Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Pulse Secure, LLC
Pulse Policy Secure 5.0R13

Certification Report
2016/98

11 February 2016
Version 1.0

Amendment Record

Version	Date	Description
1.0	11 Feb 16	Final

Executive Summary

This report describes the findings of the IT security evaluation of Pulse Secure, LLC Pulse Policy Secure 5.0R13 against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Pulse Secure, LLC Pulse Policy Secure 5.0R13 (formerly known as Junos Pulse Access Control Service 5.0) is a network device that provides a mechanism for authenticating users and assessing the health of their host machines to control network access.

The TOE protects communications between itself and web browsers used for administrator access to TOE management functions using HTTPS/TLS. The TOE includes identification and authentication services to users and supports the use of moderately complex passwords. Users may login locally or remotely. The TOE audits security-relevant events that are associated with activity on the TOE and can store these events on an external syslog server. The TOE provides protection for some network denial of service attacks. The TOE protects its own integrity by performing power-on self-tests and the ability to verify the source of updates to the TOE.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit –** auditable events are stored in Syslog files, which can be sent securely to an external server
- **Cryptological Support –** baseline cryptological module is included to provide confidentiality and integrity services for authentication
- **User Data Protection –** TOE is designed to forward packets (i.e. “information flows”) to source and destination entries as provided by TOE users
- **Identification and Authentication –** TOE requires users to provide unique identification and authentication data before any administration access to the system is granted
- **Security Management –** TOE provides for an authorised Administrator role
- **Protection of the TSF –** TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords
- **TOE Access –** TOE can be configured to terminate inactive sessions
- **Trusted Path / Channels –** TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator

The report concludes that the product has complied with the Security Requirements for Network Devices, version 1.1 (NDPP) and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by BAE Systems Applied Intelligence and was completed on 7 December 2015.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
d) The administrator should verify the hash of the downloaded software against the hash provided on the Pulse Secure website.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the Pulse Secure, LLC Pulse Policy Secure 5.0R13 against the requirements of the Common Criteria (CC), the NDPP v1.1 with Errata#3.

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 8) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is Pulse Secure, LLC Pulse Policy Secure 5.0R13.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program (AISEP)
TOE	Pulse Secure, LLC Pulse Policy Secure
Software Version	5.0R13
Hardware Platforms	• SM160 (No Cavium) • SM360 • MAG2600 (fixed configuration chassis and blade) • MAG4610 (fixed configuration chassis and blade) Note: SM160 and SM360 are blades that can be run in MAG6610 and MAG6611 chassis
Virtual Appliance Hardware	IBM Blade Center 2950 blade server with 4 CPU Cores, 4G memory and 20G disk space

Virtual Appliance Software	VMware vSphere 5.1, 5.0, and 4.1
Security Target	Pulse Secure, LLC Pulse Policy Secure 5.0R13 v1.10, dated 23 January 2016
Evaluation Technical Report	Evaluation Technical Report - Pulse Secure, LLC Pulse Policy Secure 5.0R13, V1.0, 29 January 2016 Document reference EFS-T037-ETR
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, Sept 2012, Version 3.1 Rev 4
Methodology	Common Methodology for Information Technology Security September 2012, Version 3.1.Rev 4
Conformance	NDPP v1.1 with Errata #3
Sponsor	Pulse Secure, LLC 2700 Zanker Road, Suite 200 San Jose California CA 95134 United States Website: http://www.pulsesecure.net
Developer	Pulse Secure, LLC 2700 Zanker Road, Suite 200 San Jose California CA 95134 United States Website: http://www.pulsesecure.net
Evaluation Facility	BAE Systems Applied Intelligence Level 1 / 14 Childers Street Canberra ACT 2601 Australia

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies, and its secure usage.

2.2 Description of the TOE

Pulse Policy Secure 5.0R13 is a software network device TOE. It is delivered as hardware with bundled software appliance from Pulse Secure. It is also delivered as a virtual appliance.

The TOE provides access controls for 802.1X-enabled switches and access points to provide user access to network, cloud, and other IT resources. It provides session federation for provisioning of remote access user sessions. Role and application policy enforcement provides granular access enforcement.

The TOE stores security-relevant events in local files that can be sent to an external syslog server (via TLS). Auditable events include start-up and shutdown of the audit functions, authentication events, and service requests. Audit records include the date and time, event category, event type, username, and the outcome of the event (success or failure). Local log storage limits are configurable and are monitored. In the event of storage limits being reached the oldest logs will be overwritten.

The TOE includes a FIPS 140-2 validated cryptographic module that provides confidentiality and integrity services for authentication and for protecting communications with adjacent systems. The cryptographic functions are used to support TLS communications with the syslog server and HTTPS/TLS communications with web browsers used for administration.

