Referencia: 2019-6-INF-3953- v2
Difusión: Pública
Fecha: 06.02.2023

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

INFORME DE CERTIFICACIÓN

Expediente #	**2019-6**
TOE	**DNIe versión 4.0**
Solicitante	**ESQ2826004 - Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda**
Referencias	

[EXT-4677] Solicitud de Certificación

[EXT-8134] Informe Técnico de Evaluación

Informe de Certificación del producto DNIe versión 4.0, según la solicitud de referencia [EXT-4677], de fecha 04/02/2019, evaluado por el laboratorio Applus Laboratories, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-8134], recibido el pasado 28/11/2022.

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto DNIe versión 4.0.

El TOE es una tarjeta inteligente que proporciona las funcionalidades de firma, identificación y documento de viaje. Esta tarjeta está compuesta por 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. 2.01, 2012-01, BSI-CC-PP-0059-2009-MA-01, [SSCDPP].
- 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. November 2013. [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. November 2012. [SSCDPP5].
- Common Criteria Protection Profile — Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012. Version 1.3.2, 05th December 2012. [EAC1PP].
- Common Criteria Protection Profile — Electronic document implementing Extended Access Control Version 2 based on BSI TR-03110 [EAC2_PP], BSI-CC-PP-0086. Version 1.01, May 20th, 2015. [EAC2PP].
- Common Criteria Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01. Version 1.01, 22th July 2014. [PACEPP].

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

Fecha de término de la evaluación: 21/12/2022.

Fecha de expiración[1]: 26/01/2028.

[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.

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

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto DNIe versión 4.0, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El TOE es una tarjeta inteligente formada por una plataforma previamente certificada (incluyendo su firmware y la librería criptográfica), el sistema operativo y las librerías biométricas. Esta tarjeta implementa un sistema de ficheros que incluye tres aplicaciones aisladas entre sí:

- eID (identificación de acuerdo con lo especificado en [TR03110-2])
- ePass (pasaporte [ICAO9303], conforme a [EAC1PP] y [EAC2PP])
- eSign (aplicación de firma [TR03110-2] conforme a [SSCDPP], [SSCDPP4] y [SSCDPP5]

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 los componentes adicionales ALC_DVS.2 + ATE_DPT.2 + AVA_VAN.5, según los criterios de evaluación Common Criteria v3.1 R5.

CLASE DE GARANTÍA	COMPONENTES 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 criterios de evaluación Common Criteria v3.1 R5.

SECURITY FUNCTIONAL REQUIREMENTS
FAU_SAS.1/UPD
FAU_SAS.1/EAC2PP
FAU_SAS.1/EAC1PP
FCS_COP.1/UPD_ITC
FCS_CKM.1/UPD_ITC
FCS_COP.1/UPD_DEC
FCS_CKM.1/UPD_DEC
FCS_COP.1/UPD_SIG
FCS_COP.1/UPD_INT
FCS_CKM.1/UPD_INT
FCS_CKM.4/UPD
FCS_CKM.4/UPD_OS
FCS_CKM.1/DH_PACE_EAC2PP
FCS_COP.1/SHA_EAC2PP
FCS_COP.1/SIG_VER_EAC2PP
FCS_COP.1/PACE_ENC_EAC2PP
FCS_COP.1/PACE_MAC_EAC2PP
FCS_CKM.4/EAC2PP
FCS_RND.1/EAC2PP
FCS_CKM.1/DH_PACE_EAC1PP
FCS_CKM.4/EAC1PP
FCS_COP.1/PACE_ENC_EAC1PP
FCS_COP.1/PACE_MAC_EAC1PP
FCS_RND.1/EAC1PP

