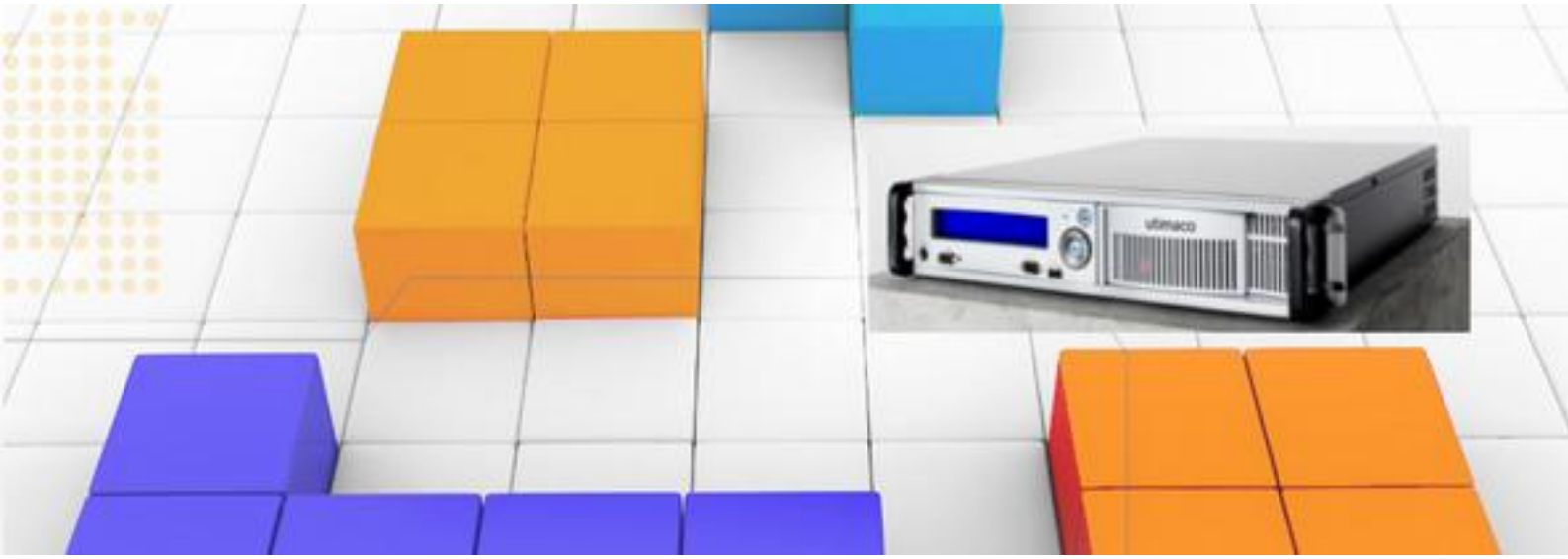
esfirma
Autoridad de certificación



[Firma con PIN]

esFIRMA

Información de seguridad

esfirma
Autoridad de certificación

esfirma
Autoridad de certificación

Índice de contenido

Control de cambios

Fecha	Responsable	Resumen de cambios
Mayo 2017	esFIRMA Team	Primera versión

esfirma
Autoridad de certificación

Introducción

El sistema [Firma con PIN] permite generar o importar y custodiar certificados de firma para los usuarios de la plataforma de administración electrónica. [Firma con PIN] permite a los usuarios realizar operaciones de firma electrónica introduciendo un clave personal de acceso una vez que han sido autenticados mediante usuario y contraseña y/o una contraseña de un sólo uso y/o certificado cliente y/o DNIe o equivalente. El nivel de autenticación requerido dependerá del nivel de la operación que el usuario desea realizar.

La clave personal del usuario protege su clave privada de firma y sólo es accesible en el interior del módulo criptográfico seguro y desde los dispositivos autorizados. En ningún momento la clave personal del usuario es accesible por nadie más que el propio usuario. De esta manera el usuario tiene un control exclusivo sobre su clave privada. La clave pública del sistema [Firma con PIN] permite cifrar la información que el usuario envía al módulo de seguridad y está disponible en este documento. La clave pública fue creada con las más altas medidas de seguridad.

Módulo de seguridad

El módulo de seguridad es un multichip criptográfico embebido que cumple con FIPS 140-2 nivel 3. El propósito principal de este módulo es proporcionar servicios criptográficos seguros como el cifrado o descifrado, huellas, la firma y la verificación de datos, generación de números aleatorios, generación de claves seguras, almacenamiento de claves a bordo y otras funciones de gestión de claves en un entorno de manipulación protegida. La comunicación hacia y desde el módulo se produce mediante mensajes cifrados y autenticados.

El módulo está encerrado en una caja de metal duro opaca que contiene mecanismos detectores de manipulación indebida. Todos los componentes de hardware criptográfico (incluyendo la unidad central de procesamiento, todos los chips de memoria, reloj de tiempo real y generador de ruido de hardware para la generación de números aleatorios) se encuentran en una placa de circuito impreso y encapsulado por capas de metal, una protección de detección de manipulación indebida.

