Reference: 2017-23-INF-2630-v1
Target: Expediente
Date: 11.12.2018

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2017-23**
TOE	**Big Switch Networks Big Cloud Fabric 4.7.0**
Applicant	**4804334 - Big Switch Networks, Inc.**

References

[EXT-3456] Certification Request

[EXT-4492] Evaluation Technical Report

Certification report of the product Big Switch Networks Big Cloud Fabric 4.7.0, as requested in [EXT-3456] dated 20/06/2017, and evaluated by Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-4492] received on 23/10/2018.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Big Switch Networks Big Cloud Fabric 4.7.0.

Big Switch Networks Big Cloud Fabric 4.7.0 software is a Software-Defined Network (SDN) that provides network scalability and resilience, centralized network management and automation for data centres, and reduced costs due to the disaggregation of network device hardware and software through the use of brite-box switches. Big Cloud Fabric (BCF) provides Layer 2 (L2) switching, Layer 3 (L3) routing, and higher layer services through service insertion and chaining.

Developer/manufacturer: Big Switch Networks, Inc.

Sponsor: Big Switch Networks, Inc..

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

ITSEF: Epoche and Espri.

Protection Profile: None.

Evaluation Level: Common Criteria EAL2+ ALC_FLR.2.

Evaluation end date: 23/10/2018.

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.2) have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2, 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 Big Switch Networks Big Cloud Fabric 4.7.0, a positive resolution is proposed.

TOE SUMMARY

BCF is installed on a Clos architecture switching fabric comprised of dual BCF Controllers configured in a High Availability (HA) cluster, and leaf-spine switches (see Figure 2). The HA cluster provides redundancy for continued network management and traffic forwarding in the event of a controller failure. The leaf-spine architecture optimizes bandwidth between switch ports within the data centre by creating a high-capacity fabric using multiple spine switches that interconnect the edge ports on each leaf switch. This design provides consistent latency and minimizes the hops between servers in different racks. The fabric design is modular and scalable; leaf switches can be added to increase the number of switch edge ports, whereas fabric bandwidth can be increased by adding more spine switches.

The fabric traffic is separated into control, management, and data networks. Control network traffic includes the configurations and policies pushed from the BCF Controller to the switches running Switch Light OS. Control network traffic is secured using SSH and TLS v1.2. The management network traffic includes traffic between the BCF Controller and the management console, RADIUS server, and Operational Environment (OE) components. Management network traffic is secured using HTTPS, SSH, and TLS v1.2. Data network traffic includes production data between the leaf and spine switches. Production data from other networks in the data centre or the internet can only ingress and egress the TOE via a leaf switch. This includes external production data from other networks, internal or external to the data centre, or the Internet.

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 ALC_FLR.2, according to Common Criteria v3.1 R5.

Class	**Family/Component**
ASE: Security Target Evaluation	ASE_CCL.1 , ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1 and ASE_TSS.1
ADV: Development	ADV_ARC.1, ADV_FSP.2 and ADV_TDS.1
AGD: Guidance documents	AGD_OPE.1 and AGD_PRE.1
ALC: Life cycle support	ALC_CMC.2, ALC_CMS.2, ALC_DEL.1 and ALC_FLR.2
ATE: Tests	ATE_COV.1, ATE_FUN.1 and ATE_IND.2
AVA: Vulnerability assessment	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to Common Criteria v3.1 R5:

Class	Component
FAU (Security Audit)	FAU_GEN.1 - Audit Data Generation FAU_GEN.2 - User Identity Association FAU_SAR.1 - Audit review
Cryptographic Support (FCS)	FCS_CKM.1 - Cryptographic key generation FCS_CKM.4 - Cryptographic key destruction FCS_COP.1 - Cryptographic operation

User Data Protection (FDP)	FDP_IFC.1(a) - Subset information flow control (BCF Controller)
	FDP_IFC.1(b) - Subset information flow control (BCF Switch)
	FDP_IFF.1(a) - Simple security attributes (BCF Controller)
	FDP_IFF.1(b) - Simple security attributes (BCF Switch)

Identification and Authentication (FIA)	FIA_UAU.2 - User authentication before any action FIA_UAU.5 - Multiple authentication mechanisms FIA_UAU.7 - Protected authentication feedback FIA_UID.2 - User authentication before any action
Security Management (FMT)	FMT_MSA.1(a) - Management of security attributes (BCF Controller) FMT_MSA.1(b) - Management of security attributes (BCF Switch) FMT_MSA.3(a) - Static attribute initialization (BCF Controller) FMT_MSA.3(b) - Static attribute initialization (BCF Switch) FMT_SMF.1 - Specification of management functions FMT_SMR.1 - Security roles
Protection of the TSF (FPT)	FPT_FLS.1 - Failure with preservation of secure state FPT_ITT.1 - Basic internal TSF data transfer protection
TOE Access (FTA)	FTA_SSL.4 - User-initiated termination
Trusted Path/Channel (FTP)	FTP_ITC.1 - Inter-TSF trusted channel FTP_TRP.1 - Trusted path

IDENTIFICATION

Product: Big Switch Networks Big Cloud Fabric 4.7.0

Security Target: Big Switch Networks Big Cloud Fabric 4.7.0 Security Target, v 0.8, October 5 2018

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL2 + ALC_FLR.2

SECURITY POLICIES

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this Security Target.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.3 (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.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.1 (Threats to Security), do not suppose a risk for the product Big Switch Networks Big Cloud Fabric 4.7.0, 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.

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 detailed in [ST], chapter 4.2 (Security objectives for the operational environment).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is separated into various subsystems that provide the TOE Security Functions. A diagram illustrating the different subsystems and TOE Security Functionality Interfaces (TSFIs) that compose the TOE (see Figure 1).

The TOE boundary does not include the hardware on which the software-only TOE is installed or any of the other operational environment components shown in

Figure 1. The TOE boundary includes the TOE's two software components BCF 4.7.0 and Switch Light OS 4.7.0, and the subsystems and TSFIs in the following table:

TOE Component	Subsystem	TSFI
BCF 4.7.0	Controller Subsystem	GUI
		CLI
		REST API
	Controller OpenSSL Crypto Subsystem	None
	BC-FJA Crypto Subsystem	None
Switch Light OS 4.7.0	Spine Switch Subsystem	None
	Spine Crypto Subsystem	None
Switch Light OS 4.7.0	Leaf Switch Subsystem	Data
	Leaf Crypto Subsystem	None

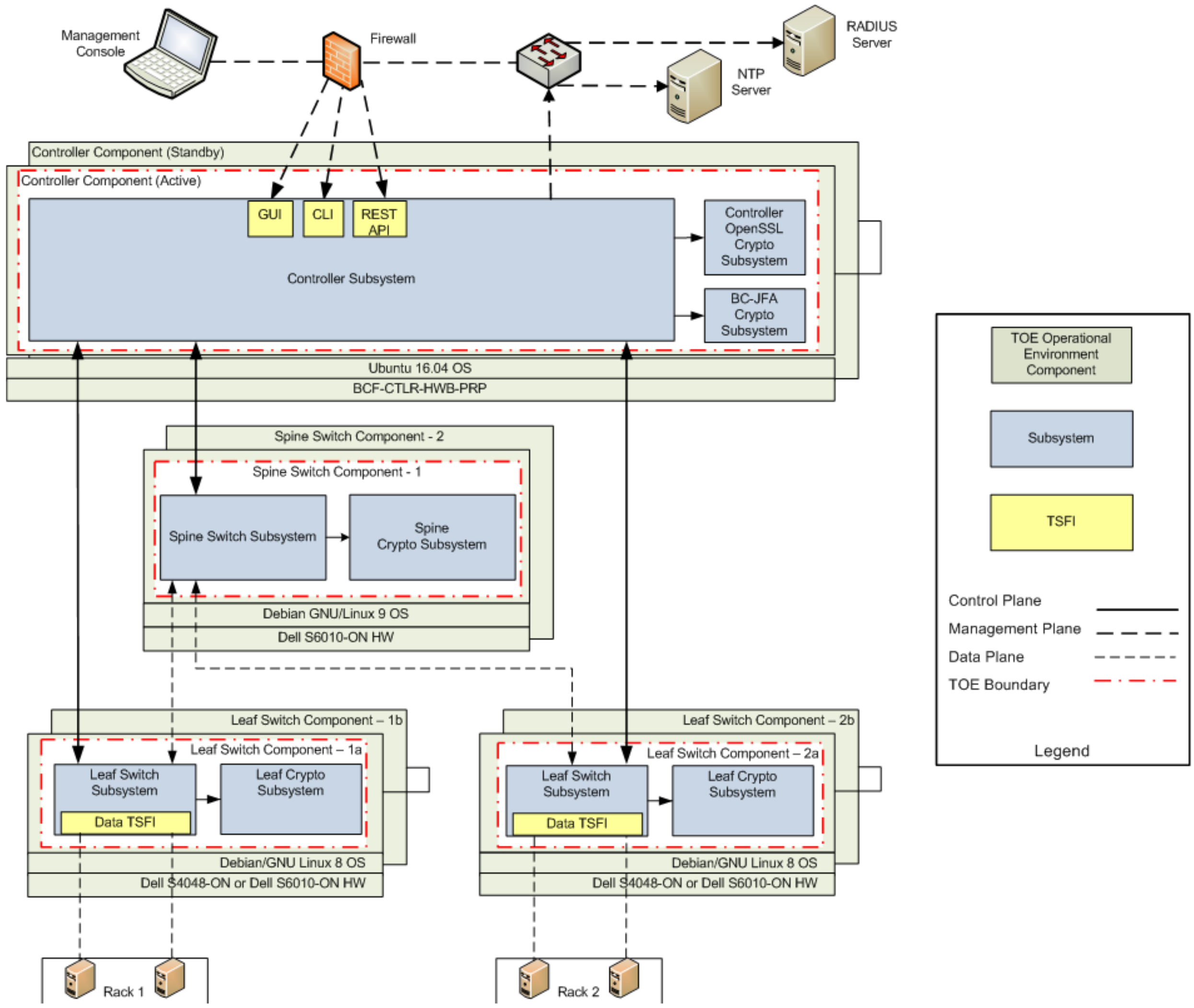

Figure 1. TOE diagram.

TLSv1.2 – Transport Layer Security version 1.2

BC-FJA – Bouncy Castle FIPS7 Java API

GNU – GNU's Not Unix

HTTPS8 – HyperText Transport Protocol Service

NTP – Network Time Protocol

OpenSSL – Open Secure Sockets Layer

OS – Operating System

RADIUS - Remote Dial-in Access Service

SSH – Secure Shell

PHYSICAL ARCHITECTURE

The leaf-spine architecture, which can be seen in Figure 2, optimizes bandwidth between switch ports within the data center by creating a high-capacity fabric using multiple spine switches that interconnect the edge ports on each leaf switch. This design provides consistent latency and minimizes the hops between servers in different racks. The fabric design is modular and scalable; leaf switches can be added to increase the number of switch edge ports, whereas fabric bandwidth can be increased by adding more spine switches.

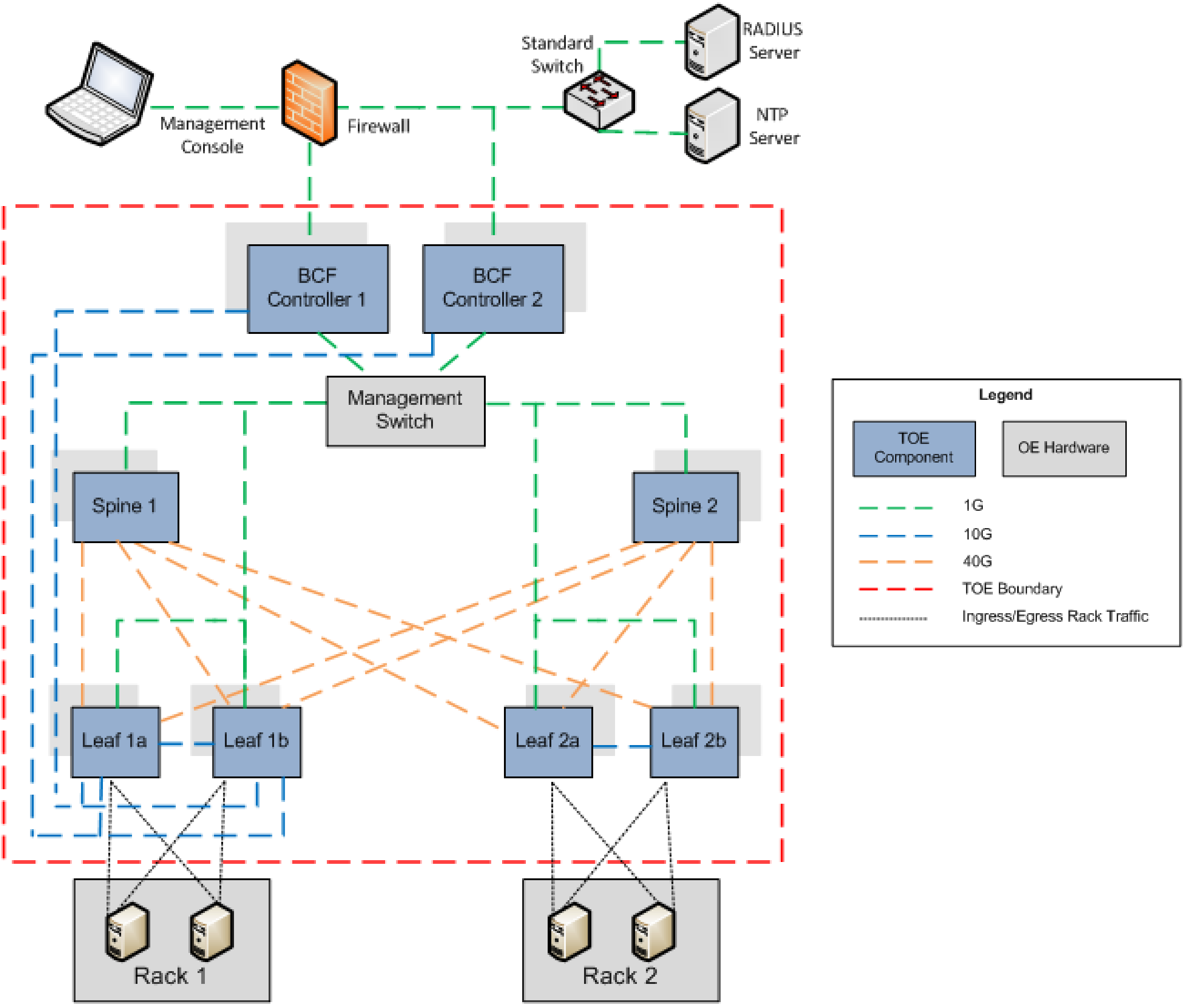

Figure 2. Evaluated Configuration of the TOE.

DOCUMENTS

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

- Big Switch Networks Big Cloud Fabric 4.7 CLI Reference Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018
- Big Switch Networks Big Cloud Fabric 4.7 Deployment Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018
- Big Switch Networks Big Cloud Fabric 4.7 GUI Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018
- Big Switch Networks Big Cloud Fabric 4.7 Hardware Compatibility List; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018
- Big Switch Networks Big Cloud Fabric 4.7 Hardware Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018
- Big Switch Networks Big Cloud Fabric 4.7.0 Release Notes; RELEASE DATE: May 24, 2018; Document Version 1.3, July 11, 2018
- Big Switch Networks Big Cloud Fabric 4.7 REST API Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018
- Big Switch Networks Big Cloud Fabric 4.7 System Messages Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018
- Big Switch Networks Big Cloud Fabric 4.7 User Guide; RELEASE DATE: May 24, 2018; Document Version 1.0, May 24, 2018
- Freeradius Installation and Setup (Ubuntu) 2017-Dec-20
- Big Switch Networks Big Cloud Fabric 4.7.0 Guidance Documentation Supplement v0.7

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.

The evaluator has devised and executed a test plan where a subset of test which covers the main number of test from the vendor has been repeated. Also the evaluator has devised and executed an independent testing plan to complement the evaluator's tests and give more assurance to the functionality coverage.

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 Big Switch Networks Big Cloud Fabric 4.7.0 it is necessary the disposition of the following software components:

- TOE software BCF v4.7.0 installed in BCF controllers (BCF Controller 1 and BCF Controller 2, see Figure 2)
- Switch Light OS v4.7.0 installed in the BCF leaf and spine switches (see Figure 2).

Regarding the hardware components, the only requirement is that they shall support the software elements previously detailed.

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

- For the BCF v4.7.0 software:
  - BCF Controller appliances (2 units) - BCF-CTLR-HWB-PRP / Intel Xeon E5-2620 v3 2.40GHz
- For the Switch Light OS v4.7.0:
  - *Spine* switches - Dell *S6010-ON* / Intel Xeon 12/24
  - *Leaf* switches - Dell *S4048-ON* / Intel Xeon 12/24

EVALUATION RESULTS

The product Big Switch Networks Big Cloud Fabric 4.7.0 has been evaluated against the Security Target [ST].

All the assurance components required by the evaluation level EAL2 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2, as defined by 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 laboratory gives the following security recommendation for the TOE environment:

The fulfilment 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 Epoche & Espri S.L.U., a positive resolution is proposed.

GLOSSARY

BCF	Big Cloud Fabric
Brite-Box	Vendor branded switches that are shipped without an embedded network operating system
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
SDN	Software-Defined Network (SDN)
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.

[ST] Big Switch Networks Big Cloud Fabric 4.7.0 Security Target, v 0.8, October 5 2018

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:

- Big Switch Networks Big Cloud Fabric 4.7.0 Security Target, v 0.8, October 5 2018.

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 recognized 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.