Validation Report

Alcatel-Lucent

Alcatel-Lucent OmniSwitch 9000E Series with AOS Release 6.4.4

Alcatel-Lucent OmniSwitch 6855 Series with AOS Release 6.4.4

Alcatel-Lucent OmniSwitch 6850E Series with AOS Release 6.4.4

Alcatel-Lucent OmniSwitch 6400 Series with AOS Release 6.4.4

Document ID: 11-1911-R-0104 V1.1

January 20, 2012

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Alcatel-Lucent OmniSwitches 9000E, 6855, 6850E, 6400 with AOS 6.4.4, the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the TOE was performed by InfoGard Laboratories, Inc., in San Luis Obispo, CA in the United States of America (USA) and was completed in October 2011. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR), and the functional testing report. The ST was written by InfoGard Laboratories, Inc. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 July 2009, Evaluation Assurance Level 2 (EAL 2), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 r.3, July 2009.

The TOE is a network switch that provides Layer-2 switching, Layer-3 routing, and traffic filtering.

Layer-2 switches analyze incoming frames and make forwarding decisions based on information contained in the frames. Layer-3 routing determines the next network point to which a packet should be forwarded toward its destination. These devices may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Routing protocols include BGP, RIP v.2, and OSPF. Filtering controls network traffic by controlling whether packets are forwarded or blocked at the switch's interfaces. Each packet is examined to determine whether to forward or drop the packet, on the basis of the criteria specified within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

The Alcatel OmniSwitch 6400 Series switches are fixed configuration stackable Gigabit Ethernet switches (10/100/1000). They provide advanced Layer-2 and basic routing capabilities.

The Alcatel OmniSwitch 6850E and 6855 series switches are fixed configuration, triple-speed (10/100/1000) Ethernet switches. They provide wire rate Layer-2 forwarding and Layer-3 routing with 10 Gigabit support. The 6850E series are either stand alone or stackable switches. The OmniSwitch 6855 series are hardened[1] Gigabit Ethernet fixed configuration switches that provide Layer-2 and Layer-3 switching only for use in harsh environmental conditions.

[1] The term hardened in this document refers to industrial, ruggedized equipment that is designed to operate in harsh electrical conditions and at extreme temperatures, vibration, noise, etc.

The Alcatel OmniSwitch 9000E (OS9000E) switches are comprised of the 9800E and 9700E models and are high performance switches for use in datacenters and campus networks. The OS9000E switches are chassis / blade systems. For example, the OS9800E switch is an 18 slot chassis, supporting two Chassis Management Modules (CMM) and 16 Network Interface (NI) modules.

AOS release 6.4.4 is the single purpose operating system that operates the management functions of all of the Alcatel OmniSwitch switches.

2 Identification of the TOE

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 organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Alcatel-Lucent OmniSwitch 9000E, 6855, 6850E, 6400 with AOS 6.4.4
Security Target	Alcatel-Lucent OmniSwitch 9000E, 6855, 6850E, 6400 with AOS 6.4.4 Security Target – EAL2
Dates of Evaluation	May 2009 – October 2011
Conformance Result	EAL 2 augmented ALC_FLR.2
Common Criteria Version	Common Criteria for Information Technology Security Evaluation Version 3.1 R3, July 2009
Common Evaluation Methodology (CEM) Version	CEM Version 3.1 R3, July 2009
Evaluation Technical Report (ETR)	11-1911-R-0066 V1.1
Sponsor/Developer	Alcatel-Lucent
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Ryan Day, Annie Browne
CCEVS Validators	Franklin Haskell, Rick Murphy

Table 1: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before May 28, 2009.

4 Security Policy

The TOE supports the following security policies as described in the Security Target:

4.1 Audit

The TOE generates audit records. The audit records are displayed on the CLI console as they are generated in a scrolling format.

The TOE writes audit logs to a text file stored in the system's flash memory for permanent storage. These audit log entries are tagged with the AOS Application that created them. The TOE also provides the ability to send switch logging information to an external syslog server.

The TOE provides the authorized administrator with the ability to increase the size of the log files from the default value of 128k to the capacity of the flash drive. Once the files are full the oldest entries are overwritten.

4.2 Identification and Authentication

There are two types of authentication performed by the TOE: Authorized Administrator Authentication and End-user Authentication (the term end-user refers to the device on the network.)

Administrator authentication can be performed locally on the TOE or the TOE can rely upon an external authentication server in the operational environment to authenticate an administrative-user (the term administrative-user refers to operators authorized to perform administrative functions). The external authentication servers supported by the TOE for administrator authentication are RADIUS, and TACACS+; an external LDAP server provides information useful in access control, but does not perform authentication.

End-user (device) authentication is used to mediate network information flows. The end-user authentication is performed by verifying the credentials of either the device or the device operator. The TOE supports three types of end-user authentication: MAC authentication, web-based authentication (Captive Portal), and IEEE 802.1X. These authentication methods require an external authentication server in the operational environment.

The TOE provides administrator configurable password settings to enforce local password complexity when a password is created or modified. The TOE also provides the ability to lockout administrative-users after an administrator configurable number of consecutive unsuccessful local authentication attempts.

4.3 Management of the TOE

The TOE provides the CLI for the TOE's security management functionality. The TOE also provides SNMPv3 management interfaces, as well as a Flash file system for storing configuration files/directories. Files can be transferred to the Flash file system via SFTP.

The TOE provides the administrator the ability to create, modify and delete policies that meditate traffic flow as implemented by the Traffic Filter SFP or VLAN SFP.

The TOE provides the administrator the ability to manage all other aspects of the TOE; for

example, configuring local administrator accounts and viewing or configuring the audit trail.

4.4 Traffic Mediation and Filtering

The TOE can mediate traffic using VLANs and 802.11Q, as well as custom created Traffic Filters.

4.5 Protection of the TSF

The switches protect themselves by requiring administrators to identify and authenticate themselves prior to performing any actions and by defining the access allowed by each administrator.

The TOE is not intended for use as a general purpose computer and only executes the services needed to perform its intended function

The TOE provides secure access for the administrator to manage the TOE via SNMPv3 or SSH v2 (including SFTP). The TOE implements SSLv2, SSLv3 and SSL v3.1 / TLS 1.0: throughout this document, any reference to "SSL" or "TLS" refers to any of these SSL or TLS versions. TLS 1.0 is an alternative name for SSL v3.1, which is backward compatible with SSLv2 and SSLv3.

4.6 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.NOEVIL	The TOE administrator is not willfully negligent in the use of the TOE.
A.TRAIN	The TOE administrator is trained in the correct & secure usage of the TOE.
A.AUDREV	The TOE administrator will periodically review the audit logs on the TOE.
A.LOCATE	The TOE shall be located in a physically secure environment.
A.MGMTLAN	There will be a secure management network for the administrator to configure & manage the TOE.
A.INTEROP	The TOE will be able to interact with other manufacturers' hardware attached to the network.
A.LOWEXP	The threat of malicious attacks aimed at exploiting the TOE is considered low.

4.7 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T.NO_ADMINAUTH	An unauthorized person may attempt to bypass the security of the TOE to access and use functions provided by the TOE without authenticating.
T.NO_AUDIT	An administrative-user or end-user of the TOE may not be accountable for the actions they perform because their actions are not logged or an administrator does not review the audit records, thus allowing an attacker to escape detection.
T.NO_MEDIATE	An authorized entity may send impermissible information through the TOE, resulting in the exploitation of resources on the internal network.

T.NO_MGMT The authorized administrator is not able to manage the secure functions of the TOE, causing the TOE to be configured in an insecure manner.

T.NO_TIME The authorized administrator is not able to verify the audit trail because the audit records are not stamped with the correct time, thus allowing an attacker to escape detection.

T.RESIDUAL An unauthorized person may gather residual information from a previous information flow.

T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.

T.EAVESDROP A malicious operator or process may observe or modify sensitive data transmitted between the TOE and a remote trusted IT entity.

5 Architectural Information

The TOE is made up of *hardware and software* components. The TOE consists of two main components: the Network interfaces and the Chassis Management Subsystem.

5.1 Network Interfaces

Network interface (NI) modules are categorized into GNI and XNI modules. Gigabit Ethernet Network Interface (GNI) modules provide 1000 Mbps (1 Gbps) connections. GNI modules can be used for backbone connections in networks where Gigabit Ethernet is used as the backbone media. XNI modules provide up to six 10000 Mbps (10 Gbps) connections per module and can be used in networks where 10-gigabit Ethernet is used as the backbone media.

5.2 Chassis Management

For the OS6400, OS6850E, and OS6855, the Chassis Management functionality resides on the main processor PCB. The OS9000E series are chassis & blade based systems consisting of one or 2 Chassis Management Modules (CMM)s and 1-18 Network Interface (NI) modules. OS9700E-CMMs and OS9800E-CMMs use identical processor boards. However, OS9800E-CMMs use twice the number of network interface-related ASICs on the fabric board. This is because OS9800E switches support up to 16 network interface (NI) modules and OS9700 switches support up to 8 NI modules.

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Network Security Platform. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is

shown with a hashed background.

The TOE is physically delivered to the End-User. The guidance documents are provided for download with the TOE software in accordance with EAL 2 requirements from the Alcatel support website and apply to the CC Evaluated configuration:

6.1 Design Documentation

Document	Revision	Date
EAL2 + ALC_FLR.2 Development Documentation Coverage: ADV_ARC.1, ADV_FSP.2, ADV_TDS.1 Alcatel-Lucent OmniSwitch 9000E, 6855, 6850E, 6400 with AOS 6.4.4	Rev. F	August 30, 2011
AOS_644_Errors.xlsx	N/A	July 22, 2011
013067-00_Alcatel-Lucent OmniSwitch FSP v0.2.xlsx	0.2	August 26, 2011
644_mibs.zip	N/A	August 26, 2011
AOS_644_SSLconfig.tar	N/A	July 22, 2011
Alcatel-Lucent OmniSwitch 6855 (Data Sheet)	N/A	March 24, 2009
Alcatel-Lucent OmniSwitch 9000 (Data Sheet)	N/A	March 24, 2009
Alcatel-Lucent OmniSwitch 6400 (Data Sheet)	N/A	March 24, 2009
Alcatel-Lucent OmniSwitch 6850 (Data Sheet)	N/A	March 24, 2009

6.2 Guidance Documentation

Document	Revision	Date
Preparation and Operation of Common Criteria Evaluated OmniSwitch Products	**A.05, Agile Rev. B**	**August 11, 2011**
OmniSwitch 6850/6850E Series Getting Started Guide	**Rev. D**	**April 2011**
OmniSwitch 6850 Series Hardware Users Guide	**Rev. F**	**September 2009**
OmniSwitch® 9000/9000E Series Getting Started Guide	**Rev. E**	**August 2009**
OmniSwitch 9000/9000E Series Hardware Users Guide	**Rev. H**	**September 2009**

Document	Revision	Date
OmniSwitch AOS Release 6 Switch Management Guide	**Rev. A**	**April 2011**
OmniSwitch AOS Release 6 Advanced Routing Configuration Guide	**Rev. K**	**September 2009**
OmniSwitch AOS Release 6 Network Configuration Guide	**Rev. A**	**April 2011**
OmniSwitch CLI Reference Guide	**Rev A**	**April 2011**
OmniSwitch Transceivers Guide	**Rev. G**	**September 2009**
OmniSwitch 6855 Series Getting Started Guide	**Rev. B**	**November 2009**
OmniSwitch 6855 Series Hardware Users Guide	**Rev. C**	**September 2009**
OmniSwitch 6400 Series Getting Started Guide	**Rev. A**	**August 2008**
OmniSwitch 6400 Series Hardware Users Guide	**Rev. C**	**September 2009**
Syslog Messages Documentation	**N/A**	**March 7, 2008**

6.3 Configuration Management and Lifecycle

Document	Revision	Date
EAL 2 + ALC_FLR.2 Life Cycle Support Documentation Coverage: ALC_CMC.4, ALC_DEL.1, ALC_DVS.1, ALC_FLR.2, ALC_LCD.1, ALC_TAT.1 Alcatel-Lucent OmniSwitch 9000E, 6855, 6850E, 6400 with AOS 6.4.4	E	August 5, 2011
Engineering Development Process	L1	January 8, 2007
Part, Document and Data, Numbers and Revisions, Policy	ZA	June 5, 2006
Change Order Procedure	ZH	December 20, 2006
Product Barcode Label Procedure	ZM	January 8, 2009
CM_Plan_020472-10.xls	N/A	July 30, 2009
Product Life Cycle ESD (8AL011302000ASASAed3b.pdf)	N/A	June 3, 2010

