centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1514

Procedimiento de Empleo Seguro
Tarjeta Criptográfica TC-FNMT 5.6

Mayo 2025

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-204-4
Fecha de Edición: Mayo de 2025

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2026.01.16 07:57:43 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1 INTRODUCCIÓN

1. La TC-FNMT es una tarjeta criptográfica con la capacidad de realizar firmas electrónicas cualificadas. Está compuesta de: un chip previamente certificado (que proporciona la librería criptográfica y el *firmware* que incluye el mecanismo de carga para la actualización del código[1]), del sistema operativo (versión 5.70) y de las librerías biométricas[2].

2. Esta tarjeta implementa un sistema de ficheros que incluye la aplicación de firma electrónica (*eSign*) según se define en [TR03110-2], tiene como objetivo generar firmas electrónicas cualificadas. La principal propiedad específica que distingue a las firmas electrónicas cualificadas de otras firmas electrónicas avanzadas es que se basan en certificados cualificados y se crean mediante dispositivos cualificados de creación de firmas (DCCF). Para la aplicación de firma electrónica, el titular de la tarjeta TC-FNMT puede controlar el acceso a la funcionalidad de firma presentando conscientemente su tarjeta TC-FNMT e introduciendo su código PIN para esta aplicación.

3. La TC-FNMT está certificada según los Criterios Comunes (*Common Criteria*) conforme a los siguientes perfiles de protección:

   a) Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation, prEN 14169-2:2012 ver. 2.0.1, 2012-01, BSI-CC-PP-0059-2009-MA-01, [SSCDPP].

   b) Protection Profiles for Secure Signature Creation Device – Part 3: Device with key import, prEN 14169-3:2012 ver. 1.0.2, 2012-07-24, BSI-CC-PP-0075, [SSCDPP3].

   c) Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application. Version: 1.0.1. 2013-11-27, BSI-CC-PP-0071. [SSCDPP4].

   d) Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application. Version: 1.0.1. 2012-11-14, BSI-CC-PP-0072. [SSCDPP5].

   e) Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application. Version: 1.0.4. 2013-04-03, BSI-CC-PP-0076. [SSCDPP6].

4. Además del cumplimiento de los requisitos en la funcionalidad de firma electrónica, la TC-FNMT v5.6 también cumple con los requisitos del Reglamento (UE) nº 910/2014 (eIDAS) en materia de identificación electrónica, requisitos derivados de la Decisión de Ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016 por la que se fijan las normas para la evaluación de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2 del Reglamento eIDAS.

[1] Dependiendo de la configuración de la TC-FNMT seleccionada.
[2] Dependiendo de la configuración de la TC-FNMT seleccionada.

2 OBJETO Y ALCANCE

5. Esta guía aplica para la tarjeta criptográfica TC-FNMT versión 5.6 (nombre comercial) con sistema operativo 5.70 (versión S.O. certificado) en cualquiera de sus diferentes configuraciones:

   a) A01 – Con biometría de Sagem.

   b) B01 – Con biometría de Siemens.

   c) C01 - actualizable y con biometría de Sagem.

   d) D01 - actualizable y con biometría de Siemens.

   e) E01 - sin biometría.

   f) F01 - actualizable sin biometría.

6. El producto TC-FNMT 5.6 ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en la familia “Herramientas para firma electrónica”.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la expedición del producto.

b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de expedición del producto.

c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de instalación del producto, para lograr una configuración segura.

d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA EXPEDICIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. En caso de que la tarjeta TC-FNMT haya sido adquirida a través de la página web de la tienda de la FNMT-RCM (https://tienda.fnmt.es), el usuario recibirá en la dirección postal indicada en su pedido, una carta serigrafiada de la FNMT con la tarjeta criptográfica TC-FNMT preparada para realizar la carga del certificado electrónico correspondiente.

8. Para verificar de forma sencilla que la tarjeta recibida se corresponde con la versión certificada (tarjeta criptográfica TC-FNMT 5.6 con versión de sistema operativo 5.70), se recomienda leer la tarjeta empleando para ello la aplicación software "*Utilidad para Gestión de Certificados en Tarjeta Criptográfica CERES*" desarrollada por la propia FNMT-RCM y que está disponible en la siguiente dirección web (https://www.sede.fnmt.gob.es/descargas/descarga-software).

9. Esta aplicación lee internamente la información relativa a la versión de la tarjeta criptográfica y muestra por pantalla la versión del sistema operativo que tiene cargado la tarjeta (en este caso el 5.70 que es el correspondiente a la versión comercial certificada TC-FNMT 5.6).

