:7a: 08:55:b5:a9:19:e0:c2:a3:b1:52:03:73:be:f9:05:

La vista de un certificado digital

b1:b0:3f:a0:55:7b:82:93:51:7a:fa:a8:5f:f0:00:
4b:86:47:73:04:7b:6d:6a:ce:e1:1a:a0:59:84:cd:
95:c3:58:7f:68:f5:74:05:ab:a9:c7:a3:53:98:2d:
44:2b:43:b8:c7:2b:2c:cd:ab:4a:47:3e:4a:b9:a7:
c7:1b:c3:98:97:70:6d:c2:46:70:2b:ec:32:1e:27:
38:cb:0b:db:c7:a0:0e:48:9c:5e:7e:95:32:3a:70:
3d:63:91:72:7b:68:fa:f1:2b:88:4a:99:cb:59:8c:
8f:cb:9c:c6:bb:ab:c2:2b:bb:19:c1:79:c8:ba:e3:
1b:b9:5f:52:95:38:88:85:c7:81:00:ab:06:68:fb:
66:90:25:04:07:3b:36:cf:98:98:fc:12:d9:ae:67:
ef:f8:ba:41:8b:62:a8:04:a3:8f:5f:eb:79:13:3a:
3c:15:19:24:1c:07:87:a2:fa:25:d9:0a:bb:9a:25:
5f:23

Exponent: 65537 (0x10001)

X509v3 extensions:

Authority Information Access:

OCSP - URI:http://ocsp.andesscd.com.co

X509v3 Subject Key Identifier:

6E:9F:3D:F8:B9:0F:1A:E1:B1:FE:8A:55:1B:A1:1A:9A:C9:8B:9F:17

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Authority Key Identifier:

La vista de un certificado digital

keyid:A8:4B:B4:F4:0B:A7:B6:5B:D4:A0:28:85:10:9D:04:13:33:C4:A7:F7

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.31304.1.2.9.2.2

User Notice:

Explicit Text:

CPS: http://www.andesscd.com.co/docs/DPC_AndesSCD_V2.2.pdf

X509v3 CRL Distribution Points:

URI:http://www.andesscd.com.co/includes/getCert.php?crl=1

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key Encipherment

X509v3 Extended Key Usage:

TLS Web Client Authentication, E-mail Protection

X509v3 Subject Alternative Name:

email:persona_juridica_pruebas@empresaparapruebas.com

Signature Algorithm: sha256WithRSAEncryption

92:3c:85:04:a9:6d:a7:c0:cb:93:7e:7f:9f:c9:af:04:f3:71:

72:2b:94:50:78:ff:13:31:27:cc:ea:18:69:60:1c:14:b3:92:

18:0e:f5:67:b5:70:ae:57:72:54:89:90:9e:c4:44:5a:96:ec:

31:b9:48:63:93:48:ec:e2:f3:b7:33:12:08:ca:56:79:74:7f:

83:c1:f9:1d:c4:2e:e8:25:2b:a1:0a:91:3e:23:8e:7c:48:32:

La vista de un certificado digital
08:01:55:3c:71:8a:1d:8e:de:f3:3c:e8:37:3a:9e:49:9d:df: c4:63:c5:ea:c5:e1:37:40:71:a4:49:aa:94:1f:fe:1c:ce:12: 75:07:21:ab:24:6a:a8:43:17:f3:a1:65:9f:14:b6:27:8b:6b: 80:bb:eb:41:e4:85:13:36:ff:3c:93:48:e7:bf:21:af:7d:4b: 78:59:fd:dc:63:c4:60:f8:4a:ed:cc:59:78:31:60:35:38:1f: 06:6d:a0:4b:06:98:ae:31:3c:25:5f:5a:1b:6f:46:f9:76:6e: be:25:df:45:08:9f:35:cc:11:08:f6:45:d9:38:f8:31:65:2a: b1:7f:5a:a5:dc:65:a1:d0:49:8e:7a:93:9f:02:b9:73:85:01: cd:8b:8d:04:97:2b:35:57:70:2d:d0:2f:b8:68:16:a2:da:f1: 18:b7:da:a0:96:17:ba:79:ac:d9:b0:b1:de:8a:b0:d3:f9:04: 88:d8:0c:f8:4e:ac:b9:a9:5e:a2:35:33:b6:25:86:fd:dc:ff: 9c:1b:05:0f:68:f1:45:fa:1a:87:f5:7c:8e:71:8b:1b:48:49: 86:1b:da:75:dd:e2:45:9f:c2:96:20:45:6b:39:35:1e:b4:94: 21:25:2f:6e:51:a4:56:f6:71:dc:28:53:33:7a:99:08:86:bf: 70:ad:ad:a5:e2:d3:46:49:a8:79:34:76:d8:37:d7:8f:8e:2e: 35:cf:fd:45:2d:41:43:2b:f8:4c:8f:e6:ff:79:a2:1d:13:b7: 00:41:70:5e:0c:2c:9c:89:11:ad:96:22:65:07:7a:a9:ec:d0: 7e:a2:d0:1b:0f:1c:a1:de:bf:83:19:04:36:2f:3a:94:e9:4f: 90:eb:81:e0:ca:05:75:02:39:1d:46:50:6e:c5:50:21:8d:f7: ac:7a:5b:16:2c:88:aa:e5:99:50:d2:d8:af:27:d2:18:3d:9c: 2d:cd:96:75:6f:21:c7:05:3f:91:e4:f0:ac:35:b8:d1:83:bf: df:36:f0:61:f3:aa:a5:6b:d8:27:0e:77:e5:7e:c7:73:0f:e5: 06:8e:3d:64:9c:70:cb:e4:ef:cd:ac:ce:e1:e0:3b:42:b7:ea:

La vista de un certificado digital
17:97:d5:43:32:ff:bf:6e

TIPO DE CERTIFICADO DIGITAL	LAPSO PARA HABILITACIÓN	LAPSO DE OPERACIÓN

Certificado Raíz o de la CA de la ECD. Validez de la cadena de confianza del *certificado digital con no repudio* de un suscriptor según la Ley 527-1999. Aplicación de lo dispuesto en la Circular 003-2016 de la ONAC. Este es el primer nivel de jerarquía al que se refiere la circular.
 	
CA: certification authority
	• Expedido antes de octubre 1 de 2016 hasta el vencimiento
	  • Algoritmo de firma de certificado de la CA:
	  • Sha1WithRSAEncryption
	  • sha256WithRSAEncryption
	  • sha384WithRSAEncryption
	  • sha512WithRSAEncryption
	  • Estos fueron válidos durante el Plan Piloto para las facturas
	
	• Expedido desde octubre 1 de 2016 hasta el vencimiento
	  • Algoritmo de firma de certificado de la CA:
	  • sha256WithRSAEncryption
	  • sha384WithRSAEncryption
	  • sha512WithRSAEncryption
	
	• El algoritmo de firma digital aplicado al certificado se detecta en la variable “Signature Algorithm” del certificado raíz de la CA.
		• Expedido desde octubre 1 de 2016 hasta el vencimiento
		  • Algoritmo de firma de certificado de la CA:
		  • sha256WithRSAEncryption
		  • sha384WithRSAEncryption
		  • sha512WithRSAEncryption
		• Se detecta en la variable “Signature Algorithm” del certificado raíz de la CA.
		• Una factura electrónica del Decreto 2242-2015 que haya sido suscrita digitalmente con un *certificado de suscriptor* cuyo *certificado de CA* no cumpla con uno de estos algoritmos podría ser tachada de utilizar una firma digital inválida. Véase el último párrafo del numeral “2” de la circular de la ONAC que se mencionó arriba.
		• PROPUESTA: la DIAN detectará esta falencia en el ***control ex post***, y le notificará el hecho al Representante Legal del *facturador electrónico*, para que se abstenga de firmar digitalmente facturas electrónicas con el *certificado digital de suscriptor*.

Certificado de una sub CA, i.e. una RA de la ECD. Validez de la cadena de confianza del *certificado digital con*	• Expedido antes de abril 11 de 2016 hasta el vencimiento
	  • Algoritmo de firma de certificado de la RA:
	  • Sha1WithRSAEncryption
		• Expedido desde abril 11 de 2016 hasta el vencimiento
		  • Algoritmo de firma de certificado de la RA:
		  • sha256WithRSAEncryption