Document	Revision	Date
First Article Procedure	K	September 10, 2002
BOM_OS6400-24C.xls	N/A	June 9, 2011
BOM_OS6400-48C.xls	N/A	June 9, 2011
BOM_OS6400-P48C.xls	N/A	June 9, 2011
BOM_OS6400-U24C.xls	N/A	June 9, 2011
BOM_OS6850E24C.xls	N/A	June 10, 2011
BOM_OS6850E48C.xls	N/A	June 10, 2011
BOM_OS6850EP48XC.xls	N/A	June 10, 2011
BOM_OS6850EU24XC.xls	N/A	June 10, 2011
BOM_OS6855-24C.xls	N/A	June 9, 2011
BOM_OS6855-U24XC.xls	N/A	June 9, 2011
BOM_OS9702E-CMM-SC.xls	N/A	June 2, 2011
BOM_OS9702E-RCBAC.xls	N/A	June 2, 2011
BOM_OS9800E-CMMC.xls	N/A	June 2, 2011
BOM_OS9800E-RCB-AC.xls	N/A	June 2, 2011
Security advisory template	N/A	June 30, 2011
Vulnerability Summary Report	N/A	June 30, 2011

6.4 Test Documentation

Document	Revision	Date
EAL2 + ALC_FLR.2 Test Documentation Coverage: ATE_COV.1, ATE_FUN.1 Alcatel-Lucent OmniSwitch 9000E, 6855, 6850E, 6400 with AOS 6.4.4	0.5 Agile Rev. A	June 15, 2011
Test Scripts	N/A	May 23, 2011
Test Plans	N/A	July 1, 2011
Test Results OS900E	N/A	July 14, 2011
6400 Results	N/A	July 13, 2011
6850E Results	N/A	July 13, 2011

Document	Revision	Date
6855 Results	N/A	July 13, 2011
Enterprise Solutions Division System Test Beds and Setups	1.1	February 1, 2007
Enterprise Solutions Division OS6850E System Release Specification	1	November 6, 2008
Enterprise Solutions Division Siebel PR Management Handbook	B	September 18, 2006
Test Engineering Release Process	A	March 12, 2007
Independent and Penetration Test Plan	1.1	October 21, 2011

6.5 Vulnerability Assessment Documentation

Document	Revision	Date
Alcatel-Lucent OmniSwitch 9000E, 6855, 6580E , 6400 with AOS 6.4.4 Common Criteria Vulnerability Analysis AVA_VAN.2 EAL2	1.1	October 20, 2011

6.6 Security Target

Document	Revision	Date
Alcatel-Lucent OmniSwitch 9000E, 6855, 6850E, 6400 with AOS 6.4.4 Security Target – EAL2	1.00 Agile Rev. C	December 19, 2011

7 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

7.1 Developer Testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces along with test tools to simulate attacks and alerts.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The

expected and actual test results are also included in the TOE Test Plan. The Developer testing effort tested the available interfaces to the TSF.

The Evaluation Team verified that the Developer's testing tested aspects of the SFRs defined in the ST. This analysis ensures adequate coverage for EAL 2. The Evaluation Team determined that the Developer's actual test results matched the Developer's expected test results.

7.2 Evaluation Team Independent Testing

The Evaluation Team conducted independent testing of the TOE. The Evaluation Team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The Evaluation Team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The Evaluation Team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation Team used the Developer's Test Plan as a basis for creating the Independent Test Plan. Due to the developers' automated, comprehensive tests, the Evaluators elected to re-run selected tests from the developers test suite. Once complete, the Evaluators analyzed the test outputs (results) and verified through sampling that tests are illustrating correct TOE behavior.

7.3 Vulnerability Analysis

The Evaluation Team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Evaluation Team's vulnerability analysis and penetration tests.

The Evaluators performed a vulnerability analysis of the TOE to identify any obvious vulnerabilities in the product and to determine if they are exploitable in the intended environment for the TOE operation. In addition, the Evaluation Team performed a public domain search for potential vulnerabilities. The public domain search did not identify any known vulnerabilities in the TOE as a whole or any components of the TOE.

