Contenido

Formato reporte auxiliar de cuentas y/o subcuentas

1. Estándar del formato reporte auxiliar de cuentas y/o subcuentas de contabilidad electrónica

El contribuyente deberá utilizar el siguiente estándar XSD, validando su forma y sintaxis en un archivo con extensión XML.

Para poder ser validado, Auxiliar de Cuentas y/o subcuentas de contabilidad electrónica deberá estar referenciado al namespace y ruta publicada por el SAT en donde se encuentra el esquema XSD objeto de la presente sección (http://www.sat.gob.mx/esquemas/ContabilidadE/1_1/AuxiliarCtas/AuxiliarCtas_1_1.xsd) de la siguiente manera:

```
<AuxiliarCtas:AuxiliarCtas
        xsi:schemaLocation="http://www.sat.gob.mx/esquemas/ContabilidadE/1_1/AuxiliarCtas/AuxiliarCtas_1_1
.xsd"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:AuxiliarCtas=" http://www.sat.gob.mx/esquemas/ContabilidadE/1_1/AuxiliarCtas">
 .....
</AuxiliarCtas:AuxiliarCtas>
```

Adicionalmente a las reglas de estructura planteadas dentro del presente estándar, el contribuyente que utilice este estándar deberá sujetarse tanto a las disposiciones fiscales vigentes, como a los lineamientos técnicos de forma y sintaxis para la generación de archivos XML especificados por el consorcio w3, establecidos en http://www.w3.org.

En particular se deberá tener cuidado de que aquellos casos especiales que se presenten en los valores especificados dentro de los atributos del archivo XML como aquellos que usan el carácter &, el carácter “, el carácter ‘, el carácter < y el carácter > que requieren del uso de secuencias de escape.

- En el caso del & se deberá usar la secuencia &
- En el caso del “ se deberá usar la secuencia "
- En el caso del < se deberá usar la secuencia <
- En el caso del > se deberá usar la secuencia >
- En el caso del ‘ se deberá usar la secuencia '

Ejemplos:

Para representar nombre=“Juan & José & “Niño”” se usará nombre=”Juan & José & "Niño"”

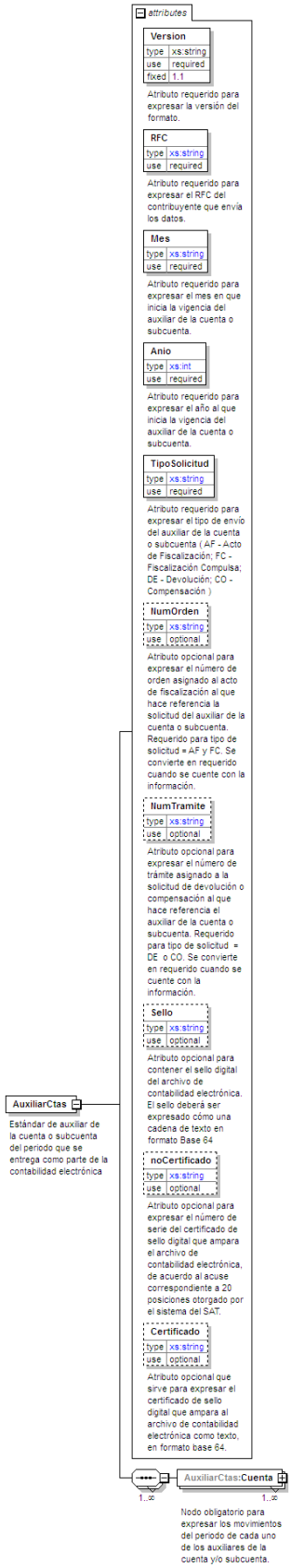
Cabe mencionar que la especificación XML permite el uso de secuencias de escape para el manejo de caracteres acentuados y el carácter ñ, sin embargo, dichas secuencias de escape no son necesarias al expresar el documento XML bajo el estándar de codificación UTF-8 si fue creado correctamente.

Estructura

Elementos

Elemento: AuxiliarCtas

Diagrama


attributes
Version
type xs:string
use required
fixed 1.1
Atributo requerido para expresar la versión del formato.
RFC
type xs:string
use required
Atributo requerido para expresar el RFC del contribuyente que envía los datos.
Mes
type xs:string
use required
Atributo requerido para expresar el mes en que inicia la vigencia del auxiliar de la cuenta o subcuenta.
Anio
type xs:int
use required
Atributo requerido para expresar el año al que inicia la vigencia del auxiliar de la cuenta o subcuenta.
TipoSolicitud
type xs:string
use required
Atributo requerido para expresar el tipo de envío del auxiliar de la cuenta o subcuenta (AF - Acto de Fiscalización; FC - Fiscalización Compulsa; DE - Devolución; CO - Compensación)
NumOrden
type xs:string
use optional
Atributo opcional para expresar el número de orden asignado al acto de fiscalización al que hace referencia la solicitud del auxiliar de la cuenta o subcuenta. Requerido para tipo de solicitud = AF y FC. Se convierte en requerido cuando se cuente con la información.
NumTramite
type xs:string
use optional
Atributo opcional para expresar el número de trámite asignado a la solicitud de devolución o compensación al que hace referencia el auxiliar de la cuenta o subcuenta. Requerido para tipo de solicitud = DE o CO. Se convierte en requerido cuando se cuente con la información.
Sello
type xs:string
use optional
Atributo opcional para contener el sello digital del archivo de contabilidad electrónica. El sello deberá ser expresado cómo una cadena de texto en formato Base 64
noCertificado
type xs:string
use optional
Atributo opcional para expresar el número de serie del certificado de sello digital que ampara el archivo de contabilidad electrónica, de acuerdo al acuse correspondiente a 20 posiciones otorgado por el sistema del SAT.
Certificado
type xs:string
use optional
Atributo opcional que sirve para expresar el certificado de sello digital que ampara al archivo de contabilidad electrónica como texto, en formato base 64.
AuxiliarCtas
Estándar de auxiliar de la cuenta o subcuenta del periodo que se entrega como parte de la contabilidad electrónica
1..∞
AuxiliarCtas:Cuenta
1..∞
Nodo obligatorio para expresar los movimientos del periodo de cada uno de los auxiliares de la cuenta y/o subcuenta.

Descripción

Estándar de auxiliar de la cuenta o subcuenta del periodo que se entrega como parte de la contabilidad electrónica

Atributos

Version

Descripción	Atributo requerido para expresar la versión del formato.
Uso	requerido
Valor Prefijado	1.1
Tipo Especial	xs:string

RFC

Descripción	Atributo requerido para expresar el RFC del contribuyente que envía los datos.
Uso	requerido
Tipo Base	xs:string
Longitud Mínima	12
Longitud Máxima	13
Patrón	[A-ZÑ&]{3,4}[0-9]{2}[0-1][0-9][0-3][0-9][A-Z0-9]?[A-Z0-9]?[0-9A-Z]?

Mes

Descripción	Atributo requerido para expresar el mes en que inicia la vigencia del auxiliar de la cuenta o subcuenta.
Uso	requerido
Tipo Base	xs:string
Valores Permitidos	01 02 03 04 05 06 07 08 09 10 11 12

Anio

Descripción	Atributo requerido para expresar el año al que inicia la vigencia del auxiliar de la cuenta o subcuenta.
Uso	requerido
Tipo Base	xs:int
Valor Mínimo Incluyente	2015
Valor Máximo Incluyente	2099

TipoSolicitud

Descripción	Atributo requerido para expresar el tipo de envío del auxiliar de la cuenta o subcuenta (AF - Acto de Fiscalización; FC - Fiscalización Compulsa; DE - Devolución; CO - Compensación)
Uso	requerido
Tipo Base	xs:string
Patrón	AF|FC|DE|CO

NumOrden

Descripción	Atributo opcional para expresar el número de orden asignado al acto de fiscalización al que hace referencia la solicitud del auxiliar de la cuenta o subcuenta. Requerido para tipo de solicitud = AF y FC. Se convierte en requerido cuando se cuente con la información.
Uso	opcional
Tipo Base	xs:string
Longitud	13
Patrón	[A-Z]{3}[0-6][0-9][0-9]{5}(/)[0-9]{2}

NumTramite

Descripción	Atributo opcional para expresar el número de trámite asignado a la solicitud de devolución o compensación al que hace referencia el auxiliar de la cuenta o subcuenta. Requerido para tipo de solicitud = DE o CO. Se convierte en requerido cuando se cuente con la información.
Uso	opcional
Tipo Base	xs:string
Longitud	10
Patrón	[0-9]{10}

Sello

Descripción	Atributo opcional para contener el sello digital del archivo de contabilidad electrónica. El sello deberá ser expresado cómo una cadena de texto en formato Base 64
Uso	opcional
Tipo Base	xs:string
Espacio en Blanco	Colapsar

noCertificado

Descripción	Atributo opcional para expresar el número de serie del certificado de sello digital que ampara el archivo de contabilidad electrónica, de acuerdo al acuse correspondiente a 20 posiciones otorgado por el sistema del SAT.
Uso	opcional
Tipo Base	xs:string
Longitud	20

