Certification Report

1830 Photonic Service Switch (PSS) R7.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment, 2015

Document number: 383-4-256-CR
Version: 1.0
Date: 12 June 2015
Pagination: i to iii, 1 to 8

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 12 June 2015, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

1830 Photonic Service Switch (PSS) R7.0 (hereafter referred to as the 1830 PSS), from Alcatel-Lucent, is the Target of Evaluation. The results of this evaluation demonstrate that the 1830 PSS meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

The 1830 PSS represents a type of photonic switching access platform for metro Wavelength Division Multiplexing (WDM). The 1830 PSS transforms traditional WDM into a fully flexible transport layer with complete visibility and control of individual wavelengths. This transformation simplifies broadband service delivery and facilitates bandwidth expansion in Optical-Transport Network (OTN)-based metro access networks. The 1830 PSS supports the transport and delivery of multiple services in a variety of environments.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 12 June 2015 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the 1830 PSS, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the 1830 PSS evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

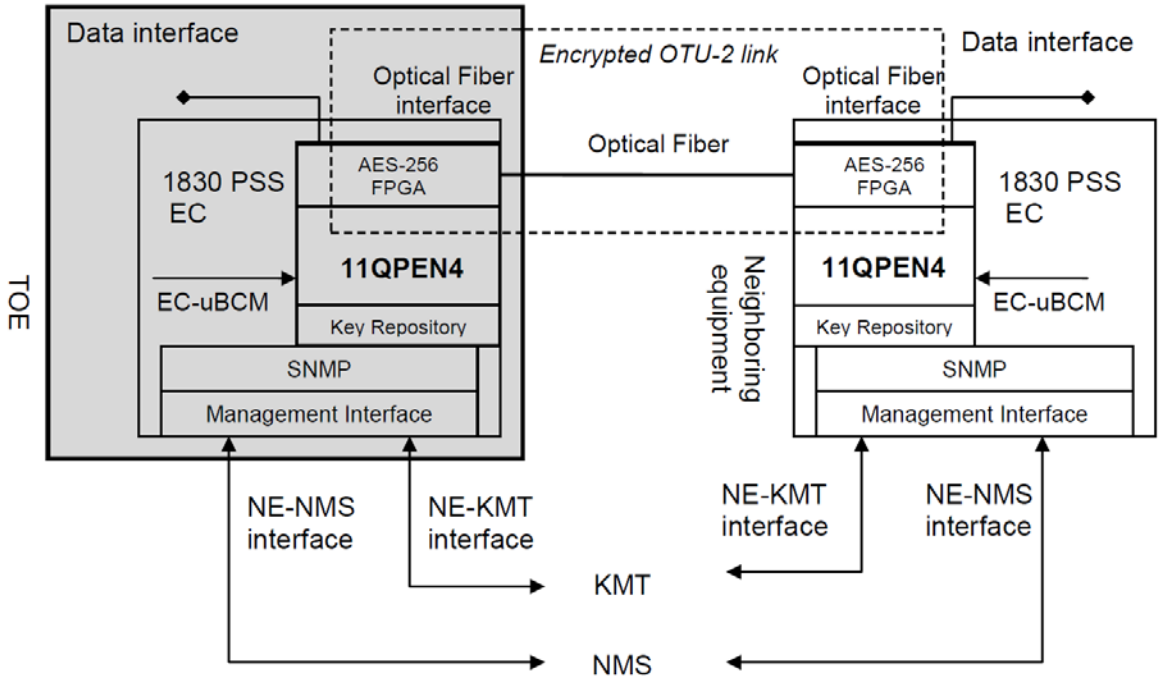
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is 1830 Photonic Service Switch (PSS) R7.0 (hereafter referred to as the 1830 PSS), from Alcatel-Lucent.

2 TOE Description

The 1830 PSS represents a type of photonic switching access platform for metro Wavelength Division Multiplexing (WDM). The 1830 PSS transforms traditional WDM into a fully flexible transport layer with complete visibility and control of individual wavelengths. This transformation simplifies broadband service delivery and facilitates bandwidth expansion in Optical-Transport Network (OTN)-based metro access networks. The 1830 PSS supports the transport and delivery of multiple services in a variety of environments.

A diagram of the 1830 PSS architecture is as follows:



3 Security Policy

The 1830 PSS implements a role-based access control policy to control administrative access to the system. In addition, the 1830 PSS implements policies pertaining to the following security functional classes:

- *Security Audit;*
- *Cryptographic Support;*

- *Security Management;*
- *Identification and Authentication;*
- *User Data Protection;*
- *Protection of the TSF; and*
- *Trusted Path/Channels.*

The following cryptographic module was evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
Alcatel-Lucent 1830 Photonic Service Switch (PSS)	*Pending* [1]

4 Security Target

The ST associated with this Certification Report is identified below:

Security Target Alcatel-Lucent 1830 Photonic Service Switch (PSS) R7.0, version 0.14, 12 June 2015.

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4,* for conformance to *the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

The 1830 PSS is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*
   - *ALC_FLR.2 Flaw Reporting Procedures.*

b. *Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:*
   - FAU_STG_EXT.1 External Audit Trail Storage.

c. *Common Criteria Part 3 conformant,* with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of the 1830 PSS should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

[1] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *Only trusted and well trained users will maintain the TOE;*
- *The TOE has been installed and set up in accordance with the delivery and installation procedures; and*
- *Alarms are monitored and event logs are examined by the administrators.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *Non-TOE components are configured following the vendor security recommendations and have the same level of physical and logical protection as the TOE;*
- *The TOE is located in a controlled and secure zone; and*
- *User data transmitted via the TOE or originating from the TOE is handled securely.*

7 Evaluated Configuration

The evaluated configuration for the 1830 PSS comprises one of the following platforms:

- PSS-4;
- PSS-16; and
- PSS-32.
  All running software 1830 PSS R7.0, build 16.18-0.

The publication Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0.0 Federal Information Processing Standards (FIPS) User Guide and Logbook describes the procedures necessary to install and operate the 1830 PSS in its evaluated configuration. The above publication makes reference to some of the documentation provided to the consumer from section 8.

8 Documentation

The Alcatel-Lucent documents provided to the consumer are as follows:

a) Alcatel-Lucent 1830 Photonic Service Switch 4 (PSS-4) Release 7.0 Installation and System Turn-up Guide, Issue 1, April 2014;
b) Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 User Provisioning Guide, Issue 2, April 2014;
c) Alcatel-Lucent 1830 Photonic Service Switch 16/32 (1830 PSS-16/PSS-32) Release 7.0 Installation and System Turn-up Guide, Issue 1, April 2014;
d) Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Maintenance and Trouble-Clearing Guide, Issue 2, April 2014;

e) Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Command Line Interface Guide, Issue 1, April 2014;
f) Alcatel-Lucent 1830 1354 RM-PhM Photonic Manager Release 12.0 EMS Reference Guide, Issue 1, April 2014;
g) Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Key Management Tool (KMT) Administration Guide, Issue 1, April 2014;
h) Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Key Management Tool (KMT) User Guide, Issue 1, April 2014;
i) Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Key Management Tool (KMT) Installation Guide, Issue 1, April 2014; and
j) Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0.0 Federal Information Processing Standards (FIPS) User Guide and Logbook, Issue 1, May 2015.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the 1830 PSS, including the following areas:

Development: The evaluators analyzed the 1830 PSS functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the 1830 PSS security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the 1830 PSS preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the 1830 PSS configuration management system and associated documentation was performed. The evaluators found that the 1830 PSS configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the 1830 PSS during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the 1830 PSS. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. Initialization: The objective of this test goal is to ensure the TOE is correctly initialized, verified and configured prior to the start of testing;

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

c. FIPS Mode Configuration: The objective of this test goal is to test the various aspects of the TOE in FIPS Mode;

d. Concurrent Login: The objective of this test goal is to confirm the concurrent login behaviour;

e. Trusted Channel: The objective of this test goal is to demonstrate the encrypted, trusted channel between the TOE and the KMT (Key Management Tool) and NMS (Network Management System) servers; and

f. Power Failure Recovery: The objective of this test goal is to demonstrate power failure recovery and that the TOE maintains the FIPS mode through a power failure.

10.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

a. Use of automated vulnerability scanning tools such as Ping Scan, Port Scan, and Nessus Scan to discover potential network, platform and application layer vulnerabilities;

b. Internet Search: The objective of this test case is to search public domains for vulnerabilities relating to the TOE;

c. Banner Grabbing: The objective of this test goal is to determine if any useful information can be gained from the 1830 PSS; and

d. Specific Nessus Scan: The objective of this test goal was to scan the TOE employing specific policies to address the following vulnerabilities:

    a. Heartbleed;

    b. Shellshock;

    c. Poodle;

    d. Ghost; and

    e. Freak.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

10.4 Conduct of Testing

The 1830 PSS was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the 1830 PSS behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

It is recommended that potential operators of the TOE familiarize themselves with the Security Target, and relevant set-up documentation, before operating the device. In particular, it is important that the device be successfully configured into FIPS mode before its operational use.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
KMT	Key Management Tool
NMS	Network Management System
OTN	Optical-Transport Network
PALCAN	Program for the Accreditation of Laboratories - Canada
PSS	Photonic Service Switch
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
WDM	Wavelength Division Multiplexing

14 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Security Target Alcatel-Lucent 1830 Photonic Service Switch (PSS) R7.0, version 0.14, 12 June 2015

e. Evaluation Technical Report Alcatel-Lucent 1830 Photonic Service Switch (PSS) R7.0, version 1.2, 10 June 2015.