SERTIT
Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-010 CR Certification Report

Issue 1.0 9 July 2009

Motorola RFS7000 RF Switch

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.0 13.09.2007

SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a party to this arrangement and is the party's claim that the certificate has been issued in accordance with the terms of this arrangement

The judgements contained in the Certificate and Certification Report are those of SERTIT which issued it and the evaluation facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

* Mutual Recognition under the CC recognition arrangement applies to EAL 4 but not to ALC_FLR.2.

Contents

Certification Statement

Motorola, Inc. Motorola RFS7000 RF Switch is a hardware device used to control operation of multiple wireless access points and to provide secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices.

Motorola RFS7000 RF Switch hardware version RFS7000 and software version RFS7000-1.0.0.0-022GR has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the EAL 4 Common Criteria Part 3 augmented requirements incorporating Evaluation Assurance Level EAL 4 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 conformant functionality. It has also met the requirements of Protection Profile US Government Wireless Local Network Access System Protection Profile for Basic Robustness Environments [8].

Author	Arne Høye Rage Certifier Arne H. Rage
Quality Assurance	Lars Borgos Quality Assurance Lars Borgos
Approved	Kjell W. Bergan Head of SERTIT Kjell W. Bergan
Date approved	9 July 2009

1 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
SERTIT	Norwegian Certification Authority for IT Security
SoF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
WLANAS PP	US Government Wireless Local Area Network (WLAN) Access System Protection Profile [8]

2 References

[1] Motorola WS5100 Wireless Switch and RFS7000 RF Switch Security Target, Document version 1.5, May 20, 2009.

[2] Common Criteria Part 1, CCMB-2005-08-001, Version 2.3, August 2005.

[3] Common Criteria Part 2, CCMB-2005-08-002, Version 2.3, August 2005.

[4] Common Criteria Part 3, CCMB-2005-08-003, Version 2.3, August 2005.

[5] The Norwegian Certification Scheme, SD001, Version 7.0, 28.03.2008.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2005-08-004, Version 2.3, August 2005.

[7] Motorola WS5100 Wireless Switch and RFS7000 RF Switch Evaluation Technical Report A-MOT-WS-5100-7000-ETR-3.0, version 2.0, May 28, 2009.

[8] US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.0, April 2006.

[9] A-MOT-WS-5100-7000-ADO-1.2 Motorola WLAN Switch Delivery and Operation Plan and Procedures, Version 1.2

[10] RFS7000 Installation Guide, 72-103197-01

[11] A-MOT-WS-7000-FIPS-0.4 FIPS 140-2 Level 2 Security Policy for RFS7000 RF Switch

[12] RFS7000 Series RF Switch CLI Reference Guide, 72E-109413-01

[13] A-MOT-WS-5100-7000-MSU-1.1 Motorola Wireless Switch Misuse Analysis

[14] A-MOT-WS-5100-7000-ATE21-1Motorola Wireless Switch Testing Plan and Procedures

[15] A-MOT-WS-5100-7000-ATE22-1 Test topology documents

[16] A-MOT-WS-5100-7000-ATE23-1Motorola Wireless Switch Test Coverage Analysis

[17] Motorola Wireless Switch Independent Testing Report EAL 4, v 0.02

[18] Motorola Wireless Switch Penetration Testing Report EAL 4, v 1.1

3 Executive Summary

3.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Motorola RFS7000 RF Switch with hardware version RFS7000 and software version RFS7000-1.0.0.0-022GR to the Sponsor, Motorola, Inc., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

3.2 Evaluated Product

The version of the product evaluated was Motorola RFS7000 RF Switch with hardware version RFS7000 and software version RFS7000-1.0.0.0-022GR.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Motorola, Inc.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

An overview of the TOE's security architecture can be found in Annex B.

3.3 TOE scope

The TOE, Motorola RFS7000 RF Switch, consists of

- Hardware version: RFS7000
- Software version: RFS7000-1.0.0.0-022GR

3.4 Protection Profile Conformance

The Security Target [1] claimed conformance to the protection profile:

US Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments, Version 1.0, April 2006 [8].

The ST [1] includes additional SFRs for the TOE IT environment to those of the protection profile to provide a more detailed description of the TOE environment.

Chapter 8.10 of the ST [1] provides a rationale for the PP conformance claim.