Certificado

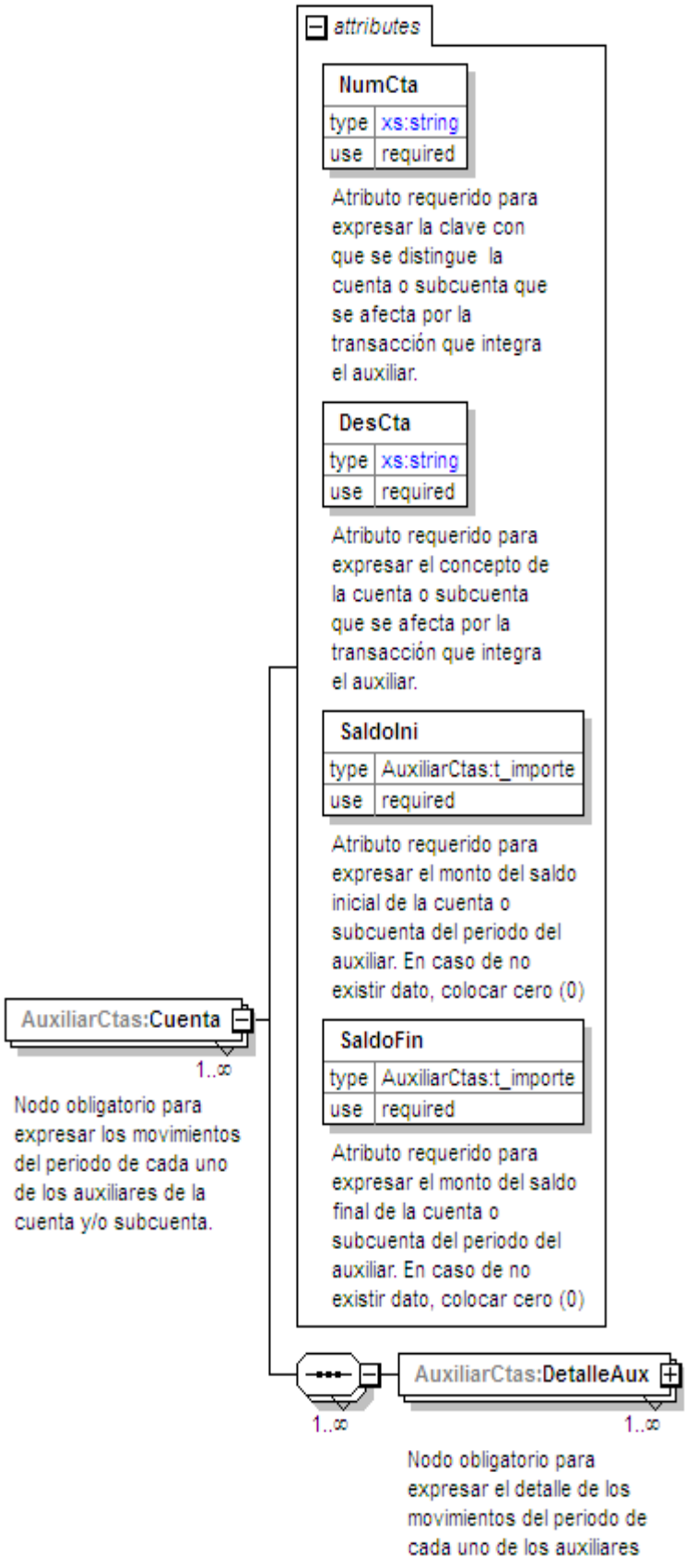
Descripción	Atributo opcional que sirve para expresar el certificado de sello digital que ampara al archivo de contabilidad electrónica como texto, en formato base 64.
Uso	opcional
Tipo Base	xs:string
Espacio en Blanco	Colapsar

Elementos Hijo (min,max)

Secuencia (1, Ilimitado)	Cuenta (1, Ilimitado)

Elemento: Cuenta

Diagrama


attributes
NumCta
type xs:string
use required
Atributo requerido para expresar la clave con que se distingue la cuenta o subcuenta que se afecta por la transacción que integra el auxiliar.
DesCta
type xs:string
use required
Atributo requerido para expresar el concepto de la cuenta o subcuenta que se afecta por la transacción que integra el auxiliar.
SaldoIni
type AuxiliarCtas:t_importe
use required
Atributo requerido para expresar el monto del saldo inicial de la cuenta o subcuenta del periodo del auxiliar. En caso de no existir dato, colocar cero (0)
SaldoFin
type AuxiliarCtas:t_importe
use required
Atributo requerido para expresar el monto del saldo final de la cuenta o subcuenta del periodo del auxiliar. En caso de no existir dato, colocar cero (0)
AuxiliarCtas:Cuenta
1..∞
Nodo obligatorio para expresar los movimientos del periodo de cada uno de los auxiliares de la cuenta y/o subcuenta.
1..∞
AuxiliarCtas:DetalleAux
1..∞
Nodo obligatorio para expresar el detalle de los movimientos del periodo de cada uno de los auxiliares

Descripción

Nodo obligatorio para expresar los movimientos del periodo de cada uno de los auxiliares de la cuenta y/o subcuenta.

Atributos

NumCta

Descripción	Atributo requerido para expresar la clave con que se distingue la cuenta o subcuenta que se afecta por la transacción que integra el auxiliar.
Uso	requerido
Tipo Base	xs:string
Longitud Mínima	1
Longitud Máxima	100

DesCta

Descripción	Atributo requerido para expresar el concepto de la cuenta o subcuenta que se afecta por la transacción que integra el auxiliar.
Uso	requerido
Tipo Base	xs:string
Longitud Mínima	1
Longitud Máxima	100

SaldoIni

Descripción	Atributo requerido para expresar el monto del saldo inicial de la cuenta o subcuenta del periodo del auxiliar. En caso de no existir dato, colocar cero (0)
Uso	requerido
Tipo Especial	AuxiliarCtas:t_importe

SaldoFin

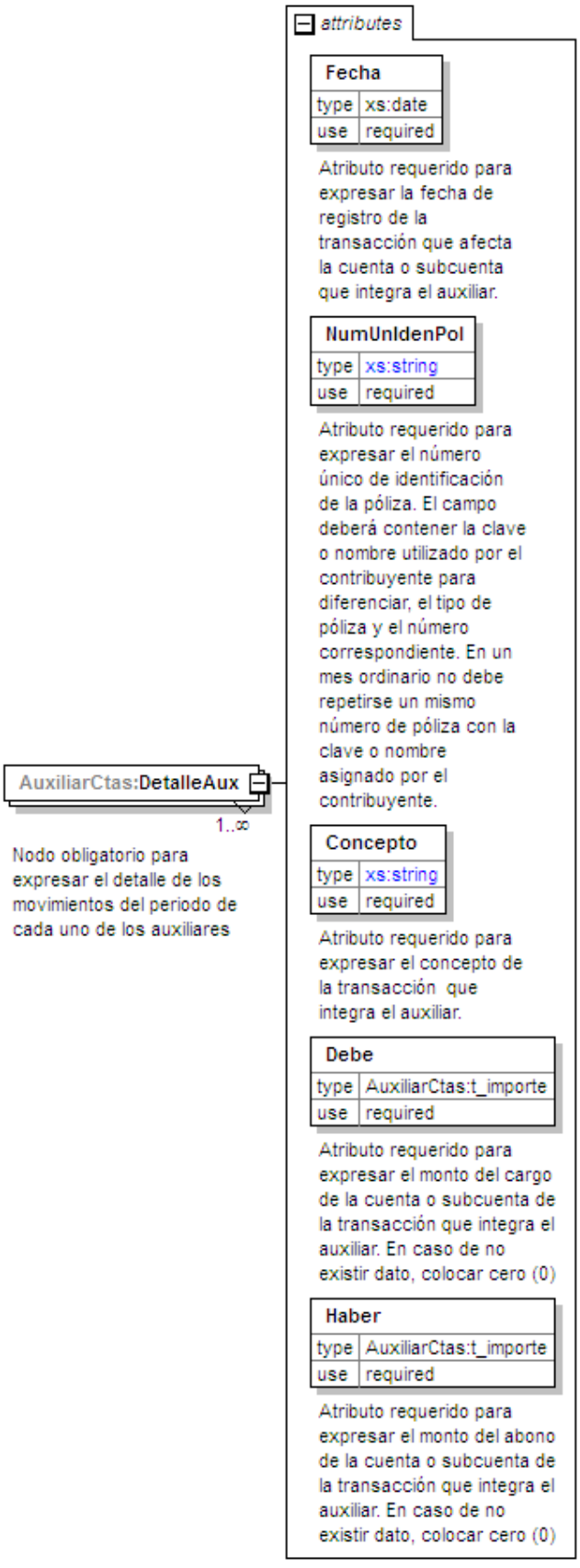
Descripción	Atributo requerido para expresar el monto del saldo final de la cuenta o subcuenta del periodo del auxiliar. En caso de no existir dato, colocar cero (0)
Uso	requerido
Tipo Especial	AuxiliarCtas:t_importe

Elementos Hijo (min,max)

Secuencia (1, Ilimitado)	DetalleAux (1, Ilimitado)

Elemento: DetalleAux

Diagrama


attributes
Fecha
type xs:date
use required
Atributo requerido para expresar la fecha de registro de la transacción que afecta la cuenta o subcuenta que integra el auxiliar.
NumUnIdenPol
type xs:string
use required
Atributo requerido para expresar el número único de identificación de la póliza. El campo deberá contener la clave o nombre utilizado por el contribuyente para diferenciar, el tipo de póliza y el número correspondiente. En un mes ordinario no debe repetirse un mismo número de póliza con la clave o nombre asignado por el contribuyente.
Concepto
type xs:string
use required
Atributo requerido para expresar el concepto de la transacción que integra el auxiliar.
Debe
type AuxiliarCtas:t_importe
use required
Atributo requerido para expresar el monto del cargo de la cuenta o subcuenta de la transacción que integra el auxiliar. En caso de no existir dato, colocar cero (0)
Haber
type AuxiliarCtas:t_importe
use required
Atributo requerido para expresar el monto del abono de la cuenta o subcuenta de la transacción que integra el auxiliar. En caso de no existir dato, colocar cero (0)
AuxiliarCtas:DetalleAux
1..∞
Nodo obligatorio para expresar el detalle de los movimientos del periodo de cada uno de los auxiliares

Descripción

Nodo obligatorio para expresar el detalle de los movimientos del periodo de cada uno de los auxiliares

Atributos

Fecha

Descripción	Atributo requerido para expresar la fecha de registro de la transacción que afecta la cuenta o subcuenta que integra el auxiliar.
Uso	requerido
Tipo Especial	xs:date

NumUnIdenPol

Descripción	Atributo requerido para expresar el número único de identificación de la póliza. El campo deberá contener la clave o nombre utilizado por el contribuyente para diferenciar, el tipo de póliza y el número correspondiente. En un mes ordinario no debe repetirse un mismo número de póliza con la clave o nombre asignado por el contribuyente.
Uso	requerido
Tipo Base	xs:string
Longitud Mínima	1
Longitud Máxima	50

Concepto

Descripción	Atributo requerido para expresar el concepto de la transacción que integra el auxiliar.
Uso	requerido
Tipo Base	xs:string
Longitud Mínima	1
Longitud Máxima	200

Debe

Descripción	Atributo requerido para expresar el monto del cargo de la cuenta o subcuenta de la transacción que integra el auxiliar. En caso de no existir dato, colocar cero (0)
Uso	requerido
Tipo Especial	AuxiliarCtas:t_importe

Haber

Descripción	Atributo requerido para expresar el monto del abono de la cuenta o subcuenta de la transacción que integra el auxiliar. En caso de no existir dato, colocar cero (0)
Uso	requerido
Tipo Especial	AuxiliarCtas:t_importe

Tipos Simples

Tipo Simple Global: t_importe

Descripción

Definición

Tipo Base	xs:decimal
Valor Mínimo Incluyente	-99999999999999.99
Valor Máximo	99999999999999.99

