API Technologies™ Netgard™ MFD

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2018-000-D102
Version: 1.1
11 July 2017

API Technologies
120 Corporate Blvd
South Plainfield, New Jersey
07080

Prepared by:
EWA-Canada
1223 Michael Street, Suite 200
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	API Technologies™ Netgard™ MFD Security Target
ST Version:	1.1
ST Date:	11 July 2017

1.3 TOE REFERENCE

TOE Identification: API Technologies™ Netgard™ MFD v1.8.0-1 CL310S, API Technologies™ Netgard™ MFD v1.8.0-1-v CL310S2 and API Technologies™ Netgard™ MFD v1.8.0-1-HP CL310HP for HP Large Format Printers

TOE Developer: API Technologies™

TOE Type: MFD Authentication Device (Access Control Device)

1.4 TOE OVERVIEW

Netgard MFD is an inline user authentication device for networked, special purpose devices such as multi-function printer/scanner/copiers.

Users of the multifunction device are required to authenticate themselves with a smartcard (Common Access Card (CAC)/Personal Identity Verification (PIV) card) and personal identification number (PIN) prior to accessing or distributing privileged materials. Prior to authentication, users are not permitted to print, scan, or send from the multi-function device to network resources.

Netgard MFD is designed to work with multifunction devices that do not natively support CAC/PIV access.

Three controlled access scenarios are included in the evaluation:

- Scan to Email
    - A user may scan a document and send it to the user's email account via a signed and encrypted email.
- Scan to Home
    - A user may scan a document and send it to the user's home directory. Authentication and protection on the network are provided using Kerberos.
- Secure Print Release
    - A user may send a document to the printer. The Netgard device encrypts and stores the document until the user authenticates. Once authenticated, the print jobs are released to the printer.

The Netgard device sits between the printer and the network and acts as a firewall, blocking any attempts to send scanned documents from the printer without proper authentication.

The TOE is a combined software and hardware TOE.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of the Netgard MFD hardware and software and attached card reader device. Figure 1 shows the evaluated configuration, which reflects a typical implementation configuration.

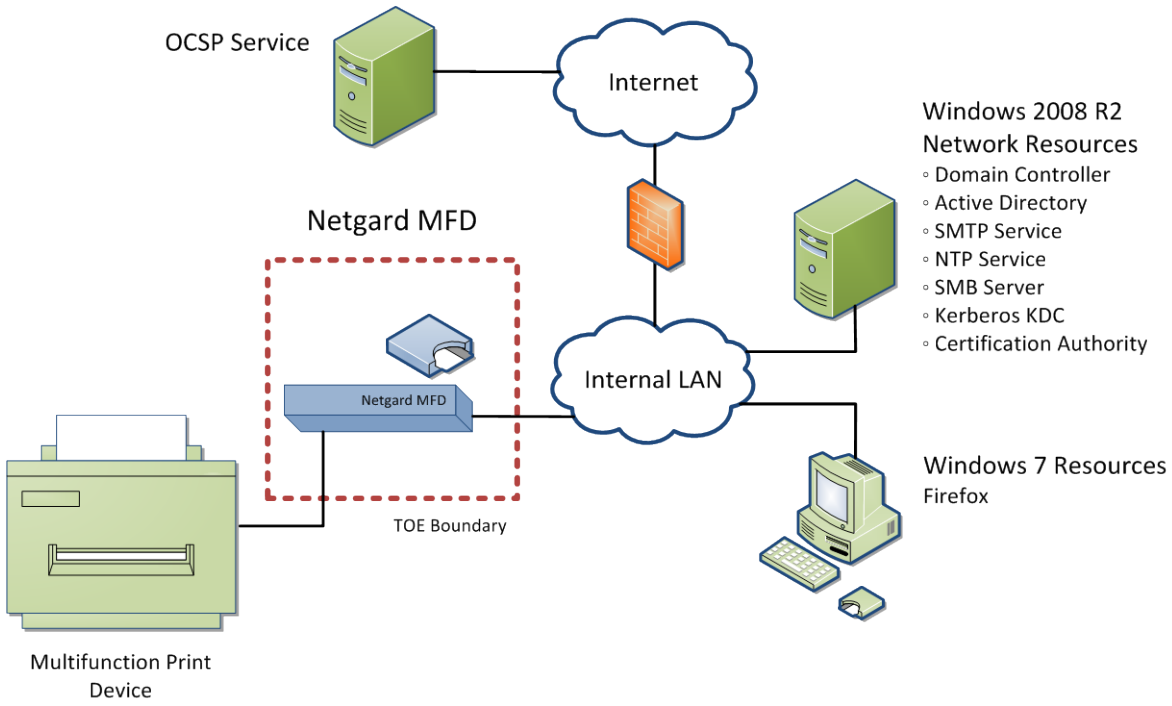

Figure 1 – Netgard MFD Diagram

The TOE consists of the following devices:

Component	Description
Netgard MFD CL310S	Netgard appliance including: • ACR Card Reader with PIN pad and metal bracket • OMNIKEY 3121 Card Reader (Optional) • Power Supply • CAT5 Cable • Packing material and documentation CD
Netgard MFD CL310S2	Netgard appliance including: • ACR Card Reader with PIN pad and metal bracket • OMNIKEY 3121 Card Reader (Optional) • Power Supply

Component	Description
	• CAT5 Cable • Packing material and documentation CD
Netgard MFD CL310 for HP Large Format Printers	Netgard appliance for HP Large Format Printers (HP Design Jet and HP PageWide XL) including: • ACR Card Reader with PIN pad and metal bracket • OMNIKEY 3121 Card Reader (Optional) • Power Supply • CAT5 Cable • Packing material and documentation CD

Table 1 – TOE Devices

1.5.2 TOE Environment

The following network components are required for operation of the TOE in the evaluated configuration.

Component	Operating System / Software / Service	Hardware
Multifunction Print Device	Not applicable	Brother HP 3500
Domain Controller	Windows Server 2008 R2	General Purpose Computer Hardware
Active Directory	Windows Server 2008 R2	General Purpose Computer Hardware
Simple Mail Transfer Protocol (SMTP) Service	Windows Server 2008 R2	General Purpose Computer Hardware
Network Time Protocol (NTP) Service	Windows Server 2008 R2	General Purpose Computer Hardware
Server Message Block (SMB) Server	Windows Server 2008 R2	General Purpose Computer Hardware
Kerberos Key Distribution Center (KDC)	Windows Server 2008 R2	General Purpose Computer Hardware
Certification Authority	Windows Server 2008 R2	General Purpose Computer Hardware

Component	Operating System / Software / Service	Hardware
Online Certificate Status Protocol (OCSP) Service	This is the OCSP service associated with the user smartcard credentials	Not applicable
Administrative Workstation	Windows 7 Firefox Browser	General Purpose Computer Hardware

Table 2 – Non-TOE Hardware and Software

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- Netgard MFD Quick Start Guide, Version 3.1
- Netgard MFD Administrator Guide, Version 1.8.0
- Netgard MFD Scan to Home and Secure Print Release Deployment Guide, Version 6
- Scan to Home for HP T2500 Plotter Deployment Guide, Version 1.6
- Netgard MFD Common Criteria Guidance Supplement, Version 1.0

1.5.4 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. Audit logs may be read from the Management Interface. Audit trail storage is protected from unauthorized deletion.
Cryptographic Support	A FIPS-validated cryptographic module provides cryptographic functions in support of secure operations.
User Data Protection	The TOE ensures the controlled flow of information, allowing only properly authenticated users to perform the following functions: • Scan a document, digitally sign the document and send to a user's home directory • Scan a document and send it to the user in a digitally signed and encrypted email • Release a print job to the printer

Functional Classes	Description
Identification and Authentication	Administrative users must identify and authenticate prior to being granted access to the Management Interface.
Security Management	The TOE provides management capabilities via a Web-Based Graphical User Interface (GUI), accessed via Hypertext Transfer Protocol Secure (HTTPS). Management functions allow the administrators to configure the system, review audit records and manage administrative users.
Protection of the TSF	Scanned documents may be sent to a user in a digitally signed and encrypted email. Reliable timestamps are provided in support of audit records.
TOE Access	Administrative sessions timeout after an administrator-configurable period of time. Authenticated user sessions timeout after 45 minutes, or at the conclusion of the current scan.
Trusted Path/Channel	The communications links between the TOE and its remote administrators are protected using HTTPS (Transport Layer Security (TLS) v1.1 and TLSv1.2).

Table 3 – Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- 802.1x security is supported for the Ethernet connection to the network; however, this was not evaluated.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 has to be taken into account.

2.2 ASSURANCE PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.ACCESS	An unauthorized person may attempt to bypass the TOE security policy to send sensitive data from the scanner of an MFD.
T.PRINTOUT	An unauthorized user may be able to view a printed document before the owner is able to retrieve it from the shared printer.
T.UNDETECT	Authorized or unauthorized users may be able to access TSF or user data or modify TOE behaviour without a record of those actions in order to circumvent TOE security functionality.
T.UNAUTH	An unauthorized user may be able to access security management functions, resulting in changes to the security configuration.

Table 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies applicable to this TOE.

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
A.ACCESS	The TOE is connected to the network in such a way that it is able to access all of the network resources required to support authentication, access to email and access to the user's home directory.

Assumptions	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The TOE must be in close proximity to the MFD.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ADMIN	The TOE will provide all the 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 or disclosure.
O.ACCESS	The TOE must ensure that only authenticated users are permitted to perform restricted scanning and printing functions.
O.AUDIT	The TOE must record audit records for changes to the TOE configuration, and use of the TOE access control functions. Audit records must be provided in a format appropriate for user interpretation.
O.CRYPTO	The TOE must use FIPS-validated cryptographic functions in support of cryptographic operations.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
O.PROTECT	The TOE must provide the ability to encrypt and digitally sign scanned data before it is sent from the TOE.
O.TERMINATE	Users must be able to terminate authenticated sessions. Authenticated sessions must timeout when no longer in use.
O.TIME	The TOE must provide reliable timestamps.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.AVAIL	The TOE environment must ensure that the appropriate MFD and network support are available and accessible to the TOE at all times.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 7 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.ACCESS	T.PRINTOUT	T.UNDETECT	T.UNAUTH	A.ACCESS	A.LOCATE	A.MANAGE	A.NOEVIL
O.ADMIN			X	X				
O.ACCESS	X	X						
O.AUDIT			X					
O.CRYPTO	X	X						
O.IDENTAUTH			X	X				
O.PROTECT	X							
O.TERMINATE	X			X				
O.TIME			X					

	T.ACCESS	T.PRINTOUT	T.UNDETECT	T.UNAUTH	A.ACCESS	A.LOCATE	A.MANAGE	A.NOEVIL
OE.AVAIL					X			
OE.PERSON							X	X
OE.PHYSICAL						X		

Table 8 – Mapping Between Objectives, Threats, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE back to the threats addressed by the TOE.

Threat: **T.ACCESS**	An unauthorized person may attempt to bypass the TOE security policy to send sensitive data from the scanner of an MFD.	
Objectives:	O.ACCESS	The TOE must ensure that only authenticated users are permitted to perform restricted scanning and printing functions.
	O.CRYPTO	The TOE must use FIPS-validated cryptographic functions in support of cryptographic operations.
	O.PROTECT	The TOE must provide the ability to encrypt and digitally sign scanned data before it is sent from the TOE.
	O.TERMINATE	Users must be able to terminate authenticated sessions. Authenticated sessions must timeout when no longer in use.
Rationale:	O.ACCESS mitigates this threat by ensuring that only authenticated users are permitted to access scanning and printing functions. O.CRYPTO ensures that cryptographic operations, including those used for authentication, are supported by FIPS-validated cryptographic functions. O.PROTECT mitigates this threat by providing integrity and confidentiality to information as it is transferred from the TOE. O.TERMINATE ensures that authenticated sessions are	

	appropriately terminated.

Threat: **T.PRINTOUT**	An unauthorized user may be able to view a printed document before the owner is able to retrieve it from the shared printer.	
Objectives:	O.ACCESS	The TOE must ensure that only authenticated users are permitted to perform restricted scanning and printing functions.
	O.CRYPTO	The TOE must use FIPS-validated cryptographic functions in support of cryptographic operations.
Rationale:	O.ACCESS mitigates this threat by ensuring that only authorized users may access restricted printing functions. O.CRYPTO mitigates the threat by ensuring that FIPS-validated cryptographic functions are provided to protect data sent to the printer.	