3.5 Assurance Level

The Security Target [1] specified the assurance requirements for the evaluation. Evaluation assurance level EAL 4 augmented with ALC_FLR.2 was used. Common

Criteria Part 3 [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [2].

3.6 Strength of Function

The overall minimum Strength of Function (SoF) was SoF-Basic. The TOE summary specification rationale does contain specific SOF-basic claims for the password-based authentication mechanism.

The cryptographic mechanisms contained in the TOE are publicly known and as such it is the policy of SERTIT not to comment on its appropriateness or strength.

3.7 Security Policy

The TOE security policies are detailed in the ST [1] chapter 3.3 and the policies are identical to those of WLANAS PP [8].

3.8 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, the threats, OSP's and assumptions which these objectives meet and security functional requirements and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2 [3] except for some explicitly stated requirements. Use of this standard facilitates comparison with other evaluated products.

3.9 Threats Countered

The threats countered by the TOE and the TOE environment are as follows:

- An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
- A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
- A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
- Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
- Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
- The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behaviour being undiscovered leading to flaws that may be exploited by a mischievous user or program.

- A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
- A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
- A user may gain unauthorized access to an unattended session.
- A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
- An unauthorized user or process may gain access to an administrative account.

3.10 Threats and Attacks not Countered

It is not described any threats or attacks that are not countered.

3.11 Environmental Assumptions and Dependencies

- Administrators are non-hostile, appropriately trained and follow all administrator guidance.
- There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment
- Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

3.12 IT Security Objectives

- The TOE will provide the capability to detect and create records of security-relevant events associated with users.
- The TOE will provide the capability to verify the correct operation of the TSF.
- The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE, or outside of the TOE.
- The TOE will use NIST FIPS 140-1/2 validated crypto modules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.
- The TOE will display an advisory warning prior to establishing an administrator session regarding use of the TOE prior to permitting the use of any TOE services that requires authentication.

- The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
- The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy.
- The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
- The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
- The TOE shall obtain reliable time stamps.
- The TOE will provide mechanisms that control a user's logical access to the TOE.
- The TOE will provide administrators with the necessary information for secure management.
- The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.
- The design of the TOE is adequately and accurately documented.
- The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
- The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.

Objectives for the environment, IT- and Non IT-objectives:

- The IT Environment will provide the capability to protect audit information and the authentication credentials.
- The IT Environment will provide the capability to selectively view audit information.
- The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
- Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
- There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
- The environment provides physical security commensurate with the value of the TOE and the data it contains.

- The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE and time service in a manner that is commensurate with the risks posed to the network.
- The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
- The environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
- The TOE IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
- The environment will provide mechanisms that support the TOE in providing a user's logical access to the TOE.
- Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

3.13 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

Audit data generation	FAU_GEN.1(1)
User identity association	FAU_GEN.2
Selective audit	FAU_SEL.1
Explicit: baseline cryptographic module	FCS_BCM_EXP.1
Cryptographic key generation	FCS_CKM.1
Cryptographic key establishment	FCS_CKM_EXP.2
Cryptographic key destruction	FCS_CKM.4
Explicit: random number generation	FCS_COP_EXP.1
Explicit: cryptographic operation	FCS_COP_EXP.2
Protection of user data	FDP_PUD_EXP.1
Subset residual information protection	FDP_RIP.1(1)
Administrator authentication failure handling	FIA_AFL.1(1)
Administrator attribute definition	FIA_ATD.1(1)
Timing of local authentication	FIA_UAU.1
Multiple authentication mechanisms	FIA_UAU_EXP.5(1)
User identification before any action	FIA_UID.2
User-subject binding	FIA_USB.1(1)
User-subject binding	FIA_USB.1(2)
Management of security functions behavior (cryptographic function)	FMT_MOF.1(1)
Management of security functions behavior (audit record generation)	FMT_MOF.1(2)
Management of security functions behavior (authentication)	FMT_MOF.1(3)

Secure security attributes	FMT_MSA.2
Management of audit data	FMT_MTD.1(1)
Management of authentication data (administrator)	FMT_MTD.1(2)
Specification of management functions (cryptographic functions)	FMT_SMF.1(1)
Specification of management functions (TOE audit record generation)	FMT_SMF.1(2)
Specification of management functions (Cryptographic key data)	FMT_SMF.1(3)
Security roles	FMT_SMR.1(1)
Non-bypassability of the TOE Security Policy (TSP)	FPT_RVM.1(1)
TSF domain separation	FPT_SEP.1(1)
Reliable time stamps	FPT_STM_EXP.1
TSF testing	FPT_TST_EXP.1
TSF testing of cryptographic modules	FPT_TST_EXP.2
TSF-initiated termination	FTA_SSL.3
Default TOE access banners	FTA_TAB.1
Inter-TSF trusted channel	FTP_ITC_EXP.1(1)
Trusted path	FTP_TRP.1

3.14 Security Policy

The security policies that apply for the TOE are detailed in the ST [1] chapter 3.3 and they are the same as the policies found in the WLANAS PP [8].

