Reference: 2018-20-INF-4155- v1
Target: Limitada al expediente
Date: 18.09.2023

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2018-20**
TOE	**SOMA-c007 Machine Readable Electronic Document SSCD Application version 4**
Applicant	**IT12845840151 - HID Global**
References	

[EXT-4075] Certification Request

[EXT-8601] Evaluation Technical Report

Certification report of the product SOMA-c007 Machine Readable Electronic Document SSCD Application version 4, as requested in [EXT-4075], and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-8601] received on 05/07/2023.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SOMA-c007 Machine Readable Electronic Document SSCD Application version 4.

Developer/manufacturer: HID Global

Sponsor: HID Global.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profile: Protection profiles for secure signature creation device – Part 2: Device with key generation, v2.0.1, January 2012, BSI-CC-PP-0059-2009-MA-01.

Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, November 2012, BSI-CC-PP-0071-2012.

Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, November 2012, BSI-CC-PP-0072-2012.

Evaluation Level: Common Criteria version 3.1 R5 - EAL5 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 07/07/2023.

Expiration Date[1]: 15/09/2028.

All the assurance components required by the evaluation level EAL5 (augmented with ALC_DVS.2 and AVA_VAN.5) 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 EAL5 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria version 3.1 R5 and the CEM version 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product SOMA-c007 Machine Readable Electronic Document SSCD Application version 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 is a combination of hardware and software configured to securely create, use, and manage Signature Creation Data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature creation process solely by its Signatory.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature.

The TOE provides the following functions:

1. to generate Signature Creation Data (SCD) and the corresponding Signature Verification Data (SVD),
2. to export the SVD for certification to the CGA over a trusted channel,
3. to prove the identity as SSCD to external entities,
4. to, optionally, receive and store certificate info,
5. to switch the SSCD from a non-operational state to an operational state, and
6. if in an operational state, to create digital signatures for data with the following steps:
   a. select an SCD if multiple are present in the SSCD,
   b. authenticate the Signatory and determine its intent to sign,
   c. receive data to be signed or a unique representation thereof (DTBS/R) from the SCA over a trusted channel,
   d. apply an appropriate cryptographic signature creation function to the DTBS/R using the selected SCD.

The TOE is prepared for the Signatory’s use by:

1. generating at least one SCD/SVD pair, and
2. personalizing for the Signatory by storing in the TOE:
   a. the Signatory’s Reference Authentication Data (RAD),
   b. optionally, certificate info for at least one SCD in the TOE.

After preparation, the SCD shall be in a non-operational state. Upon receiving a TOE, the Signatory shall verify its non-operational state and change the SCD state to operational.

After preparation, the intended legitimate user should be informed of the Signatory’s Verification Authentication Data (VAD) required for use of the TOE in signing. The means of providing this information is expected to protect the confidentiality and the integrity of the corresponding Reference Authentication Data (RAD).

If the use of an SCD is no longer required, then it shall be destroyed.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5 and the evidences required by the additional components ALC_DVS.2 and AVA_VAN.5, according to Common Criteria v3.1 R5.

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.5
	ADV_IMP.1
	ADV_INT.2
	ADV_TDS.4
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.5
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.2
ATE	ATE_COV.2
	ATE_DPT.3
	ATE_FUN.1
	ATE_IND.2
AVA	**AVA_VAN.5**

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the functional requirements, according to Common Criteria v3.1 R5, Part 2 extended and can be found in section 6 Security Requirements of the [ST].

IDENTIFICATION

Product: SOMA-c007 Machine Readable Electronic Document SSCD Application version 4

Security Target: TCAE180037 - SOMA-c007 Machine Readable Electronic Document - Security Target SSCD Application - Recertification, version 1.4, 18.10.2022.

Protection Profile: Protection profiles for secure signature creation device – Part 2: Device with key generation, v2.0.1, January 2012, BSI-CC-PP-0059-2009-MA-01.

Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, November 2012, BSI-CC-PP-0071-2012.

Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, November 2012, BSI-CC-PP-0072-2012.