FCS_CKM.1/CA_EAC1PP
FCS_COP.1/CA_ENC_EAC1PP
FCS_COP.1/SIG_VER_EAC1PP
FCS_COP.1/CA_MAC_EAC1PP
FCS_CKM.1/RSA_SSCDPP
FCS_CKM.1/AES_PRO
FCS_CKM.1/EC_SSCDPP
FCS_CKM.4/RSA_SSCDPP
FCS_CKM.4/AES_PRO
FCS_CKM.4/EC_SSCDPP
FCS_COP.1/RSA_SSCDPP
FCS_COP.1/AES_PRO
FCS_COP.1/SHA_SSCDPP
FCS_COP.1/EC_SSCDPP
FDP_ACF.1/TRM
FDP_ACC.1/UPD
FDP_ACF.1/UPD
FDP_IFC.1/UPD
FDP_IFF.1/UPD
FDP_RIP.1/UPD
FDP_ACC.1/TRM_EAC2PP
FDP_ACF.1/TRM_EAC2PP
FDP_RIP.1/EAC2PP
FDP_UCT.1/TRM_EAC2PP
FDP_UIT.1/TRM_EAC2PP
FDP_ACC.1/TRM_EAC1PP
FDP_ACF.1/TRM_EAC1PP
FDP_RIP.1/EAC1PP
FDP_UCT.1/TRM_EAC1PP
FDP_UIT.1/TRM_EAC1PP
FDP_ACC.1/SCD/SVD_Generation_SSCDPP
FDP_ACF.1/SCD/SVD_Generation_SSCDPP
FDP_ACC.1/SCD/SVD_Transfer_SSCDPP
FDP_ACF.1/SCD/SVD_Transfer_SSCDPP
FDP_ACC.1/Signature_Creation_SSCDPP
FDP_ACF.1/Signature_Creation_SSCDPP
FDP_RIP.1/SSCDPP
FDP_SDI.2/Persistent_SSCDPP
FDP_SDI.2/DTBS_SSCDPP
FDP_DAU.2/SVD_SSCDPP4
FDP_UIT.1/DTBS_SSCDPP5
FIA_AFL.1/UPD

FIA_UID.1/UPD
FIA_UAU.1/UPD
FIA_AFL.1/Suspend_PIN_EAC2PP
FIA_AFL.1/Block_PIN_EAC2PP
FIA_API.1/CA_EAC2PP
FIA_UID.1/PACE_EAC2PP
FIA_UID.1/EAC2_Terminal_EAC2PP
FIA_UAU.1/PACE_EAC2PP
FIA_UAU.1/EAC2_Terminal_EAC2PP
FIA_UAU.4/PACE_EAC2PP
FIA_UAU.5/PACE_EAC2PP
FIA_UAU.6/CA_EAC2PP
FIA_AFL.1/PACE_EAC2PP
FIA_UAU.6/PACE_EAC2PP
FIA_UAU.1/PACE_EAC1PP
FIA_UAU.4/PACE_EAC1PP
FIA_UAU.5/PACE_EAC1PP
FIA_UAU.6/PACE_EAC1PP
FIA_UAU.6/EAC_EAC1PP
FIA_API.1/EAC1PP
FIA_AFL.1/PACE_EAC1PP
FIA_UID.1/PACE_EAC1PP
FIA_UID.1/SSCDPP
FIA_AFL.1/SSCDPP
FIA_AFL.1/BIO_SSCDPP
FIA_API.1/SSCDPP4
FIA_UAU.1/SSCDPP
FMT_SMR.1
FMT_LIM.1/Loader
FMT_LIM.2/Loader
FMT_SMF.1/UPD
FMT_MTD.1/UPD_SK_PICC
FMT_MTD.1/UPD_KEY_READ
FMT_SMR.1/UPD
FMT_MTD.1/CVCA_INI_EAC2PP
FMT_MTD.1/CVCA_UPD_EAC2PP
FMT_SMF.1/EAC2PP
FMT_SMR.1/PACE_EAC2PP
FMT_MTD.1/DATE_EAC2PP
FMT_MTD.1/PA_EAC2PP
FMT_MTD.1/SK_PICC_EAC2PP
FMT_MTD.1/KEY_READ_EAC2PP

FMT_MTD.1/Initialize_PIN_EAC2PP
FMT_MTD.1/Change_PIN_EAC2PP
FMT_MTD.1/Resume_PIN_EAC2PP
FMT_MTD.1/Unblock_PIN_EAC2PP
FMT_MTD.1/Activate_PIN_EAC2PP
FMT_MTD.3/EAC2PP
FMT_LIM.1/EAC2PP
FMT_LIM.2/EAC2PP
FMT_MTD.1/INI_ENA_EAC2PP
FMT_MTD.1/INI_DIS_EAC2PP
FMT_SMF.1/EAC1PP
FMT_SMR.1/PACE_EAC1PP
FMT_LIM.1/EAC1PP
FMT_LIM.2/EAC1PP
FMT_MTD.1/INI_ENA_EAC1PP
FMT_MTD.1/INI_DIS_EAC1PP
FMT_MTD.1/CVCA_INI_EAC1PP
FMT_MTD.1/CVCA_UPD_EAC1PP
FMT_MTD.1/DATE_EAC1PP
FMT_MTD.1/CAPK_EAC1PP
FMT_MTD.1/PA_EAC1PP
FMT_MTD.1/KEY_READ_EAC1PP
FMT_MTD.3/EAC1PP
FMT_SMR.1/SSCDPP
FMT_SMF.1/SSCDPP
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/Admin_SSCDPP
FMT_MTD.1/Signatory_SSCDPP
FPT_EMS.1/UPD
FPT_FLS.1/UPD
FPT_TST.1/UPD
FPT_EMS.1/EAC2PP
FPT_FLS.1/EAC2PP
FPT_TST.1/EAC2PP
FPT_PHP.3/EAC2PP
FPT_EMS.1/EAC1PP
FPT_FLS.1/EAC1PP

FPT_TST.1/EAC1PP
FPT_PHP.3/EAC1PP
FPT_EMS.1/SSCDPP
FPT_FLS.1/SSCDPP
FPT_PHP.1/SSCDPP
FPT_PHP.3/SSCDPP
FPT_TST.1/SSCDPP
FTP_ITC.1/UPD
FTP_ITC.1/PACE_EAC2PP
FTP_ITC.1/CA2_EAC2PP
FTP_ITC.1/PACE_EAC1PP
FTP_ITC.1/SVD_SSCDPP4
FTP_ITC.1/VAD_SSCDPP5
FTP_ITC.1/DTBS_SSCDPP5

IDENTIFICACIÓN

Producto: DNIe versión 4.0.

Declaración de Seguridad: Declaración de Seguridad de la tarjeta DNIe 4.0, versión 2.0, revisión 0.

Perfil de Protección:

- Protection profiles for secure signature creation device – Part 2: Device with key generation, prEN 14169-2:2012 ver. 2.01, 2012-01, BSI-CC-PP-0059-2009-MA-01, [SSCDPP].
- 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. November 2013. [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. November 2012. [SSCDPP5].
- Common Criteria Protection Profile — Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012. Version 1.3.2, 05th December 2012. [EAC1PP].
- Common Criteria Protection Profile — Electronic document implementing Extended Access Control Version 2 based on BSI TR-03110 [EAC2_PP], BSI-CC-PP-0086. Version 1.01, May 20th, 2015. [EAC2PP].
- Common Criteria Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01. Version 1.01, 22th July 2014. [PACEPP].

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 DNIe versión 4.0, 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.

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 de la Declaración de Seguridad.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto DNIe versión 4.0, 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 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 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 tres aplicaciones:

- eID : identificación [TR03110-2].
- ePass: pasaporte [ICAO9303], conforme a [EAC1PP] y [EAC2PP].
- eSign: aplicación de firma [TR03110-2] conforme a [SSCDPP], [SSCDPP4] y [SSCDPP5].

Estas aplicaciones están aisladas entre sí. El MF (MasterFile), por encima de estas aplicaciones, contiene ficheros de configuración del TOE.

El TOE protege los datos con canales seguros: eID protege los datos con PACE y EAC2, ePass con PACE y EAC1 ó EAC2, y eSign con PACE y EAC2. El TOE implementa, además, el canal administrativo PRO [EN419212-1] con autenticación con intercambio de claves y autenticación de dispositivo con protección de privacidad. Este canal es requerido para la actualización del TOE, renovación de certificados, desbloqueo del PIN en instalaciones de la DGP, entre otros. Los protocolos PACE, EAC1 y EAC2 utilizan ECC. El canal PRO se puede implementar utilizando RSA o ECC.

El TOE implementa mecanismo de autenticación de usuario por PIN y por Biometría (dos huellas). El PIN se puede cambiar y desbloquear. Esto puede requerir clave APP (del administrador), canal administrador PRO, el PUK del PIN, el PIN anterior o una combinación de ellos, según sea requerido por el S.O.

La huella se verifica dentro del sistema operativo (*match on card*). Según su configuración, el TOE empleará la librería biométrica de Sagem[2] o la de Siemens[3].