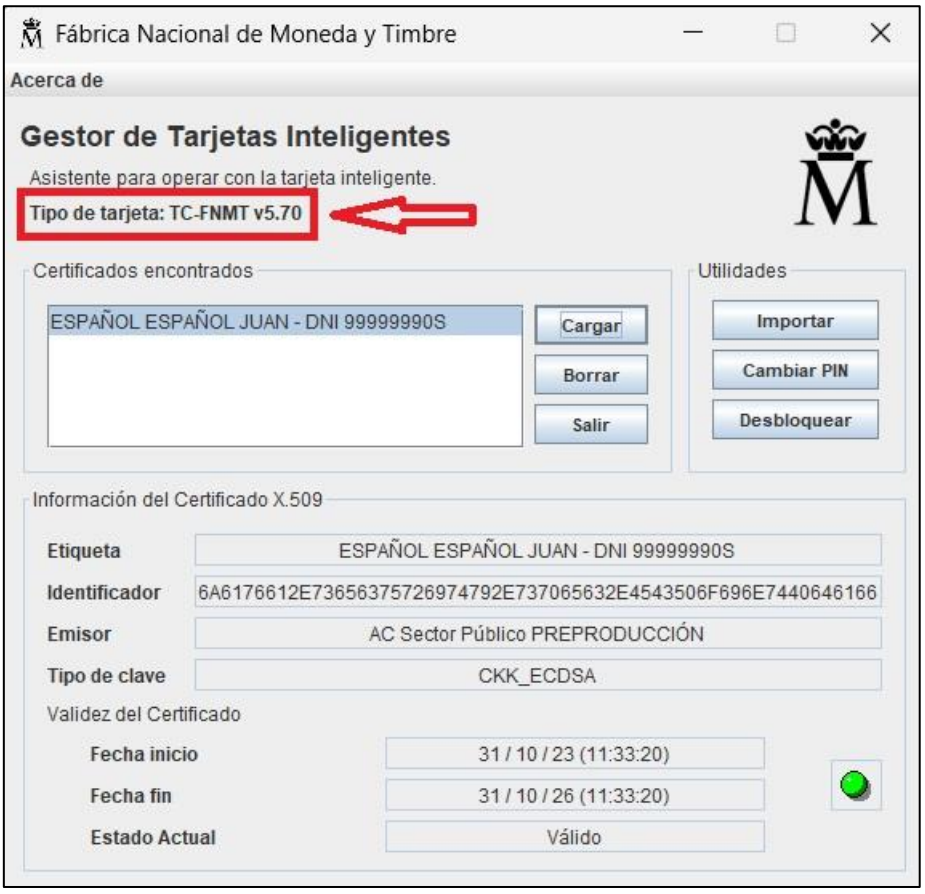

Ilustración 1. Comprobación de versión

10. En caso de que la tarjeta TC-FNMT forme parte de un lote de tarjetas adquirido para su uso en un colectivo (organismo, empresa, etc.), la persona responsable de recepcionar el lote de tarjetas TC-FNMT deberá seguir el siguiente procedimiento:

    a) Recibir copia impresa de la Guía Preparativa de la TC-FNMT [GP].

    b) Descifrar los documentos y scripts que se referencian en el Anexo correspondiente de la [GP] y comprobar el *hash* de cada uno de ellos.

    c) Al recibir el albarán, el cliente comprueba que se corresponde con el lote correcto.

    d) Verificar que el lote está compuesto por el número de cajas esperado y que el plástico que lo forma no ha sido manipulado.

    e) Desembalar el lote de cajas y analizar que ninguna de las cajas que lo conforman se encuentra abierta.

    f) Para cada una de las cajas que forman parte del lote, comprobar que el número de tarjetas que contiene es el adecuado. Confirmar que el número total de tarjetas corresponde con el indicado en el albarán de entrega.

    g) Por último, abrir una o varias de las cajas que componen el lote y extraer alguna/s de las tarjetas. Verificar que el producto se corresponde con la versión esperada del producto (TC-FNMT 5.6 con sistema operativo 5.70). Para ello es necesario analizar el ATR de las tarjetas.

    h) Adicionalmente, se recomienda comprobar el contenido del fichero de versiones para verificar que la configuración de la tarjeta es la deseada (A01, B01, C01, D01, E01 ó F01).

    i) Restablecer los embalajes originales.

4.2 ENTORNO DE EXPEDICIÓN SEGURO

11. En el caso de que el organismo, empresa, etc. haya comprado un lote de tarjetas que desee personalizar de forma individual, deberá disponer de un sistema de expedición cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa para esta tarea.

4.3 CONSIDERACIONES PREVIAS

12. La funcionalidad fundamental la tarjeta criptográfica TC-FNMT es la realización de firmas electrónicas cualificadas. Para que la tarjeta mantenga su certificación de seguridad Common Criteria como dispositivo cualificado de creación de firma (DCCF) se debe cumplir, entre otros requisitos, que la generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante solo puedan correr a cargo de un prestador cualificado de servicios de confianza.