Threat: **T.UNDETECT**	Authorized or unauthorized users may be able to access TSF or user data or modify TOE behaviour without a record of those actions in order to circumvent TOE security functionality.	
Objectives:	O.ADMIN	The TOE will provide all the 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 or disclosure.
	O.AUDIT	The TOE must record audit records for changes to the TOE configuration, and use of the TOE access control functions. Audit records must be provided in a format appropriate for user interpretation.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.ADMIN mitigates this threat by providing access control to the functions used to administer the TOE. O.AUDIT mitigates this threat by ensuring that changes to the TOE configuration are audited, and that audit records are readily available for review by authorized administrators. O.IDENTAUTH ensures that only identified and authenticated users	

	have access to TOE functions. O.TIME ensures that audit data is supported with accurate time information.

Threat: **T.UNAUTH**	An unauthorized user may be able to access security management functions, resulting in changes to the security configuration.	
Objectives:	O.ADMIN	The TOE will provide all the 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 or disclosure.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.TERMINATE	Users must be able to terminate authenticated sessions. Authenticated sessions must timeout when no longer in use.
Rationale:	O.ADMIN mitigates the threat by ensuring that only authorized users have access to security management functions. O.IDENTAUTH mitigates the threat by ensuring that users are identified and authenticated prior to being granted access to administrative functions. O.TERMINATE mitigates the threat by ensuring that user sessions are terminated when no longer in use.	

4.3.2 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: **A.ACCESS**	The TOE is connected to the network in such a way that it is able to access all of the network resources required to support authentication, access to email and access to the user's home directory.	
Objectives:	OE.AVAIL	The TOE environment must ensure that the appropriate MFD and network support are available and accessible to the TOE at all times.

Rationale:	OE.AVAIL supports this assumption by ensuring the availability of required network resources.

Assumption: A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The TOE must be in close proximity to the MFD.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: A.MANAGE	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
Rationale:	OE.PERSON supports this assumption by ensuring that trained individuals are in place to manage the TOE.	

Assumption: A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
Rationale:	OE.PERSON supports this assumption by ensuring that the individuals managing the TOE have been specifically chosen to be careful, attentive and non-hostile.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section5, summarized in Table 9 - Summary of Security Functional Requirements.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (AES and RSA)
	FCS_CKM.1(2)	Cryptographic key generation (RSA)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_IFC.1	Subset information flow control

Class	Identifier	Name
(FDP)	FDP_IFF.1	Simple security attributes
Identification and Authentication (FIA)	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
Trusted path/channels (FTP)	FTP_TRP.1	Trusted path

Table 9 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*user authentication, application of access control, login to the management interface, configuration changes*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other information*].

6.2.1.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*authorized administrators*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1(1) Cryptographic key generation (AES and RSA)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Deterministic Random Bit Generator*] and specified cryptographic key sizes [*128, 192, 256 bits (symmetric); 2048 bits (asymmetric)*] that meet the following: [*SP800-90A*].

6.2.2.2 FCS_CKM.1(2) Cryptographic key generation (RSA)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*RSA Key Pair Generation*] and specified cryptographic key sizes [*2048 bits*] that meet the following: [*ANSIX9.31*].

6.2.2.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2*].

6.2.2.4 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations listed in column 1 of Table 10*] in accordance with a specified cryptographic algorithm [*listed in column 2 of Table 10*] and cryptographic key sizes [*listed in column 3 of Table 10*] that meet the following: [*standards listed in column 4 of Table 10*].

Function	Algorithm	Details	Standard
Encryption and Decryption	AES	Key Size (bits) 128, 192, 256	FIPS 197
Digital Signature	RSA	Key Size (bits) 1024[1], 2048	FIPS 186-2
Keyed-Hash Message Authentication Code	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384	Digest Length (bits) 160, 256, 384 Key Size (bits) 512, 1024	FIPS 198
Secure Hash	SHA-1 SHA-256 SHA-384	Digest Length (bits) 160, 256, 384	FIPS 180-3

Table 10 - Cryptographic Operations

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*authenticated user flow control SFP*] on [
Subjects: MFD Users
Information: Data to be scanned or printed

[1] 1024 bit RSA is supported for signature verification only.

Operations: Scan, Print
].

6.2.3.2 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [*authenticated user information flow control SFP*] based on the following types of subject and information security attributes: [
Subjects: MFD Users
Subject security attributes: authentication information
Information: Data to be scanned or printed
Information security attributes: none
].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [
1. An authenticated user may scan a document and send it to the user's email account via a signed and/or encrypted email
2. An authenticated user may scan a document and send it to the user's own networked home directory
3. A document will only be released to the printer once the user has been authenticated by the Netgard device].

FDP_IFF.1.3 The TSF shall enforce the [*no additional rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*no additional rules*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*no additional rules*].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.2 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: FIA_UAU.2 and FIA_UID.2 apply to administrative users accessing the management interface. Authentication of MFD users is described in FDP_IFC.1 and FDP_IFF.1.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*authenticated user information flow control SFP(s)*] to restrict the ability to [[*configure*]] the security attributes [*authentication options*] to [*authorized administrators assigned to the admin role*].

6.2.5.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*authenticated user information flow control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow ~~the~~ [*authorized administrators assigned to the admin role*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*configuration of user authentication options, scan and print set up, audit log review, and management of administrative users*].

6.2.5.4 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*admin, guest*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

6.2.6.2 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*an administrator-configurable interval of user inactivity*].

6.2.7.2 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.8 Trusted Path/Channels (FTP)

6.2.8.1 FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication, [*remote administration*]].

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The following Table provides a mapping between the Security Functional Requirements (SFRs) and Security Objectives.

	O.ADMIN	O.ACCESS	O.AUDIT	O.CRYPTO	O.IDENTAUTH	O.PROTECT	O.TERMINATE	O.TIME
FAU_GEN.1			X					
FAU_SAR.1			X					
FCS_CKM.1(1)				X				
FCS_CKM.1(2)				X				
FCS_CKM.4				X				
FCS_COP.1				X				
FDP_IFC.1		X						
FDP_IFF.1		X						
FIA_UAU.2					X			
FIA_UID.2					X			
FMT_MSA.1	X							
FMT_MSA.3	X							
FMT_SMF.1	X							
FMT_SMR.1	X							
FPT_ITC.1						X		
FPT_STM.1								X
FTA_SSL.3							X	
FTA_SSL.4							X	
FTP_TRP.1	X							

Table 11 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.ADMIN**	The TOE will provide all the 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 or disclosure.	
Security Functional Requirements:	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FTP_TRP.1	Trusted path
Rationale:	FMT_SMF.1 provides the management functions required to manage the security functionality of the TOE. FMT_SMR.1 provides the roles that allow restriction of functions to authorized users. FMT_MSA.1 and FMT_MSA.3 ensure that the security attributes used by the access control mechanism may be configured, and have appropriate default values. FTP_TRP.1 ensures that the access to the management functions is protected from unauthorized use or disclosure.	

Objective: **O.ACCESS**	The TOE must ensure that only authenticated users are permitted to perform restricted scanning and printing functions.	
Security Functional Requirements:	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Rationale:	FDP_IFC.1 and FDP_IFF.1 ensure that only authenticated users are able to perform the scanning and printing functions associated with scan to email, scan to home and secure print release functions.	

Objective: **O.AUDIT**	The TOE must record audit records for changes to the TOE configuration, and use of the TOE access control functions. Audit records must be provided in a format appropriate for user interpretation.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
Rationale:	FAU_GEN.1 outlines what data must be included in audit records and what events must be audited. FAU_SAR.1 ensures that the records are provided to authorized	

	administrators in an appropriate format.

Objective: O.CRYPTO	The TOE must use FIPS-validated cryptographic functions in support of cryptographic operations.	
Security Functional Requirements:	FCS_CKM.1(1)	Cryptographic key generation (AES and RSA)
	FCS_CKM.1(2)	Cryptographic key generation (RSA)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Rationale:	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.4 and FCS_COP.1 detail the cryptographic key generation, key destruction and cryptographic operation required to support TOE functionality for user authentication, send to home, send to email and secure print release.	

Objective: O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Rationale:	FIA_UAU.2 and FIA_UID.2 ensures that administrative users are identified and authenticated before being granted access to TOE functions.	

Objective: O.PROTECT	The TOE must provide the ability to encrypt and digitally sign scanned data before it is sent from the TOE.	
Security Functional Requirements:	FPT_ITC.1	Inter-TSF confidentiality during transmission
Rationale:	FPT_ITC.1 ensures that scanned data may be encrypted to protect it from unauthorized disclosure before it is sent from the TOE.	

Objective: O.TERMINATE	Users must be able to terminate authenticated sessions. Authenticated sessions must timeout when no longer in use.	
Security	FTA_SSL.3	TSF-initiated termination

Functional Requirements:	FTA_SSL.4	User-initiated termination
Rationale:	FTA_SSL.3 ensures that authenticated sessions timeout when no longer in use. FTA_SSL.4 ensures that users are able to terminate authenticated sessions.	

