

Reference: 2021-22-INF-4236- v1  
Target: Limitada al expediente  
Date: 15.01.2024

Created by: I003  
Revised by: CALIDAD  
Approved by: TECNICO

## CERTIFICATION REPORT

---

Dossier #	<b>2021-22</b>
TOE	<b>Samsung STRONG_V2P10_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0</b>
Applicant	<b>124-81-00998 - SAMSUNG Electronics Co. Ltd</b>
References	
	[EXT-6771] Certification Request
	[EXT-8801] Evaluation Technical Report

---

Certification report of the product Samsung STRONG\_V2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0, as requested in [EXT-6771] dated 08/04/2021, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-6771] received on 09/11/2023.

## CONTENTS

EXECUTIVE SUMMARY .....	3
TOE SUMMARY.....	3
SECURITY ASSURANCE REQUIREMENTS .....	4
SECURITY FUNCTIONAL REQUIREMENTS.....	5
IDENTIFICATION .....	6
SECURITY POLICIES.....	6
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT .....	7
CLARIFICATIONS ON NON-COVERED THREATS .....	7
OPERATIONAL ENVIRONMENT FUNCTIONALITY .....	7
ARCHITECTURE.....	7
LOGICAL SCOPE .....	7
PHYSICAL SCOPE.....	8
DOCUMENTS.....	9
PRODUCT TESTING.....	10
EVALUATED CONFIGURATION .....	10
EVALUATION RESULTS .....	11
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM .....	12
CERTIFIER RECOMMENDATIONS.....	12
GLOSSARY .....	12
BIBLIOGRAPHY .....	12
SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE).....	13
RECOGNITION AGREEMENTS .....	14
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA).....	14
International Recognition of CC – Certificates (CCRA).....	14

## EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Samsung STRONG\_V2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0.

The TOE is a Secure Sub-Systems implemented in a SoC, which is designed and packaged specially for mobile applications.

**Developer/manufacturer:** SAMSUNG Electronics Co. Ltd

**Sponsor:** SAMSUNG Electronics Co. Ltd.

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

**ITSEF:** Applus Laboratories.

**Protection Profile:** Eurosmart Security IC Platform Protection Profile with Augmentation Packages, version 1.0, BSI-CC-PP-0084-2014.

**Evaluation Level:** Common Criteria v3.1 R5 EAL5+AVA\_VAN.5+ALC\_CMC.5+ALC\_DVS.2+ALC\_TAT.3.

**Evaluation end date:** 27/11/2023.

**Expiration Date<sup>1</sup>:** 06/01/2029.

All the assurance components required by the evaluation level EAL5 (augmented with AVA\_VAN.5 + ALC\_CMC.5 + ALC\_DVS.2 + ALC\_TAT.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 EAL5 + AVA\_VAN.5 + ALC\_CMC.5 + ALC\_DVS.2 + ALC\_TAT.3, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Samsung STRONG\_V2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0, a positive resolution is proposed.

## TOE SUMMARY

The Target of Evaluation (TOE), the STRONGV2P10\_LN04LPE secure subsystem featuring the TORNADO-H cryptographic coprocessor, is a Hard macro instantiated within an SOC which is composed of a processing unit, security components, hardware circuit for testing purpose during the manufacturing process and volatile and non-volatile memories (hardware). The TOE also

---

<sup>1</sup> This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in an STRONGV2P10\_LN04LPE after being delivered by the IC Manufacturer. Such software (also known as IC bootloader/firmware) is used for providing additional services to facilitate the usage of the hardware and/or to provide additional services, a random number generation library and a random number generator. All other software is called Security IC Embedded Software and is not part of the TOE. The SoC S5E9925 is necessary to operate the STRONGV2P10\_LN04LPE but it is not TOE hardware. The Security IC Embedded Software is initially stored in encrypted form in external NVM (Flash).

