Reference: 2025-10-INF-4676- v1
Target: Limitada al expediente
Date: 04.02.2026

Created by: CERT15
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2025-10**
TOE	**Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic running iOS 18.4**
Applicant	**94-2404110 - Apple Inc.**

References

[EXT-9467] 2025-02-04_2025-10_solicitud_certificacion

[EXT-9844] 2025-09-22_2025-10_ETR_v2

Certification report of the product Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic running iOS 18.4, as requested in [EXT-9467] dated 04/02/2025, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9844] received on 22/09/2025.

CONTENTS

EXECUTIVE SUMMARY 4
- TOE SUMMARY 5
- SECURITY ASSURANCE REQUIREMENTS 5
- SECURITY FUNCTIONAL REQUIREMENTS 6

IDENTIFICATION 7

SECURITY POLICIES 7
- ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 8
- CLARIFICATIONS ON NON-COVERED THREATS 8
- OPERATIONAL ENVIRONMENT FUNCTIONALITY 8

ARCHITECTURE 8
- LOGICAL SCOPE 9
- PHYSICAL SCOPE 9
- Subsystems of the TOE 10

DOCUMENTS 12

PRODUCT TESTING 13

EVALUATED CONFIGURATION 13

EVALUATION RESULTS 15

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 15

CERTIFIER RECOMMENDATIONS 15

GLOSSARY 15

BIBLIOGRAPHY 16

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE) 16

RECOGNITION AGREEMENTS 18
- European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) 18
- International Recognition of CC – Certificates (CCRA) 18

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic running iOS 18.4.

The TOE is a combination of Hardware and Software components that implement Strong Customer Authentication and Dynamic Linking for Apple Pay on mobile devices.

Developer/manufacturer: Apple Inc.

Sponsor: Apple Inc.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Protection Profile: N/A

Evaluation Level: Common Criteria 2022 Revision 1, EAL2 + ADV_FSP.3 and ALC_FLR.3.

Evaluation end date: 01/12/2025

Expiration Date[1]: 16/01/2026

All the assurance components required by the evaluation level EAL2 (augmented with ADV_FSP.3 + ALC_FLR.3) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2 + ADV_FSP.3 + ALC_FLR.3, as defined by the Common Criteria 2022 Revision 1 and the CEM 2022 Revision 1.

Considering the obtained evidences during the instruction of the certification request of the product Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic running iOS 18.4, a positive resolution is proposed.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

TOE SUMMARY

The TOE platform includes the components implementing Strong Customer Authentication (SCA) and dynamic linking for Apple Pay.

User authentication is managed by the Secure Enclave. The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs). The Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even if the Applica-tion Processor kernel were to be compromised.

iOS allows the Apple Pay services and other security functions of the TOE to operate.

The Secure Element (outside of the TOE) is the secure component that holds the Apple Pay secrets and pro-cesses the Apple Pay transactions.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ADV_FSP.3 + ALC_FLR.3 to the table, according to Common Criteria 2022 Revision 1.

ASSURANCE CLASS	ASSURANCE COMPONENT
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.3
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
	ALC_FLR.3
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria 2022 Revision 1:

SECURITY FUNCTIONAL REQUIREMENT
FIA_UID.2
FIA_UAU.2
FIA_UAU.5
FIA_AFL.1/Biometric
FIA_AFL.1/Erase
FIA_AFL.1/Delay
FIA_UAU.6
FDP_DAU.1
FIA_ATD.1
FDP_ACC.2/Authentication_SFP
FDP_ACF.1/Authentication_SFP
FDP_ITT.1
FDP_ETC.2/Transaction
FDP_ACC.2/Payment_SFP
FDP_ACF.1/Payment_SFP
FDP_ACC.2/Card_Perso_SFP
FDP_ACF.1/Card_Perso_SFP
FDP_ETC.2/Card_Perso_SFP
FPT_ITC.1
FDP_ITC.1
FTP_ITC.1/SE
FDP_UCT.1/SE

FDP_UIT.1/SE
FPT_RPL.1/SE
FPR_UNO.1
FDP_RIP.1
FDP_SDI.1
FMT_SMR.1
FMT_SMF.1
FMT_MSA.3
FMT_MSA.1
FMT_MTD.1
FMT_MTD.3

IDENTIFICATION

Product: Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic running iOS 18.4

Security Target: Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic Bionic running iOS 18.4: Security Target, v1.3

Protection Profile: N/A.

Evaluation Level: Common Criteria 2022 Revision 1, EAL2 + ADV_FSP.3 and ALC_FLR.3.

SECURITY POLICIES

The use of the product Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic running iOS 18.4 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in section 4.6 (“Organizational Security Policies”).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 4.3 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic running iOS 18.4, although the agents implementing attacks have the attack potential to the Basic attack potential level of EAL2 + ADV_FSP.3 + ALC_FLR.3 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 4.5 ("Threats").

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 5.2 ("Security Objectives for the operational Environment").

ARCHITECTURE

The TOE platform includes the components implementing Strong Customer Authentication (SCA) and dynamic linking for Apple Pay.

User authentication is managed by the Secure Enclave. The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs). The Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even if the Applica-tion Processor kernel were to be compromised.

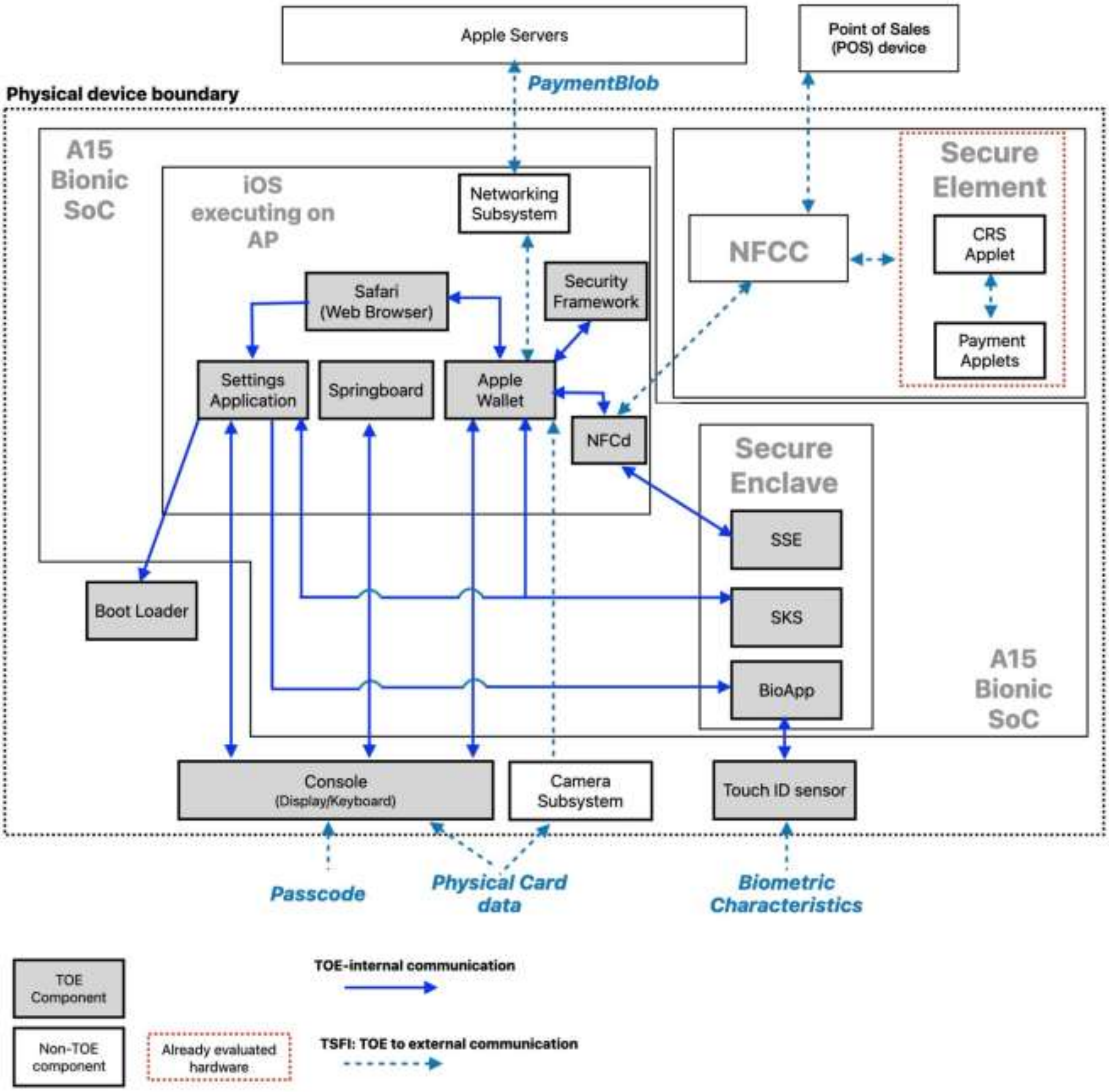
LOGICAL SCOPE

The logical security features of the TOE are summarized as follows:

- User authentication and management
- Secure channel between the Secure Enclave and the Biometric sensor
- Secure channel between the Secure Enclave and the Secure Element
- Card Data management
- Apple Pay payment transaction processing and management
- Operating System update
- iCloud logout and device reset

PHYSICAL SCOPE

The physical architecture is depicted in the following figure:



Subsystems of the TOE

The subsystems of the TOE consist of:

- Secure Enclave: The software components of the TOE residing in the Secure Enclave. This subsys-tem includes several applications executing on the Secure Enclave operating system:
    - BioApp is an application which provides functionality for processing biometric data and generat-ing biometric templates.

  - The SKS (Secure Key Store) is a hardware cryptographic module. The module is embedded in-side the Secure Enclave and packaged within the Application Processor.
  - The SSE (Secure Enclave-Secure Element) manages the pairing between the Secure Enclave and the Secure Enclave, allowing the Secure Enclave to process only genuine and authorized Apple Pay transactions. The SSE application maintains sensitive pairing material, allowing Secure En-clave and Secure Enclave to perform a mutual authentication before exchanging data.
- Apple Wallet: The Wallet app subsystem is an application executing as part of iOS that handles the enrollment of payment applications and governs the payment operation.
- iOS components executing on Application Processor (AP):
  - Springboard: The component of iOS that handles I/O with the console, and thereby provides the functionality for the iOS user interface
  - NFCd: This daemon facilitates the communication between Apple Wallet and the Secure Element
  - Safari browser: Web browser included with the OS. Provides a web interface to conduct pay-ment transactions
  - Security Framework: This is an API provided by the OS to provide cryptographic support that can be used to protect information, establish trust, and control access to software
  - Settings application: This application allows the user to modify various system settings
- Device components:
  - Touch ID sensor: This is the hardware component and associated drivers that allow fingerprint data to be captured and passed to BioApp to allow for enrollment and matching
  - Boot-loader: This subsystem consists of code that is executed during the boot sequence of the device. The boot-loader is responsible for ensuring that the device boots using software with as-sured integrity and authenticity
  - Console: This is the hardware and associated drivers that handles user input via the keyboard, and displays output via the screen. The touchscreen hardware is also part of the TOE

All other device hardware and iOS components are outside of the TOE, including the Secure Element to-gether with the NFCC hardware, and the XNU iOS kernel. The iOS subsystem components are individual ap-plications

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic Bionic running iOS 18.4: Security Target, v1.3
- Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic Bionic running iOS 18.4: Guidance, v1.1
- Apple Pay Support, https://support.apple.com/apple-pay, v1.0
- Apple Cash Support, https://support.apple.com/apple-cash, v1.0
- Apple Platform Security, Dec 2024, https://support.apple.com/guide/security, v1.18
- Check Your Service and Support Coverage (review your Apple warranty status), https://checkcoverage.apple.com, v1.0
- PSD2 security certifications - Device Identity, If you forgot your iPhone passcode, https://support.apple.com/118430, v1.0
- Set up your iPhone, https://support.apple.com/105132, v1.0
- Find the software version on your iPhone, https://support.apple.com/109065, v1.0
- Apple iOS Software License Agreement, B. Apple Pay Supplemental Terms and Conditions, https://www.apple.com/legal/sla/docs/iOS18_iPadOS18.pdf, v1.0
- Update the iOS on your iPhone, https://support.apple.com/118575, v1.0
- Identify your iPhone model, https://support.apple.com/108044, v1.0
- Use a passcode with your iPhone, https://support.apple.com/119586, v1.0
- Personal Safety User Guide for Apple devices, Set a unique passcode or password on devices, https://support.apple.com/guide/personal-safety/welcome/1.0/web, v1.0
- Registration form for Apple security-announce mailing list, https://lists.apple.com/mailman/listinfo/security-announce/, v1.0
- Get help with security issues, https://support.apple.com/111756, v1.0
- Report a security or privacy vulnerability, https://support.apple.com/102549, v1.0
- Apple security releases, https://support.apple.com/100100, v1.1
- Find the serial number of your iPhone, https://support.apple.com/108037, v1.0
- About Touch ID advanced technology, https://support.apple.com/105095, v1.0