The TOE protects from residual information retention from network packets sent during administrator sessions by erasing used memory. This ensures that no residual information from packets in a previous information stream can traverse through the TOE. The TOE also clears secret cryptographic keys when they are no longer needed.

The TOE requires administrators to be successfully identified and authenticated using configured user name and password before allowing any administrative access to the TOE functions and data. Passwords can be configured to a minimum of 15 characters and can include special characters. Once authenticated, users are presented with an administrator-defined warning banner and then granted access only to the functions and data defined by their user role. Failed login attempts provide only obscured feedback and are logged in the audit logs.

The TOE provides an authorised Administrator role that is responsible for the configuration, maintenance and administrative tasks. The TOE is managed through a web-based administrator console interface that is accessible both locally and remotely.

The administrator can update the TOE and verify the updates using RSA digital signatures provided by the crypto module.

The TOE provides protection mechanisms for cryptographic keys and administrator passwords by storing them in an AES 128 encrypted file system. The TOE provides for both cryptographic and non-cryptographic self-tests in order to ensure the integrity of the TOE software. Also, a reliable system clock is provided by the underlying hardware for use to timestamp audit logs and to determine session timeouts.

The TOE can be configured to terminate interactive user sessions. The administrator can configure the idle timeout interval.

The TOE creates trusted channels between itself and the syslog server using TLS. The TOE uses HTTPS with TLS to establish trusted paths between itself and remote administrators and users that protect the confidentiality and integrity of communications.

The functionality defined in the Security Target (Ref 8) that was subsequently evaluated is as follows:

- **Security Audit:** The TOE stores security-relevant events in local files that can be sent to an external syslog server (via TLS). Auditable events include start-up and shutdown of the audit functions, authentication events, and service requests. Audit records include the date and time, event category, event type, username, and the outcome of the event (success or failure). Local log storage limits are configurable and are monitored. In the event of storage limits being reached the oldest logs will be overwritten.
- **Cryptographic Support:** The TOE includes a FIPS 140-2 validated cryptographic module that provides confidentiality and integrity services for authentication and for protecting communications with adjacent systems. The cryptographic functions are used to support TLS communications with the syslog server and HTTPS/TLS communications with web browsers used for administration.
- **User Data Protection:** The TOE protects from residual information retention from network packets sent during administrator sessions by erasing used memory. This ensures that no residual information from packets in a previous information stream can traverse through the TOE. The TOE also clears secret cryptographic keys when they are no longer needed.
- **Identification and Authentication:** The TOE requires administrators to be successfully identified and authenticated using configured user name and password before allowing any administrative access to the TOE functions and data. Passwords can be configured to a minimum of 15 characters and can include special characters. Once authenticated, users are presented with an administrator-defined warning banner and then granted access only to the functions and data defined by their user role. Failed login attempts provide only obscured feedback and are logged in the audit logs.
- **Security Management:** The TOE provides an authorised Administrator role that is responsible for the configuration, maintenance and administrative tasks. The TOE is managed through a web-based administrator console Interface that is accessible both locally and remotely. The administrator can update the TOE and verify the updates using RSA digital signatures provided by the crypto module.

- **Protection of the TSF:** The TOE provides protection mechanisms for cryptographic keys and administrator passwords by storing then in an AES 128 encrypted file system. The TOE provides for both cryptographic and non-cryptographic self-tests in order to ensure the integrity of the TOE software. Also, reliable a system clock is provided by the underlying hardware for use to timestamp audit logs and to determine session timeouts.
- **TOE Access:** The TOE can be configured to terminate interactive user sessions. The administrator can configure the idle timeout interval.
- **Trusted Path/Channels:** The TOE creates trusted channels between itself and the syslog server using TLS. The TOE uses HTTPS with TLS to establish trusted paths between itself and remote administrators and users that protect the confidentiality and integrity of communications.

2.3 TOE Functionality

The TOE provides access controls for 802.1X-enabled switches and access points to provide user access to network, cloud, and other IT resources. It provides session federation for provisioning of remote access user sessions. Role and application policy enforcement provides granular access enforcement.