3.15 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and the Common Evaluation Methodology (CEM) [6].

SERTIT monitored the evaluation which was carried out by the evaluation facility Aspect Labs, a division of BKP Security, Inc. (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR) [7] to SERTIT in 28 May 2009. SERTIT then produced this Certification Report.

3.16 General Points

The evaluation addressed the security functionality claimed in the Security Target [1] with reference to the assumed operating environment specified by the Security Target [1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

4 Evaluation Findings

4.1 Introduction

The evaluation addressed the requirements specified in the Security Target [1]. The results of this work were reported in the ETR [7] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

4.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been comprised in delivery. Details can be found in the delivery and operation plan and procedures [9].

4.3 Installation and Guidance Documentation

The procedures for installation of the TOE in evaluated configuration can be found in the following documents:

- The delivery and operation plan and procedures [9]
- The installation guide [10]
- FIPS 140-2 configuration document [11]
- RFS7000 Series RF Switch CLI Reference Guide [12]

The Reference Guide [12] describes administrator and user security functions and interfaces, as well as the initial setup of the TOE in the Common Criteria evaluated configuration.

4.4 Misuse

The evaluators have verified that the guidance identifies all possible modes of operation of the TOE, their consequences and implications for maintaining secure operation. The Misuse Analysis [13] provides rationale for completeness of the guidance.

The ST [1] requires the TOE to be FIPS 140-2 compliant and to run in the Common Criteria evaluated configuration.

When the TOE goes into a security error state the data output and cryptographic operations are disabled.

For secure operation one shall also configure the IT environment to comply with the ST requirements for the IT environment.

4.5 Vulnerability Analysis

The evaluators reviewed the developer's vulnerability analysis and determined that the developer has performed a vulnerability search using publicly available vulnerability databases. Each vulnerability was reviewed and a rationale provided for this vulnerability being either not applicable or non-exploitable to the version of the binary used by the developer.

The evaluators also performed an independent vulnerability analysis and performed penetration testing based on both the developer's and the independent vulnerability analysis.

The penetration testing is documented in the Penetration Testing Report [18] produced by the developers.

4.6 Developer's Tests

The evaluators have examined the developer's test documents [14], [15] and [16] and found that the developer's tests cover all TSFs. The evaluators have also found that the documents contain test descriptions, setup pre-condition, test procedures, expected results, actual results and that the test description identify the security function that is tested. Testing documentation produced by the developer is very extensive and includes over 700 pages.

4.7 Evaluators' Tests

The evaluators devised a set of independent tests based on the following criteria:

- Each testable TSF had to be covered by a test.
- Each External Interface had to be covered by a test.
- Each TOE Subsystem had to be covered by a test
- Preference was given to tests that implicitly tested many security functions and subsystems

The independent tests are documented in the Independent Testing Report [17] produced by the evaluators.

The evaluators devised a subset of the developer's tests covering each class of security functions, each external interface and each TOE subsystem. The sample was approximately 20% of the developer's tests.

5 Evaluation Outcome

5.1 Certification Result

After due consideration of the ETR [7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Motorola RFS7000 RF Switch with hardware version RFS7000 and software version RFS7000-1.0.0.0-022GR meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 conformant functionality and the Protection Profile US Government Wireless Local Network Access System Protection Profile for Basic Robustness Environments [8], in the specified environment.

5.2 Recommendations

Prospective consumers of Motorola RFS7000 RF Switch with hardware version RFS7000 and software version RFS7000-1.0.0.0-022GR should understand the specific scope of the certification by reading this report in conjunction with the Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 3.3 "TOE Scope" and Section 4 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE is uniquely identified as:

Motorola RFS7000 RF Switch with hardware version RFS7000 and software version RFS7000-1.0.0.0-022GR.