TIPO DE CERTIFICADO DIGITAL	LAPSO PARA HABILITACIÓN	LAPSO DE OPERACIÓN
no repudio de un suscriptor según la Ley 527-1999. Aplicación de lo dispuesto en la Circular 003-2016 de la ONAC. Este es el segundo nivel de jerarquía al que se refiere la circular. RA: registration authority	• sha256WithRSAEncryption • sha384WithRSAEncryption • sha512WithRSAEncryption • Estos fueron válidos durante el Plan Piloto para las facturas • Expedido desde octubre 1 de 2016 hasta el vencimiento • Algoritmo de firma de certificado de la RA: • sha256WithRSAEncryption • sha384WithRSAEncryption • sha512WithRSAEncryption • El algoritmo de firma digital aplicado al certificado se detecta en la variable "Signature Algorithm" del mismo certificado de la RA.	• sha384WithRSAEncryption • sha512WithRSAEncryption • Se detecta en la variable "Signature Algorithm" del certificado de la RA. • Una factura electrónica del Decreto 2242-2015 que haya sido suscrita digitalmente con un *certificado de suscriptor* cuyo *certificado de RA* no cumpla con uno de estos algoritmos podría ser tachada de utilizar una firma digital inválida. Véase el último párrafo del numeral "2" de la circular de la ONAC que se mencionó arriba. • PROPUESTA: la DIAN detectará esta falencia en el ***control ex post***, y le notificará el hecho al Representante Legal del *facturador electrónico*, para que se abstenga de firmar digitalmente facturas electrónicas con el *certificado digital de suscriptor*.
Certificado de suscriptor. Validez de la cadena de confianza del *certificado digital con no repudio* de un suscriptor según la Ley 527-1999. Aplicación de lo dispuesto en la Circular 003-2016 de la ONAC. Este es el	• Expedido antes de abril 11 de 2016 hasta el vencimiento • Algoritmo de firma de certificado de la RA: • Sha1WithRSAEncryption • sha256WithRSAEncryption • sha384WithRSAEncryption • sha512WithRSAEncryption	• Expedido desde abril 11 de 2016 hasta el vencimiento • Algoritmo de firma de certificado de la RA: • sha256WithRSAEncryption • sha384WithRSAEncryption • sha512WithRSAEncryption • Se detecta en la variable "Signature Algorithm" del certificado de la RA.

TIPO DE CERTIFICADO DIGITAL	LAPSO PARA HABILITACIÓN	LAPSO DE OPERACIÓN

segundo nivel de jerarquía o inferiores a los que se refiere la circular.	• Estos fueron válidos durante el Plan Piloto para las facturas
	
	• Expedido desde abril 11 de 2016 hasta el vencimiento
	  • Algoritmo de firma de certificado de la RA:
	  • sha256WithRSAEncryption
	  • sha384WithRSAEncryption
	  • sha512WithRSAEncryption
	
	• El algoritmo de firma digital aplicado al certificado se detecta en la variable "Signature Algorithm" del mismo *certificado de suscriptor*.
		• Una factura electrónica del Decreto 2242-2015 que haya sido suscrita digitalmente con un *certificado de suscriptor* cuyo *certificado de RA* no cumpla con uno de estos algoritmos podría ser tachada de utilizar una firma digital inválida. Véase el último párrafo del numeral "2" de la circular de la ONAC que se mencionó arriba.
		• PROPUESTA: la DIAN detectará esta falencia en-línea, y hará la anotación de "validación fallida: certificado no cumple reglamentación ONAC" en el conjunto de las "ocho -8-"que le notificará al *facturador electrónico*, quien se abstendrá a partir de ese momento en firmar digitalmente facturas electrónicas con el *certificado digital de suscriptor*.

16. Sobre el CANON de los documentos electrónicos y la validez de la firma digital

La manera más efectiva de que los documentos electrónicos de la DIAN mantengan válida la firma digital es aplicando las transformaciones según el elemento /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:SignedInfo/ds:CanonicalizationMethod/@Algorithm de tal forma que el documento que se someta al procedimiento de ***firma digital*** sea el resultante del canon "No utilice 'pretty-print' ni 'indent="yes"' ni CR-LF ni Tab ni chr(32), i.e. Todos los UBL.tag deben formar una cadena de caracteres válidos UTF-8, sin separadores ni caracteres de control; y deben omitirse los fragmentos "<!—comentario -->" .

17. Momento desde el cual será medido el tiempo al que se refiere el “Artículo 7. Ejemplar de la factura electrónica para la DIAN” del Decreto 2242-2015.

El lapso definido en este artículo como el máximo para la entrega del documento electrónico será medido a partir del valor contenido en el elemento /fe:Invoice/ext:UBLExtensions/ext:UBLExtension[2]/ext:ExtensionContent/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SigningTime.

Sin perjuicio de que las actividades de control fiscal investiguen sobre las desviaciones que ocurran respecto a la fecha que haya sido registrada en los elementos /fe:Invoice/cbc:IssueDate y /fe:Invoice/cbc:IssueTime.