Incluyente	
Posiciones Decimales	2

Código Fuente

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:AuxiliarCtas="www.sat.gob.mx/esquemas/ContabilidadE/1_1/AuxiliarCtas"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="www.sat.gob.mx/esquemas/ContabilidadE/1_1/AuxiliarCtas"
elementFormDefault="qualified" attributeFormDefault="unqualified">
	<xs:element name="AuxiliarCtas">
		<xs:annotation>
			<xs:documentation>Estándar de auxiliar de la cuenta o subcuenta del periodo que
se entrega como parte de la contabilidad electrónica</xs:documentation>
		</xs:annotation>
		<xs:complexType>
			<xs:sequence maxOccurs="unbounded">
				<xs:element name="Cuenta" maxOccurs="unbounded">
					<xs:annotation>
						<xs:documentation>Nodo obligatorio para expresar los
movimientos del periodo de cada uno de los auxiliares de la cuenta y/o subcuenta.</xs:documentation>
					</xs:annotation>
					<xs:complexType>
						<xs:sequence maxOccurs="unbounded">
							<xs:element name="DetalleAux"
maxOccurs="unbounded">
<xs:annotation>
<xs:documentation>Nodo
obligatorio para expresar el detalle de los movimientos del periodo de cada uno de los
auxiliares</xs:documentation>
</xs:annotation>
<xs:complexType>
<xs:attribute name="Fecha"
type="xs:date" use="required">
<xs:annotation>

	<xs:documentation>Atributo requerido para expresar la fecha de registro de la transacción que afecta
la cuenta o subcuenta que integra el auxiliar.</xs:documentation>
</xs:annotation>
</xs:attribute>
<xs:attribute
name="NumUnIdenPol" use="required">
<xs:annotation>

	<xs:documentation>Atributo requerido para expresar el número único de identificación de la póliza. El
campo deberá contener la clave o nombre utilizado por el contribuyente para diferenciar, el tipo de póliza y el
número correspondiente. En un mes ordinario no debe repetirse un mismo número de póliza con la clave o
nombre asignado por el contribuyente.</xs:documentation>
</xs:annotation>
<xs:simpleType>

	<xs:restriction base="xs:string">

	<xs:minLength value="1"/>

	<xs:maxLength value="50"/>

	</xs:restriction>
</xs:simpleType>
</xs:attribute>
```

<xs:attribute name="Concepto" use="required">
<xs:annotation>
<xs:documentation>Atributo requerido para expresar el concepto de la transacción que integra el auxiliar.</xs:documentation>
</xs:annotation>
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:minLength value="1"/>
<xs:maxLength value="200"/>
</xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="Debe" type="AuxiliarCtas:t_importe" use="required">
<xs:annotation>
<xs:documentation>Atributo requerido para expresar el monto del cargo de la cuenta o subcuenta de la transacción que integra el auxiliar. En caso de no existir dato, colocar cero (0)</xs:documentation>
</xs:annotation>
</xs:attribute>
<xs:attribute name="Haber" type="AuxiliarCtas:t_importe" use="required">
<xs:annotation>
<xs:documentation>Atributo requerido para expresar el monto del abono de la cuenta o subcuenta de la transacción que integra el auxiliar. En caso de no existir dato, colocar cero (0)</xs:documentation>
</xs:annotation>
</xs:attribute>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="NumCta" use="required">
<xs:annotation>
<xs:documentation>Atributo requerido para expresar la clave con que se distingue la cuenta o subcuenta que se afecta por la transacción que integra el auxiliar.</xs:documentation>
</xs:annotation>
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:minLength value="1"/>
<xs:maxLength value="100"/>
</xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="DesCta" use="required">
<xs:annotation>
<xs:documentation>Atributo requerido para expresar el concepto de la cuenta o subcuenta que se afecta por la transacción que integra el auxiliar.</xs:documentation>
</xs:annotation>
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:minLength value="1"/>
<xs:maxLength value="100"/>
</xs:restriction>
</xs:simpleType>

```
                                                </xs:attribute>
                                                <xs:attribute name="SaldoIni"
type="AuxiliarCtas:t_importe" use="required">
                                                        <xs:annotation>
                                                                <xs:documentation>Atributo requerido
para expresar el monto del saldo inicial de la cuenta o subcuenta del periodo del auxiliar. En caso de no existir
dato, colocar cero (0)</xs:documentation>
                                                        </xs:annotation>
                                                </xs:attribute>
                                                <xs:attribute name="SaldoFin"
type="AuxiliarCtas:t_importe" use="required">
                                                        <xs:annotation>
                                                                <xs:documentation>Atributo requerido
para expresar el monto del saldo final de la cuenta o subcuenta del periodo del auxiliar. En caso de no existir
dato, colocar cero (0)</xs:documentation>
                                                        </xs:annotation>
                                                </xs:attribute>
                                        </xs:complexType>
                                </xs:element>
                        </xs:sequence>
                        <xs:attribute name="Version" type="xs:string" use="required" fixed="1.1">
                                <xs:annotation>
                                        <xs:documentation>Atributo requerido para expresar la versión
del formato.</xs:documentation>
                                </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="RFC" use="required">
                                <xs:annotation>
                                        <xs:documentation>Atributo requerido para expresar el RFC del
contribuyente que envía los datos.</xs:documentation>
                                </xs:annotation>
                                <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                                <xs:minLength value="12"/>
                                                <xs:maxLength value="13"/>
                                                <xs:pattern value="[A-ZÑ&amp;]{3,4}[0-9]{2}[0-1][0-9][0-
3][0-9][A-Z0-9]?[A-Z0-9]?[0-9A-Z]?"/>
                                        </xs:restriction>
                                </xs:simpleType>
                        </xs:attribute>
                        <xs:attribute name="Mes" use="required">
                                <xs:annotation>
                                        <xs:documentation>Atributo requerido para expresar el mes en
que inicia la vigencia del auxiliar de la cuenta o subcuenta.</xs:documentation>
                                </xs:annotation>
                                <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                                <xs:enumeration value="01"/>
                                                <xs:enumeration value="02"/>
                                                <xs:enumeration value="03"/>
                                                <xs:enumeration value="04"/>
                                                <xs:enumeration value="05"/>
                                                <xs:enumeration value="06"/>
                                                <xs:enumeration value="07"/>
                                                <xs:enumeration value="08"/>
                                                <xs:enumeration value="09"/>
                                                <xs:enumeration value="10"/>
                                                <xs:enumeration value="11"/>
                                                <xs:enumeration value="12"/>
                                        </xs:restriction>
                                </xs:simpleType>
                        </xs:attribute>
```