Objective: **O.TIME**	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 ensures that the TOE provides reliable time stamps.	

6.4 DEPENDENCY RATIONALE

Table 12 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FCS_CKM.1 (1)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1
	FCS_CKM.4	✓	
FCS_CKM.1 (2)	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(1) and FCS_CKM.1(2)
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1(1) and FCS_CKM.1(2)
	FCS_CKM.4	✓	
FDP_IFC.1	FDP_IFF.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_IFC.1
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_ITC.1	None	N/A	
FPT_STM.1	None	N/A	
FTA_SSL.3	None	N/A	
FTA_SSL.4	None	N/A	
FTP_TRP.1	None	N/A	

Table 12 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in Table 13– Security Assurance Requirements.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 13 – Security Assurance Requirements

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 SECURITY AUDIT

Netgard generates logs for security related events including user authentication and the application of Netgard firewall rules, login to the management interface, and configuration changes. System startup is logged. System shutdown may be identified in the log files as the time at which logs are no longer being captured.

Audit logs may be reviewed by authorized administrators using the management interface by selecting 'View Event Logs' from the Monitoring tab. All of the roles supported by the management interface allow the viewing of audit records.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_SAR.1.

7.2 CRYPTOGRAPHIC SUPPORT

Cryptographic support is provided by the Common Crypto Module for PRIISMS, PRIISMS RD, SA5600-IA and NetGard MFD, Version 1.0, Cryptographic Module Validation Program (CMVP) certificate 2070.

AES keys are generated in accordance with SP800-90A and RSA keys are generated in accordance with SP800-90A and ANSI X9.31. The key destruction function overwrites the memory occupied by the keys with zeroes and deallocates the memory.

Cryptographic support is provided in support of the following functions:

- TLS is supported between the device and the browser for use of the management interface. TLS 1.1 and TLS 1.2 are supported.
- Authentication is performed using the keys on the CAC/PIV card.
- Email that is sent from the Netgard device is signed and encrypted using the keys from the CAC/PIV card, and a Netgard generated symmetric key.
- Digital signing is provided as part of the SMB protocol when files are sent to an SMB share.
- Netgard acts as a Kerberos client in support of Kerberos authentication.
- For secure print release, the files are stored encrypted on the device, and are decrypted when released. The keys are created on the device and are maintained for a limited period of time. If power is lost, the keys and the files are deleted.

TOE Security Functional Requirements addressed: FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.4, FCS_COP.1.

7.3 USER DATA PROTECTION

The TOE supports three user data protection functions:

- Scan to Email
- Scan to Home
- Secure Print Release

7.3.1 Scan to Email

This feature allows an authenticated user to generate an email from the device and pass it to the organization's Local Area Network (LAN) for delivery. The 'From' address will be changed from the default, and the 'To:' address may be changed as well. The replacement addresses may be retrieved from the Lightweight Directory Access Protocol (LDAP) directory, or from the user's CAC/PIV card. In the evaluated configuration, the email is sent to the originating user, and the email is encrypted and signed.

7.3.2 Scan to Home

The MFD acts as an SMB client to transfer the file through the SMB server on the Netgard device. The Netgard device then acts as an SMB client to send the file to the user's home SMB Server. When the MFD writes a file to SMB, it is written directly to the user's home directory. The user's home directory must be defined in the LDAP user profile. LDAP and Kerberos authentication must be implemented.

7.3.3 Secure Print Release

When the secure print release feature is implemented, print jobs sent to the network printer are stored on the Netgard MFD device in an encrypted file system. When the user authenticates to the device, any outstanding print jobs for that user are released to the printer. The keys used to encrypt the file system are created on the device at boot time and are destroyed when the power is interrupted to the device. Once the print job has been printed, or the hold time has expired, the print jobs are destroyed. Print jobs and keys will also be deleted if the disk becomes full to the configured percentage threshold. The default configuration is 90%. Once the system reaches this threshold, the Netgard application deletes the oldest print jobs until enough storage space has been released to put the disk storage below the configured threshold.

7.3.4 Authentication Options

There are several authentication options offered:

- PIN only. This verifies that the smartcard PIN is correct. PIN only is not an option used in the evaluated configuration.
- X.509 certificate authentication. Netgard verifies that the user certificate is valid and trusted.
- X.509 certificate authentication with OCSP. Netgard verifies that the user certificate is valid, trusted and has not been revoked.

- LDAP. Netgard performs an LDAP lookup to verify that the user exists in the domain and has not been disabled. The lookup is performed using data from the card. This may be the user's name as it appears in an X.509 certificate, or it may be other data on the card depending upon the system configuration.
- Kerberos and LDAP. The user must have a certificate that is trusted by the KDC, and LDAP must be implemented. Kerberos authentication is performed using the Microsoft implementation of Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) protocol (Request for Comments (RFC) 4556).

Table 14 shows the allowable Authentication Selections for the Scan to Email, Scan to Home and Secure Print Release features. It should be noted that the PIN only option is not used in the evaluated configuration. The OCSP checking option is only used with X.509 authentication.

Feature	Required Authentication Selections				
	PIN	X.509	OCSP	LDAP	Kerberos
Scan to Email	Required	Optional	Optional	Optional	Optional
Scan to Home	Required	Optional	Optional	Required	Required
Secure Print Release	Required	Optional	Optional	Required	Optional

Table 14 – Required Authentication Selections

TOE Security Functional Requirements addressed: FDP_IFC.1, FDP_IFF.1.

7.4 IDENTIFICATION AND AUTHENTICATION

Users of the management interface must be identified and authenticated before being granted access to any functionality.

FIA_UAU.2 and FIA_UID.2 apply to administrative users accessing the management interface. Authentication of MFD users is described in FDP_IFC.1 and FDP_IFF.1.

TOE Security Functional Requirements addressed: FIA_UAU.2, FIA_UID.2.

7.5 SECURITY MANAGEMENT

Users are authenticated and information is allowed to flow based on the attributes on the smartcard and in the LDAP database. The TOE security management functionality does not allow manipulation of these attributes, but does allow configuration of which attributes are to be used for authentication. The default values are restrictive in that authentication is not enabled until the system has been configured.

Netgard MFD is managed using the management interface. This is a web based application that allows configuration of the user authentication options, scan and print set up, review of audit records and management of administrative users. There are two user roles supported for this interface. Users in the 'admin' role are able to perform all functions. Users in the 'guest' role have read only access to the interface functions.

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

7.6 PROTECTION OF THE TSF

In the evaluated configuration, a document scanned at the MFD is sent in an encrypted email from the Netgard device to the user's inbox.

Reliable time is provided by an NTP server and is used by the Netgard device to create reliable timestamps for use in audit logging.

TOE Security Functional Requirements addressed: FPT_ITC.1, FPT_STM.1.

7.7 TOE ACCESS

An interactive session on the Management interface times out after a period of inactivity. The default is five minutes of inactivity; however, this may be configured by an administrator in the 'admin' role. Administrative users may terminate their own sessions at any time by selecting 'Logout' in the upper right hand of the Management interface screen.

User sessions start when the card is inserted into the card reader and terminate when the card is removed. Sessions also terminate after 45 minutes, or at the conclusion of the current scan, if a scan is in progress at the 45 minute mark.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_SSL.4.

7.8 TRUSTED PATH / CHANNELS

The connection between a remote user and the Management interface is protected using TLS. The user identifies the Management interface by selecting the IP address of the Netgard device. The Netgard device requires a username and password to identify the user. The link is protected from modification and disclosure using the TLS protocol. The trusted path is initiated by the remote user, and is used for remote administration of the device.

TOE Security Functional Requirements addressed: FTP_TRP.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
admin	This is the default administrator account. All administrative permissions have been granted to this account, and this account may not be deleted. This is also the name of the role associated with this account. Users in the 'admin' role have all Management interface permissions.

Table 15 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CAC	Common Access Card
CAT5	Category 5
CC	Common Criteria
CD	Compact Disk
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HP	Hewlett-Packard
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
KDC	Key Distribution Center
LAN	Local Area Network

Acronym	Definition
LDAP	Lightweight Directory Access Protocol
MFD	Multi-function Device
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKINIT	Public Key Cryptography for Initial Authentication in Kerberos
PP	Protection Profile
RFC	Request for Comments
RSA	Rivest, Shamir and Adleman
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SP	Special Publication
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

Table 16 – Acronyms