Based on the results of the Evaluation Team's vulnerability analysis, the Evaluation Team was not able to create any useful penetration tests within the scope of EAL2. Due to the exhaustive nature of the developer tests, the Evaluators could gain no more assurance from any evaluator-devised tests.

8 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 3. 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 3.

InfoGard has determined that the TOE meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 + ALC_FLR.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in October 2011.

9 Validator Comments/Recommendations

Potential customers should be careful to take note of the excluded TOE features. The only major functionality not evaluated is the web interface. Other functionality excluded is support for superseded protocols.

10 Security Target

Alcatel-Lucent OmniSwitch 9000E, 6855, 6850E, 6400 with AOS6.4.4 Security Target, Version 1.00 (Agile Rev. C), December 19, 2011.

11 Terms

11.1 Glossary

ACL	Access control List
Administrative-user	An administrative user of the TOE, authorized to control TOE settings, as opposed to end-users, associated with general network traffic
AOS	Alcatel Operating System for the switches
ASIC	Application-Specific Integrated Circuit
ASA	Authenticated Switch Access
Appletalk	AppleTalk protocol. Also captures Datagram Delivery Protocol (DDP) and AppleTalk ARP (AARP).
Application	In the context of AOS auditing there are several ‘applications’ that log records. These are identified by a number and abbreviation.
ASA	Authenticated Switch Access
Authenticated VLANs	Authenticated VLANs control operator access to network resources based on VLAN assignment and a operator log-in process;
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol

CMM	Chassis Management Module. Physically a separate blade for 9000 series switches. Logically a separate piece of functionality built into the Management of the 6850E series
Decnet	DECNET Phase IV (6003) protocol.
DHCP	Dynamic Host Configuration Protocol
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAP	Extensible Authentication Protocol
End-user	Network traffic, non-administrative users of the TOE
GNI	Gigabit Ethernet Network Interface
GigE	Gigabit Ethernet
HMAC	Keyed-Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IEEE 802.1X	IEEE 802.1X is an IEEE Standard for port-based Network Access Control
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ip-e2	IP Ethernet-II protocol. Also captures Address Resolution Protocol (ARP)
ip-snap	IP SNAP protocol
ipv6	IPv6 protocol
IPX	Internet Protocol Exchange
LDAP	Lightweight Directory Access Protocol
MAC Address	Media Access Control Address, also known as the hardware or adaptor address.
NI	Network Interface Module. Physically a separate blade for the 9000 series switches. Logically a separate piece of functionality

	built into the Management of the 6850E series
OSPF	Open Shortest Path First is a dynamic routing protocol.
OS6400	Alcatel-Lucent OmniSwitch, 6400 Series with AOS Release 6.4.4
OS6850E	Alcatel-Lucent OmniSwitch 6850E Series with AOS Release 6.4.4
OS6855	Alcatel-Lucent Omniswitch 6855 Series with AOS Release 6.4.4
OS9000E	Alcatel-Lucent OmniSwitches 9000E Series with AOS Release 6.4.4
POE	Power over Ethernet
Port Mobility	The ability for the Alcatel Switches to dynamically tag incoming traffic into a specific VLAN irrespective of the physical port the traffic enters
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RIP	Routing information Protocol is a dynamic routing protocol.
SFP	Small Form Factor Pluggable transceiver (used in Section 1.4.1) Or Security Function Policies (used in Section 6)
SLB	Server Load Balancing
SNMP	Simple Network Management Protocol (inclusive of functionality from all supported versions of SNMP). SNMPv3 provides data confidentiality and integrity features.
SSH	Secure Shell
Stackable	6850E series switches that can be connected with a special function cable that allows them to function as a virtual chassis using a central management point
TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol

UDP	User Datagram Protocol
VLAN, (Virtual LAN) / Logical Network	The term VLAN was specified by IEEE 802.1Q; it defines a method of differentiating traffic on a LAN by tagging the Ethernet frames. By extension, VLAN is used to mean the traffic separated by Ethernet frame tagging or similar mechanisms. In this ST Logical network and VLAN are used interchangeably
VoIP	Voice Over IP
WebView	The web based GUI to manage the TOE
XNI	10-gigabit Ethernet Network Interface

12 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.