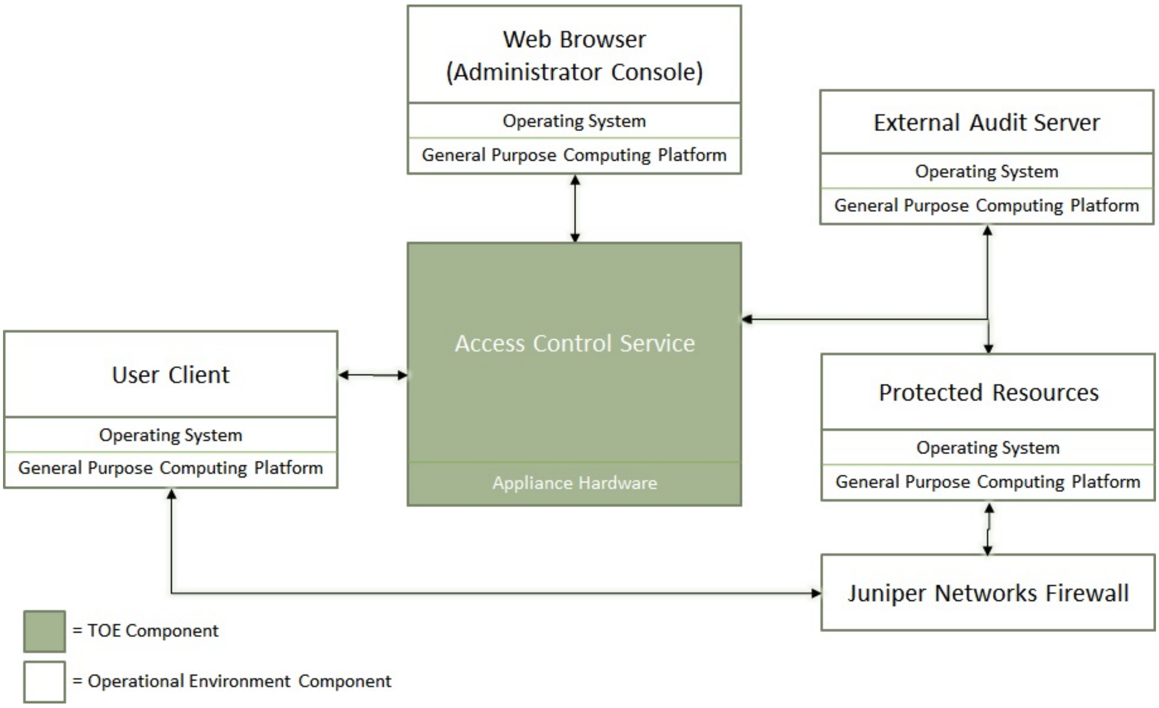
The TOE protects communications between itself and web browsers used for administrator access to TOE management functions using HTTPS/TLS. The TOE includes identification and authentication services to users and supports the use of moderately complex passwords. Users may login locally or remotely. The TOE audits security-relevant events that are associated with activity on the TOE and can store these events on an external syslog server. The TOE protects its own integrity by performing power-on self-tests and the ability to verify the source of updates to the TOE.

2.4 TOE Architecture

The TOE interfaces are comprised of the following:

1. Network interfaces which pass traffic
2. Management interface through which handle administrative actions.

The TOE boundary is shown below:



2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Pulse Policy Secure Configuration Guide (Ref 9).

The scope of the evaluation was limited to those claims made in the Security Target (Ref 8).

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from NDPP (Ref 5) and sufficiently demonstrate the security functionality of the TOE.

The evaluated security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 7) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

2.6 Security

2.6.1 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected.

This evaluation was performed against the U.S Government Protection Profile for Security Requirements for Network Devices (NDPP) Version 1.1 (Ref 5), Errata #3, 3 November 2014 (Ref 6) and no Security Policy Model was provided for the TOE.

2.7 Usage

2.7.1 Evaluated Configuration

The evaluated configuration is based on default installation of the TOE with additional configuration taken from the Operational User Guidance and Preparative Procedures document (Ref 9).

2.7.2 Secure Delivery

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. The customer should perform the following checks upon receipt of a device to verify the integrity of the platform:

- Outside packaging: If the outside shipping box and tape have not been broken, and the outside shipping label properly identifies the customer and the product, then the product has not been tampered with.
- Inside packaging: If the plastic bag or seal on the plastic bag are damaged or removed, the device may have been tampered with.
- Delivery times: if delivery times coincide with the tracking information from the carrier, it can be assumed that the package was not tampered. It is assumed that the trusted carriers (FedEx and UPS) provide reasonable measures to protect the products from tampering during shipping. If the customer identifies a problem during the inspection, he or she should immediately contact the supplier. Provide the order number, tracking number, and a description of the identified problem to the supplier.

Additionally, there are several checks that can be performed to ensure that the customer has received a box sent by Pulse Secure and not a different company masquerading as

Pulse Secure. The customer should perform the following checks upon receipt of a device to verify the authenticity of the device:
When an appliance is shipped, an Advanced Shipment Notification is sent to the email address provided by the customer when the order is taken. This email includes the following information:

- Purchase Order Number
- Pulse Secure Order Number to be used to track the shipment
- Carrier tracking number to be used to track the shipment
- List of Items shipped including serial numbers
- Address and contacts of the customer who ordered the product and who the product will be shipped to
- If a customer wants to verify that a box they have received was sent by Pulse Secure they can do the following:
    - Compare the carrier tracking number or the Pulse Secure order number listed in the Pulse Secure shipment notification with the tracking number on the package received.
    - Log onto the Pulse Secure online customer support portal to view the Order Status. Compare the carrier tracking number or the Pulse Secure order number listed in the Pulse Secure shipment notification with the tracking number on the package received.

