Referencia: 2018-63-INF-4217- v1
Difusión: Limitada al expediente
Fecha: 11.01.2024

Creado por: I003
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente #	**2018-63**
TOE	**TC-FNMT versión 5.6**
Solicitante	**Q2826004J - Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda**

Referencias

[EXT-4520] Solicitud de Certificación

[EXT-8749] Informe Técnico de Evaluación

Informe de Certificación del producto TC-FNMT versión 5.6, según la solicitud de referencia [EXT-4520], de fecha 30/11/2018, evaluado por el laboratorio Applus Laboratories, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-8749], recibido el pasado 29/09/2023.

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto TC-FNMT versión 5.6.

El TOE es una tarjeta criptográfica con la capacidad de realizar firmas electrónicas. El TOE está compuesto de un chip previamente certificado (que proporciona la librería criptográfica y el firmware con el loader para la actualización del código), el sistema operativo y las librerías biométricas.

Fabricante: Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda.

Patrocinador: Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda.

Organismo de Certificación: Centro Criptológico Nacional (CCN).

Laboratorio de Evaluación: Applus Laboratories.

Perfil de Protección:

- 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].
- 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].
- 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].
- 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].
- 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].

Nivel de Evaluación: Common Criteria v3.1 R5 EAL4 + ALC_DVS.2 + ATE_DPT.2 + AVA_VAN.5.

Fecha de término de la evaluación: 15/11/2023.

Fecha de expiración[1]: 02/01/2029.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 (aumentado con ALC_DVS.2 + ATE_DPT.2 + AVA_VAN.5) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Applus Laboratories asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer

[1] Este campo se refiere a la fecha de expiración del reconocimiento del certificado en el ámbito de los acuerdos de reconocimiento mutuo firmados por este Organismo de Certificación.

todas las acciones del evaluador a nivel EAL4 + ALC_DVS.2 + ATE_DPT.2 + AVA_VAN.5, definidas por los Common Criteria v3.1 R5 y la CEM v3.1 R5.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto TC-FNMT versión 5.6, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El TOE es una tarjeta criptográfica con la capacidad de realizar firmas electrónicas. El TOE está compuesto de un chip previamente certificado (que proporciona la librería criptográfica y el firmware con el loader para la actualización del código), el sistema operativo y las librerías biométricas. Esta tarjeta implementa un sistema de ficheros que incluye la siguiente aplicación:

- eSign (aplicación de firma [TR03110-2] conforme a [SSCDPP], [SSCDPP3], [SSCDPP4], [SSCDPP5] y [SSCDPP6].

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL4, más las requeridas para el componente adicional ALC_DVS.2 + ATE_DPT.2 + AVA_VAN.5, según los Common Criteria v3.1 R5.

CLASE DE GARANTÍA	COMPONENTE DE GARANTÍA
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ADV	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.2

	ALC_LCD.1
	ALC_TAT.1
ATE	ATE_COV.2
	ATE_DPT.2
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.5

REQUISITOS FUNCIONALES DE SEGURIDAD

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, según los Common Criteria v3.1 R5.

SECURITY FUNCTIONAL REQUIREMENTS
FAU_SAS.1/EAC2
FAU_SAS.1/UPD
FCS_CKM.1/AES_PRO
FCS_CKM.1/DH_PACE
FCS_CKM.1/EC_SSCDPP
FCS_CKM.1/RSA_SSCDPP
FCS_CKM.1/UPD_DEC
FCS_CKM.1/UPD_INT
FCS_CKM.1/UPD_ITC
FCS_CKM.4/AES_PRO
FCS_CKM.4/EAC2
FCS_CKM.4/EC_SSCDPP
FCS_CKM.4/RSA_SSCDPP
FCS_CKM.4/UPD
FCS_CKM.4/UPD_OS
FCS_COP.1/AES_PRO
FCS_COP.1/EC_SSCDPP
FCS_COP.1/PACE_ENC
FCS_COP.1/PACE_MAC
FCS_COP.1/RSA_SSCDPP
FCS_COP.1/SHA
FCS_COP.1/SHA_SSCDPP
FCS_COP.1/SIG_VER
FCS_COP.1/UPD_DEC
FCS_COP.1/UPD_INT

