Reference: 2015-11-INF-3525- v2
Target: Limitada al expediente
Date: 17.06.2021

Created by: CERT9
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2015-11**
TOE	**Positive Technologies Application Firewall 3.6.3.758**
Applicant	**1077761087117 - Positive Technologies**
References	

[Tipo-Código] Ref - Description

Certification report of the product Positive Technologies Application Firewall 3.6.3.758, as requested in [EXT-2781] dated 22/07/2015, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [Tipo-6562] received on 19/02/2021.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Positive Technologies Application Firewall 3.6.3.758.

The PT Application Firewall (TOE) is a self-learning web application firewall designed to reduce the risks of application attacks if they occur. PT AF applies algorithms to analyze the traffic specifics and the activity of the users who use the applications. Information about the standard user activity is applied to detect potential attacks and deviations in typical user behaviour.

Developer/manufacturer: Positive Technologies

Sponsor: Positive Technologies.

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

ITSEF: DEKRA Testing and Certification S.A.U.

Protection Profile: ---.

Evaluation Level: EAL2+ (ALC_FLR.2)

Evaluation end date: 25/05/2021

Expiration Date[1]: 18/06/2026

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.2) have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2+ (ALC_FLR.2)., as defined by the CC v 3.1 R5 and the CEM v 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Positive Technologies Application Firewall 3.6.3.758, a positive resolution is proposed.

TOE SUMMARY

The PT Application Firewall (TOE) is a self-learning web application firewall designed to reduce the risks of application attacks if they occur. PT AF applies algorithms to analyze the traffic specifics and the activity of the users who use the applications. Information about the standard user activity is applied to detect potential attacks and deviations in typical user behavior.

The TOE can manage network traffic in multiple modes:

- In Sniffer Mode, traffic is analyzed without blocking requests and preventing attacks.

[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.

- In Reverse Proxy Mode, analysis of all requests to a Web application with the possibility of active prevention attacks is performed. The mode is designed to protect the Web application as much as possible: requests are possible only after processing them.
- In Transparent Proxy Mode, all HTTP requests to the web application are analyzed with the ability to actively prevent attacks in transparent mode. The TOE operation in this mode is similar to the reverse proxy mode, but does not require changes in the settings of the protected application and network infrastructure.
- Bridge Mode is designed to detect intrusions without interfering with the operation of applications. When connecting to the bridge scheme, the TCP session does not break, so the TOE does not affect the functioning of the protected application

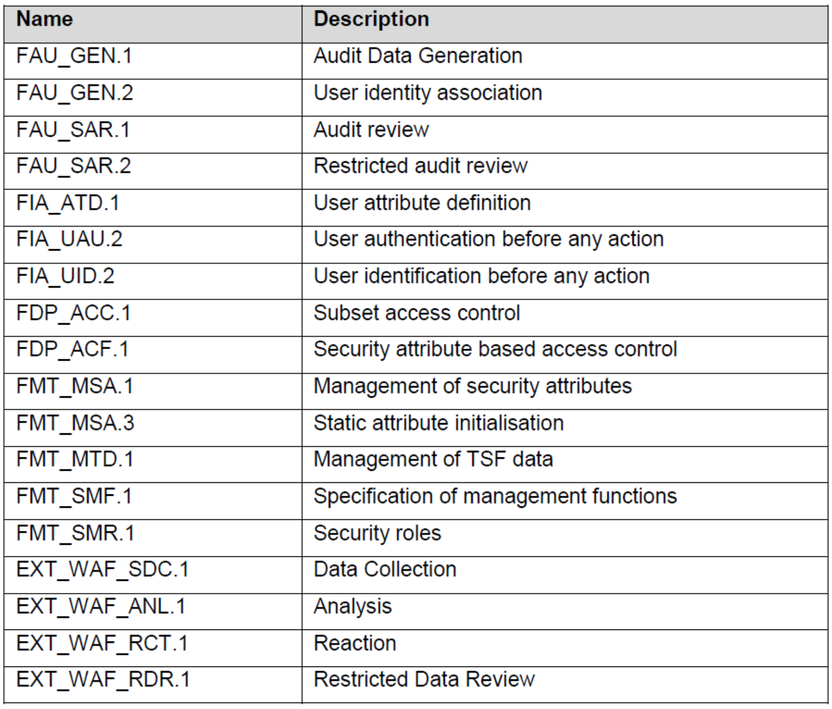
SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 (see table below) and the evidences required by the additional component ALC_FLR.2, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
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 v3.1 R5:



Name	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
EXT_WAF_SDC.1	Data Collection
EXT_WAF_ANL.1	Analysis
EXT_WAF_RCT.1	Reaction
EXT_WAF_RDR.1	Restricted Data Review

IDENTIFICATION

Product: Positive Technologies Application Firewall 3.6.3.758

Security Target: Positive Technologies Application Firewall Common Criteria Certification Security Target, version 2.9, February 2020.