Evaluation Level: Common Criteria version 3.1 R5 - EAL5 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product SOMA-c007 Machine Readable Electronic Document SSCD Application version 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 the Security Target, section 4.3 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 4.4 Assumptions.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product SOMA-c007 Machine Readable Electronic Document SSCD Application version 4, although the agents implementing attacks have a **High** attack potential according to the assurance level of EAL5 + ALC_DVS.2 + AVA_VAN.5 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 4.2 Threats.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

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

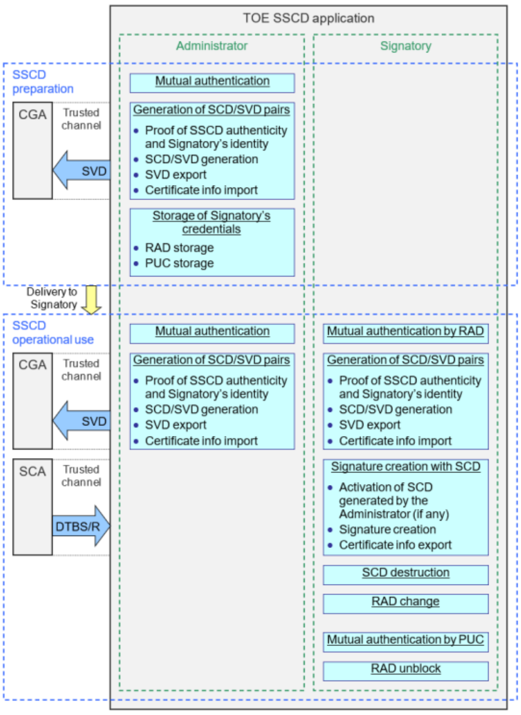
The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 5.2 Security Objectives for the operational Environment.

ARCHITECTURE

LOGICAL SCOPE

The SSCD application of the TOE supports the same SSCD life cycle phases, i.e. SSCD preparation and SSCD operational use, as well as the same SSCD roles, i.e. Administrator and Signatory, as those defined in the PPs [PP-0059] [PP-0071] [PP-072].

The following figure illustrates the operations supported by the SSCD application of the TOE, split according to the SSCD life cycle phases and the SSCD roles for which they are actually available.


TOE SSCD application
Administrator
Signatory
SSCD preparation
CGA
Trusted channel
SVD
Mutual authentication
Generation of SCD/SVD pairs
• Proof of SSCD authenticity and Signatory's identity
• SCD/SVD generation
• SVD export
• Certificate info import
Storage of Signatory's credentials
• RAD storage
• PUC storage
Delivery to Signatory
SSCD operational use
CGA
Trusted channel
SVD
SCA
Trusted channel
DTBS/R
Mutual authentication
Generation of SCD/SVD pairs
• Proof of SSCD authenticity and Signatory's identity
• SCD/SVD generation
• SVD export
• Certificate info import
Mutual authentication by RAD
Generation of SCD/SVD pairs
• Proof of SSCD authenticity and Signatory's identity
• SCD/SVD generation
• SVD export
• Certificate info import
Signature creation with SCD
• Activation of SCD generated by the Administrator (if any)
• Signature creation
• Certificate info export
SCD destruction
RAD change
Mutual authentication by PUC
RAD unblock

PHYSICAL SCOPE

The TOE is comprised of the following parts:

- dual-interface chip Infineon M7892 G12 equipped with IC Dedicated Software (cf. [ST] Appendix A for more details);
- smart card operating system SOMA-c007 version 4;
- a Secure Signature Creation Device (SSCD) application compliant with Commission Implementing Decision (EU) 2016/650 [2016/650/EU] and the Regulation (EU) No 910/2014 [910/2014/EU], repealing the European Parliament Directive 1999/93/EC [1999/93/EU]
- guidance documentation about the initialization of the TOE and the preparation and use of the SSCD application, composed by:
  - the Initialization Guidance,
  - the Pre-personalization Guidance,
  - the Personalization Guidance,
  - the Operational User Guidance.

The following table describes the format, delivery method, recipients and the hash value of each TOE components.

