¿Qué es la Firma Electrónica? ¿Por qué el Tamaño de la Clave si Importa?

La firma electrónica usa criptografía asimétrica y debe tener claves privadas de al menos 2048 bits. Aprende cómo funciona, su importancia en el SII y por qué evitar certificados con claves inseguras.

LibreDTE · 21/07/2019 · #ayuda-normativa-y-consejos

¿Qué es la Firma Electrónica? ¿Por qué el Tamaño de la Clave si Importa?

La firma electrónica que usamos para los procesos con SII en Chile utiliza criptografía asimétrica usando certificados digitales. Este tipo de criptografía usa dos partes:

- Una clave pública.
- Una clave privada.

Esta firma electrónica también se conoce como certificado digital y puede ser simple o avanzada. La principal diferencia es que la simple es solo un archivo que contiene tanto la clave pública como la privada, mientras la firma avanzada hace uso de un token (dispositivo USB). Para los procesos con SII es suficiente una firma electrónica simple.

Usamos esta criptografía para asegurar que un Documento Tributario Electrónico (ejemplo: factura) ha sido realmente emitido por un usuario autorizado. La forma de operar es la siguiente:

1. David emite una factura electrónica.
2. David firma la factura con la clave privada de su firma electrónica (*aka*: certificado digital).
3. David envía la factura al destinatario, en este caso es Ana.
4. Ana valida con la clave pública de David que la factura haya sido realmente emitida por él.
5. Ana puede procesar la factura con confianza porque sabe que efectivamente David la emitió.

Estos pasos solo garantizan que David emitió realmente la factura, pero ¿cómo sabemos que David está autorizado para emitir la factura en nombre de la empresa “Mi Súper Empresa SpA”?. Esa parte la garantiza el SII:

1. David emite una factura electrónica.
2. David firma la factura con la clave privada de su firma electrónica (*aka*: certificado digital).
3. David envía la factura al SII.
4. El SII valida con la clave pública de David que la factura haya sido realmente emitida por él.
5. El SII valida que el usuario David tenga permisos para emitir/firmar documentos a nombre de “Mi Súper Empresa SpA”.
6. El SII publica para todo el mundo el estado del DTE enviado y que está aceptado por ellos (por lo tanto David si puede emitir documentos a nombre de “Mi Súper Empresa SpA”).

Es importante que al recibir un documento se validen ambas cosas:

- Que la firma del XML que recibimos sea válida.
- Que el documento esté aceptado en SII.

Es la única forma de asegurarnos que el DTE está válidamente emitido.

Pero… yo tengo solo un archivo de firma

Si, la firma electrónica, y en general el certificado digital, puede estar contenido en un único archivo. En este archivo se unen tanto la clave pública, la clave privada y otros datos asociados a la firma.

Este archivo normalmente está protegido con una contraseña para poder ser usado (“la contraseña de la firma”).

La contraseña de la firma es diferente a la clave privada de la firma electrónica. Cuando hablamos de clave pública y privada nos referimos a los datos que permiten operar con criptografía asimétrica. La contraseña de la firma se usa para abrir la firma solamente, pero no para firmar.

Exportar firma

Al exportar la firma electrónica que tenemos en el navegador, se nos puede preguntar:

- ¿Quiere exportar la clave privada de la firma?
- ¿Quiere exportar los datos extendidos de la firma?

Es muy importante exportar siempre ambos puntos, ya que de no hacerlo, la firma no estará completa.

¡El tamaño de la clave privada si importa!

Ahora lo importante, y motivo original de este artículo, el tamaño de la clave privada.

En criptografía el tamaño siempre importa, entre más grande el tamaño de la clave, más segura será. Esto tiene que ver con la cantidad de combinaciones posibles que existen para una clave dependiendo del tamaño.

Por ejemplo, una clave que son solo números del 0 al 9 y tiene tamaño de 4 números (típica del cajero bancario) tendrá como máximo 10.000 combinaciones (del 0000 al 9999). O sea bastaría probar 10.000 combinaciones y podemos adivinar la contraseña. ¿Fácil? para un computador si, muy fácil.

Las claves privadas tienen muchas más posibilidades. En las claves privadas el tamaño se mide en bits, donde 1 bit solo tiene 2 posibles valores: 0 o 1.

- **Tamaño 512 bits:** combinaciones 2^512 = 1,340780792994260 x 10^154
- **Tamaño 1024 bits:** combinaciones 2^1024 = 1,797693134862316 x 10^308
- **Tamaño 2048 bits:** combinaciones 2^2048 = 3,231700607131101 x 10^616
- **Tamaño 4096 bits:** combinaciones 2^4096 = 1,044388881413153 x 10^1233

Si aún no lo has notado, esos son muchos ceros que si importan. Muchas posibilidades.

Nota: debido a los diferentes algoritmos usados en encriptación, el tamaño de una clave asimétrica no es igualmente difícil de calcular al de una simétrica (en una clave simétrica ambos lados usan la misma clave). Por esto, las claves asimétricas deben ser mayores en tamaño a las simétricas. De esta forma una clave simétrica de 512 bits podría ser buena, pero asímetrica del mismo tamaño pésima.

Ok... ¿y por qué debería importarme esto del tamaño?

Ahora lo interesante. A **inicios de siglo las claves privadas de 1024 bits** eran consideradas las de tamaño mínimo para proveedor seguridad. Sin embargo **¡eso era hace casi 20 años!** Hoy la recomendación es usar **mínimo claves privadas de tamaño 2048 bits** .

Considerando lo anterior y saltándome muchas explicaciones de por qué no usar claves de 1024 bits hoy, es que ya no se recomienda usar claves de menor tamaño a 2048 bits. Insistimos, no usar claves de menor tamaño a 2048 bits.

Lamentablemente, hay proveedores en Chile de firma electrónica (ejemplo: E-CERTCHILE) que aún proveen firmas electrónicas con claves privadas de tamaño menor a 2048 bits. Esto se verificó con una firma comprada el 6 de junio de 2019, hasta ese momento, aún entregaban firmas con tamaño de clave no recomendado.

OpenSSL, que es el estándar para trabajar con certificados digitales, en su versión 1.1.1c está rechazando el uso de certificados con claves privadas de tamaño menor a 2048 bits con el siguiente mensaje:

```
could not load PEM client certificate, OpenSSL
error error:140AB18F:SSL routines:SSL_CTX_use_certificate:ee key too small, (no key
found, wrong pass phrase,
or wrong file format?)
```

¿Nuestra recomendación? compra tu firma electrónica solo en empresas que entreguen claves de tamaño mínimo 2048 bits.

Last updated on 25/08/2026