Protection Profile: N/A

Evaluation Level: EAL2+ (ALC_FLR.2).

SECURITY POLICIES

The use of the product Positive Technologies Application Firewall 3.6.3.758 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 3.4 ("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 3.5 (“Assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Positive Technologies Application Firewall 3.6.3.758, although the agents implementing attacks have the attack potential according to the basic attack potential of EAL2 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 3.3 (“Threats”).

OPERATIONAL ENVIRONMENT FUNCTIONALITY

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

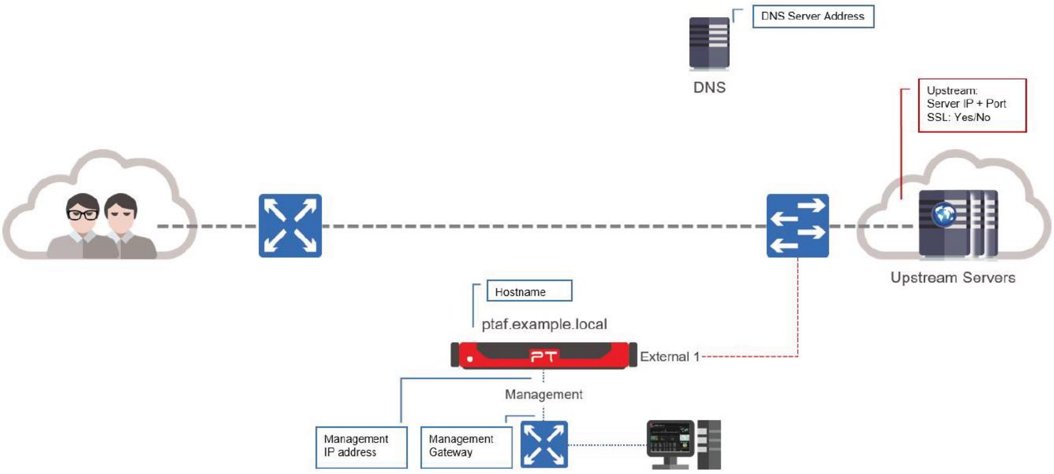
The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 (“Security Objectives for the operational Environment”).

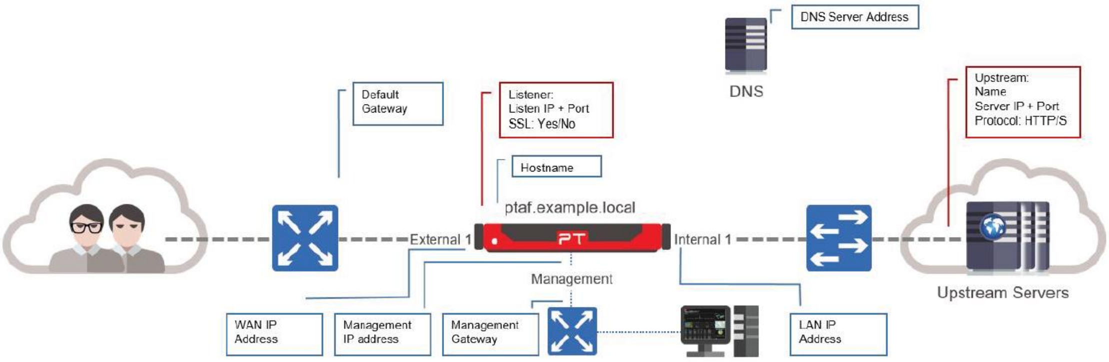
ARCHITECTURE

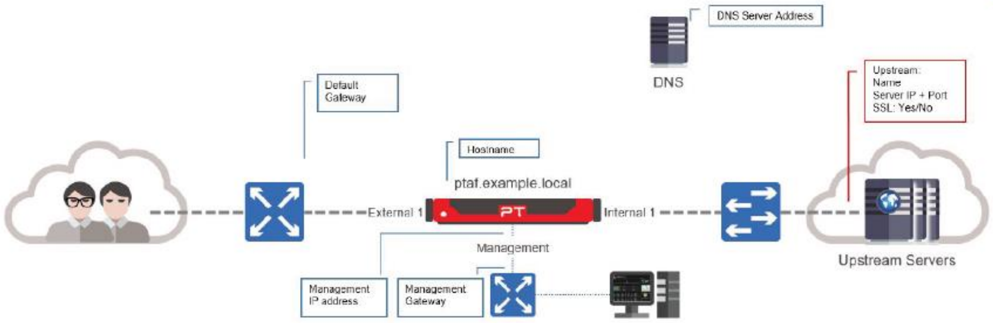
LOGICAL ARCHITECTURE

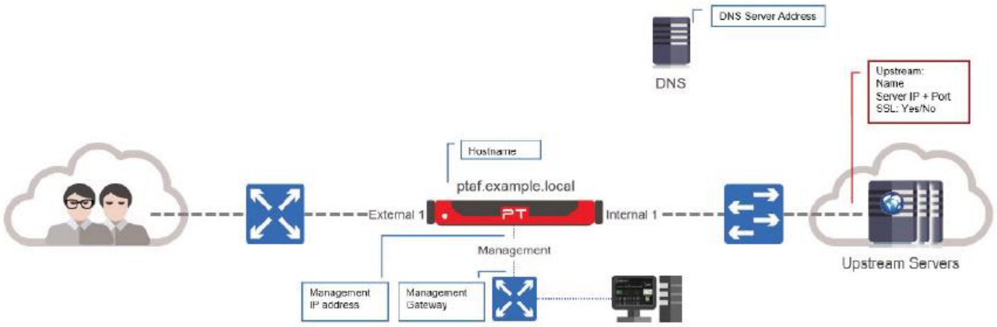
The PT Application Firewall (TOE) is a self-learning web application firewall designed to reduce the risks of application attacks if they occur. PT AF applies algorithms to analyze the traffic specifics and the activity of the users who use the applications. Information about the standard user activity is applied to detect potential attacks and deviations in typical user behavior.

The TOE can manage network traffic in multiple modes:


DNS Server Address
DNS
Upstream:
Server IP + Port
SSL: Yes/No
Upstream Servers
Hostname
ptaf.example.local
PT
External 1
Management
Management
IP address
Management
Gateway


DNS Server Address
DNS
Default
Gateway
Listener:
Listen IP + Port
SSL: Yes/No
Upstream:
Name
Server IP + Port
Protocol: HTTP/S
Hostname
ptaf.example.local
External 1
PT
Internal 1
Upstream Servers
Management
WAN IP
Address
Management
IP address
Management
Gateway
LAN IP
Address





In Sniffer Mode, traffic is analyzed without blocking requests and preventing attacks.

In Reverse Proxy Mode, analysis of all requests to a Web application with the possibility of active prevention attacks is performed. The mode is designed to protect the Web application as much as possible: requests are possible only after processing them.

In Transparent Proxy Mode, all HTTP requests to the web application are analyzed with the ability to actively prevent attacks in transparent mode. The TOE operation in this mode is similar to the reverse proxy mode, but does not require changes in the settings of the protected application and network infrastructure.

Bridge Mode is designed to detect intrusions without interfering with the operation of applications. When connecting to the bridge scheme, the TCP session does not break, so the TOE does not affect the functioning of the protected application

PHYSICAL ARCHITECTURE

Depending on the modes explained in the logical architecture, the physical architecture will be different according to the pictures.

DOCUMENTS

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

№	Item	Description
1	TOE – PT Application Firewall virtual machine	File: *pt_application_firewall_3.6.3.758.ova* Hash (SHA256): *20a7ec952a073adc5d7de4f4969758899c69888a4dd4d79f577efa7e2961f5b7*
2	PT Application Firewall Administrator Guide	File: PT_AG_1.8.pdf Hash (SHA256): *dd5851d405bacb3a1726955732a10ebaa477c006c5b72c362618d4dc4ce83b00*
3	PT Application Firewall Quick Start Guide	File: *PT_QSG_1.5.pdf* Hash (SHA256): *a858e5f7cbfdfc28df96b0cf3bd62dbb80e90e2498cf602e846f6abc46fa294b*
4	PT Application Firewall – Guidance Addendum	File: PT_AGD_2.0.pdf Hash (SHA256): *ce5bf92baf20656e483c8a67f750de0de29bb737b0bad6c88033d4aa37d94b41*

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 repeated all the developer functional tests in the developer premises. Likewise, he has selected and repeated the developer functional tests in the testing platform implemented in the evaluation laboratory, selecting one test for each of the most relevant functional class.

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.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Positive Technologies Application Firewall 3.6.3.758 it is necessary the disposition of the following software components:

№	**Item**	**Description**
1	TOE – PT Application Firewall virtual machine	File: *pt_application_firewall_3.6.3.758.ova* Hash (SHA256): *20a7ec952a073adc5d7de4f4969758899c69888a4dd4d79f577efa7e2961f5b7*
2	PT Application Firewall Administrator Guide	File: PT_AG_1.8.pdf Hash (SHA256): *dd5851d405bacb3a1726955732a10ebaa477c006c5b72c362618d4dc4ce83b00*
3	PT Application Firewall Quick Start Guide	File: *PT_QSG_1.5.pdf* Hash (SHA256): *a858e5f7cbfdfc28df96b0cf3bd62dbb80e90e2498cf602e846f6abc46fa294b*
4	PT Application Firewall – Guidance Addendum	File: PT_AGD_2.0.pdf Hash (SHA256): *ce5bf92baf20656e483c8a67f750de0de29bb737b0bad6c88033d4aa37d94b41*

The TOE is deployed on ESXi 6.0 Hypervisor as a virtual machine.

It has been provisioned with the following hardware and software requirements:

- PTAF – Virtual machine:
    - X86-64 Compatible processor

- 16GB of RAM
- 300GB of persistence storage
- Debian 7.8 “Wheezy” as operating system
- Including PT Application Firewall (version 3.6.3.758)

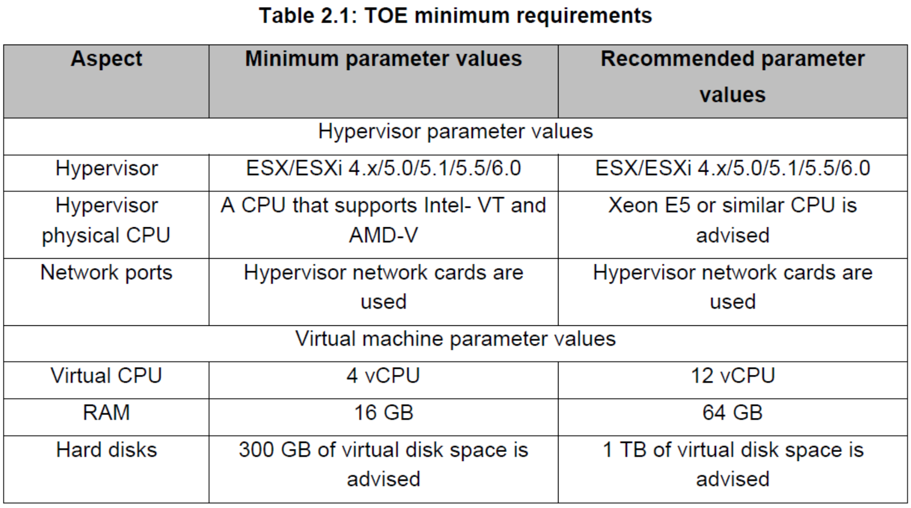


Table 2.1: TOE minimum requirements

Aspect	Minimum parameter values	Recommended parameter values
Hypervisor parameter values		
Hypervisor	ESX/ESXi 4.x/5.0/5.1/5.5/6.0	ESX/ESXi 4.x/5.0/5.1/5.5/6.0
Hypervisor physical CPU	A CPU that supports Intel- VT and AMD-V	Xeon E5 or similar CPU is advised
Network ports	Hypervisor network cards are used	Hypervisor network cards are used
Virtual machine parameter values		
Virtual CPU	4 vCPU	12 vCPU
RAM	16 GB	64 GB
Hard disks	300 GB of virtual disk space is advised	1 TB of virtual disk space is advised

EVALUATION RESULTS

The product Positive Technologies Application Firewall 3.6.3.758 has been evaluated against the Security Target “Positive Technologies Application Firewall Common Criteria Certification Security Target, version 2.9, February 2020”.

All the assurance components required by the evaluation level EAL2+ (ALC_FLR.2) have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2+ (ALC_FLR.2), as defined by the Common Criteria for Information Technology Security Evaluation Version 3.1 R5 and the Common Criteria for Information Technology Security Evaluation Methodology 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 TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment.

- The fulfillment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product DEKRA Testing and Certification S.A.U., 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.

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: Positive Technologies Application Firewall Common Criteria Certification Security Target, version 2.9, February 2020

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.org.

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 SOGIS-MRA for all assurance components selected.