TOE Documentation

The supporting guidance documents evaluated were:

- The installation guide [10]
- FIPS 140-2 configuration document [11]
- RFS7000 Series RF Switch CLI Reference Guide [12]

TOE Configuration

The following configuration was used for testing:

- One RF Switch RFS7000 with CC build
- One PoE Switch (To supply Power to the Access Point)
- One L2 Switch for connecting the RF switch and Windows 2003 machine
- One Access Point AP300 connected to the switch
- Laptop with Wireless LAN card
- Windows 2003 machine with Kiwi syslogs server installed

The Windows 2003 Server distribution includes Microsoft NTP server and the authentication server (IAS). The Audit Server in the test configuration is the Kiwi syslog server. The Laptop with Wireless LAN card plays the role of the wireless client.

In addition the following tools were used for testing:

- Wildpackets Omnipeek Wireless Sniffer - version 6.0
- ZENMAP port scanning tool - version 4.85BETA7
- Ethereal Network Protocol Analyzer - version 0.10.14
- Wireshark Network Protocol Analyzer - version 1.0.2
- Odyssey Client Manager - version 4.01.0.1886
- Kiwi Syslog Daemon - version 8.2.5
- PuTTY - release 0.59

Environmental Configuration

TOE uses services of an external RADIUS authentication server for user authentication. The authentication server supports EAP-TLS, EAP-TTLS and PEAP authentication protocols.

Reliable time stamps are provided by an external Network Time Protocol (NTP) server.

Audit records generated by the TOE are transmitted to the external syslog audit server. The audit server provides protected storage for audit records, as well as a capability to view and search audit records.

Network connections between the TOE and external authentication, audit and time servers are protected by a trusted channel, as required by the WLANAS PP [8]. The IPSec/IKE security protocol is used to establish secure network connections for the trusted channel.

Annex B: Product Security Architecture

This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

The TOE is a device used to control operation of multiple wireless access points and to provide secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices. The TOE is installed at a wired network location, and is logically connected to a set of wireless access point devices over a wired Ethernet network. Wireless access point devices are hardware radio devices, which do not provide security functionalities and are used to tunnel wireless network traffic between the TOE and wireless client devices.

The TOE protects data exchanged with wireless client devices using IEEE 802.11i wireless security protocol, which provides data authentication and encryption using the AES-CCM cryptographic algorithm. The TOE uses FIPS 140-2 compliant cryptographic implementations for all cryptographic purposes and is operated in the FIPS 140-2 approved mode of operation.

Wireless users are required to authenticate before access to the wired network is granted by the TOE. The authentication is based on IEEE 802.1X EAP-TLS, EAP-TTLS and PEAP authentication protocols. The TOE acts as the 802.1X authenticator and utilizes services of an external RADIUS authentication server to provide wireless user authentication. During the authentication phase the TOE serves as an intermediary passing authentication messages between the wireless client device and the external authentication server. If the authentication is successful, the authentication server passes to the TOE 802.11i session keys used to establish a 802.11i secure connection between the TOE and the wireless client device. Once the connection is established, the wireless client device may access the protected wired network utilizing the TOE as a gateway. The network connection between the TOE and the external authentication server is protected using the IPSec/IKE security protocol. EAP-TLS authentication protocol uses a client certificate for wireless user authentication, EAP-TTLS and PEAP protocols use password-based authentication.

The TOE provides remote management capabilities using SSH security protocol, as well as local management capabilities via a local serial port connection. The TOE administrators are required to authenticate using a username/password combination. The TOE provides an option to authenticate administrators against an internal administrator database, or against the external authentication server, however only internal administrator database is used in the evaluated configuration.

The TOE provides capabilities to terminate idle wireless user and administrator sessions after the inactivity time limit has been reached, as well as disable a remote administrator account after a predefined number of failed authentication attempts had been reached. The account can then be re-enabled using a local serial port administration session.

The TOE provides auditing capabilities which utilize services of an external syslog audit server. The network connection between the TOE and the external audit server is secured using IPSec/IKE security protocol.

The TOE utilizes services of an external Network Time Protocol (NTP) server to obtain reliable time stamps used in audit records. The network connection between the TOE and the external NTP server is secured using IPSec/IKE security protocol.

The TOE provides capabilities to run a set of self-test on power-on and on demand to verify the integrity and critical functions of the TOE. The security of network data is maintained by zeroizing the memory location corresponding to a network packet, after the packet has been processed by the TOE.