Type	TOE component	Format	Delivery method	Delivery recipient	HASH VALUE (SHA-512)
IC with Dedicated Software and Crypto Library	M7892 G12	Module on chip	Secure courier	-	CF. [M7892], SECTION 10
OS and ICAO Application	SOMA-c007 version 4 Machine Readable Electronic Document (TOE Identification data: 53h 4Fh 4Dh 41h 2Dh 63h 30h	HEX file	Secure IC Manufacturer's Web application	Infineon	2328A2C0C731BC0DC37A63CD7CE80530FB582E24306842890919CFCC1DF8B3C823FA9B970250075AF90AADD55CCF08D5081865211E3C8C74B39DE44ED3DCE94C

	30h 37h 5Fh 34h)				
Document	Initialization Guidance for SOMA-c007 Machine Readable Electronic Document v2.5, ref. TCAE160012	docx	Encrypted email message	Initialization Agent	A67B927BB875030ADD05FDFDD922D52A9C01B95A1CA74AAC2810674EDB1F3626EC89BC3EB9BE89035D34711EB7EF4A42221E30E4EB02C386F8493B7F31A012AE
Document	Pre-personalization Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application v2.4, ref. TCAE160016	docx	Encrypted email message	Pre-personalization Agent	1AABDEAB60484FB75EA5D3DC35654DF1F31622632161CDBC5CAED27DBCEC57B8F22A16C8F4044617E8832F216D9C903126EBA3EC106A7D720A74C2EACE1B2ECF
Document	Personalization Guidance for SOMA-c007 Machine Readable	docx	Encrypted email message	Personalization Agent	49A55FBE96A2DCC8FD10F1502562A9BD6CCDFF511F56EC40160D214AEAF77E68F9853787F551151076B4B9AF415D5DF102A5D67621D3

	Electronic Document SSCD application, version 2.3, ref. TCAE160014				ED2C39D02116CFE33CFE
Document	Operational User Guidance for SOMA-c007 Machine Readable Electronic Document SSCD application, version 2.3, ref. TCAE160015	docx	Encrypted email message	User (Inspection System)	13B258FF3F3078698D1DCDC50A729CF1560309B5985E707550405F3C3EB7E671E0FBD4DACF46DC183F2A8A01507C39979FC8A9DFF57779EF7FBEFC4EE88AA36E

The delivery procedure for the TOE is described in detail in Secure Delivery Procedure, ref. TCAE110027.

DOCUMENTS

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

- Initialization Guidance for SOMA-c007 Machine Readable Electronic Document, version 2.5, ref. TCAE160012.
- Pre-personalization Guidance for SOMA-c007 Machine Readable Electronic Document SSCD application, version 2.3, ref. TCAE160013.
- Personalization Guidance for SOMA-c007 Machine Readable Electronic Document SSCD application, version 2.3, ref. TCAE160014.
- Operational User Guidance for SOMA-c007 Machine Readable Electronic Document SSCD application, version 2.3, ref. TCAE160015.

- Secure Delivery Procedure, version 2.5, ref. TCAE110027.

PRODUCT TESTING

The evaluation has been performed according to the Composite Evaluation Scheme as defined in the guides [JILCOMP] and [JILADVARC] in order to assess that the combination of the TOE with the underlying platform did not lead to any exploitable vulnerability.

This evaluation has then taken into account the evaluation results and security recommendations for the platform which is part of the evaluated composite TOE, and was already certified with certificate BSI-DSZ-CC-0891-V6-2021.

The developer has executed test for all the declared security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process, each test unit has been executed to check that the declared security functionality has been identified and also to check that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using a 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 evaluation team has applied a sampling strategy and has concluded that the information is complete and coherent enough to reproduce tests and identify the functionality tested. Moreover, the evaluation team has planned and executed additional tests independently of those executed by the developer.

The obtained results have been checked to be conformant to the expected results and in cases where a deviation relative to the expected results has been detected the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

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 according to JIL supporting documents [JILAAPS] and [JILADVARC]. Within these activities all aspects of the security architecture which were not covered by functional testing have been considered.

