Generación de sellos digitales para la Constancia de sueldos, salarios, conceptos asimilados, crédito al salario y subsidio para el empleo (incluye ingresos por acciones) (Formato 37) y Constancia de pagos y retenciones del ISR, IVA e IEPS (Formato 37-A)

Elementos utilizados en la generación de Sellos Digitales:

- Cadena Original, el elemento a sellar, en este caso de una constancia de sueldos, salarios, conceptos asimilados, crédito al salario y subsidio para el empleo (Formato 37) y Constancia de pagos y retenciones del ISR, IVA e IEPS (Formato 37-A).
- 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.

Por consecuencia una constancia firmada digitalmente por el contribuyente tiene las siguientes características:

- Es infalsificable.
- La firma digital no es reciclable (es único por documento).
- Una cadena original de una constancia firmada digitalmente, que hubiese sido alterada es detectable.
- Una cadena original de una constancia firmada digitalmente no puede ser repudiada.

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

SHA-1 ó SHA-2, que es una función hash (digestión, picadillo o resumen) de un sólo sentido tal que para cualquier entrada produce una salida compleja 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.

A manera de referencia y para obtener información adicional, se recomienda consultar el sitio de Firma Electrónica Avanzada que se encuentra dentro del portal del SAT: www.sat.gob.mx

Cadena Original

Se entiende como cadena original, a la secuencia de datos formada con la información contenida dentro de la constancia. Siguiendo para ello las reglas y secuencia aquí especificadas:

Reglas Generales:

1. Ninguno de los atributos deberá contener el caracter | (“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 el nombre del contribuyente es “PEDRO” sólo se expresará |PEDRO| y nunca |NOMBRE PEDRO|.
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 para la cadena original de la Constancia de Sueldos, Salarios, Conceptos Asimilados, Crédito al Salario y subsidio para el empleo (Incluye Ingresos por Acciones) (Formato 37):

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 "Periodo que ampara la constancia"

    a. Mes inicial
    b. Mes final
    c. Ejercicio

2. Información del nodo "Datos del trabajador"

    d. Registro Federal de Contribuyentes.
    e. Clave Única de Registro de Población.
    f. Apellido Paterno
    g. Apellido materno
    h. Nombre (s)

3. Información del nodo "Impuesto Sobre la Renta por Sueldos y Salarios"

    i. Suma del ingreso gravado por sueldos y salarios.
    j. Suma del ingreso exento por sueldos y salarios
    k. Suma de ingresos por sueldos y salarios
    l. Monto del impuesto local a los ingresos por sueldos, salarios y en general por la prestación de un servicio personal subordinado retenido.
    m. Impuesto retenido durante el ejercicio.
    n. Impuesto retenido por otro(s) patrón (es) durante el ejercicio.
    o. Saldo a favor determinado en el ejercicio que declara que el patrón compensará durante el siguiente ejercicio o solicitará su devolución.
    p. Saldo a favor del ejercicio anterior no compensado durante el ejercicio que ampara la constancia.
    q. Suma de las cantidades que por concepto del crédito al salario le correspondió al trabajador.
    r. Crédito al salario entregado en efectivo al trabajador durante el ejercicio.
    s. Monto total de ingresos obtenidos por concepto de prestaciones de previsión social.
    t. Suma de ingresos exentos por concepto de prestaciones de previsión social.
    u. Monto del subsidio para el empleo entregado en efectivo al trabajador durante el ejercicio que declara.

4. Información del nodo Datos del retenedor

    v. Registro Federal de Contribuyentes.
    w. Clave Única de Registro de Población (Sólo Personas Físicas)
    x. Apellido Paterno, Materno y Nombre (s) o Denominación o Razón Social.
    y. Clave Única de Registro de Población (Representante Legal)
    z. Apellido Paterno, Materno y Nombre(s). (Representante Legal)

Secuencia de Formación para la Constancia de Pagos y Retenciones (Formato 37-A)

1. Información del nodo “Periodo que ampara la constancia".
   a. Mes inicial
   b. Mes Final
   c. Ejercicio
2. Información del nodo “Datos de identificación del tercero”.

   c. Registro Federal de Contribuyentes
   d. Clave Única de Registro de Población (Sólo personas Físicas)
   e. Apellido Paterno, Materno y Nombre (s) o Denominación o Razón social

3. Información del nodo “Dividendos o utilidades distribuidos”.

   f. Tipo de dividendo o utilidad
   g. Monto del dividendo o utilidad distribuido
   h. Monto del dividendo o utilidad acumulable
   i. Monto del ISR acreditable

4. Información del nodo “Otros pagos y retenciones”.

   j. Clave del pago
   k. Monto del interés nominal
   l. Pagos provisionales efectuados por la fiduciaria (tratándose de arrendamiento y fideicomiso)
   m. Deducciones correspondientes (tratándose de arrendamiento y fideicomiso)
   n. Tipo de pago (si se seleccionó la clave de pago G1)
   o. Monto de la operación o actividad gravada (ISR)
   p. Monto de la operación o actividad gravada (IVA)
   q. Monto de la operación o actividad gravada (IEPS)
   r. Monto de la operación o actividad Exenta (ISR)
   s. Monto de la operación o actividad Exenta (IVA)
   t. Monto de la operación o actividad Exenta (IEPS)
   u. Impuesto Retenido (ISR)
   v. Impuesto Retenido (IVA)
   w. Impuesto Retenido (IEPS)

5. Información del nodo “Datos del Retenedor”.

   x. Registro Federal de contribuyentes
   y. Clave Única de Registro de Población (Sólo personas Físicas)
   z. Apellido Paterno, Materno y Nombre(s), Denominación o Razón Social
   aa. Apellido Paterno, Materno y Nombre(s) (Representante Legal)
   bb. Registro Federal de Contribuyentes (Representante Legal)
   cc. Clave Única de Registro de Población (Representante Legal)

Generación de la Firma 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 o SHA-2 (recomendado) a la cadena original a firmar.

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

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 firma digital:

GqDiRrea6E2wQhqOCVzwME4866yVEME/8PD1S1g6AV48D8VrLhKUDq0Sjqnp9IwfMAbX0ggwUCLRKa
Hg5q8aYhya63If2HVqH1sA08poer080P1J6ZBwTrQkhcb5Jw8jENXoErkFE8qdOcIdFFAuZPVT9mkTb0X
n5Emu5U8=