National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Fortinet, Inc.

326 Moodie Drive
Ottawa, ON K2H 8G3, Canada
www.fortinet.com

FortiSwitch™ blade appliances with FortiTRNG running FortiOS™ 5.0 Patch Release 7

Report Number: **CCEVS-VR-VID10555-2014**
Dated: **November 07, 2014**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
The MITRE Corporation

Bradford O'Neill
The MITRE Corporation

Jerome F. Myers
The Aerospace Corporation

Kenneth B. Stutterheim
The Aerospace Corporation

Jay Vora
The MITRE Corporation

Common Criteria Testing Laboratory

Swapna Katikaneni
Greg McLearn
Dustin Cheung

CGI Global IT Security Labs.
9700 Capital Court
Manassas VA 20110

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 3
3.1 TOE Evaluated Configuration 3
3.2 Physical Scope of the TOE 4
3.3 Supported non-TOE Hardware/ Software/ Firmware 4
4 Security Policy 5
4.1 Security Audit 5
4.2 Cryptographic Support 5
4.3 User Data Protection 5
4.4 Identification and Authentication 6
4.5 Security Management 6
4.6 Protection of the TSF 6
4.7 TOE Access 7
4.8 Trusted Path/Channels 7
5 Assumptions 8
6 Threats 8
7 Organizational Security Policies 8
8 Clarifications of Scope 9
9 Documentation 9
10 IT Product Testing 10
11 Evaluated Configuration 10
12 Results of the Evaluation 10
13 Validator Comments/Recommendations 11
14 Security Target 11
15 Glossary 11
16 Bibliography 12

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of FortiSwitch™ blade appliances with FortiTRNG running FortiOS™ 5.0 Patch Release 7 provided by Fortinet, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the CGI ITSL Common Criteria Testing Laboratory (CCTL) Manassas, VA, United States of America, and was completed in October, 2014. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by CGI ITSL. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the requirements from Network Devices Protection Profile (NDPP) v1.1, June 8, 2013, including the following optional requirements [TLS and TLS/HTTPS] and NDPP Errata #2, 13 January 2014.

The TOE is FortiSwitch™ blade appliances with FortiTRNG running FortiOS™ 5.0 Patch Release 7. The TOE is the FortiSwitch 5203B Advanced Telecommunications Computing Architecture (ATCA) compliant hub/switch blade running version 5.0.7 of the FortiOS code housed inside an ATCA chassis. The blade contains one FortiTRNG entropy source for the purposes of seeding the validated cryptographic module with Entropy. The TOE is configured in stand-alone Accelerated Packet Forwarding and Policy Enforcement configuration using the validated cryptography offered in "FIPS/CC mode"[1]. The TOE is designed to provide layer 3 switching services, Virtual Domains (vDOMs), vLAN segregation and network connectivity to devices connected to the chassis.

The TOE performs following security functionality: Security Audit, Cryptographic Support, User data Protection, Identification and Authentication, Security Management, Protection of the TSF, TOE Access and Trusted Path/Channels.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at CGI ITSL Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). A validation team from NIAP monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and

[1] FIPS/CC mode is a specific command that must be enabled on FortiOS products and is not present on all builds. Details as to how to configure this mode of operation as well as additional guidance are provided by Fortinet in a guidance supplement.

reviewed the individual work units and verdicts of the ETR. The team found that the evaluation showed that the product satisfies all of the security functional and assurance requirements stated in the ST. The evaluation also showed that the product met all the security requirements and Assurance Activities contained in the NDPP (including errata #2). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

CGI ITSL evaluation team concluded that the Common Criteria requirements from Network Devices Protection Profile (NDPP) v1.1 including errata #2 have been met. The technical information included in this report was obtained from the FortiSwitch™ blade appliances with FortiTRNG running FortiOS™ 5.0 Patch Release 7 Security Target

2 Identification

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	FortiSwitch™ blade appliances with FortiTRNG running FortiOS™ 5.0 Patch Release 7
Protection Profile	Network Devices Protection Profile (NDPP) v1.1, June 8, 2013, including the following optional requirements [TLS and TLS/HTTPS]. The NDPP Errata #2, 13 January 2014
ST:	FortiSwitch™ blade appliances with FortiTRNG running FortiOS™ 5.0 Patch Release 7 Security Target, Version 1.0, November 7,2014 2014
Evaluation Technical Report	Evaluation Technical Report For FortiSwitch™ blade appliances with FortiTRNG running FortiOS™ 5.0 Patch Release 7