FCS_COP.1/UPD_ITC
FCS_COP.1/UPD_SIG
FCS_RND.1/EAC2
FDP_ACC.1/SCD/SVD_Generation_SSCDPP
FDP_ACC.1/SCD_Import_SSCDPP3
FDP_ACC.1/Signature_Creation_SSCDPP
FDP_ACC.1/SVD_Transfer_SSCDPP
FDP_ACC.1/TRM
FDP_ACC.1/UPD
FDP_ACF.1/SCD/SVD_Generation_SSCDPP
FDP_ACF.1/SCD_Import_SSCDPP3
FDP_ACF.1/Signature_Creation_SSCDPP
FDP_ACF.1/SVD_Transfer_SSCDPP
FDP_ACF.1/TRM
FDP_ACF.1/UPD
FDP_DAU.2/SVD_SSCDPP4
FDP_IFC.1/UPD
FDP_IFF.1/UPD
FDP_ITC.1/SCD_SSCDPP3
FDP_RIP.1/EAC2
FDP_RIP.1/SSCDPP
FDP_RIP.1/UPD
FDP_SDI.2/DTBS_SSCDPP
FDP_SDI.2/Persistent_SSCDPP
FDP_UCT.1/SCD_SSCDPP3
FDP_UCT.1/TRM
FDP_UIT.1/DTBS_SSCDPP5
FDP_UIT.1/TRM
FIA_AFL.1/BIO_SSCDPP
FIA_AFL.1/Block_PIN
FIA_AFL.1/SSCDPP
FIA_AFL.1/Suspend_PIN
FIA_AFL.1/UPD
FIA_API.1/CA
FIA_API.1/SSCDPP4
FIA_UAU.1/EAC2_Terminal
FIA_UAU.1/PACE
FIA_UAU.1/SSCDPP
FIA_UAU.1/UPD
FIA_UAU.4/PACE
FIA_UAU.5/PACE
FIA_UAU.6/CA
FIA_UAU.6/PACE

FIA_UID.1/EAC2_Terminal
FIA_UID.1/PACE
FIA_UID.1/SSCDPP
FIA_UID.1/UPD
FMT_LIM.1/Loader
FMT_LIM.2/Loader
FMT_MOF.1/SSCDPP
FMT_MSA.1/Admin_SSCDPP
FMT_MSA.1/Signatory_SSCDPP
FMT_MSA.2/SSCDPP
FMT_MSA.3/SSCDPP
FMT_MSA.4/SSCDPP
FMT_MTD.1/Activate_PIN
FMT_MTD.1/Admin_SSCDPP
FMT_MTD.1/Change_PIN
FMT_MTD.1/CVCA_INI
FMT_MTD.1/CVCA_UPD
FMT_MTD.1/DATE
FMT_MTD.1/INI_DIS
FMT_MTD.1/INI_ENA
FMT_MTD.1/Initialize_PIN
FMT_MTD.1/KEY_READ
FMT_MTD.1/PA
FMT_MTD.1/Resume_PIN
FMT_MTD.1/Signatory_SSCDPP
FMT_MTD.1/SK_PICC
FMT_MTD.1/Unblock_PIN
FMT_MTD.1/UPD_KEY_READ
FMT_MTD.1/UPD_SK_PICC
FMT_MTD.3/EAC2
FMT_SMF.1/EAC2
FMT_SMF.1/SSCDPP
FMT_SMF.1/UPD
FMT_SMR.1
FMT_SMR.1/PACE
FMT_SMR.1/SSCDPP
FMT_SMR.1/UPD
FPT_EMS.1/SSCDPP
FPT_EMS.1/UPD
FPT_FLS.1/SSCDPP
FPT_FLS.1/UPD
FPT_PHP.1/SSCDPP
FPT_PHP.3/EAC2

FPT_PHP.3/SSCDPP
FPT_TST.1/SSCDPP
FPT_TST.1/UPD
FTP_ITC.1/CA2
FTP_ITC.1/DTBS_SSCDPP5
FTP_ITC.1/PACE
FTP_ITC.1/SCD_SSCDPP3
FTP_ITC.1/SVD_SSCDPP4
FTP_ITC.1/UPD
FTP_ITC.1/VAD_SSCDPP5

IDENTIFICACIÓN

Producto: TC-FNMT versión 5.6.

Declaración de Seguridad: Declaración de Seguridad de la tarjeta TC-FNMT 5.6, versión 2.0, revisión 3.

Perfil de Protección:

- 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].
- 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].
- 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].
- 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].
- 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].

Nivel de Evaluación: Common Criteria v3.1 R5 EAL4 + ALC_DVS.2 + ATE_DPT.2 + AVA_VAN.5.

POLÍTICA DE SEGURIDAD

El uso del producto TC-FNMT versión 5.6, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de estas políticas se encuentra en la Declaración de Seguridad en el apartado 4.3 ("*Organizational Security Policies*").

HIPÓTESIS Y ENTORNO DE USO

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas. Por tanto, para garantizar el uso seguro del TOE, se parte de las siguientes hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE. Se pueden encontrar en el apartado 4.4 ("*Assumptions*") de la Declaración de Seguridad.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto TC-FNMT versión 5.6, aunque los agentes que realicen ataques tengan potencial de ataque Alto correspondiente a EAL4 + ALC_DVS.2 + ATE_DPT.2 + AVA_VAN.5, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Las amenazas cubiertas por las propiedades de seguridad del TOE se encuentran en el apartado 4.2 ("*Threats*") de la Declaración de Seguridad.

FUNCIONALIDAD DEL ENTORNO

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

Los objetivos que se deben cubrir por el entorno de uso del TOE se encuentran en el apartado 5.2 ("*Security Objectives for the Operational Environment*") de la Declaración de Seguridad.

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad) o de los requisitos de seguridad del TOE se encuentran en la correspondiente Declaración de Seguridad.

ARQUITECTURA

ARQUITECTURA LÓGICA

El TOE implementa un sistema de ficheros en el que hay la siguiente aplicación:

- eSign: (aplicación de firma [TR03110-2] conforme a [SSCDPP], [SSCDPP3], [SSCDPP4], [SSCDPP5] y [SSCDPP6].

ARQUITECTURA FÍSICA

El TOE está compuesto por los siguientes cinco elementos:

- IC plataforma subyacente: ST31G480 E05 (ST Microelectronics)
- Firmware: v3.0.1
- Librería criptográfica: Neslib 6.2.1
- Sistema Operativo: DNIe, versión 5.70

- Librerías biométricas: Sagem[2] v5.00 ó Siemens[3] v5.00

El alcance físico del TOE incluye también los documentos que se citan en la sección siguiente.

DOCUMENTOS

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

DOCUMENTO	VERSIÓN
Guía preparativa – Tarjeta TC-FNMT 5.6	v2.0 r3. 27/02/2023
Guía operativa para usuario final – Tarjeta TC-FNMT 5.6	v2.0 r3. 27/02/2023
Guía operativa para administrador. Tarjeta TC-FNMT 5.6	v2.0 r3. 27/02/2023
Guías operativas – TC-FNMT 5.6	v2.0 r3. 27/02/2023
Anexo I Ejemplo – Guía Operativa para usuario final	v2.0 r3. 27/02/2023
Especificación funcional. Manual de comandos. TC-FNMT 5.6	v2.0 r4. 27/02/2023
Scripts de expedición: • TCFNMT_5_70_Expedicion_eSign_Sin_Claves_No_Bio_v01.esc (Para la opción de TOE sin biometría). • TCFNMT_5_70_Expedicion_eSign_Sin_Claves_BIOMETRIA_v01.esc (Para la opción de TOE con biometría: sea Sagem o Siemens). • TCFNMT_5_70_Expedicion_CerrarTCFNMT_v01.esc • PACE_192.esc • PRO_RSA.esc	La indicada en el nombre del fichero.