13. Por este motivo, los certificados electrónicos de firma electrónica que se almacenen en la tarjeta TC-FNMT deben ser certificados electrónicos cualificados expedidos por un prestador cualificado de servicios de confianza, en este caso, la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda.

14. Para mayor información, se recomienda la consulta de la “Declaración general de prácticas de servicios de confianza y de certificación electrónica” [DPC] de la Fábrica

Nacional de Moneda y Timbre – Real Casa de la Moneda disponible en su sede electrónica: (https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion).

15. La dirección de contacto de la FNMT-RCM como Prestador de Servicios de Confianza es la siguiente:

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda
Dirección de Sistemas de Información - Departamento CERES
C/ Jorge Juan, 106 28009 – MADRID
E-mail: ceres@fnmt.es Teléfono: +34 91 740 69 82

16. Por otra parte, también es importante tener en cuenta una serie de recomendaciones relativas a la obtención, uso y custodia de los certificados que se recogen en https://www.sede.fnmt.gob.es/preguntas-frecuentes/problemas-y-dudas/-/asset_publisher/fVZppcBHj0oa/content/1714-recomendaciones-sobre-la-custodia-de-los-certificados y entre las que se destaca que **los certificados electrónicos** (**y**, por tanto, **la tarjeta criptográfica TC-FNMT** que los contiene) **son personales e intransferibles**.

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

17. Para poder operar con la tarjeta TC-FNMT únicamente es necesario disponer de un lector de tarjetas inteligentes compatible conectado al ordenador personal correspondiente.

18. Se puede encontrar un listado de lectores de tarjetas evaluados y compatibles en el siguiente enlace: https://www.cert.fnmt.es/catalogo-de-servicios/tarjetas-criptograficas/lectores-de-tarjetas

19. Los terminales correspondientes y su entorno deben garantizar la confidencialidad e integridad de los datos respectivos que manejan (por ejemplo, confidencialidad de las contraseñas, integridad de los certificados, etc.) para un funcionamiento seguro de la TC-FNMT.

5 FASE DE EXPEDICIÓN

20. En este apartado se hace referencia a la operativa que debe llevar a cabo aquel organismo, empresa, etc. (en adelante cliente) que ha adquirido un lote de tarjetas TC-FNMT para sus empleados/usuarios y desea personalizarlas.

21. Las operaciones a realizar en esta fase se realizan mediante el sistema de expedición del cliente que actúa de Agente Personalizador.

22. La FNMT proporciona guías para el entorno de expedición del cliente como la Guía Preparativa de la Tarjeta TC-FNMT [GP]. Las recomendaciones indicadas para la operación de la tarjeta TC-FNMT en el entorno de expedición han de seguirse estrictamente, de lo contrario, la FNMT no garantiza el cumplimiento de los requisitos de seguridad y la correspondiente declaración de seguridad.

23. Del mismo modo, también se facilita una estructura de ficheros con las recomendaciones proporcionadas al cliente sobre qué ficheros y condiciones de acceso se deben generar en su sistema de expedición.

24. Hay que subrayar que para que los mecanismos de acceso a la tarjeta se mantengan con la fortaleza adecuada a los perfiles de protección, es decir, fortaleza alta, los valores de los ficheros de claves han de ser modificados de modo que éstos sean aleatorios, es decir, no deterministas, ni predecibles, ni deducibles y además han de tener una longitud igual o superior a doce bytes.

25. Los posibles errores o excepciones que se pudieran producir a la hora de interactuar con la tarjeta en el proceso de expedición de la misma se encuentran descritos en el Manual de Comandos de la Tarjeta TC-FNMT [CMD].

26. El cliente es responsable de disponer de un sistema de expedición que cumpla con el procedimiento se encuentra descrito e implementado en los scripts de expedición entregados junto con la Declaración de Seguridad de la Tarjeta TC-FNMT [STTCFNMT].

27. El cliente puede consultar dichos scripts mediante un editor de texto para generar su propia implementación. Los scripts entregados solo se pueden ejecutar con una herramienta propietaria de la FNMT. Esta herramienta no forma parte de la evaluación de seguridad de la tarjeta y no se entrega al cliente, si el cliente desea disponer de dicha herramienta debe ponerse en contacto con la FNMT.

28. Los ficheros opcionales dentro del Master File EF.XXXX definidos en la [GP] son ficheros opcionales que el cliente puede utilizar para uso propietario de la organización. Estos ficheros opcionales deben usar las mismas reglas de nomenclatura para el identificador que el resto de ficheros [CMD].