The implementations of the requirements of the provided platform’s ETR for Composition and guidance, as well as of the security mechanisms of the TOE in general have been verified by the evaluation team. An appropriate test set was devised to cover these potential vulnerabilities.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the High attack potential has been successful in the TOE’s operational environment as defined in the security target when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the SOMA-c007 Machine Readable Electronic Document SSCD Application version 4 it is not necessary any additional software or hardware components.

The version of the software may be retrieved by following the procedure in section 4.2 (Retrieval of TOE, product and chip information) of the "Initialization Guidance for SOMA-c007 Machine Readable Electronic Document, version 2.5, ref. TCAE160012".

To identify the TOE is necessary for the initialization agent to execute the "GET DATA (Even INS)" command with P1 = 01h and P2 = 20h. APDU shall be encoded as follows:

- CLA = E0h
- INS = CAh
- P1 = 01h
- P2 = 20h
- LE = 00h

The e-Document certified under Common Criteria v.3.1 at the EAL5+ security assurance level shall return SOMA-c007_4 (ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 30h 30h 37h 5Fh 34h), representing the TOE Identification Data.

EVALUATION RESULTS

The product SOMA-c007 Machine Readable Electronic Document SSCD Application version 4 has been evaluated against the Security Target TCAE180037 - SOMA-c007 Machine Readable Electronic Document - Security Target SSCD Application - Recertification, version 1.4, 18.10.2022.

All the assurance components required by the evaluation level EAL5 + ALC_DVS.2 + AVA_VAN.5 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 EAL5 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria version 3.1 R5 and the CEM version 3.1 R5.

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.

The evaluation team makes the following security recommendations:

- 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.
- To periodically review the status of the certification of the underlying platform.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product SOMA-c007 Machine Readable Electronic Document SSCD Application version 4, a positive resolution is proposed.

The certifier strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on guidance documents as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

Some of the key lengths for some of the cryptographic mechanisms defined in the ST are considered as legacy mechanisms according to [ACM]. Please check [ACM] to consult recommended dates to sunset the applicable key lengths.

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:

[1999/93/EU] European Parliament: Directive 1999/93/EC on a Community framework for electronic signatures, December 1999.

[2016/650/EU] European Parliament: Commission Implementing Decision (EU) 2016/650, 25 April 2016.

[910/2014/EU] European Parliament: Regulation (EU) No 910/2014 of the European Parliament and of the Council, 23 July 2014.

[ACM] SOG-IS agreed cryptographic mechanisms, version 1.3. SOG-IS crypto working group. February 2023.

[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]Joint Interpretation Library. Application of Attack Potential to Smartcards, version 3.2. Nov.2022.

[JILADVARC] Joint Interpretation Library. Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.1, Jul, 2021.

[JILCOMP] Joint Interpretation Library. Composite Product evaluation for Smart Cards and similar devices, version 1.5.1. May 2018.

[M7892] Infineon: Security Target Lite, Common Criteria EAL6 augmented / EAL6+, M7892 Design Steps D11 and G12, Document version 3.6 as of 2021-10-06.

[PP-0059] CEN: Protection profiles for secure signature creation device, Part 2: Device with Key Generation, version 2.0.1, ref. BSI-CC-PP-0059-2009-MA-01, January 2012.

[PP-0071] CEN: Protection profiles for secure signature creation device, Part 4: Extension for device with key generation and trusted communication with certificate generation application, version 1.0.1, ref. BSI-CC-PP-0071-2012, November 2012.

[PP-0072] CEN: 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, ref. BSI-CC-PP-0072-2012, November 2012.

[ST] TCAE180037 - SOMA-c007 Machine Readable Electronic Document - Security Target SSCD Application - Recertification, version 1.4, 18.10.2022.

SECURITY TARGET / SECURITY TARGET LITE

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:

- TCAE180037 - SOMA-c007 Machine Readable Electronic Document - Security Target SSCD Application - Recertification, version 1.4, 18.10.2022.

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:

- TCLE180038 - SOMA-c007 Machine Readable Electronic Document - Security Target SSCD Application - Recertification, version 1.3, 06.03.2023.

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.