Regarding the public key cryptographic libraries, the user has the possibility to tailor this IC Dedicated Software part of the TOE during the manufacturing process by deselecting the public key cryptographic libraries. Hence the TOE can be delivered with or without the functionality of the public key cryptographic libraries what is resulting in two TOE configurations. This is considered in this Security Target and corresponding notes (indicated by “optional”) are added where required. If the user decides not to use the public key cryptographic libraries, the library is not delivered to the user and the accompanying RSA and Elliptic Curve cryptographic mechanisms are not provided by the TOE.

## 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 AVA\_VAN.5 + ALC\_CMC.5 + ALC\_DVS.2 + ALC\_TAT.3 to the table, 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.5
	ALC_CMS.5

	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.3
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 following functional requirements, according to the Common Criteria v3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS
FAU_SAS.1
FCS_CKM.1/ECDSA
FCS_CKM.1/RSA
FCS_CKM.5
FCS_COP.1/AES
FCS_COP.1/ECDH
FCS_COP.1/ECDSA
FCS_COP.1/HMAC
FCS_COP.1/RSA
FCS_COP.1/SHA
FCS_COP.1/SHA_HW
FCS_COP.1/TDES
FCS_COP.1/X25519
FCS_RNG.1/DRG.3
FCS_RNG.1/PTG.2
FDP_ACC.1
FDP_ACC.1/Loader
FDP_ACF.1
FDP_ACF.1/Loader
FDP_DAU.2/PM
FDP_IFC.1
FDP_IRA.1/PM
FDP_ITT.1
FDP_SDC.1
FDP_SDC.1/PM

FDP_SDI.2
FDP_SDI.2/PM
FDP_UCT.1
FDP_UIT.1
FDP_URC.1/PM
FIA_API.1
FIA_UID.1/PM
FMT_LIM.1/Debug
FMT_LIM.1/Test
FMT_LIM.2/Debug
FMT_LIM.2/Test
FMT_MSA.1
FMT_MSA.3
FMT_SMF.1
FPT_FLS.1
FPT_ITT.1
FPT_PHP.3
FPT_RPL.1/PM
FRU_FLT.2
FTP_ITC.1

## IDENTIFICATION

**Product:** Samsung STRONG\_V2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0

**Security Target:** STRONGV2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software, version 2.7 (04/09/2023).

**Protection Profile:** Eurosmart Security IC Platform Protection Profile with Augmentation Packages, version 1.0, BSI-CC-PP-0084-2014.

**Evaluation Level:** Common Criteria v3.1 R5 EAL5+AVA\_VAN.5+ALC\_CMC.5+ALC\_DVS.2+ALC\_TAT.3.

## SECURITY POLICIES

The use of the product Samsung STRONG\_V2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0 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 3.3 (“*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 3.4 (“*Assumptions*”).

## **CLARIFICATIONS ON NON-COVERED THREATS**

The following threats do not suppose a risk for the product Samsung STRONG\_V2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0, although the agents implementing attacks have the attack potential according to the High of EAL5 + AVA\_VAN.5 + ALC\_CMC.5 + ALC\_DVS.2 + ALC\_TAT.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 3.2 (“*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 4.3 (“*Security Objectives for the Operational Environment*”).

## **ARCHITECTURE**

### **LOGICAL SCOPE**

The CORTEX-M35P CPU architecture of STRONGV2P10\_LN04LPE follows the Harvard architecture, that is, it has separate program and data memories. Using those separate memory access paths, both instruction and data can be fetched simultaneously without causing a stall.