```
<xs:attribute name="Anio" use="required">
	<xs:annotation>
		<xs:documentation>Atributo requerido para expresar el año al que inicia la vigencia del auxiliar de la cuenta o subcuenta.</xs:documentation>
	</xs:annotation>
	<xs:simpleType>
		<xs:restriction base="xs:int">
			<xs:minInclusive value="2015"/>
			<xs:maxInclusive value="2099"/>
		</xs:restriction>
	</xs:simpleType>
</xs:attribute>
<xs:attribute name="TipoSolicitud" use="required">
	<xs:annotation>
		<xs:documentation>Atributo requerido para expresar el tipo de envío del auxiliar de la cuenta o subcuenta ( AF - Acto de Fiscalización; FC - Fiscalización Compulsa; DE - Devolución; CO - Compensación )</xs:documentation>
	</xs:annotation>
	<xs:simpleType>
		<xs:restriction base="xs:string">
			<xs:pattern value="AF|FC|DE|CO"/>
		</xs:restriction>
	</xs:simpleType>
</xs:attribute>
<xs:attribute name="NumOrden" use="optional">
	<xs:annotation>
		<xs:documentation>Atributo opcional para expresar el número de orden asignado al acto de fiscalización al que hace referencia la solicitud del auxiliar de la cuenta o subcuenta. Requerido para tipo de solicitud = AF y FC. Se convierte en requerido cuando se cuente con la información.</xs:documentation>
	</xs:annotation>
	<xs:simpleType>
		<xs:restriction base="xs:string">
			<xs:length value="13"/>
			<xs:pattern value="[A-Z]{3}[0-6][0-9][0-9]{5}(/)[0-9]{2}"/>
		</xs:restriction>
	</xs:simpleType>
</xs:attribute>
<xs:attribute name="NumTramite" use="optional">
	<xs:annotation>
		<xs:documentation>Atributo opcional para expresar el número de trámite asignado a la solicitud de devolución o compensación al que hace referencia el auxiliar de la cuenta o subcuenta. Requerido para tipo de solicitud  = DE  o CO. Se convierte en requerido cuando se cuente con la información.</xs:documentation>
	</xs:annotation>
	<xs:simpleType>
		<xs:restriction base="xs:string">
			<xs:length value="10"/>
			<xs:pattern value="[0-9]{10}"/>
		</xs:restriction>
	</xs:simpleType>
</xs:attribute>
<xs:attribute name="Sello" use="optional">
	<xs:annotation>
		<xs:documentation>Atributo opcional para contener el sello digital del archivo de contabilidad electrónica. El sello deberá ser expresado cómo una cadena de texto en formato Base 64</xs:documentation>
	</xs:annotation>
	<xs:simpleType>
		<xs:restriction base="xs:string">
			<xs:whiteSpace value="collapse"/>
		</xs:restriction>
```

```
                                        </xs:simpleType>
                                </xs:attribute>
                                <xs:attribute name="noCertificado" use="optional">
                                        <xs:annotation>
                                                <xs:documentation>Atributo opcional para expresar el número de serie del certificado de sello digital que ampara el archivo de contabilidad electrónica, de acuerdo al acuse correspondiente a 20 posiciones otorgado por el sistema del SAT.</xs:documentation>
                                        </xs:annotation>
                                        <xs:simpleType>
                                                <xs:restriction base="xs:string">
                                                        <xs:length value="20"/>
                                                </xs:restriction>
                                        </xs:simpleType>
                                </xs:attribute>
                                <xs:attribute name="Certificado" use="optional">
                                        <xs:annotation>
                                                <xs:documentation>Atributo opcional que sirve para expresar el certificado de sello digital que ampara al archivo de contabilidad electrónica como texto, en formato base 64.</xs:documentation>
                                        </xs:annotation>
                                        <xs:simpleType>
                                                <xs:restriction base="xs:string">
                                                        <xs:whiteSpace value="collapse"/>
                                                </xs:restriction>
                                        </xs:simpleType>
                                </xs:attribute>
                        </xs:complexType>
                </xs:element>
                <xs:simpleType name="t_importe">
                        <xs:restriction base="xs:decimal">
                                <xs:fractionDigits value="2"/>
                                <xs:minInclusive value="-99999999999999.99"/>
                                <xs:maxInclusive value="99999999999999.99"/>
                        </xs:restriction>
                </xs:simpleType>
</xs:schema>
```

2. Generación opcional de sellos digitales.

Elementos utilizados en la generación opcional de Sellos Digitales:

- Cadena Original, del elemento a sellar.
- Certificado de Sello Digital y su correspondiente clave privada.
- Algoritmos de criptografía de clave pública para firma electrónica avanzada.
- Especificaciones de conversión de la firma electrónica avanzada a Base 64.

Para la generación de sellos digitales se utiliza criptografía de clave pública aplicada a una cadena original.

Criptografía de la Clave Pública

La criptografía de Clave Pública se basa en la generación de una pareja de números muy grandes relacionados íntimamente entre sí, de tal manera que una operación de encripción sobre un mensaje tomando como clave de encripción a uno de los dos números, produce un mensaje alterado en su significado que solo puede ser devuelto a su estado original mediante la operación de desencripción correspondiente tomando como clave de desencripción al otro número de la pareja.

Uno de estos dos números, expresado en una estructura de datos que contiene un módulo y un exponente, se conserva secreta y se le denomina "clave privada", mientras que el otro número llamado "clave pública", en formato binario y acompañado de información de identificación del emisor, además de una calificación de validez por parte

de un tercero confiable, se incorpora a un archivo denominado "certificado de firma electrónica avanzada o certificado para sellos digitales".

El Certificado puede distribuirse libremente para efectos de intercambio seguro de información y para ofrecer pruebas de autoría de archivos electrónicos o acuerdo con su contenido mediante el proceso denominado "firma electrónica avanzada ", que consiste en una característica observable de un mensaje, verificable por cualquiera con acceso al certificado digital del emisor, que sirve para implementar servicios de seguridad para garantizar: La integridad (facilidad para detectar si un mensaje firmado ha sido alterado), autenticidad, certidumbre de origen (facilidad para determinar qué persona es el autor de la firma y valida el contenido del mensaje) y no repudiación del mensaje firmado (capacidad de impedir que el autor de la firma niegue haber firmado el mensaje).

Estos servicios de seguridad proporcionan las siguientes características a un mensaje con firma electrónica avanzada:

- Es infalsificable.
- La firma electrónica avanzada no es reciclable (es única por mensaje).
- Un mensaje con firma electrónica avanzada alterado, es detectable.
- Un mensaje con firma electrónica avanzada, no puede ser repudiado.

Los certificados de sello digital se generan de manera idéntica a la firma electrónica avanzada y al igual que las firmas electrónicas avanzadas el propósito del sello digital es emitir documentos digitales con autenticidad, integridad, verificables y no repudiables por el emisor. Para ello bastará tener acceso al mensaje original o cadena original, al sello digital y al certificado de sello digital del emisor.

Al ser el certificado de sello digital idéntico en su generación a una firma electrónica avanzada, proporciona los mismos servicios de seguridad y hereda las características de las firmas digitales.

Por consecuencia un archivo sellado digitalmente por el contribuyente tiene las siguientes características:

- Es infalsificable.
- El sello digital no es reciclable (es único por documento).
- Una cadena original de un documento digital sellada digitalmente, que hubiese sido alterada es detectable.
- Una cadena original de un archivo sellada digitalmente no puede ser repudiada.

Los algoritmos utilizados en la generación de un sello digital son los siguientes:

SHA-1, que es una función hash (digestión, o resumen) de un solo sentido tal que para cualquier entrada produce una salida compleja de 160 bits de salida, 80 para seguridad del mensaje y 80 para la identificación del mensaje (20 bytes) denominada ‘digestión’.

SHA-2, que es una función hash (digestión o resumen) de un solo sentido tal que para cualquier entrada produce una salida compleja de 256 bits de salida, 128 para seguridad del mensaje y 128 para la identificación del mensaje (32 bytes) denominada ‘digestión’.

RSAPrivateEncrypt, que utiliza la clave privada del emisor para encriptar la digestión del mensaje.

RSAPublicDecrypt, que utiliza la clave pública del emisor para desencriptar la digestión del mensaje.

Cadena Original

Se entiende como cadena original, a la secuencia de datos formada con la información contenida dentro del archivo, establecida en el Rubro A “Estándar del Formato Reporte Auxiliar de Cuentas y/o subcuentas de Contabilidad Electrónica” de este anexo. Siguiendo para ello las reglas y la secuencia aquí especificadas:

Reglas Generales:

1. Ninguno de los atributos que conforman el archivo deberá contener el carácter | (“pipe”) debido a que este será utilizado como carácter de control en la formación de la cadena original.
2. El inicio de la cadena original se encuentra marcado mediante una secuencia de caracteres || (doble “pipe”).
3. Se expresará únicamente la información del dato sin expresar el atributo al que hace referencia. Esto es, si la valor de un campo es la “A” solo se expresará |A| y nunca |campo A|.
4. Cada dato individual se encontrará separado de su dato subsiguiente, en caso de existir, mediante un carácter | (“pipe” sencillo).
5. Los espacios en blanco que se presenten dentro de la cadena original serán tratados de la siguiente manera:
    a. Se deberán remplazar todos los tabuladores, retornos de carro y saltos de línea por espacios en blanco.
    b. Acto seguido se elimina cualquier carácter en blanco al principio y al final de cada separador | (“pipe” sencillo).
    c. Finalmente, toda secuencia de caracteres en blanco intermedias se sustituyen por un único carácter en blanco.
6. Los datos opcionales no expresados, no aparecerán en la cadena original y no tendrán delimitador alguno.
7. El final de la cadena original será expresado mediante una cadena de caracteres || (doble “pipe”).
8. Toda la cadena de original se expresará en el formato de codificación UTF-8.

Secuencia de Formación:

La secuencia de formación será siempre en el orden que se expresa a continuación, tomando en cuenta las reglas generales expresadas en el párrafo anterior.

1) Información del nodo AuxiliarCtas
    a) Version
    b) RFC
    c) Mes
    d) Anio
    e) TipoSolicitud
    f) NumOrden
    g) NumTramite
2) Información del nodo Cuenta
    a) NumCta
    b) DesCta
    c) SaldoIni
    d) SaldoFin
3) Información del nodo DetalleAux
    a) Fecha
    b) NumUnIdenPol
    c) Debe
    d) Haber

Generación del Sello Digital

Para toda cadena original a ser sellada digitalmente, la secuencia de algoritmos a aplicar es la siguiente:

I. Aplicar el método de digestión SHA-1 a la cadena original a sellar. Este procedimiento genera una salida de 160 bits (20 bytes) para todo mensaje. La posibilidad de encontrar dos mensajes distintos que produzcan una misma salida es de 1 en $2^{(60\text{-colision})}$, y por lo tanto en esta posibilidad se basa la inalterabilidad del sello, así como su no reutilización. Es de hecho una medida de la integridad del mensaje sellado, pues toda alteración del mismo provocará una digestión totalmente diferente, por lo que no se podrá autentificar el mensaje.

Aplicar el método de digestión SHA-2 a la cadena original a sellar. Este procedimiento genera una salida de 256 bits (32 bytes) para todo mensaje. La posibilidad de encontrar dos mensajes distintos que produzcan una misma salida no ha sido encontrada una colisión y por lo tanto en esta posibilidad se basa la inalterabilidad del sello, así como su no reutilización. Es de hecho una medida de la integridad del mensaje sellado, pues toda alteración del mismo

provocará una digestión totalmente diferente, por lo que no se podrá autentificar el mensaje.

II. Con la clave privada correspondiente al certificado de sello digital del emisor, encriptar la digestión del mensaje obtenida en el paso I utilizando para ello el algoritmo de encripción RSA.

Nota: La mayor parte del software comercial podría generar los pasos I y II invocando una sola función y especificando una constante simbólica. En el SAT este procedimiento se hace en pasos separados, lo cual es totalmente equivalente. Es importante resaltar que prácticamente todo el software criptográfico comercial incluye APIs o expone métodos en sus productos que permiten implementar la secuencia de algoritmos aquí descrita. La clave privada solo debe mantenerse en memoria durante la llamada a la función de encripción; inmediatamente después de su uso debe ser eliminada de su registro de memoria mediante la sobre escritura de secuencias binarias alternadas de "unos" y "ceros".

III.- El resultado será una cadena binaria que no necesariamente consta de caracteres imprimibles, por lo que deberá traducirse a una cadena que sí conste solamente de tales caracteres. Para ello se utilizará el modo de expresión de secuencias de bytes denominado "Base 64", que consiste en la asociación de cada 6 bits de la secuencia a un elemento de un "alfabeto" que consta de 64 caracteres imprimibles. Puesto que con 6 bits se pueden expresar los números del 0 al 63, si a cada uno de estos valores se le asocia un elemento del alfabeto se garantiza que todo byte de la secuencia original puede ser mapeado a un elemento del alfabeto Base 64, y los dos bits restantes formarán parte del siguiente elemento a mapear. Este mecanismo de expresión de cadenas binarias produce un incremento de 25% en el tamaño de las cadenas imprimibles respecto de la original.

La codificación en base 64, así como su decodificación, se hará tomando los bloques a procesar en el sentido de su lectura, es decir, de izquierda a derecha.

El alfabeto a utilizar se expresa en el siguiente catálogo:

Elemento del Alfabeto	Valor B64	Valor ASCII	Elemento del Alfabeto	Valor B64	Valor ASCII	Elemento del Alfabeto	Valor B64	Valor ASCII
0	A	65	23	X	88	46	u	117
1	B	66	24	Y	89	47	v	118
2	C	67	25	Z	90	48	w	119
3	D	68	26	a	97	49	x	120
4	E	69	27	b	98	50	y	121
5	F	70	28	c	99	51	z	122
6	G	71	29	d	100	52	0	48
7	H	72	30	e	101	53	1	49
8	I	73	31	f	102	54	2	50
9	J	74	32	g	103	55	3	51
10	K	75	33	h	104	56	4	52
11	L	76	34	i	105	57	5	53
12	M	77	35	j	106	58	6	54
13	N	78	36	k	107	59	7	55
14	O	79	37	l	108	60	8	56
15	P	80	38	m	109	61	9	57
16	Q	81	39	n	110	62	+	43
17	R	82	40	o	111	63	/	47
18	S	83	41	p	112			
19	T	84	42	q	113			
20	U	85	43	r	114			
21	V	86	44	s	115			
22	W	87	45	t	116			

Por tanto, los caracteres utilizados en el alfabeto de Base 64 son:

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, +, /

Y en el orden descrito les corresponden los índices del 0 al 63 en un arreglo de 64 elementos. Para traducir de binario a Base 64, se examina la secuencia binaria evaluando 6 bits a la vez; si el valor de los primeros 6 bits es 0, entonces se imprime la letra A; si es 1, entonces se imprime la letra B y así sucesivamente hasta completar la evaluación de todos los bits de la secuencia binaria evaluados de 6 en 6.

La función inversa consiste en reconstruir la secuencia binaria original a partir de la cadena imprimible que consta de los elementos del alfabeto de Base 64. Para ello se toman 4 caracteres a la vez de la cadena imprimible y sus valores son convertidos en los de los tres caracteres binarios correspondientes (4 caracteres B64 x 6 bits = 3 caracteres binarios x 8 bits), y esta operación se repite hasta concluir la traducción de la cadena imprimible.

Ejemplo de Sello digital:

GqDiRrea6+E2wQhqOCVzwME4866yVEME/8PD1S1g6AV48D8VrLhKUDq0Sjqnp9IwfMAbX0ggwUCLRKa+Hg5q8a
Yhya63If2HVqH1sA08poer080P1J6Z+BwTrQkhcb5Jw8jENXoErkFE8qdOcIdFFAuZPVT+9mkTb0Xn5Emu5U8=