PRUEBAS DEL PRODUCTO

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todas las pruebas han sido realizadas por el fabricante, en sus instalaciones, con resultado satisfactorios.

Durante el proceso de evaluación se han verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas, acorde a la arquitectura identificada en la Declaración de Seguridad.

[2] Sagem, Morpho e Idemia son los distintos nombres que desde el lanzamiento del proyecto de TC-FNMT ha ido tomando el proveedor de una de las librerías Match On Card. Todos ellos se refieren al mismo proveedor.

[3] Siemens y Atos son los distintos nombres que desde el lanzamiento del proyecto de TC-FNMT ha ido tomando el proveedor de una de las librerías Match On Card. Se refieren al mismo proveedor.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Dada la similitud entre el TOE del presente expediente y del expediente 2019-06 (TOE "*DNIe versión 4.0*"), y tras analizar las diferencias y el impacto, el evaluador ha reutilizado los resultados obtenidos en la repetición de pruebas del expediente 2019-06 en los casos posibles y ha repetido las pruebas en el TOE del expediente 2018-63 en los casos en los que la reutilización no era posible. Se han verificado el resultado del 100% de las pruebas del plan de pruebas del fabricante.

Adicionalmente, el laboratorio ha desarrollado un plan de pruebas independiente con el objetivo de cubrir escenarios o casos de pruebas no contemplados en el plan de pruebas del fabricante. A través del plan de pruebas independiente se han probado el 4.9% de los SFR y el 18,18% de las TSFI.

Teniendo en cuenta la lista de vulnerabilidades aplicables al TOE por su naturaleza y su entorno operacional, el equipo de evaluación desarrolló un análisis de vulnerabilidades teniendo en cuenta el estado del arte en el momento de la evaluación de este expediente y preparó un entorno de pruebas para realización de pruebas de penetración de acuerdo a los documentos de apoyo de JIL (*Joint Interpretation Library*) aplicables al dominio técnico de "*Smartcards and Similar devices*" [JILAAPS] y [JILADVARC].

El equipo de evaluación analizó también la lista de requisitos de seguridad de la plataforma certificada subyacente basándose en el informe técnico de evaluación compuesto y teniendo en cuenta el estado del arte en el momento de emisión del nuevo informe de análisis de vulnerabilidades, junto con los requisitos específicos del TOE y su entorno operacional declarados en la declaración de seguridad aplicable.

Teniendo en cuenta lo anterior, se diseñaron y ejecutaron una serie de pruebas de penetración. Como resultado final de las pruebas realizadas, el equipo evaluador concluye que, teniendo en cuenta el estado del arte a la fecha de emisión de su informe, no existe ninguna vulnerabilidad explotable en el entorno operacional declarado, por lo tanto el TOE es resistente a atacantes con potencial de ataque Alto según se define en Common Criteria versión 3.1 revisión 5.

CONFIGURACIÓN EVALUADA

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Así, para el funcionamiento del producto TC-FNMT versión 5.6 es necesario disponer de los siguientes componentes:

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Así, para el funcionamiento del producto TC-FNMT versión 5.6 es necesario disponer de los siguientes componentes:

- IC plataforma subyacente: ST31G480 E05 (ST Microelectronics)
- Firmware: v3.0.1

- Librería criptográfica: Neslib 6.2.1
- Sistema Operativo: DNIe, versión 5.70
- Librerías biométricas: Sagem[4] v5.00 ó Siemens[5] v5.00

El TOE presenta seis opciones de configuración, que dependen de la capacidad o no de actualizar el código y de la librería biométrica utilizada. Estas configuraciones y la identificación del TOE correspondiente a cada una de ellas son las siguientes:

- Chip ST31G480 E05 y Biometría de Sagem (TCFNMT 05.70 A01 H 00B8)
- Chip ST31G480 E05 y Biometría de Siemens (TCFNMT 05.70 B01 H 00B8)
- Chip ST31G480 E05 actualizable y Biometría de Sagem (TCFNMT 05.70 C01 H 00B8)
- Chip ST31G480 E05 actualizable y Biometría de Siemens (TCFNMT 05.70 D01 H 00B8)
- Chip ST31G480 E05 sin biometría (TCFNMT 05.70 E01 H 00B8)
- Chip ST31G480 E05 actualizable sin biometría (TCFNMT 05.70 F01 H 00B8)

El consumidor del TOE puede verificar la configuración del mismo siguiendo el procedimiento de recepción definido en el apartado 2.3.2 "*Entrega segura y recepción segura*" del documento "*Guía preparativa tarjeta TC-FNMT 5.6*", versión 2.0, Revisión 3, de 27 de febrero de 2023.

RESULTADOS DE LA EVALUACIÓN

El producto TC-FNMT versión 5.6 ha sido evaluado en base a la Declaración de Seguridad Declaración de Seguridad de la tarjeta TC-FNMT 5.6, versión 2.0, revisión 3.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 + ALC_DVS.2 + ATE_DPT.2 + AVA_VAN.5 presentan el veredicto de "PASA". Por consiguiente, el laboratorio Applus Laboratories asigna el **VEREDICTO de "PASA"** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4 + ALC_DVS.2 + ATE_DPT.2 + AVA_VAN.5, definidas por los Common Criteria v3.1 R5 y la CEM v3.1 R5.

[4] Sagem, Morpho e Idemia son los distintos nombres que desde el lanzamiento del proyecto de TC-FNMT ha ido tomando el proveedor de una de las librerías Match On Card. Todos ellos se refieren al mismo proveedor.

[5] Siemens y Atos son los distintos nombres que desde el lanzamiento del proyecto de TC-FNMT ha ido tomando el proveedor de una de las librerías Match On Card. Se refieren al mismo proveedor.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación, se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

- El usuario debe seguir estrictamente las guías de seguridad del TOE.
- El usuario debe mantener el TOE bajo su control personal, así como establecer las medidas de seguridad exigibles al entorno operacional.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto TC-FNMT versión 5.6, se propone la resolución estimatoria de la misma.

El certificador recomienda a los potenciales consumidores del TOE prestar especial atención a las recomendaciones y comentarios de los evaluadores, seguir estrictamente las indicaciones recogidas en las guías del fabricante detalladas en la sección DOCUMENTOS del presente informe y revisar las hipótesis declaradas en la definición del problema de seguridad que aparece en la sección 4.4 de la Declaración de Seguridad.

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[JILAAPS] Application of Attack Potential to Smartcards, version 2.9. Jan. 2013. Joint Interpretation Library.

[JILADVARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.0. Jan 2012. Joint Interpretation Library.

[ST] Declaración de Seguridad de la tarjeta TC-FNMT 5.6, versión 2.0, revisión 3.

[ST-Lite] Declaración de Seguridad reducida de la tarjeta TC-FNMT 5.6, versión 2.1, revisión 0.

[SSCDPP] Protection profiles for secure signature creation device – Part 2: Device with key generation, prEN 14169-2:2012. Version 2.01, 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. Version 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.

DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

- Declaración de Seguridad de la tarjeta TC-FNMT 5.6, versión 2.0, revisión 3.

La versión pública de este documento constituye la “Declaración de Seguridad LITE” que ha sido revisada siguiendo el documento con código [CCDB-2006-04-004], y se publica con el informe de certificación en las webs del CCRA y del OC. El identificador de la “Declaración de Seguridad LITE” es:

- Declaración de Seguridad reducida de la tarjeta TC-FNMT 5.6, versión 2.1, revisión 0.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.