The main security features of the TOE are:

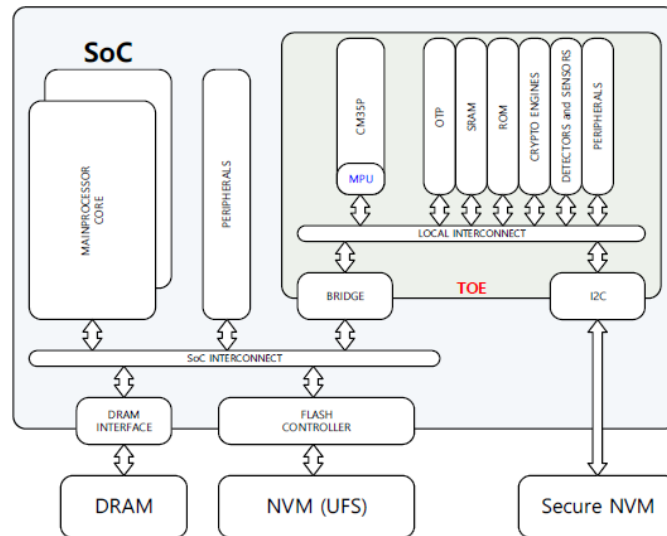
- Security sensors or detectors including High and Low Temperature detectors, High and Low Supply Voltage detectors, Supply Voltage Glitch detector and Laser detector.

- Active Shields against physical intrusive attacks.
- Life time detector for detecting if detector signals are modified or not.
- Dedicated tamper-resistant design based on synthesizable glue logic and secure topology.
- Dedicated hardware mechanisms against side-channel attacks such as Random Branch insertion and ROM and SRAM encryption mechanisms.
- Secure TDES, AES (AES in CRYPTO block and AES in Security Controller block) Symmetric Cryptography support.
- Key Manager (KDF).
- ECC/ Parity / CRC-32 calculators.
- One Hardware True Random Number Generator (TRNG) that meet PTG.2 class of BSI AIS31 (German scheme).
- SHA256/384/512 based on HASH standard-NIST FIPS 180-4 in Security Controller block.
- SHA2-based HMAC in Security Controller block.
- Direct Memory Access (SC\_DMA).
- Secure AHB Bridge(XIP).
- The IC Dedicated Software includes:
  - The optional modular arithmetic libraries for the support of RSA and ECC (with SHA) cryptographic operations (optional)
  - TRNG library built around Hardware TRNG together with corresponding TRNG application notes. This library meets PTG.2 class of BSI-AIS31 (German scheme).
  - DRBG library is for deterministic random bit generator as specified in NIST SP 800-90A and FIPS 197 using seed from TRNG. This library meets DRG.3 class of BSI-AIS31 (German scheme).
  - Boot Loader includes the loader for the SoC and for TOE booting (Secure Bootloader) and it copies the embedded software from external FLASH storage into the internal SRAM

## **PHYSICAL SCOPE**

The physical architecture is depicted in the following figure. The TOE is delimited by the green area.





## DOCUMENTS

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

Item type	Item	Version	Form of delivery
Document	HW TRNG and TRNG Library Application Note (STRONGV2P10_TRNG_HS_MRO9_Library_Application_Note_v1.1.pdf)	1.1	Softcopy
Document	DRBG Library Application Note (STRONGV2P10_DRBG_Library_Application_Note_v1.6.pdf)	1.6	Softcopy
Document	AH2 RSA/ECC Library API Manual (AH2 RSA ECC SHA Library API Manual v1.14 .pdf)	1.14	Softcopy. This document is optional
Document	Hardware User's manual (STRONGV2P10_LN04LPE of S5E9925 Hardware_UM_v1.0.pdf)	1.0	Softcopy
Document	Security Application Note (SAN_S5E9925_v0.5.pdf)	0.5	Softcopy
Document	Chip Delivery Specification (DeliverySpec_S5E9925 Rev0.5.pdf)	0.5	Softcopy
Document	Bootloader User's Manual (STRONGV2P10_LN04LPE_Secure_Boot Loader_Manual_v0.8.pdf)	0.8	Softcopy
Document	CPU Reference Manual (Cortex M35P_Reference_Manual_v0.0.pdf)	0.0	Softcopy

## PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with 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 developed 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 applied sampling strategy and has concluded that the information is complete and coherent enough to reproduce tests and identify the functionality tested. Through the tests performed by the Laboratory, it is concluded that 42,42% of the developer tests were covered.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product. Through the tests performed by the Laboratory it is concluded that 77,77% of the SFRs and 87,5% of the TSFI groups defined in the Functional Specification.

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment [JILAAPS], the evaluation team has devised vulnerability analysis and attack scenarios for penetration testing according to JIL supporting documents [JILAAPS] and [JILADVARCS]. Within these activities all aspects of the security architecture which were not covered by functional testing have been considered.

No attack scenario with the attack potential High according to Common Criteria v3.1 R5 has been successful in the TOE's operational environment as defined in the Security Target when all security measures required by the developer are applied.

## EVALUATED CONFIGURATION

The TOE is defined by its commercial name and version STRONGV2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0.

The TOE hardware components are:

Item type	Item	Version	Form of delivery
Hard macro	STRONGV2P10_LN04LPE Hard macro, Secure Element Platform	1.0	Hard macro instantiated within an SOC packaged PoP
Hardware	Package SoC	1298-FCMSP-14.0X13.9	PoP(Package-on-
Hardware	SoC S5E9925 embedding the STRONGV2P10_LN04LPE hard macro	1.2	SOC packaged PoP

The TOE software comprises the following components:

- The optional modular arithmetic libraries for the support of RSA and ECC (with SHA) cryptographic operations (optional)
- TRNG library built around Hardware TRNG together with corresponding TRNG application notes. This library meets PTG.2 class of BSI-AIS31 (German scheme).
- DRBG library is for deterministic random bit generator as specified in NIST SP 800-90A and FIPS 197 using seed from TRNG. This library meets DRG.3 class of BSI-AIS31 (German scheme).
- Boot Loader includes the loader for the SoC and for TOE booting (Secure Bootloader) and it copies the embedded software from external FLASH storage into the internal SRAM

The acceptance procedure for the evaluated configuration of the TOE is described in document “*Chip Delivery Specification*”, version 0.5.

Here it is reminded that to fulfil the requirements defined in the Security Target, the TOE consumer must strictly follow the security recommendations that can be found on documents Security Application Note For STRONGV2P10\_LN04LPE of S5E9925 (version 0.5), STRONGV2P10\_LN04LPE HW TRNG HS\_MRO9 and TRNG HS\_MRO9 Library Application Note (revision 1.1), STRONGV2P10\_LN04LPE DRBG library Application Note (revision 1.6) and PKA Library API Manual (AH2 RSA/ECC/SHA Library API Manual v1.14) as well as to observe the operational environment requirements and assumptions defined in the applicable Security Target.

The TOE also includes the documents identified in section “DOCUMENTS” of this certification report that shall be distributed and made available together to the users of the evaluated version.

## EVALUATION RESULTS

The product Samsung STRONG\_V2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0 has been evaluated against the Security Target STRONGV2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software, version 2.7 (04/09/2023).

All the assurance components required by the evaluation level EAL5 + AVA\_VAN.5 + ALC\_CMC.5 + ALC\_DVS.2 + ALC\_TAT.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 EAL5 + AVA\_VAN.5 + ALC\_CMC.5 + ALC\_DVS.2 + ALC\_TAT.3., as defined by the Common Criteria v3.1 R5 and the CEM v3.1 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.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Samsung STRONG\_V2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software revision 1.0, 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, 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. Joint Interpretation Library. Version 3.1. June 2020. Joint Interpretation Library.

[JILADVARCS] Security Architecture requirements (ADV\_ARC) for Smart Cards and similar devices, version 2.0. January 2012. Joint Interpretation Library.

[ST] Security Target of STRONGV2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software, version 2.7 (04/09/2023).

[ST Lite] Security Target Lite of STRONGV2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software, version 0.0 (06/09/2023).

## **SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)**

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:

- Security Target of STRONGV2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software, version 2.7 (04/09/2023).

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:

- Security Target Lite of STRONGV2P10\_LN04LPE of S5E9925 with Specific IC Dedicated Software, version 0.0 (06/09/2023).

## 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.