

Elementos utilizados en la generación de Sellos Digitales:

- Cadena Original, el elemento a sellar, en este caso de un comprobante fiscal digital por Internet.
- 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 entre sí, de tal manera que una operación de encriptación sobre un mensaje tomando como clave de encriptación 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 desencriptación correspondiente tomando como clave de desencriptación 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" en adelante Certificado.

El Certificado puede distribuirse libremente para efectos de intercambio seguro de información y para ofrecer pruebas de autoría de archivos electrónicos o confirmación de estar de acuerdo con su contenido ambos mediante el proceso denominado "firmado electrónico avanzado ", 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),
- La autenticidad,
- Certidumbre de origen (facilidad para determinar qué persona es el autor de la firma que 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 los certificados de e.firma y al igual que las firmas electrónicas avanzadas el propósito del sello digital es emitir comprobantes fiscales 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 un certificado de e.firma, proporciona los mismos servicios de seguridad y hereda las características de las firmas digitales. Por consecuencia un comprobante fiscal digital firmado digitalmente por el contribuyente tiene las características señaladas previamente.

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

- SHA-2 256, que es una función hash de un solo sentido tal que para cualquier entrada produce una salida compleja de 256 bits (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.

A manera de referencia y para obtener información adicional, se recomienda consultar el sitio de Factura Electrónica 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

del comprobante fiscal digital por Internet que ampara retenciones e información de pagos, establecida en el Rubro II.A. de este anexo. Construida aplicando las siguientes reglas.

Reglas Generales:

1. Ninguno de los atributos que conforman al comprobante fiscal digital deberá contener el carácter | ("pleca") debido a que éste es 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 "pleca").
3. Se expresa únicamente la información del dato sin expresar el atributo al que hace referencia. Esto es, si el folio interno (FolioInt) del comprobante es "P29" solo se expresará |P29| y nunca |FolioInt P29|.
4. Cada dato individual se encontrará separado de su dato subsiguiente, en caso de existir, mediante un carácter | ("pleca" sencilla).
5. Los espacios en blanco que se presenten dentro de la cadena original son tratados de la siguiente manera:
 - a. Se debe reemplazar todos los tabuladores, retornos de carro y saltos de línea por el carácter espacio (ASCII 32).
 - b. Acto seguido se elimina cualquier espacio al principio y al final de cada separador | (pleca).
 - c. Finalmente, toda secuencia de caracteres en blanco se sustituyen por un único carácter espacio (ASCII 32).
6. Los datos opcionales no expresados, no aparecerán en la cadena original y no tienen delimitador alguno.
7. El final de la cadena original se expresa mediante una cadena de caracteres || (doble "pleca").
8. Toda la cadena de original se expresa en el formato de codificación UTF-8.
9. El nodo o nodos adicionales <Complemento> se integran al final de la cadena original respetando la secuencia de formación para cada complemento y número de orden del Complemento.
10. El nodo Timbre Fiscal Digital del SAT se integra posterior a la validación realizada por un proveedor autorizado por el SAT que forma parte de la Certificación Digital del SAT. Dicho nodo no se integrará a la formación de la cadena original del CFDI, las reglas de conformación de la cadena original del nodo se describen en el Rubro III.B. del presente anexo.

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 la sección de la Cadena Original.

- a. Información del Nodo Retenciones
 1. Version
 2. NoCertificado
 3. FolioInt
 4. FechaExp
 5. LugarExpRetenc
 6. CveRetenc
 7. DescRetenc
- b. Información del Nodo CfdiRetenRelacionados
 1. TipoRelacion
 2. UUID
- c. Información del Nodo Emisor
 1. RfcE
 2. NomDenRazSocE
 3. RegimenFiscalE
- d. Información del Nodo Receptor
 1. NacionalidadR
- e. Información del Nodo Nacional
 1. RfcR

- 2. NomDenRazSocR
- 3. CurpR
- 4. DomicilioFiscalR
- f. Información del Nodo Extranjero
 - 1. NumRegIdTribR
 - 2. NomDenRazSocR
- g. Información del Nodo Periodo
 - 1. MesIni
 - 2. MesFin
 - 3. Ejercicio
- h. Información del Nodo Totales
 - 1. MontoTotOperacion
 - 2. MontoTotGrav
 - 3. MontoTotExent
 - 4. MontoTotRet
 - 5. UtilidadBimestral
 - 6. ISRCorrespondiente
- i. Información del Nodo ImpRetenidos
 - 1. BaseRet
 - 2. ImpuestoRet
 - 3. MontoRet
- 4. TipoPagoRet

j. El nodo o nodos adicionales <Complemento> se integran al final de la cadena original respetando la secuencia de formación para cada complemento y número de orden del Complemento, de acuerdo con lo expresado en el Rubro III.C

El nodo Timbre Fiscal Digital del SAT se integra posterior a la validación realizada por un proveedor autorizado por el SAT que forma parte de la Certificación Digital del SAT. Dicho nodo no se integra a la formación de la cadena original del Comprobante Fiscal Digital a través de Internet que ampara retenciones e información de pagos, las reglas de conformación de la cadena original del nodo se describen en el Rubro III.B. del presente anexo.

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-2 256 a la cadena original a sellar incluyendo los nodos Complementarios. 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 es de 1 en 2^{256} , 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 debe reconocer como válido el mensaje.

a. SHA-2 256 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 encriptación 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 encriptación; 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 utiliza 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 33% en el tamaño de las cadenas imprimibles respecto de la original.

La **codificación en base 64**, así como su decodificación, se realiza 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 2048:

AM0PWKyhvpj1Pf7AJVzAAGjaYU0t6r5hjk0DOj+wISCSdA2LZj7jmnBKivivgU8J5svcto9kABfNm246HG2y8Q6YcQJmB6Dw2bUBoZfrPE54yP+S5MfPtCw5QhS948Pc91gJcLPrHmaRXINaEqq0mTGWr4aWSAZxcb9DqI9KnlcXt30KISnbc2+4m9RtpsTPLk2joKFGxf8eejGL69vO8txmLqioInFDhTPWQcIKMdUutUbREsSsQ SfmOuoQdVBCCMY7SUK2ZtGDaCnshQSOVz/GHGfLQT4Qj0hetPtaDi60YPM5Mf3cekonBHb4jc2+FuCJW+JKCsnl7sJ4+iYg=