ARQUITECTURA FÍSICA

El TOE está compuesto por los siguientes cinco elementos:

- IC plataforma subyacente: ST31G480 E02 (ST Microelectronics)
- Firmware: v3.0.1
- Librería criptográfica: Neslib 6.2.1
- Sistema Operativo: DNIe, versión 5.51
- 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 DNIe 4.0	v2.0 r0. 04/07/22
Guía operativa para usuario final. Tarjeta DNIe 4.0	v2.0 r0. 04/07/22
Guía operativa para administrador. Tarjeta DNIe 4.0	v2.0 r0. 04/07/22
Guías Operativas	v2.0 r0. 04/07/22
Anexo I Ejemplo - Guía Operativa para usuario final	v2.0 r0. 04/07/22
Especificación funcional. Manual de comandos. Tarjeta DNIe 4.0	v2.0 r0. 04/07/22
Scripts de expedición: • DNIe_5_51_Expedicion_CerrarDNIe_v06 • DNIe_5_51_Expedicion_ePassport_v02 • DNIe_5_51_Expedicion_eID_v03 • DNIe_5_51_Expedicion_eSign_v03	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.

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

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.

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

Para verificar los resultados de las pruebas del fabricante, el laboratorio ha repetido en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido el 100% de las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación, seleccionando una prueba por cada una de las clases funcionales más relevantes.

Adicionalmente, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados, así obtenidos, son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no representa un problema para la seguridad, ni supone una merma en la capacidad funcional del producto.

ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

Teniendo en cuenta la lista de vulnerabilidades aplicables al TOE por su naturaleza y su entorno operacional, el equipo de evaluación desarrolló nuevo 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 DNIe versión 4.0 es necesario disponer de los siguientes componentes:

- IC plataforma subyacente: ST31G480 E02 (ST Microelectronics)
- Firmware: v3.0.1
- Librería criptográfica: Neslib 6.2.1
- Sistema Operativo: DNIe, versión 5.51
- Librerías biométricas: Sagem[4] v5.00 ó Siemens[5] v5.00

El TOE presenta cuatro 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 E02 y Biometría de Sagem (DNIe 05.51 A01 H 00B8)
- Chip ST31G480 E02 y Biometría de Siemens (DNIe 05.51 B01 H 00B8)
- Chip ST31G480 E02 actualizable y Biometría de Sagem (DNIe 05.51 C01 H 00B8)
- Chip ST31G480 E02 actualizable y Biometría de Siemens (DNIe 05.51 D01 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 DNIe 4.0*", versión 2.0, Revisión 0, de 4 de julio de 2022.

RESULTADOS DE LA EVALUACIÓN

El producto DNIe versión 4.0 ha sido evaluado en base a la Declaración de Seguridad de la tarjeta DNIe 4.0, versión 2.0, revisión 0.

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 "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 criterios de evaluación Common Criteria v3.1 R5 y la metodología de evaluación CEM v3.1 R5.

[4] Sagem, Morpho e Idemia son los distintos nombres que desde el lanzamiento del proyecto de DNIe 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 DNIe 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 DNIe versión 4.0, se propone la resolución estimatoria de la misma.

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAC1	Extended Access Control version 1
EAC2	Extended Access Control version 2
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ETR	Evaluation Technical Report
OC	Organismo de Certificación
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PUK	Personal Unblocking Key
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 DNIe 4.0, versión 2.0, revisión 0.

[ST-Lite] Declaración de Seguridad reducida de la tarjeta DNIe 4.0, versión 2.0, revisión 2.

[SSCDPP] Protection profiles for secure signature creation device – Part 2: Device with key generation, prEN 14169-2:2012 ver. 2.01, 2012-01, BSI-CC-PP-0059-2009-MA-01.

[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. November 2013.

[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. November 2012.

[EAC1PP] Common Criteria Protection Profile — Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012. Version 1.3.2, 05th December 2012.

[EAC2PP] Common Criteria Protection Profile — Electronic document implementing Extended Access Control Version 2 based on BSI TR-03110 [EAC2_PP], BSI-CC-PP-0086. Version 1.01, May 20th, 2015.

[PACEPP] Common Criteria Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01. Version 1.01, 22th July 2014.

[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.

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 DNIe 4.0, versión 2.0, revisión 0.

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 DNIe 4.0, versión 2.0, revisión 2.

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.