El módulo criptográfico ha sido inicializado con unas altas medidas de seguridad.

Usos del certificado

El certificado emitido tendrá como finalidad permitir a un usuario de la plataforma de administración electrónica firmar documentos. Este certificado podrá sustituir la firma manuscrita por la electrónica en las relaciones del usuario con terceros en los casos que la AC emisora así lo proporcione.

Los certificados emitidos por [Firma con PIN] solamente podrán emplearse para firmar electrónicamente (no repudio y compromiso con lo firmado). El perfil de los certificados no contempla el uso de dichos certificados y sus claves asociadas para cifrar ningún tipo de información.

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, esta deberá ser complementada con la información del estado del certificado asociado en el momento en que la

misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Para que la firma pueda ser validada a largo plazo, la firma electrónica que se genera ha de incluir evidencias para que no pueda ser repudiada.

Para ello la plataforma de administración de electrónica proporciona un servicio que mantiene dichas evidencias actualizadas las claves y el materiales criptográficos asociados antes de que sean vulnerables.

Publicación de ese documento

Este documento se ubicará en:

WEB: https://esfirma.com/doc-pki/CSIGN-InfoSeg.pdf

y será actualizado en el momento en que se apruebe cualquier modificación del mismo.

esfirma
Autoridad de certificación

Clave pública de [Firma con PIN]

CLAVE PUBLICA DEL MODULO DE FIRMA CON PIN

```
Public-Key: (2048 bit)

Modulus:
    00:a1:f0:a2:55:5b:ed:bf:a2:92:2b:c1:85:9d:ed:
    56:43:0a:36:1e:32:b9:d7:96:6e:74:3c:b1:c9:5d:
    55:ee:a7:24:4f:2f:3c:76:18:11:4a:c5:02:e6:74:
    40:94:9f:9e:8f:46:e2:d1:eb:c1:a9:25:9e:89:06:
    cf:c3:c8:47:44:6a:f2:94:af:0e:7a:84:46:ba:8c:
    44:d0:c5:c4:d3:ab:1b:ca:0c:73:04:31:38:8f:ce:
    be:15:8f:f9:e3:3e:5b:1f:70:e7:e5:b1:79:de:f1:
    66:dd:32:73:3a:4f:83:a4:f6:7f:4f:00:4c:b4:ad:
    6d:22:87:f1:f3:89:db:9f:26:37:72:68:66:1a:ec:
    27:5f:11:a8:1a:93:46:3f:bb:ba:2d:3b:5e:ed:e2:
    89:73:4e:89:32:58:ac:81:7d:2b:bd:26:76:b9:39:
    07:1a:3f:7f:1a:b1:69:0f:c1:43:aa:11:ca:e1:73:
    70:1c:7f:2d:2f:65:29:95:75:3f:85:b3:9b:6a:9a:
    05:98:d4:8d:ca:e3:eb:05:8d:fc:0d:19:c4:83:1f:
    81:4f:b2:a4:84:0e:dd:e2:c4:ef:ab:4d:20:d5:30:
    4f:d3:2e:17:b0:e2:ec:d8:2a:72:87:42:75:72:ad:
    02:88:26:6d:d8:eb:30:8d:ab:0c:ec:92:1e:17:5c:
    d2:31

Exponent: 65537 (0x10001)
```

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAofCiVVvtv6KSK8GFne1W
Qwo2HjK515ZudDyxyV1V7qckTy88dhgRSsUC5nRAlJ+ej0bi0evBqSWeiQbPw8hH
RGrylK8OeoRGuoxE0MXE06sbygxzBDE4j86+FY/54z5bH3Dn5bF53vFm3TJzOk+D
pPZ/TwBMtK1tIofx84nbnyY3cmhmGuwnXxGoGpNGP7u6LTte7eKJc06JMlisgX0r
vSZ2uTkHGj9/GrFpD8FDqhHK4XNwHH8tL2UplXU/hbObapoFmNSNyuPrBY38DRnE
gx+BT7KkhA7d4sTvq00g1TBP0y4XsOLs2Cpyh0J1cq0CiCZt2OswjasM7JIeF1zS
MQIDAQAB
-----END PUBLIC KEY-----

SHA-256:
    00:6f:c5:e3:8f:
    e6:1b:1d:e2:27:
    f9:fb:27:3e:ce:
    c7:9d:b5:a3:50:
    37:20:1a:4f:fc:
    ea:0f:c2:3f:96:
    5e:fc

SHA-512:
    08:cc:61:e6:27:
    a0:0f:35:40:f3:
    f4:f2:be:a2:5b:
    7c:bf:38:1f:cd:
    70:44:de:3d:79:
    cd:98:ee:17:80:
    72:2d:fe:ad:37:
    cb:bc:1b:e5:ca:
    86:40:da:6c:4c:
    d3:4a:d3:57:8a:
    31:96:e4:22:6c:
    3a:30:47:06:4f:
    d4:f6:d2:89
```