F. Estándar de Consulta para Códigos Retroalimentados.

El contribuyente que consulte la información de los códigos retroalimentados por medio del servicio web deberá generarlo bajo el siguiente estándar XSD, validando su forma y sintaxis en un archivo con extensión XML.

Para poder ser validado, deberá estar referenciado al namespace y la validación del mismo a la ruta publicada por el SAT en donde se encuentra el esquema XSD objeto de la presente sección (http://esquemas.clouda.sat.gob.mx/archivos/Tabacos/1/ConsultaCodigo/TBCConsulCodigo.xsd) de la siguiente manera:

<conCod:TBCConsulCodigo

xmlns: conCod ="http://esquemas.clouda.sat.gob.mx/archivos/Tabacos/1/ConsultaCodigo"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="

http://esquemas.clouda.sat.gob.mx/archivos/Tabacos/1/ConsultaCodigo

http://esquemas.clouda.sat.gob.mx/archivos/Tabacos/1/ConsultaCodigo/TBCConsulCodigo.xsd"

……..

</conCod:TBCConsulCodigo>

Cadena Original

Se entiende como cadena original, a la secuencia de datos formada con la información contenida dentro de la solicitud o descarga de códigos de seguridad. Siguiendo para ello las reglas y la secuencia aquí especificada:

Reglas Generales:

1. Ninguno de los atributos que conforman las operaciones con códigos de seguridad deberán contener el carácter | (“pipe”) debido a que éste 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 el valor del atributo “País” es “MX” solo se expresará |MX| y nunca |País MX|.
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:

1. RFCContribuyente
2. Codigo
3. Version

Generación de la firma o sello

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

I.- Aplicar el método de digestión SHA256 a la cadena original. Este procedimiento genera una salida de 256 bits (128 bytes) para todo mensaje. Por la posibilidad de encontrar dos mensajes distintos que produzcan una misma salida, 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.

SHA-2 no requiere semilla alguna. El algoritmo cambia su estado de bloque en bloque de acuerdo a la entrada previa.

II.- Con la clave privada correspondiente al certificado digital del emisor del mensaje y del sello digital, 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
0	A	65
1	B	66
2	C	67
3	D	68
4	E	69
5	F	70
6	G	71
7	H	72
8	I	73
9	J	74
10	K	75
11	L	76
12	M	77
13	N	78
14	O	79

Elemento del Alfabeto	Valor B64	Valor ASCII
23	X	88
24	Y	89
25	Z	90
26	a	97
27	b	98
28	c	99
29	d	100
30	e	101
31	f	102
32	g	103
33	h	104
34	i	105
35	j	106
36	k	107
37	l	108

Elemento del Alfabeto	Valor B64	Valor ASCII
46	u	117
47	v	118
48	w	119
49	x	120
50	y	121
51	z	122
52	0	48
53	1	49
54	2	50
55	3	51
56	4	52
57	5	53
58	6	54
59	7	55
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.

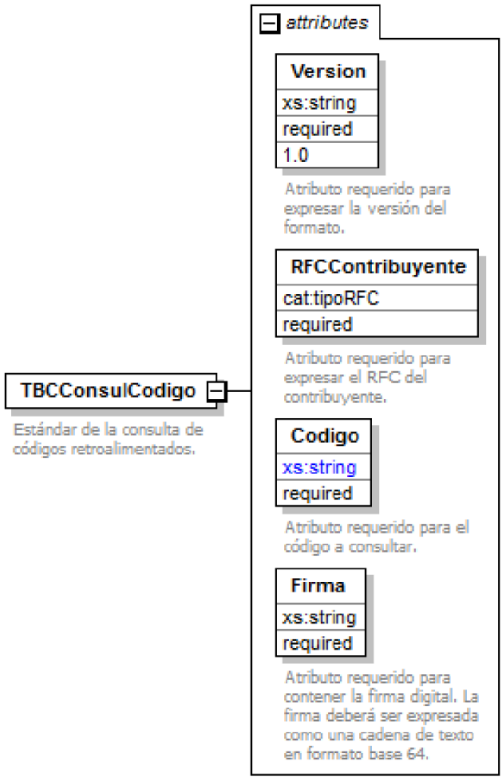
La función inversa consiste en reconstruir la secuencia binaria original a partir de la cadena imprimible que consta de los elementos del alfabeto de Base 64. Para ello se toman 4 caracteres a la vez de la cadena imprimible y sus valores son convertidos en los de los tres caracteres binarios correspondientes (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.

Estructura

Elementos

Elemento: TBCConsulCodigo

Diagrama



Descripción

Estándar de la consulta de códigos retroalimentados.

Atributos

Version

Descripción	Atributo requerido para expresar la versión del formato.
Uso	requerido
Tipo Base	xs:string
Valor Fijo	1.0

Codigo

Descripción	Atributo requerido para el código a consultar.
Uso	requerido
Tipo Base	xs:string
Patron	[A-Z0-9]{12}

Firma

Descripción	Atributo requerido para contener la firma digital. La firma deberá ser expresada como una cadena de texto en formato base 64.

Uso	requerido
Tipo Base	xs:string

RFCContribuyente

Descripción	Atributo requerido para expresar el RFC del contribuyente.
Uso	requerido
Tipo Especial	cat:tipoRFC

Código Fuente

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
xmlns:conCod="http://esquemas.clouda.sat.gob.mx/archivos/Tabacos/1/ConsultaCodigo"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:cat="http://esquemas.clouda.sat.gob.mx/archivos/Tabacos/1/Catalogos"
targetNamespace="http://esquemas.clouda.sat.gob.mx/archivos/Tabacos/1/ConsultaCodigo"
elementFormDefault="qualified" attributeFormDefault="unqualified">
 <xs:import namespace="http://esquemas.clouda.sat.gob.mx/archivos/Tabacos/1/Catalogos"
schemaLocation="http://esquemas.clouda.sat.gob.mx/archivos/Tabacos/1/Catalogos/catTabacos.
xsd"/>
 <xs:element name="TBCConsulCodigo">
<xs:annotation>
 <xs:documentation>Estándar de la consulta de códigos retroalimentados.</xs:documentation>
</xs:annotation>
<xs:complexType>
 <xs:attribute name="Version" type="xs:string" use="required" fixed="1.0">
<xs:annotation>
 <xs:documentation>Atributo requerido para expresar la versión del formato.</xs:documentation>
</xs:annotation>
 </xs:attribute>
 <xs:attribute name="RFCContribuyente" type="cat:tipoRFC" use="required">
<xs:annotation>
 <xs:documentation>Atributo requerido para expresar el RFC del
contribuyente.</xs:documentation>
</xs:annotation>
 </xs:attribute>
 <xs:attribute name="Codigo" use="required">
<xs:annotation>
 <xs:documentation>Atributo requerido para el código a consultar.</xs:documentation>
</xs:annotation>
<xs:simpleType>
 <xs:restriction base="xs:string">
<xs:pattern value="[A-Z0-9]{12}"/>
```

```
 </xs:restriction>
</xs:simpleType>
 </xs:attribute>
 <xs:attribute name="Firma" type="xs:string" use="required">
<xs:annotation>
 <xs:documentation>Atributo requerido para contener la firma digital. La firma deberá ser expresada como una cadena de texto en formato base 64.</xs:documentation>
</xs:annotation>
 </xs:attribute>
</xs:complexType>
 </xs:element>
</xs:schema>
```