- If Touch ID isn't working on iPhone, https://support.apple.com/101612, v1.0
- Use Touch ID on iPhone, https://support.apple.com/102528, v1.0
- iPhone User Guide, https://support.apple.com/guide/iphone/welcome/ios, v1.0

PRODUCT TESTING

The laboratory followed a sampling strategy based on executing all the test cases that could be replicable by the laboratory. Due to the nature of the TOE, many of the tests require the usage of internal tools only available to the developer to perform binaries or kernel modifications. In order to gain assurance of the correct behavior of the TOE, the laboratory performed a witnessing session covering the test cases that could not be executed by the laboratory. All test repeated by the laboratory, as well as the tests executed by the developer during the witnessing session, obtained a satisfactory result. During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test. All the tests have been executed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results. To verify the results of the developer tests, the evaluator has repeated the 31% of the developer functional tests, and witnessed the remaining 69% of them.

In addition, the laboratory devised a test subset complementing the test plan provided by the developer. The test plan was executed verifying that the TOE and its TSFIs behaved as expected.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised attack scenarios for penetration tests. Verification and characterization tests were proposed in order to confirm possible attack paths or verify certain countermeasures. The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Basic has been successful in the TOE's operational environment defined in the security target.

EVALUATED CONFIGURATION

The TOE consists of a range of hardware and software components as listed below, which are all developed by Apple.

TOE Component	Version	Description

TOE Component	Version	Description
Apple Wallet App (Wallet)	App part of iOS 18.4	Authentication policy on data and services In-app transaction data management
Application Processor (AP)[2]	A15 Bionic	Authentication policy on data and services In-app transaction data management
Biometric Sensor (Touch ID)	Fingerprint sensor built into the home button of the iPhone SE (3rd generation)	Sensor for fingerprint capture
Boot Loader	iOS 18.4	Allows the device to start and boot the operating system
Secure Enclave	sepOS part of iOS 18.4	Authentication Setup: • Enrollment of the authentication material, • User authentication verification, Authentication Prover: • Passcode verification, • Biometrics matching, • Authentication policy on data
• **SSE**		Manages the pairing between the Secure Enclave and the Secure Element
• **SKS**		Hardware Cryptographic module
• **BioApp**		Provides functionality for processing biometric data and generating biometric templates
iOS Platform	Device operating system platform (iOS 18.4) executing on Application Processor (AP) with the following Apple Pay services that are included in the TOE:	
• **Security Framework**	iOS 18.4	Provides functionality to protect information, establish trust, and control access to software
• **NFCd**	iOS 18.4	Provides functionality for near field communication
• **Safari**	iOS 18.4	Browser
• **Settings**	iOS 18.4	Allows the user to indicate their preferred settings for the device, operating system, and applications
• **Springboard**	iOS 18.4	Provides the functionality for the iOS user interface
Console	Touchscreen of the iPhone SE (3rd generation) Device drivers part of iOS 18.4	Provides the functionality for input/output (I/O)

[2] Only the parts of the AP related to the TSF are included within the TOE scope. The GPU of the AP is not relevant to the TSF and is therefore not part of the TOE.

The hardware that executes all those components is the iPhone SE (3rd generation) with A15 Bionic running iOS 18.4.

EVALUATION RESULTS

The product Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic running iOS 18.4 has been evaluated against the Security Target • Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic Bionic running iOS 18.4: Security Target, v1.3.

All the assurance components required by the evaluation level EAL2 + ADV_FSP.3 and ALC_FLR.3 have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2 + ADV_FSP.3 and ALC_FLR.3, as defined by the Common Criteria 2022 Revision 1 and the CEM:2022.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- To follow the security guidance’s of the TOE strictly.
- To keep the TOE under personal control and set all other security measures available from the environment.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Strong Customer Authentication for Apple Pay on iPhone SE (3rd generation) with A15 Bionic running iOS 18.4, a positive resolution is proposed.

GLOSSARY

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

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, November 2022, CC:2022, Revision 1

[CC_P2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, November 2022, CC:2022, Revision 1

[CC_P3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, November 2022, CC:2022, Revision 1

[CC_P4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, November 2022, CC:2022, Revision 1

[CC_P5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022, Revision 1

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, November 2022, CC:2022, Revision 1

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- <IdST>.

<OR>

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- <IdST>.

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- <IdST LITE>.

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 selected.