29. El cliente puede crear múltiples ficheros opcionales y puede almacenar cualquier tipo de datos que crea necesarios. El límite de ficheros opcionales adicionales posibles viene dado por la propia memoria del chip. Como recomendación, en la [GP] se definen dos archivos con distintos tamaños de datos, aunque no esté limitado a dos. Además, se recomienda que se usen los mismos permisos de seguridad que los que aparecen definidos en el mapa de memoria de la [GP].

30. El cliente debe asegurarse de que los Agentes de Personalización que actúan en su nombre:

a) establezcan la identidad correcta del titular de la tarjeta TC-FNMT y creen los datos biográficos para la tarjeta TC-FNMT,

b) registren los datos de referencia biométrica[3] del titular de la tarjeta TC-FNMT,

c) escriban un subconjunto de estos datos en el documento físico (personalización óptica) y los almacenen en la tarjeta TC-FNMT (personalización electrónica) para el titular de la tarjeta TC-FNMT como se define en [ICAO],

d) escribir los datos de los detalles del documento,

e) escribir los datos de la funcionalidad de seguridad iniciales,

f) firmar el Objeto de Seguridad del Documento definido en [ICAO].

31. El cliente debe asegurarse que únicamente se llevan a cabo las acciones necesarias para la consecución del mapa de ficheros correspondiente a la TC-FNMT expedida (definido en el Anexo VII de la [GP]) y que en ningún caso:

a) se crean o escriben ficheros con nuevos identificadores de la TC-FNMT,

b) se replican ficheros que ya estén definidos,

c) se crean ficheros fuera del Master File (MF),

d) se crean ficheros libres en escritura,

e) se dejan de cumplir las condiciones de acceso establecidas.

NOTA: En caso de que la TC-FNMT sea adquirida por parte del usuario final a través de la tienda en línea de la FNMT, el proceso de expedición lo realiza la propia FNMT dentro de sus instalaciones.

[3] Si la configuración elegida de la TC-FNMT emplea biometría.

6 FASE DE INSTALACIÓN

32. La FNMT-RCM ha desarrollado un programa "Instalable" que integra todos los elementos necesarios para el funcionamiento de los certificados electrónicos del usuario en la tarjeta TC-FNMT.

33. Los elementos que se instalan son:

    a) Software adicional para certificados de usuario en tarjeta criptográfica. (Requiere Java v.8 Update 45 hasta Java 15)

    b) Módulo PKCS#11, para trabajar en Mozilla.

    c) Módulo Smart Card Minidriver para Windows.

34. Pulse en el enlace correspondiente dependiendo de si su sistema operativo es de 32 o de 64 bits:

    a) Para sistemas de 32 bits:

    https://www.sede.fnmt.gob.es/documents/10445900/10900326/Instalador_Tarjetas_TC-FNMT_DNIe_x86.exe

    b) Para sistemas de 64 bits:

    https://www.sede.fnmt.gob.es/documents/10445900/10900326/Instalador_Tarjetas_TC-FNMT_DNIe_x64.exe

35. Para su correcto funcionamiento descargue el ejecutable en su ordenador, cierre los navegadores, haga clic sobre el mismo con permisos de administrador e instale el programa.

7 FASE DE USUARIO

7.1 MODO DE OPERACIÓN SEGURO

36. Para tener acceso a las funcionalidades de la tarjeta, ésta se ha de introducir (si se desea emplear el interfaz con contactos) o aproximar (si se desea emplear el interfaz sin contactos) en/a un lector de tarjetas conectado a la máquina correspondiente.

37. Una vez que la tarjeta se encuentra dentro del lector, es posible realizar las siguientes operaciones:

    a) Importación y eliminación de certificados

    b) Cambio de PIN

    c) Desbloqueo de PIN

    d) Firma electrónica

38. Debido a la criticidad de las operaciones, éstas se han de realizar siempre en condiciones de máxima confidencialidad y seguridad exigiéndose, por tanto, el establecimiento de un canal seguro.

39. Para facilitar la realización de estas operaciones y, con objeto de que la gestión de los canales seguros y el envío de los comandos a la tarjeta sea transparente al usuario, la FNMT ha desarrollado la aplicación software "Utilidad para Gestión de Certificados en Tarjeta Criptográfica CERES" disponible en la siguiente dirección web: https://www.sede.fnmt.gob.es/descargas/descarga-software.

40. Dicha aplicación permite al usuario utilizar su tarjeta TC-FNMT de forma sencilla.

41. Para la realización de las firmas electrónicas, se puede emplear el programa AutoFirma desarrollado por el Ministerio de Hacienda y Administraciones Públicas.

42. Autofirma es una herramienta de escritorio con interfaz gráfica que permite la ejecución de operaciones de firma de ficheros locales en entornos de escritorio (Windows, Linux y Mac OS X). Ofrece la posibilidad de realizar firmas de en cualquier tipo de documento de forma sencilla y se puede descargar desde https://firmaelectronica.gob.es/Home/Descargas.htm

43. El dispositivo externo donde se autentique el usuario debe garantizar la confidencialidad y la integridad de los datos de verificación de autenticación (PIN, Huella dactilar[4]) según lo necesite el método de autenticación empleado, esto incluye la exportación a la TC-FNMT por medio de un canal confiable. En concreto, se debe emplear un canal confiable para importar los datos de verificación de autenticación (PIN, Huella dactilar) si la TC-FNMT lo requiere.

44. El usuario empleando la aplicación de creación de firma confiable, la cual genera el "hash" que representa los datos a ser firmados que pretenden ser firmados por el usuario en una forma apropiada para la firma por la TC-FNMT, envía el "hash" a la TC-FNMT habilitando la verificación de la integridad del "hash" por la TC-FNMT. La firma producida por la TC-FNMT se adjunta a los datos a ser firmados o se proporciona de manera separada.

[4] En las configuraciones con biometría.

Nota: La aplicación de creación de firma debería poder admitir firmas electrónicas avanzadas. Actualmente, existen tres formatos definidos por ETSI reconocidos por cumplir con los requisitos necesarios para la firma electrónica avanzada: CAdES, XAdES y PAdES. Estos tres formatos obligan a incluir el "hash" del certificado de clave pública del firmante en los datos a firmar. Para respaldar la movilidad del firmante, se recomienda almacenar la información del certificado en la TC-FNMT para que lo utilice aplicación de creación de firma y la identificación de la clave secreta correspondiente si se almacenase más de una en la TC-FNMT.

45. El entorno operacional debe asegurar que el "hash" no puede ser alterado en el tránsito entre la aplicación de creación de firma y la TC-FNMT. En concreto, la aplicación de creación de firma debe emplear un canal confiable con la TC-FNMT para garantizar que el "hash" no se puede alterar sin ser detectado en el tránsito entre la aplicación de creación de firma y la TC-FNMT.

46. El usuario debe comprobar que las claves privadas almacenadas en la TC-FNMT recibida del proveedor de servicios se encuentran en estado no operacional o, en su defecto, que la transición de la TC-FNMT desde el estado no operacional a estado operacional se realice en su presencia. El usuario debe mantener la confidencialidad de su PIN.

47. La longitud del PIN debe ser de, al menos, 12 bytes.

48. El titular del documento puede revelar, si es necesario, sus valores de verificación de la contraseña PACE a una persona o dispositivo autorizado que indudablemente actúe conforme a las regulaciones respectivas y sea confiable. Se recomienda que en caso de tener que desvelar la contraseña PACE, se indique el número CAN impreso en la superficie de la TC-FNMT y que es visible con la simple exhibición del documento.

7.2 AUTENTICACIÓN

7.2.1 ESTABLECIMIENTO DEL CANAL SEGURO (CON O SIN CONTACTOS)

49. Para el establecimiento del canal seguro, en primer lugar, se realiza un intercambio de las claves públicas de la tarjeta y el terminal mediante certificados que serán verificados por ambas partes.

50. A continuación, se realiza un protocolo de autenticación mutua, con intercambio de semillas para la derivación de una semilla común que dé lugar a las claves de sesión de cifrado y autenticado.

51. Una vez concluido el protocolo para el establecimiento de la semilla común todos los mensajes deben transmitirse securizados.

52. Si se rompe el canal seguro establecido debido a que se haya recibido un comando APDU que no respete el formato de mensaje securizado o a que la información de autenticación o MAC sea errónea, el canal queda deshabilitado y el estado de seguridad de la tarjeta es reseteado (se borran las claves de sesión y los secretos presentados quedan invalidados).

53. El canal seguro se puede establecer empleando tanto el interfaz con contactos como el sin contactos.

54. Este procedimiento permite que cada una de las partes (tarjeta y aplicación externa) confíe en la otra, mediante la presentación mutua de certificados, y su verificación. En el proceso, también se incluye el intercambio seguro de unas claves de sesión, que deberán

ser utilizadas para securizar (encriptar) todos los mensajes intercambiados posteriormente.

7.2.1.1 AUTENTICACIÓN CON INTERCAMBIO DE CLAVES

55. Este procedimiento corresponde con el apartado 3.9 del documento [EN419212-3], en el que se utilizan claves RSA de 3072 a 3840 bits, y SHA-256 en la validación de certificados y en los comandos de autenticación.

7.2.1.2 AUTENTICACIÓN DE DISPOSITIVO CON PROTECCIÓN DE PRIVACIDAD

56. Este procedimiento corresponde con el apartado 3.6 del documento [EN419212-3], en el que se utilizan claves EC de 256 a 521 bits, y SHA-256 en la validación de certificados y en los comandos de autenticación.

7.2.1.3 PROTOCOLO EAC

57. Este procedimiento corresponde con el apartado 3.7 del documento [EN419212-3] y con las especificaciones [TR03110-2], en el que se utilizan claves EC de 256 a 521 bits, y SHA-256 en la validación de certificados y en los comandos de autenticación.
58. La aplicación de firma electrónica soporta EAC2, es decir, Chip Authentication versión 2 y Terminal Authentication versión 2.

7.2.1.4 PROTOCOLO PACE

59. Es un protocolo Diffie-Hellman key agreement que se basa en una contraseña (CAN, PIN o PUK) definido en [TR03110-2]. Se debe establecer antes de cualquier otro canal para acceder a la aplicación de firma de la TC-FNMT. También es utilizado como canal seguro en la verificación del PIN en la aplicación de firma electrónica.
60. La TC-FNMT soporta la versión 2 de PACE según [TR03110-1], con el algoritmo ECDH AES 192 con curvas de 256 bits, 384 bits, 512 bits y 521 bits.
61. Esta alternativa se basa en la capacidad de la tarjeta para verificar certificados firmados por una autoridad certificadora raíz, posiblemente a través de autoridades certificadoras intermedias, y en la comprobación mediante protocolos de desafío-respuesta de que la otra parte dispone de la clave privada asociada al certificado.
62. Cuando se completa con éxito el establecimiento de un canal seguro, se adquiere un nuevo estado de seguridad en el diálogo con la tarjeta, que, en función del certificado utilizado por el terminal, podrá ser:

    a) Canal Seguro Administrativo. Corresponde a la condición de acceso “PRO”, y por lo tanto se podrá acceder a los recursos que requieran esta condición. Solamente se puede establecer con los canales Autenticación con intercambio de claves o Autenticación de dispositivo con protección de privacidad definidos en [EN419212-3].

    b) Canal Seguro de Usuario. Se corresponde con el canal EAC2 definido en [TR03110-2].

c) Canal Seguro de PIN. Se emplea para la presentación de los códigos PIN. Necesario como paso previo a la realización de la operación de firma. Se corresponde con el canal PACE definido en [TR03110-2].

7.2.2 SECURIZACIÓN DE MENSAJES

63. La TC-FNMT puede, previo establecimiento de un canal seguro, securizar los mensajes transmitidos. Para el establecimiento es necesaria la autenticación previa del terminal y la tarjeta, mediante el uso de certificados electrónicos.

64. Cuando el canal está establecido, los mensajes intercambiados entre la tarjeta y terminal se cifran y autentican, de tal forma que se asegura una comunicación una-a-uno entre los dos puntos originarios de canal. El canal seguro puede ser requerido por la aplicación o puede ser una restricción de acceso impuesta a algún recurso de la tarjeta.

7.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN

65. La tarjeta TC-FNMT dispone de distintos métodos de autenticación, mediante los que una entidad externa demuestra su identidad, o el conocimiento de algún dato secreto almacenado en la tarjeta.

66. La correcta realización de cada uno de estos métodos, permite obtener unas condiciones de seguridad, que podrán ser requeridas para el acceso a los distintos recursos de la tarjeta.

7.2.3.1 AUTENTICACIÓN DE USUARIO MEDIANTE PIN

67. La tarjeta soporta verificación de usuario (CHV- Card Holder Verification) para el acceso a determinados ficheros. La verificación es realizada, a través del canal seguro de PIN, comprobando el código facilitado por la entidad externa a través del comando diseñado para tal fin. El dato es comparado con la información de referencia almacenada en el fichero CHV. El código CHV (PIN) es una secuencia de 12-16 bytes.

68. Cada código CHV tiene su propio contador de intentos. Tras una presentación válida de PIN, el contador de reintentos correspondiente es automáticamente puesto a su valor inicial (3 intentos). El contador de intentos es decrementado cada vez que se realiza una presentación errónea, pudiendo llegar a bloquearlo si el contador llega a cero. Es posible desbloquear un código CHV tras una correcta presentación del código de desbloqueo.

69. La operación de desbloqueo se realiza con la presentación de la clave PUK o con biometría más “clave APP”.

7.2.3.2 DESBLOQUEO DE PIN (OPCIÓN 1: BIOMETRÍA)

70. La tarjeta TC-FNMT tiene soporte para biometría con algoritmo “Match on Card”, es decir, la verificación de los datos biométricos frente a los datos de referencia se realiza dentro de la propia tarjeta. Por tanto, se mantienen los datos sensibles de biometría siempre internos a la tarjeta, y su utilización está controlada mediante control de acceso. Esta característica de “Match on Card” confiere una importante diferencia frente a algoritmos “Match off Card”, donde la tarjeta sólo es utilizada como soporte de los datos para la verificación externa.

7.2.3.3 DESBLOQUEO DE PIN (OPCIÓN 2: PUK)

71. El desbloqueo del PIN con PUK se realiza a través del canal seguro de usuario, comprobando el código facilitado por la entidad externa a través del comando diseñado para tal fin. El dato es comparado con la información de referencia almacenada en el fichero CHV. El código CHV (PUK) es una secuencia de 16 bytes.

72. El código PUK tiene su propio contador de intentos. Tras una presentación válida de PUK, el contador de reintentos del PIN es automáticamente puesto a su valor inicial (3 intentos). El contador de intentos del PUK es decrementado cada vez que se realiza una presentación errónea, pudiendo llegar a bloquearlo si el contador llega a cero. No es posible desbloquear un código PUK.

7.3 ADMINISTRACIÓN DEL PRODUCTO

7.3.1 ADMINISTRACIÓN LOCAL

73. Se distinguen dos ámbitos en los que la TC-FNMT es utilizada por el administrador. El primero de ellos, será durante el proceso de expedición y el segundo, en la realización de funciones administrativas, ya en fase de usuario.

74. Las acciones a realizar para el proceso de expedición se encuentran descritas en el apartado **5 FASE DE EXPEDICIÓN**.

75. Existen una serie de procesos administrativos que son ejecutados por el administrador. Estos procesos se describen en las siguientes secciones.

76. Para más información se recomienda consultar la Guía Operativa del Administrador de la TC-FNMT [GOA].

7.3.1.1 DESBLOQUEO Y ACTUALIZACIÓN DE PIN MEDIANTE BIOMETRÍA

77. En el caso de que el usuario haya olvidado su código PIN o bien éste esté bloqueado, se permite el desbloqueo del PIN haciendo uso de la biometría. Permite establecer un nuevo valor de código PIN.

78. Debido a la criticidad de esta operación, el cambio de PIN se ha de realizar siempre en condiciones de máxima confidencialidad y seguridad, exigiéndose, por tanto, el establecimiento de un canal seguro.

7.3.1.2 ACTUALIZACIÓN DEL SISTEMA OPERATIVO

79. La actualización del sistema operativo de la TC-FNMT únicamente está permitida en terminales específicamente habilitados a tal efecto y no se puede realizar bajo ningún concepto en otros terminales.

7.3.1.3 VERIFICACIÓN DEL SISTEMA OPERATIVO RECIÉN ACTUALIZADO

80. La verificación del sistema operativo del producto se debe realizar una vez que haya finalizado el proceso de carga indicado en el párrafo anterior.

7.3.2 CONFIGURACIÓN DE ADMINISTRADORES

81. Únicamente existe un rol de usuario de administración que se obtiene al establecer un canal seguro administrativo.

82. Para ello, el terminal del administrador contará con un certificado de administrador y podrá establecer un canal seguro administrativo que dará acceso a los recursos de la tarjeta que requieran esta condición.

83. Solamente se puede establecer con los canales Autenticación con intercambio de claves o Autenticación de dispositivo con protección de privacidad definidos en [EN419212-3].

84. Para más información se recomienda consultar la Guía Operativa del Administrador de la TC-FNMT [GOA].

7.4 GESTIÓN DE CERTIFICADOS

85. El entorno de operación de la TC-FNMT debe cumplir los siguientes requisitos y recomendaciones de seguridad:

    a) Las claves de firma se deberán generar con un tamaño mínimo de clave de 3072 bits para RSA y de 256 bits para curvas elípticas.

    b) La longitud del PIN debe ser de, al menos, 12 bytes.

7.5 ACTUALIZACIONES

86. Es posible que, durante el tiempo de vida útil de la Tarjeta Criptográfica TC-FNMT, se desarrolle alguna actualización del sistema operativo (superior a la 5.70). Esto daría lugar a una nueva versión de la Tarjeta Criptográfica (superior a la 5.6) que debería ser certificada de nuevo. Dado que el soporte físico (plástico) no forma parte de la funcionalidad de seguridad de firma electrónica asociada a la TC-FNMT, teóricamente se podría reutilizar dicho soporte cargando en el componente electrónico (chip) la nueva TC-FNMT certificada (que estaría formada por el mismo chip y el nuevo sistema operativo). Para que esto sea posible, la configuración elegida de la TC-FNMT actual deber incluir expresamente la funcionalidad de carga de un nuevo código.

87. El entorno operativo debe garantizar que los terminales de actualización se coloquen en un entorno seguro que evite el acceso físico no autorizado y que sean operados únicamente por personal autorizado. El entorno operativo también debe garantizar, por ejemplo, políticas y procedimientos organizacionales, por los que el personal autorizado supervisa el procedimiento de actualización completo.

88. El entorno operativo también debe garantizar mediante, por ejemplo, procedimientos organizativos, apoyados por medios criptográficos, que solo aquellas entidades que tienen políticas implementadas que garantizan un entorno de operación seguro reciben terminales de actualización. Además, el entorno operativo garantiza que los terminales de actualización puedan desactivarse funcionalmente si estas políticas ya no están vigentes o no se aplican en las entidades.

89. Para mayor información se recomienda consultar la Guía Operativa del Administrador de la TC-FNMT [GOA].

7.6 AUTO-CHEQUEOS

90. La Tarjeta Criptográfica ejecuta periódicamente auto-chequeos. La información relativa los mismos es de carácter confidencial.

7.7 AUDITORÍA

7.7.1 REGISTRO DE EVENTOS

91. Durante el tiempo de vida de la Tarjeta Criptográfica TC-FNMT, es posible que se produzcan ciertos eventos relevantes de seguridad para prevenir ataques. Estos eventos quedan registrados en la propia tarjeta y, en función de su severidad, es posible que se bloquee de forma irreversible. En ese caso, dicho registro únicamente puede ser consultado por la FNMT-RCM.

8 REFERENCIAS

[CMD] Especificación funcional. Manual de comandos. TC-FNMT 5.6. v2.0 r4. 27/02/2023.

[DPC] Declaración general de prácticas de servicios de Confianza y de certificación electrónica. v6.1. 11/04/2024.

[EN419212-3] EN 419212-3. Interfaz de aplicación para tarjetas inteligentes utilizadas como dispositivos seguros de creación de firma. Parte 3: Protocolos de autentificación de dispositivos. Noviembre 2017.

[GOA] Guía Operativa para administrador – TC-FNMT 5.6. v2.0 r3. 27/02/2023.

[GP] Guía Preparativa – TC-FNMT 5.6. v2.0 r3. 27/02/2023.

[ICAO] International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, Version Seventh Edition, 2015.

[SSCDPP] Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation, prEN 14169-2:2012 ver. 2.0.1, 2012-01, BSI-CC-PP-0059-2009-MA-01.

[SSCDPP3] Protection Profiles for Secure Signature Creation Device – Part 3: Device with key import, prEN 14169-3:2012 ver. 1.0.2, 2012-07-24, BSI-CC-PP-0075.

[SSCDPP4] Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application. Version: 1.0.1. 2013-11-27, BSI-CC-PP-0071.

[SSCDPP5] Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application. Version: 1.0.1. 2012-11-14, BSI-CC-PP-0072.

[SSCDPP6] Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application. Version: 1.0.4. 2013-04-03, BSI-CC-PP-0076.

[STTCFNMT] Declaración de Seguridad reducida de la Tarjeta TC-FNMT 5.6. v2.1 r0. 29/06/2023.

[TR03110-1] Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1. Version 2.20. 26. February 2015

[TR03110-2] Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS). Version 2.21. 21. December 2016.

9 ABREVIATURAS

APDU	Application Protocol Data Unit, Unidad de Datos del Protocolo de Aplicación
ATR	Answer to Reset, Respuesta al Reset
CAdES	CMS Advanced Electronic Signatures
CAN	Card Access Number, Número de Acceso a la Tarjeta
CHV	Card Holder Verification, Verificación del Portador de la Tarjeta
CMD	Manual de Comandos
CPSTIC	Catálogo de Productos de Seguridad TIC
DCCF	Dispositivo Cualificado de Creación de Firmas
DPC	Declaración de Prácticas de Certificación
EAC	Extended Access Control, Control de Acceso Extendido
ECDH	Elliptic Curve Diffie-Hellman
eIDAS	Electronic Identification, Authentication, and Trust Services (Reglamento (UE) nº 910/2014)
ENS	Esquema Nacional de Seguridad
eSign	Electronic Signature (Aplicación de firma electrónica)
FNMT-RCM	Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda
GOA	Guía Operativa del Administrador
GP	Guía Preparativa
ICAO	International Civil Aviation Organization
PACE	Password Authenticated Connection Establishment
PAdES	PDF Advanced Electronic Signatures
PIN	Personal Identification Number, Número de Identificación Personal
PKCS	Public Key Cryptography Standards, Estándares de Criptografía de Clave Pública
PKCS#11	Public Key Cryptography Standards #11
PUK	Pin Unblocking Key, Clave de Desbloqueo del PIN
RSA	Rivest-Shamir-Adleman
SHA-256	Secure Hash Algorithm 256-bit
SSCDPP	Secure Signature Creation Device Protection Profile
STTCFNMT	Declaración de Seguridad de la Tarjeta TC-FNMT
TC-FNMT	Tarjeta Criptográfica de la Fábrica Nacional de Moneda y Timbre
XAdES	XML Advanced Electronic Signatures

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL