E. Generación de la firma para la solicitud y descarga de códigos de seguridad.

Elementos utilizados en la generación de la firma:

- Cadena Original, el elemento a firmar de la solicitud o descarga de códigos de seguridad.
- Certificado de Sello Digital y su correspondiente clave privada.

El Servicio de Administración Tributaria pone a disposición del Contribuyente la aplicación “SOLCEDI” (Solicitud de Certificado Digital), a fin de facilitar la generación de claves.

Nota: *Es responsabilidad del Contribuyente el utilizar un equipo de cómputo de su confianza para la generación de su par de claves y guardar en lugar seguro la Clave Privada generada y sus contraseñas.*

Se recomienda utilizar contraseñas fuertes con el fin de conservar la confidencialidad en las transacciones, por ejemplo:

- Longitud mínima de 12 caracteres.
- Alfanuméricas (Letras mayúsculas y minúsculas)
- Mínimo 2 caracteres especiales.

Ya que de esto hace difícil que se pueda romper la contraseña, se pueden combinar letras por números para ayudar a recordar esta contraseña (pe. 3$l0V4K142%#), espaciar números y letras (que no sean contiguos).

- Algoritmos de criptografía de clave pública del certificado de sello digital.
- Especificaciones de conversión del certificado de sello digital a Base 64.

Para la generación de firma o 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 sello digital ".

El Certificado puede distribuirse libremente para efectos de intercambio seguro de información y para ofrecer pruebas de autoría de archivos electrónicos o de acuerdo con su contenido mediante el proceso de “firma” o “sello”, 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 o sellado ha sido alterado), autenticidad, certidumbre de origen (facilidad para determinar qué persona es el autor de la firma o sello y valida el contenido del mensaje) y no repudiación del mensaje firmado o sellado (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 o sello:

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

Los algoritmos utilizados en la generación de una firma o sello digital son los siguientes:

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’.

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:

Solicitud de códigos de seguridad.

1. Información del Nodo: Solicitud
    a) RFC
2. Información del Nodo: TBCSlcCodSeg
    a) Fecha
3. Información del Nodo: Solicitud
    a) CantidadCodigos
4. Información del Nodo: Solicitud
    a) Version
    b) RFCProveedorCertificado
    c) Descarga de archivos
5. Información del Nodo: TBCSolDescarga
    a) RFC
    b) Nomarch
    c) Folio
    d) Version
    e) RFCProveedorCertificado

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	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:

GqDiRrea6+E2wQhqOCVzwME4866yVEME/8PD1S1g6AV48D8VrLhKUDq0Sjqnp9IwfMAbX0ggwUCLRKa+Hg5q8aYhya63If2HVqH1sA08poer080P1J6Z+BwTrQkhcb5Jw8jENXoErkFE8qdOcIdFFAuZPVT+9mkTb0Xn5Emu5U8=