Item	Identifier
	(Proprietary), Version 1.0, November 7,2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Fortinet, Inc.
Developer	Shawn Pinet, CGI ITSL
Common Criteria Testing Lab (CCTL)	CGI ITSL 9700 Capital Court Manassas VA 20110
CCEVS Validators	Paul Bicknell, The MITRE Corporation, Bedford, MA Bradford O'Neill, The MITRE Corporation, Bedford, MA Jerome F. Myers, The Aerospace Corporation, Columbia, MD Kenneth B. Stutterheim, The Aerospace Corporation, Columbia, MD Jay Vora, The MITRE Corporation, Ft Mead, MD

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Evaluated Configuration

The TOE is the FortiSwitch 5203B Advanced Telecommunications Computing Architecture (ATCA) compliant hub/switch blade running version 5.0.7 of the FortiOS code housed inside an ATCA chassis. The blade contains one FortiTRNG entropy source for the purposes of seeding the validated cryptographic module with Entropy. The TOE is configured in stand-alone Accelerated Packet Forwarding and Policy Enforcement configuration using the validated cryptography offered in "FIPS/CC mode"

3.2 Physical Scope of the TOE

The physical scope of the TOE includes the TOE hardware as well as the firmware. Details on the environment and TSFI's are shown below:

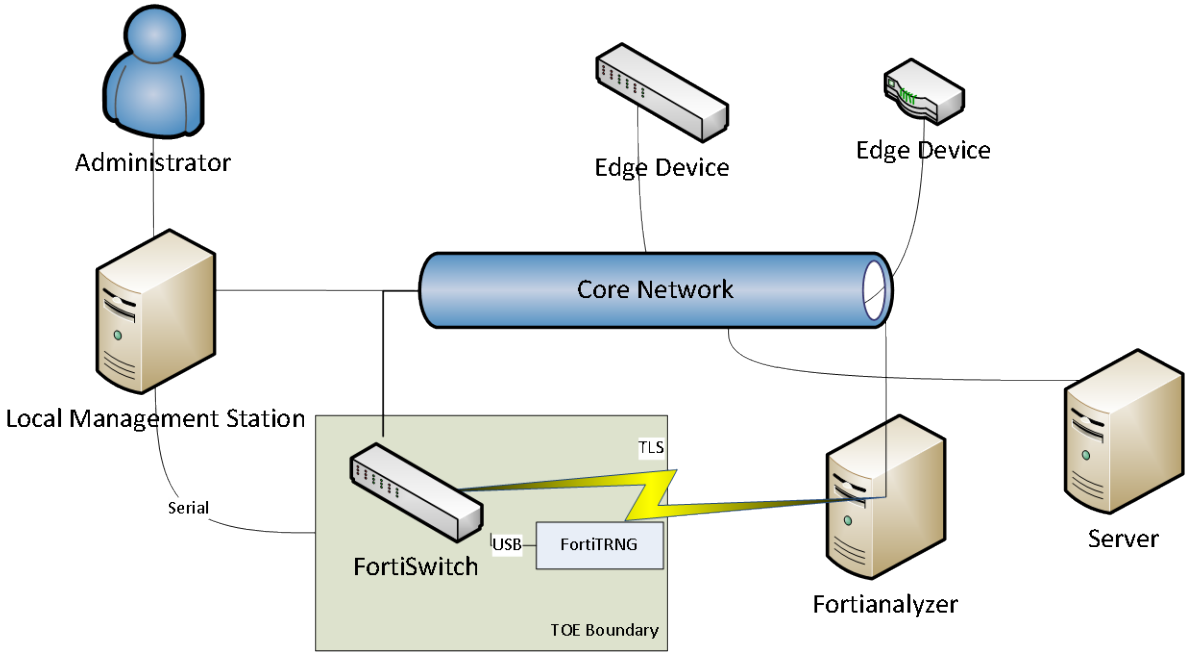

Figure 1 – TOE Physical Boundary

The only TOE hardware platforms claimed for this evaluation is the FortiSwitch 5203B running inside an ATCA chassis. This hardware platform requires a FortiTRNG to seed the TOE cryptographic system with entropy from the ambient environment.

3.3 Supported non-TOE Hardware/ Software/ Firmware

The following hardware, firmware and software, which are supplied by the IT environment, are excluded from the TOE boundary.

- ATCA Chassis
- Local management including
  - Local Serial Console Software
  - Supported Web Browser
    - Internet Explorer 9 or 10
    - Mozilla Firefox version 24
    - Google Chrome version 28
    - Apple Safari version 5.1 and 6.0
- Logging Server
  - FortiAnalyzer 5.0.7 or higher configured for use with the FortiSwitch over TLS

4 Security Policy

This section outlines the boundaries of the security functionality of the TOE

4.1 Security Audit

The TOE is capable of generating and securely transmitting Security Audit logs to a remote, trusted FortiAnalyzer server for further processing and review. The TOE will generate auditable events as specified in the NDPP which may help indicate a number of potential security concerns including resonance, password guessing and tampering with the trusted paths and channels. For all auditable events the TOE will associate a user (either IP address or with administrative credentials) to the session and use this identifier for all logging to the audit server.

An authorized administrator may delete the local audit trail. An authorized administrator may configure additional auditable events, configure the back-up of audit data to an external FortiAnalyzer source and manage audit data storage.

The auditing function is supported by reliable timestamps provided by the TOE.

4.2 Cryptographic Support

The TOE's cryptographic modules are FIPS PUB 140-2 validated and meet Security Level 1 overall and Security Level 2 for cryptographic module ports and interfaces, roles, services and authentication, and design assurance. The TOE is capable of generating cryptographic keys using a properly seeded random bit generator in order to provide cryptographic services to the network. The TOE is also capable of importing cryptographic keys and certificates from outside the TOE boundary. These keys are zeroized when no longer required and the TOE offers a function to zeroize these keys on demand.

The TOE is designed such that the cryptographic keys and other critical security parameters are not exposed through the various interfaces made available to the TOE administrator(s). Passwords including administrative passwords and pre-shared keys are stored on the TOE in the configuration file. These passwords and the configuration file itself are encrypted by the TOE using a cryptographic key generated by the TOE upon initialization and displayed in ciphertext only. Certificates are not viewable from any interface and may only be imported to the TOE through the GUI which is a cryptographically protected trusted and validated channel.

4.3 User Data Protection

The TOE ensures that all information is zeroized on allocation of memory to ensure that all memory is cleared of residual information prior to being written to. Keys and CSP's are zeroized per the FIPS 140-2 module validations.

4.4 Identification and Authentication

All administration requires authentication by the user identification and password mechanism. Administration may either be performed locally using the Local Console CLI or remotely using the Network Web-Based GUI. When authenticating locally or remotely the TOE supports complex, configurable password rules and supports complex character sets.

When authenticating over the GUI remote authentication data is protected via an encrypted trusted path between the TOE and administrator. Any individual attempting to log on for an interactive session will be shown a warning message that they must accept prior to being presented with a prompt to attempt their authentication.

4.5 Security Management

The TOE provides remote and local administrative interfaces that permit role based administration to configure and manage the TOE both locally and remotely. When fully initialized and configured the TOE is connected to two or more networks and remote administration data flows from a Network Management Station to the TOE. On the TOE hardware model there is also a Local Console which can be connected to from within the physically secured area described within table 7 of the NDPP and consists of a physical serial interface to the TOE.

An administrator account is associated with an access profile, which determines the permissions of the individual administrator. Additionally, each FortiOS™ install comes with a default administrator account with all permissions, which may not be deleted. The term ‘authorized administrator’ is used throughout this ST to describe an administrator given the appropriate permission to perform tasks as required.

These administration tasks include, but are not limited to configuring appropriate cryptographic protocols available for negotiation, the capacity to query the version information and the ability to update the TOE to a new version.

4.6 Protection of the TSF

Inter-TSF communications are protected to ensure availability, confidentiality and detection of modification. This is accomplished through the usage of cryptographic communications for any and all communications with remote IT entities, other components of the TOE and remote administrators. By default detection of modification and audit logging are enabled on TLS connections.

The TOE prevents the reading of all administrator passwords, pre-shared keys, symmetric keys and private keys through obscuring them with a one-way function prior to storing them into the TOE configuration file. These keys are not viewable through the TSFI’s

directly. They are available only as an encrypted value within the configuration file which may be backed up by the administrator.

The TOE is capable of querying its current version and displaying it back to the administrator via the trusted interfaces. The TOE also provides a method to verify updates and update the TOE through any of the administrative interfaces. Updates to the TOE software are verified by the TOE during the initial phase of the update process. During this process the TOE verifies that the candidate update is signed by the developer's 2048 bit RSA signature in order to ensure the authenticity of the update. This cryptographic key is used for all FIPS firmware images.

The TOE maintains its own timestamp which are free from outside interference. This timestamp is used for the purposes of generating audit logs and other time-sensitive operations on the TOE including cryptographic key regeneration intervals.

The TOE implements a number of self-tests on start-up to ensure the correct operation and configuration of the TOE. These include but are not limited to hardware and entropy source self-tests, checksums of the firmware binaries and correct operation of the FIPS approved cryptographic module. Additionally the TOE maintains ongoing health tests associated with the FIPS cryptographic module and the hardware noise source.

4.7 TOE Access

The TOE is capable of terminating both local and remote administrative sessions upon detection of administrator inactivity. The TOE is also capable of terminating a remote session upon request from a remote administrator such as when a request to logout is received.
The TOE provides administrators with a configurable warning banner prior to initiating any interactive session with the administrator.

4.8 Trusted Path/Channels

A cryptographically protected trusted communications channel is required for all communications with the audit server. For the purposes of auditing the TOE is capable of securing its FortiAnalyzer audit server communications via TLS. The TOE or the remote peer may initiate this cryptographically protected channel.

The TOE will ensure that HTTPS is used for a trusted path between the TOE and the trusted remote administrator. This path will be used for both the initial administrator authentication and all remote administration requests and is terminated upon session timeout or explicit request from an administrator.

5 Assumptions

The following specific conditions are assumed to exist in an environment where the TOE is employed.

Assumption	Description
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

6 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter.

Threat	Description
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

7 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE and its operational environment are intended to fulfill.

OSP	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

8 Clarifications of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

9 Documentation

The following lists the TOE Guidance Documentation to install, configure, and maintain the TOE.
FortiOS™ Handbook for FortiOS 5.0 01-500-99686-20131209 December 9, 2013
FortiGate™ Log Message Reference – FortiOS 5.0.6 01-506-112804-20140401 April 1, 2014
FortiOS™ CLI Reference for FortiOS 5.0 01-506-99686-20140313 March 13, 2014
FortiAnalyzer v5.0 Patch Release 6 Administration Guide March 10, 2014
FortiSwitch 5203b Security System Guide 01-400-145204-20120216 Retrieved May 28, 2014
FortiOS v5.0 Patch Release 7 Release Notes 01-507-238147-20140821 August 21, 2014

The security target used is:

FortiSwitch™ blade appliances with FortiTRNG running FortiOS™ 5.0 Patch Release 7 Security Target, Version 1.0, November 7, 2014

10 IT Product Testing

The evaluation team performed all the test activities identified in Network Devices Protection Profile (NDPP) v1.1, June 8, 2013, including the following optional requirements [TLS and TLS/HTTPS] and NDPP Errata #2, 13 January 2014.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE using the guidance documentation provided by the customer and exercised the Team Test Plan on the test configuration setup within the CCTL.

The test configuration required the use of the following:
TOE
Hardware: FortiSwitch 5203 installed in a Fortigate 5140B ATCA chassis
OS: FortiOS v5.0.7 build 3608

FortiAnalyzer (FAZ) over TLS
FortiAnalyzer-400B
OS : 5.2.0 build 0546

OpenVAS workstation
Kali VM running OpenVAS

Management PC Running Putty v0.62 for serial connections to the TOE
Model: Dell Latitude E6520
OS: Windows 7

The TOE passed all the required test activities from NDPPv1.1 (including errata#2).

11 Evaluated Configuration

The only TOE hardware platforms claimed for this evaluation is the FortiSwitch 5203B running inside an ATCA chassis. This hardware platform requires a FortiTRNG to seed the TOE cryptographic system with entropy from the ambient environment.

12 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

CGI ITSL has determined that the TOE meets the security criteria in the Security Target, which specifies assurance requirements from Network Devices Protection Profile (NDPP) v1.1,

June 8, 2013, including the following optional requirements [TLS and TLS/HTTPS] and NDPP Errata #2, 13 January 2014.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

This evaluation is the candidate evaluation for CGI ITSL and has been monitored by a team of validators. All the evaluation activities were completed satisfactorily and the TOE passed all the test activities. The details of the evaluation results are recorded in the Evaluation Technical Report (proprietary) and Independent Test Report provided by the CCTL.

13 Validator Comments/Recommendations

The validators did not have any specific additional comments or recommendations.

14 Security Target

FortiSwitch™ blade appliances with FortiTRNG running FortiOS™ 5.0 Patch Release 7 Security Target, Version 1.0, November 07, 2014.

15 Glossary

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCCS	Canadian Common Criteria Scheme
CEM	Common Evaluation Methodology
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameters
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
FSSO	Fortinet Single Sign-On
HMAC	Keyed-Hash Message Authentication Code
NDPP	Network Device Protection Profile

OFB	Output Feedback
OSP	Organizational Security Policy
PP	Protection Profile
RBG	Random Bit Generator
SA	Security Association
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 **Bibliography**

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CGI ITSL (http://www.cgi.com/en/information-security/it-security-product-evaluation-and-testing).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2012 Version 3.1 Revision 4 Final, CCMB-2012-09-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2012 Version 3.1 Revision 4 Final, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2012 Version 3.1 Revision 4 Final, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, September 2012 Version 3.1 Revision 4 Final, CCMB-2012-09-004.