2.7.3 Installation of the TOE

The Configuration Guide (Ref 9) contains all relevant information for the secure configuration of the TOE.

2.8 Version Verification

The verification of the TOE is largely automatic, as demonstrated in testing. The TOE cannot load a modified software image. Authentic software images can be downloaded from the Pulse Secure website. In addition to the automated verification, the site includes individual MD5 hashes for each image. The administrator should verify the hash of the software before installing it into the hardware platform.

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The guidance documentation (Ref 9) is available to the consumer when the TOE is purchased.

All guidance material is available for download at **www.pulsesecure.net.** All common criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au.**

2.10 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions, taken directly from the NDPP, must hold in order to ensure the security objectives of the TOE are met.

- 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
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment
- Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the NDPP (Ref 5), Errata #3 (Ref 6), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Ref 1 and 2).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 3).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref 4) were also upheld.

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from Pulse Secure configuration guide (Ref 9).

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the evaluators were taken from the NDPP. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in the Security Target and the Protection Profile were exercised during testing.

3.3.2 Test phases

Testing is determined in the assurance activities in the Protection Profiles. The evaluation was conducted in two phases.

a) **Phase 1**: The TOE was in its default configuration. The first phase of testing was between 31 July 2014 and 06 August 2014.

b) **Phase 2**: The developer updated the TOE to resolve issues identified during first phase of testing. Retesting of the TOE was performed during 19 October 2015 to 02 December 2015.

Cryptographic Algorithm Validation Systems (CAVS) testing was completed on 16 October 2015

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 11).

3.5 Penetration Testing

Penetration tests are based on an independent vulnerability analysis of the TOE using the guidance documentation and available public information. The evaluators used these tests to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential. The following factors have been taken into consideration during the penetration tests:

- Time taken to identify and exploit (elapsed time)
- Specialist technical expertise required (specialist expertise)
- Knowledge of the TOE design and operation (knowledge of the TOE)
- Window of opportunity
- IT hardware/software or other equipment required for exploitation.

The search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables.

Documentation supplied as evidence for the evaluation of the TOE was analysed to identify possible vulnerabilities.

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

4.2 Assurance

This certification is focused on the evaluation of product compliance with a Protection Profile that covers the technology area of network devices. Agencies can have confidence that the scope of an evaluation against an ASD approved Protection Profiles cover the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the Protection Profile (PP). The PP provides assurance by a full security target and an analysis of the SFR in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by testing as outlined in the NDPP, assurance activities, and a vulnerability analysis (based upon TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

Compliance also provides assurance through evidence of secure delivery procedures.

4.3 Certification Result

After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref 10) the Australasian Certification Authority **certifies** the evaluation of the Pulse Secure, LLC Pulse Policy Secure 5.0R13 product performed by the Australasian Information Security Evaluation Facility, BAE Systems Applied Intelligence.

BAE Systems Applied Intelligence **has determined** that Pulse Secure, LLC Pulse Policy Secure 5.0R13 uphold the claims made in the Security Target (Ref 8) and **has met** the requirements of the NDPP.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles.

The analysis is supported by testing as outlined in the NDPP assurance activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 7) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled

b) Configure and operate the TOE according to the vendor's product administrator guidance

c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved

d) The administrator should verify the hash of the downloaded software, as present on the Pulse Secure Website.

Annex A – References and Abbreviations

A.1 References

1. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012, Version 3.1 Revision 4

2. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012, Version 3.1 Revision 4

3. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4

4. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014

5. US Government approved Protection Profile – Protection Profile for Network Devices (NDPP) version 1.1, 8 June 2012

6. Security Requirements for Network Devices – Errata #3, 3 November 2014

7. 2015 Australian Government Information Security Manual (ISM), Australian Signals Directorate

8. Security Target – Pulse Secure, LLC Pulse Policy Secure 5.0R13, Version 1.10, 23 Jan 2016

9. Operational User Guidance and Preparative Procedures –Pulse Secure, LLC Pulse Policy Secure 5.0, Version 1.2, 9 Sep 2015

10. Evaluation Technical Report - Pulse Secure, LLC Pulse Policy Secure 5.0R13, Version 1.0, dated 29 January 2016. Document reference EFS-T037-ETR

11. Seeding of the RNG in SA/UAC Series Devices, Version 4.0, 17 Jun 2015

12. NIST publication SP800-90A Recommendations for Random Number Generation Using Deterministic Random Bit Generation, January 2012.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certification Authority
CAVS	Cryptographic Algorithm Validation System
CC	Common Criteria
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy