FIPS 140-2 Security Policy

Ultra Electronics DNE Technologies PacketAssure iQ1000

---

50 Barnes Park North
Wallingford, CT 06492

December 18, 2015

Document Version 3.14
Firmware Versions 3.2.0 and 3.4.0
Chassis V.003
PSM V.101

DNE TECHNOLOGIES

Table of Contents

1. Module Specification 4
   1.1. Module Description 4
   1.2. Purpose 7
   1.3. Security level 7
   1.4. References 7
   1.5. Glossary 8
2. Cryptographic Module Ports and Interfaces 9
3. Roles, Services, and Authentication 9
   3.1. Roles 9
      Unauthenticated Services 9
      Non-Approved Mode Services 10
      User Role Services (Approved Mode) 11
      Crypto-officer Role Services (Approved Mode) 12
   3.2. Authentication Mechanisms and Strength 14
4. Finite State Model 15
5. Physical Security 15
   5.1. Enclosure 16
   5.2. Tamper Evidence 16
   5.3. Physical Security Rules 16
   5.4. Secure Operation Initialization Rules 17
6. Operational Environment 18
7. Definition of SRDIs Modes of Access 18
   7.1. Cryptographic Keys, CSPs, and SRDIs 19
   7.2. Access Control Policy 22
8. Electromagnetic Interface/Electromagnetic Compatibility 23
9. Self Tests 23
   9.1. Power-Up Self Tests 24
   9.2. Conditional Self tests 24
10. Mitigation of Other Attacks 25

List of Figures

Figure 1 PacketAssure iQ1000, IOM Side 4
Figure 2 Cryptographic Boundary 6
Figure 3 Tamper Evidence Seal Locations 16

List of Tables

Table 1 Items Excluded from Cryptographic Boundary 5
Table 2 Security Levels 7
Table 3 Ports and Interfaces 9
Table 4 Unauthenticated Services 10
Table 5 Non-Approved Services 10
Table 6 User Roles 12
Table 7 Crypto-officer Role 14
Table 8 Approved Cryptographic Algorithms 17
Table 9 Non-Approved Cryptographic Algorithms 18
Table 10 Key, CSPs and SRDIs 22
Table 11 SRDI Access 23

FIPS 140-2 Security Policy

Ultra Electronics DNE Technologies PacketAssure iQ1000

Firmware Versions 3.2.0 and 3.4.0 (Freescale PowerQUICC II Pro)

Chassis V.003

PSM V.101

1. Module Specification

1.1. *Module Description*

The Ultra Electronics DNE Technologies PacketAssure iQ1000, see Figure 1, is a rugged, one 19" rack unit Service Delivery Management (SDM) appliance. It integrates adaptation of legacy circuit based traffic with high performance layer-2 IP switching and intelligent IP quality of service to precisely classify/manage voice, video and data services.

The PacketAssure iQ1000 provides the following features:

- High-performance, intelligent, traffic management assures application delivery meets service objectives.
- Robust VLAN awareness and capabilities for traffic segregation and broadcast domain control.
- Multi-layer traffic classification gives administrators consistent, end-to-end control of service priority.
- A customized web user interface that improves operator efficiency and reduces training costs.
- A full Command Line Interface (CLI).

Figure 1 PacketAssure iQ1000, IOM Side

The iQ1000 is modular, with a basic system configuration consisting of the chassis, power supply, Packet Switching Module (PSM), System Interface Module (SIM), Fan module and Filter Module. The PSM provides all packet switching, service delivery

management, configuration/status and cryptographic functions. The SIM provides Ethernet and Serial local user interfaces and a network timing input. Up to three Interface Option Modules (IOMs) complete the appliance, providing Serial, Ethernet and T1/E1 data interfaces. No Data I/O cards, including the SIM (System Interface Module) need be installed for the cryptographic module to operate. However, in order to locally manage the device, a SIM card must be installed. For remote management at least one IOM must be installed.

The iQ supports both a FIPS 140-2 approved mode of operation and a non-approved mode operation. All security functions and cryptographic algorithms are performed in Approved mode. If the iQ cannot run in the FIPS Approved mode because FIPS self-test failed, the unit faults and all operations are halted.

The iQ supports SSH, TLS, and SNMP. By IG D.8 Scenario 4, these protocols are allowed to be used in the FIPS approved mode, but are non-compliant. The module also incorporates a security log which records user authentication and other security events. These include user login (successful or unsuccessful), user logout, configuration changes and system file changes.

The iQ1000 satisfies FIPS 140-2 Level 2 requirements for multiple-chip standalone modules. Figure 2 shows a functional block diagram of the iQ1000 looking down from the top as if looking through the top cover. All cryptographic functions are contained within the PSM. The cryptographic boundary, delineated in red, consists of the chassis, the top cover, the front panel of the PSM and the mid-plane. Tamper evidence seals, described in section 5.2 indicate when the removable cover or removable PSM have been disturbed. Louvers inside the chassis allow cooling airflow through the unit and satisfy FIPS opacity requirements. The louvers prevent viewing crypto module components on the PSM through the ventilation holes and fans. On the opposite side the louvers prevent viewing PSM components when the filter is removed, as must be allowed for maintenance. All IOMs, the SIM, the fan tray and the power supply are outside the cryptographic boundary.

Item	Rationale for Exclusion
Power Supply	No security relevance
Hot-swappable Fan Module	No security relevance
Hot-swappable Interface Option Modules	No security relevance
Hot-swappable System Interface Module	No security relevance
Removable Filter Module	No security relevance

Table 1 Items Excluded from Cryptographic Boundary

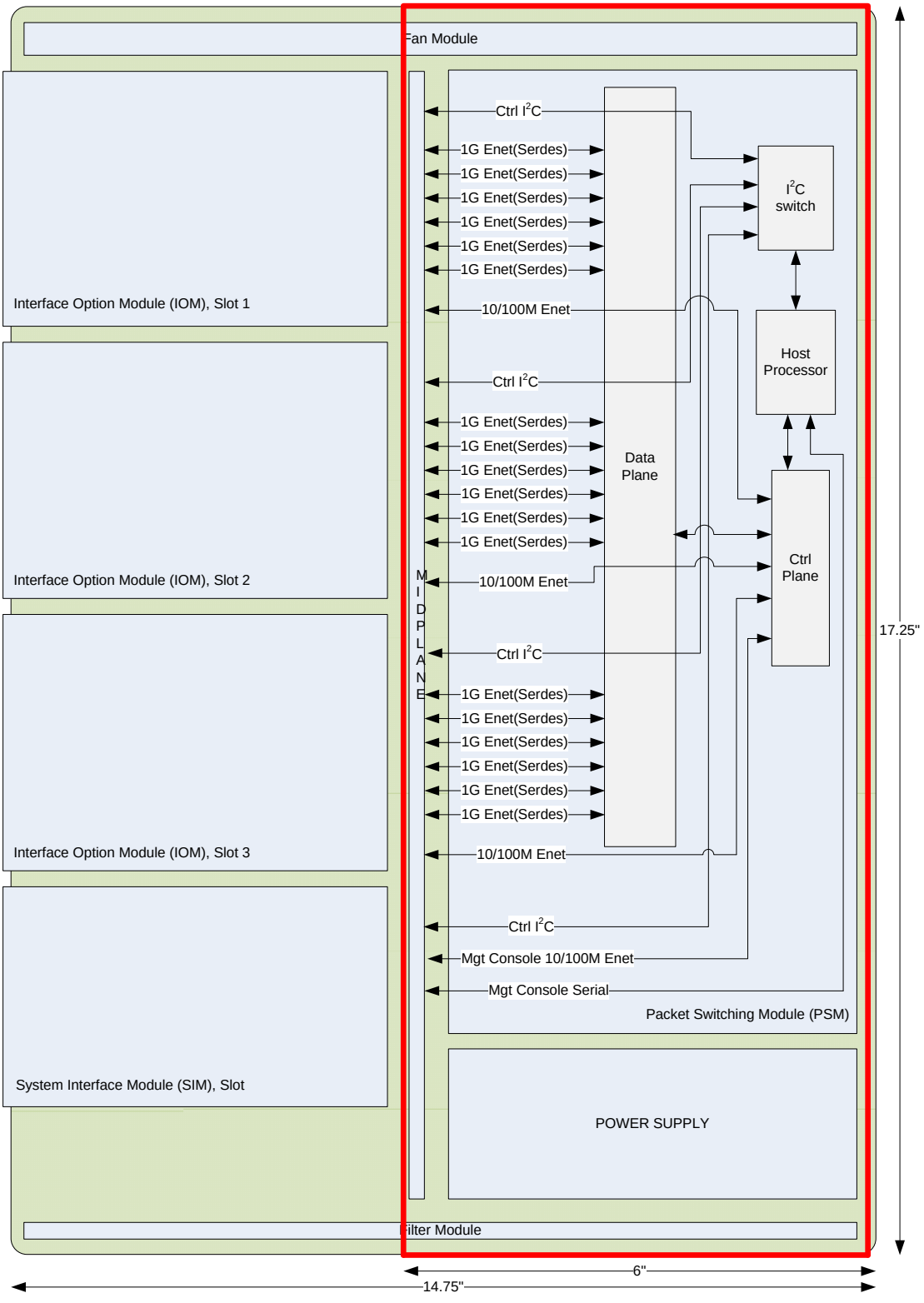

Figure 2 Cryptographic Boundary

The module is 1.75” in height (not shown in this diagram).

1.2. *Purpose*

This Cryptographic Module Security Policy describes how the cryptographic module in the iQ1000, referred to as the "Module" in the remainder of this document, meets the requirements of FIPS140-2 Level 2; and how to operate the Module in a secure, FIPS-compliant manner. Only features and operation associated with FIPS-140 cryptographic security are presented. Complete product documentation including installation and operations manuals can be downloaded at http://www.ultra-dne.com/.

The complete FIPS140-2 submission package consists of:

- Security Policy
- Vendor Evidence
- Finite State Model

This document is non-proprietary and may be distributed without restriction while all other documents are proprietary to Ultra Electronics DNE Technologies and only available under Non-Disclosure Agreement (NDA). For access to these documents contact Ultra Electronics DNE Technologies.

1.3. *Security level*

The module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Security Level	
Security Requirements Specification	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2 Security Levels

1.4. *References*

Title	Document File Name
OpenSSL FIPS Object Module Version 1.2.3, Open Source Software Institute, 5/3/2011	SecurityPolicy-1.2.3.pdf

PacketAssure iQ1000 Product Documentation	http://www.ultra-dne.com/

1.5. *Glossary*

Term/Acronym	Description
BIST	Built In Self Test
BOM	Bill Of Materials
CLI	Command Line Interface
Enet	Ethernet
IC	Integrated Circuit
ICD	Interface Control Document
IOM	Interface Option Module
PSM	Packet Switching Module
POST	Power On Self Test
SDA	Service Delivery Appliance
SerDes	Serializer/Deserializer
SIM	System Interface Module

2. Cryptographic Module Ports and Interfaces

Table 3 below illustrates the logical to physical mapping of interfaces contained inside the cryptographic boundary of the module. Logical mapping is accomplished using the four FIPS 140-2 defined logical interfaces.

Logical Interfaces	Physical Interface	Count
Control Input Interface Status Output Interface Data Input Interface Data Output Interface	1G Ethernet Ports (Serdes)	18
Control Input Interface Status Output Interface Data Input Interface Data Output Interface	10/100M Ethernet Management Port	1
Control Input Interface Status Output Interface	Serial Management Port	1
Status Output Interface	Power LED	1
Status Output Interface	Alarm LED	1
Power Interface (2 switches, 1 power cord)	Power	2

Table 3 Ports and Interfaces

3. Roles, Services, and Authentication

Each user assigned to a role can be distinguished by identity and is authenticated upon initial access to the module. The module implements three separate roles, of which two are User Roles and one is the Crypto-officer Role. The Administrator (admin) of the iQ1000 takes on the Crypto-officer Role and configures and maintains the module.

3.1. *Roles*

The module maintains the following three roles: admin, config and oper. The oper and config roles can be considered as user roles with the config role having read-write privileges and the oper role having read-only privileges. The admin role is equivalent to the Crypto Officer role defined in the FIPS DTR.

Unauthenticated Services

All services require authentication with the exception of those listed in Table 4. The Table 4 services can only be performed from the Serial Management Interface.

Service	Input	Output	Description
Bootloader factory default	factory-reset command	Command result	Return module to its factory default state.
Bootloader switch code banks	switch command	Command result	Two versions of application code can be stored, one in each bank

			of memory. Users can select which version to boot from.
Power on/off	NA	NA	Power the module on or off.

Table 4 Unauthenticated Services

Non-Approved Mode Services

Non-Approved services can be performed from the Serial Management Interface, the Ethernet Management Interface, or the 1GB Ethernet Interface (Inband Management).

Service	Input	Output	Description
Configuration and status services using SNMP	Module configuration input Module status	Success or error messages The module information or error message	Status of the iQ via SNMP (SNMP gets only) using non-Approved key strengths <112 bits. Any use of AES or Triple-DES with these key strengths is non-Approved.
Configuration and status services using HTTPS (TLS)	Module configuration input Module status	Success or error messages The module information or error message	Status of the iQ via HTTPS (TLS). Uses RSA key wrapping with public keys <2048 bits with key strengths <112 bits. Any use of AES or Triple-DES with keys established in this manner is non-Approved.
Configuration and status services using SSH	Module configuration input Module status	Success or error messages The module information or error message	Status of the iQ via SSH. Uses Diffie-Hellman with keys <2048 bits with key strengths <112 bits. Any use of AES or Triple-DES with keys established in this manner is non-Approved.
User role validation using Radius	Module configuration input Module status	Success or error messages The module information or error message	RADIUS is disabled by default. Enabling RADIUS is non-approved

Table 5 Non-Approved Services

User Role Services (Approved Mode)

The User Role services can be performed from the Serial Management Interface, the Ethernet Management Interface, or the 1GB Ethernet Interface (Inband Management).

Service	Input	Output	Description
Secure configuration and status services using SNMP	Module configuration input Module status	Success or error messages The module information or error message	Configuration and status of the iQ via SNMP (SNMP gets only) using Approved key strengths >=112 bits. Any use of AES or Triple-DES with these keys is Approved. Note 1
Secure configuration and status services using HTTPS (TLS)	Module configuration input Module status	Success or error messages The module information or error message	Configuration and status of the iQ via HTTPS (TLS). Uses RSA key wrapping with public keys >=2048 bits with >=112 bits of security strength. Any use of AES or Triple-DES with keys established in this manner is Approved. Note 1
Secure configuration and status services using SSH	Module configuration input Module status	Success or error messages The module information or error message	Configuration and status of the iQ via SSH. Uses Diffie-Hellman with keys >=2048 bits with >=112 bits of security strength. Any use of AES or Triple-DES with keys established in this manner is Approved. Note 1
Change password	Old and new passwords	Success or error message	Users may change their own passwords only.
Configure interfaces	Interface parameters	Success or error message	Configure Serial/Ethernet/TE1 physical interfaces.
Configure services	Service parameters	Success or error message	Configure CES & Ethernet services.
Configure system timing	Timing parameters	Success or error message	Configure system timing sources.
View iQ1000 module	Select the type information to	The module information or error	Status functions: view status of module,

information	view	message	temperature, memory status, CPU utilization status; view physical interfaces status, packet statistics, services status; review system logs.

Table 6 User Roles

Note 1 - SSH, TLS and SNMP protocols and KDFs are allowed to be used in FIPS Approved mode.

Crypto-officer Role Services (Approved Mode)

The Crypto-Officer Role services can be performed from the Serial Management Interface, the Ethernet Management Interface, or the 1GB Ethernet Interface (Inband Management).

Service	Input	Output	Description
Factory reset of module	factory-reset command	Success or error message	Delete all configuration data and restore the factory default settings.
System security management using SNMP	Security parameters	Success or error message	Configure security and management preferences. Configure SNMP trap listeners. Uses key strengths >=112 bits. Any use of AES or Triple-DES with these keys is Approved.[Note 1]
System security management using HTTPS (TLS)	Security parameters	Success or error message	Remote access to the module via HTTPS (TLS). Configure in-band and out-band interfaces. Configure IPv4 and IPv6 routes. Uses RSA key wrapping with public keys >=2048 bits and >=112 bits of security strength. Any use of AES or Triple-DES with keys established in this manner is Approved. [Note 1]
System security	Security	Success or error	Remote access to the

management using SSH	parameters	message	module via SSH. Configure in-band and out-band interfaces. Configure IPv4 and IPv6 routes. Uses Diffie-Hellman with keys >=2048 bits and >=112 bits of security strength. Any use of AES or Triple-DES with keys established in this manner is Approved. Note 1
User management	User parameters	Success or error message	Add/Delete/Modify users. Change passwords and roles for the existed users.
Perform Self Tests	Select tests	Success or error message	Perform SHA-256 sum file integrity verification test.
Configure secure server	Server parameters	Success or error message	Configure secure server used for file transfer.
Reboot module	Reboot command	Success or error message	Reboot iQ1000 module to initiate the power-up self test on demand.
Software upgrade service	Software package	Success or error message	Perform the software upgrade process.
Switch banks	Switch command	Success or error message	Switch the flash bank.
Secure configuration and status services using SNMP	Module configuration input Module status	Success or error messages The module information or error message	Configuration and status of the iQ via SNMP (SNMP gets only) using Approved key strengths >=112 bits. Any use of AES or Triple-DES with these keys is Approved. Note 1
Secure configuration and status services using HTTPS (TLS)	Module configuration input Module status	Success or error messages The module information or error message	Configuration and status of the iQ via HTTPS (TLS). Uses RSA key wrapping with public keys >=2048 bits with >=112 bits of security strength. Any use of AES or Triple-DES with keys established in this

			manner is Approved. Note 1
Secure configuration and status services using SSH	Module configuration input Module status	Success or error messages The module information or error message	Configuration and status of the iQ via SSH. Uses Diffie-Hellman with keys >=2048 bits with >=112 bits of security strength. Any use of AES or Triple-DES with keys established in this manner is Approved. Note 1
Configure interfaces	Interface parameters	Success or error message	Configure Serial/Ethernet/TE1 physical interfaces.
Configure services	Service parameters	Success or error message	Configure CES & Ethernet services.
Configure system timing	Timing parameters	Success or error message	Configure system timing sources.
Set system date and time	Date and time	Success or error message	Set system date & time.
View iQ1000 module information	Select the type information to view	The module information or error message	Status functions: view status of module, temperature, memory status, CPU utilization status; view physical interfaces status, routing tables, packet statistics, services status; view active sessions; review system logs.

Table 7 Crypto-officer Role

Note 1 - SSH, TLS and SNMP protocols and KDFs are allowed to be used in FIPS Approved mode.

3.2.*Authentication Mechanisms and Strength*

Access control restrictions for Data Paths, Action Paths, and CLI commands will be defined for all privilege groups. These restrictions will be implemented by command and data authorization rules defined within the AAA system. The PacketAssure iQ1000 provides two-factor authentication to secure user logins and protect against account takeover and data theft. Two-factor authentication systems overcome the issues of single secret authentication by the requirement of a second secret. Two-factor authentication uses a combination of the following items:

- Something that the user has, such as a smart card.
- Something that the user knows, such as a password.

User Authentication is identity based, where the identity is defined by the username and password.
Password rules are as follows:

- Passwords must contain between 8 and 32 characters.
- Passwords must consist of at least 2 lower case letters, 2 upper case letters, 2 numerical digits and 2 special characters. Consecutive characters must not repeat.
- New passwords must differ from old password(s) by a minimum of 4 characters. The password reuse check is configurable from 0 to 16 previous passwords by the crypto-officer. The default reuse check is 8 passwords. Configuring the reuse check to 0 has the same effect as configuring reused check to 1 – the new password is only checked against the immediately previous password.
- Only the MD5 hash of user passwords is stored in the system database. When the user enters his/her password, the MD5 hash of the entered password will be calculated and compared to the stored MD5 hash. MD5 is not a FIPS approved algorithm and therefore considered no more secure than plaintext.
- During the login process no character echo will take place.

With a minimum 8 character authentication password and the required use of 2 upper/lower case characters(26), 2 numbers(10) and 2 special characters(at least 10) there is approximately a 1 in (26)(25)(26)(25)(10)(9)(10)(9)8! = (1.37 e14) possibilities of random access succeeding. The password rules are non-modifiable and to decrease the probability of correctly guessing a password within a reasonable timeframe, the module will not accept another password attempt for a minimum of ten seconds after three consecutive unsuccessful attempts. The failed login attempt delay can be configured by the cryptographic officer to be from ten to sixty seconds, with the default being sixty seconds. Assuming the minimum failed login delay of ten seconds, the theoretical maximum number of login attempts per minute is 18. With a maximum 18 attempts to use the authentication mechanism during a one-minute period, the probability is less than 1 in 7,665,840,000,000 that a random access will succeed.

4. Finite State Model

The finite state model is defined in the proprietary FIPS140_FSM document, see section 1.2 for guidance.

5. Physical Security

The iQ1000 incorporates a multi-chip standalone cryptographic module which is designed to meet FIPS 140-2 security level 2 requirements. These requirements are described in the following sections:

5.1. *Enclosure*

The enclosure is comprised of a metal chassis with a metal cover. The top, bottom and sides of the enclosure are opaque. Internal louvers are installed so no part of the module is visible through ventilation holes.

5.2. *Tamper Evidence*

Four holographic tamper evidence seals (TES), NovaVision Inc Ultra-Guard label, product code UG4-08, will be applied to the enclosure. The hologram image will contain an embedded "VOID OPENED" pattern. Three tamper evidence seals prevent removal of cover screws while a fourth TES prevents removal of another cover screw and the PSM, see Figure 3.

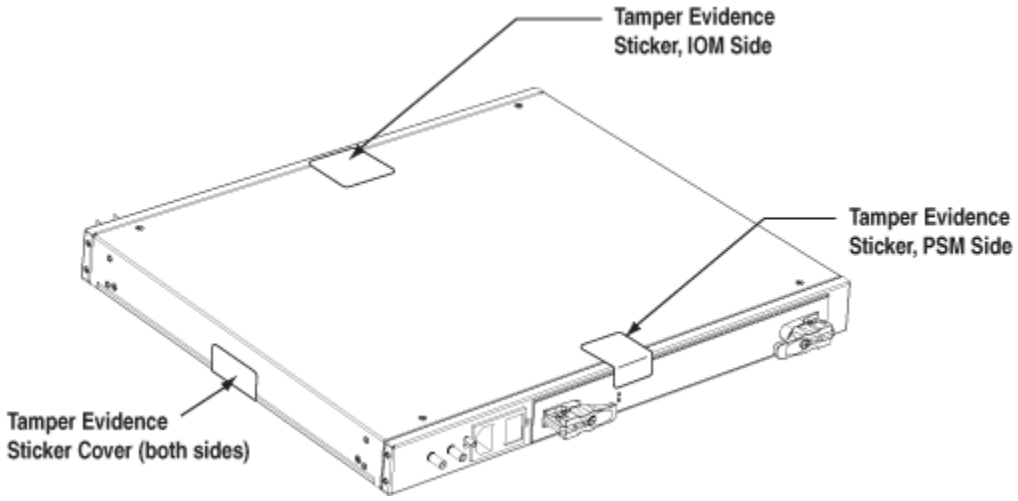

Figure 3 Tamper Evidence Seal Locations

5.3. *Physical Security Rules*

The crypto-officer of the module is required to inspect the enclosure periodically looking for:

- Tamper evidence seals that have "VOID OPENED" visible.
- Disfiguration of the cover, such as creases, indicating that someone has attempted to pry the cover open.

The crypto officer should perform a factory reset on the module if tamper evidence is detected. The factory reset procedure is described in the Administrator Guide (DNE document number 24001197) available on the DNE website http://www.ultra-dne.com. The crypto-officer should also replace any damaged tamper evidence seals. Prior to replacing the seals, the crypto-officer shall remove the damaged labels and clean off any remaining residue on the mounting surface using an adhesive remover. Tamper evidence seals can be obtained from Ultra Electronics DNE Technologies, DNE part number 57005924-000.

5.4. *Secure Operation Initialization Rules*

PacketAssure iQ1000 software versions 3.2.0 and 3.4.0 were validated for compliance with FIPS140-2 and are the only allowable software version for FIPS-Approved operation. FIPS140 compliant self-tests execute automatically at power-up. Failure of any test puts the module in an error state and no services are provided. The module is in an approved mode when using the approved services; and in a non-approved mode when using non-approved services. Encryption strength must not be less than 112 bits when in the approved mode.

The module implements several cryptographic algorithms for use in its operation. The following table identifies the FIPS approved algorithms:

Algorithm	Implementation Details	Algorithm Certificate
Image A		
AES	AES keys 128, 192, 256 bits; encrypt and decrypt.	#2191
TDES	Triple-DES keys 168 bits; encrypt/decrypt.	#1384
DSA	DSA keys 1024 bits; verify.	#685[Note 1]
PRNG (ANSI X9.31 Appendix A.2.4 using AES)	PRNG seed value is 128 bits; seed key values are 128, 192, and 256 bits,	#1109
RSA (X9.31, PKCS #1.5, PSS)	RSA keys 2048 to 4096 bits; sign and verify.	#1130[Note 2]
SHA-1, 224, 256, 384, 512	Hashing.	#1899
HMAC-SHA-1, 224, 256, 384, 512	HMAC key; message integrity.	#1343

Table 8 Approved Cryptographic Algorithms

Note 1 - DSA (Cert. #685, non-compliant with the functions from the CAVP Historical DSA list):
FIPS186-2:
PQG(gen) MOD(1024);
KEYGEN(Y) MOD(1024);
SIG(gen) MOD(1024)

Note 2 - RSA (Cert. #1130, non-compliant with the functions from CAVP Historical RSA list):
FIPS186-2:
ALG[ANSIX9.31]:KEY(gen)(MOD:1024, 1536 PubKey Values: 3, 17, 65537)
ALG[ANSIX9.31]:SIG(gen); 1024, 1536, SHS: SHA-1, SHA-256, SHA-384, SHA-512, 2048, 3072, 4096, SHS:SHA-1
ALG[RSASSA-PKCS1_V1_5]:SIG(gen): 1024, 1536, SHS: SHA-224, SHA-256, SHA-384, SHA-512
ALG[RSASSA-PSS]: SIG(gen);1024, 1536, SHS: SHA-224, SHA-256, SHA-384, SHA-512

The module supports the following non-Approved algorithms in the Approved mode of operation as allowed.

Algorithm	Algorithm Type	Utilization

AES	AES 128, 192, 256 bit	Key wrapping Note 2
Diffie-Hellman	Key establishment	Key establishment methodology supports 2048 to 4096 bit keys, providing between 112 and 150 bits of encryption strength Note 1
RSA encrypt/decrypt	Key establishment / Key wrapping	RSA (key wrapping; key Establishment methodology supports 2048 to 4096 bit keys providing 112 – 150 bits of encryption strength. Note 1
HMAC SHA-1	HMAC	SNMPv3 USM authentication key Note 2
SHA-1	Hash	SSH Key Derivation Function Note 2
SHA-1 / MD5	Hash	TLS (PRF) Key Derivation Function
SHA-1	Hash	SNMP Key Derivation Function Note 2
NDRNG	Non-Deterministic Random Number Generator	Part of PRNG seed

Table 9 Non-Approved Cryptographic Algorithms

Note 1 – Non-compliant when encryption strength is less than 112 bits.

Note 2 – These are approved algorithms but their specific use specified here is non-approved.

SSH, TLS and SNMP protocols and KDFs are allowed to be used in FIPS Approved mode.

In addition the following algorithms are used in non-Approved mode when using non-Approved key strengths <112 bits: AES, Triple-DES

6. Operational Environment

Since the iQ1000 does not allow operators to load or modify software or firmware that was not included as part of the validation of the module, it is considered “non-modifiable” and is therefore not subject to the requirements of the Operational Environment component of the FIPS specification.

7. Definition of SRDIs Modes of Access

This section specifies the module’s Security Relevant Data Items as well as the access control policy enforced by the module.

7.1. *Cryptographic Keys, CSPs, and SRDIs*

While operating in a FIPS-compliant manner, the module contains the following security relevant data items. Unless otherwise noted, All keys are generated using FIPS approved algorithms, using a FIPS approved RNG.

ID	Algorithm	Size	Description	Origin	Storage	Zeroization Method
General Keys/CSPs						
User Password	Password	Variable (8-32 characters)	Used to authenticate local users	The user sets their password on first login	NVRAM (plaintext)	Zeroized by overwriting with new password
External Secure Server Password	Password	Variable (0-128 characters)	Used to authenticate users on remote SFTP server	The crypto officer sets the password of a remote server	NVRAM (AES 128-bits)	Zeroized by overwriting with new password OR deleting the server
Security Log Pass Phrase	Password	Variable (1-128 characters)	Used to encrypt the security log file, which is only claimed to be obfuscated.	The crypto officer sets the pass phrase	NVRAM (AES 128-bits)	Zeroized by overwriting with new pass phrase
RNG Seed	ANSI X9.31 Appendix 2.4 using AES	16 bytes	This is the seed for ANSI X9.31 RNG	This key is NDRNG based and created during RNG initialization at power on.	DRAM (plaintext)	Zeroized by power cycling the device
RNG Seed Key	ANSI X9.31 Appendix 2.4 using AES	32 bytes	This is the seed key for ANSI X9.31 RNG	This key is NDRNG based and created during RNG initialization at power on.	DRAM (plaintext)	Zeroized by power cycling the device
Diffie-Hellman public exponent	DH	2048-4096 bits	The public exponent used in Diffie-Hellman (DH) exchange	This key is Created using the OpenSSL library during key establishment.	DRAM (plaintext)	Automatically after shared secret generated
Diffie-Hellman private exponent	DH	2048-4096 bits	The private exponent used in Diffie-Hellman (DH) exchange	This key is Created using the OpenSSL library during key establishment.	DRAM (plaintext)	Automatically after shared secret generated
Diffie-Hellman Shared Secret	DH	2048-4096 bits	This is the shared secret agreed upon as part of DH exchange	This key is Created using the OpenSSL library during key establishment.	DRAM (plaintext)	Zeroized upon deletion
Database						

AES Key	AES CFB	128-bits	This is the AES key and IV used to encrypt/decrypt CSPs in the database	This key is automatically created during startup of a factory defaulted system	NVRAM (plaintext)	# factory-reset
Software Upgrade						
Package Public Key	RSA	2048-bits	This key is the public product key used to verify software packages	This key is installed with the system software	NVRAM (plaintext)	This is not zeroized
Package Pass Phrase	Password	Fixed (11 characters)	This password is used to decrypt software packages	This phrase is installed with the system software	NVRAM (plaintext)	This is not zeroized
SNMPv3[Note 2]						
Trap Listener Password[Note 1]	Password	Variable (8-32 characters)	Used to authenticate and encrypt SNMPv3 traps	This key is created when the crypto officer creates trap listeners	NVRAM (plaintext)	Zeroized by overwriting with new password or deleting the listener
Authentication Key	HMAC-SHA-1	16 bytes	This is the SNMPv3 USM authentication key	This key is automatically created when a user or v3 trap listener is created	NVRAM (plaintext)	Zeroized by overwriting with new password or deleting the user
Privacy Key	AES	16 bytes	This is the SNMPv3 USM encryption key	This key is automatically created when a user or v3 trap listener is created	NVRAM (plaintext)	Zeroized by overwriting with new password or deleting the user
SSH[Note 2]						
SSH RSA public key	RSA	2048-bits	This is the SSH RSA host key	This key is automatically created during startup of a factory defaulted system	NVRAM (plaintext)	# factory-reset
SSH RSA private key	RSA	2048-bits	This is the SSH RSA host key	This key is automatically created during startup of a factory defaulted system	NVRAM (plaintext)	# factory-reset
SSH session key	Triple-DES AES	168 bits 128-bits 192-bits 256-bits	This is the SSH session symmetric key	This key is automatically created during session creation	DRAM (plaintext)	Zeroized when SSH session is terminated

SSH session authenticati on key	HMAC SHA-1	96-bits or 160-bits	This is the SSH session authentication key	This key is automatically created during session creation	DRAM (plaintext)	Zeroized when SSH session is terminated
SSH authenticati on keys	RSA,	2048 bits, 4096 bits	Allowed SSH public keys	The crypto officer adds/removes entries	NVRAM (plaintext)	# factory-reset
TLS[2]						
TLS CA public key	RSA	2048-bits	The internal CA certificate used to self-sign the generated TLS server certificate	This key is automatically created during startup of a factory defaulted system	NVRAM (plaintext)	# factory-reset
TLS CA private key	RSA	2048-bits	The CA certificate private key	This key is automatically created during startup of a factory defaulted system	NVRAM (plaintext)	# factory-reset
TLS Server public key	RSA	2048-bits	Identity certificate for module itself and also used in TLS negotiations. This certificate is self-signed on a default system, but can later be replaced by a signed CSR by an external CA.	This key is automatically created during startup of a factory defaulted system OR loaded by the Crypto Officer as a part of server certificate installation	NVRAM (PEM)	# factory-reset
TLS Server private key	RSA	2048-bits	The TLS Server private key	This key is automatically created during startup of a factory defaulted system OR as a part of Certificate Signing Request	NVRAM (PEM)	# factory-reset
TLS premaster secret	Shared Secret	384-bits	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created	This key is automatically created during session creation	DRAM (plaintext)	Zeroized when TLS session is terminated

TLS Master Secret	Shared Secret	384-bits	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created	This key is automatically created during session creation	DRAM (plaintext	Zeroized when TLS session is terminated
TLS session key	Triple-DES AES	168 bits 128-bits 192-bits 256-bits	This is the TLS session key	This key is automatically created during session creation	DRAM (plaintext)	Zeroized when TLS session is terminated
X.509 Trust Points	RSA	2048-bits	Manually loaded X.509 certificates used in path validation	Trust points are installed/removed by the crypto-officer. Used by two-factor authentication.	NVRAM (DER)	# factory-reset
X.509 CRLs	SHA-256, RSA	2048-bits	Digitally signed CRLs used in x.509 path validation	CRLs are installed/removed by the crypto-officer. Used by two-factor authentication.	NVRAM (DER)	# factory-reset
X.509 Cached Certificates	RSA	2048-bits	Automatically downloaded X.509 certificates used in path validation	Certificates are cached automatically via HTTP or LDAP from external servers as client certificates are validated	DRAM (PEM)	# factory-reset
X.509 Cached CRLs	SHA-256, RSA	2048-bits	Digitally signed CRLs used in x.509 path validation	CRLs are cached automatically via HTTP or LDAP from external servers as client certificates are validated	DRAM (DER)	# factory-reset

Table 10 Key, CSPs and SRDIs

Note 1 - The Trap Listener password must be at least 8 characters to comply with FIPS.
Note 2 - SSH, TLS and SNMP protocols and KDFs are allowed to be used in FIPS Approved mode, but are non-compliant.

7.2.*Access Control Policy*

The terminal allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SRDI while operating the module in a given role performing a specific service (command). The permissions

are categorized as a set of four separate permissions: **r**ead, **w**rite, e**x**ecute, **d**elete. If no permission is listed, then an operator outside the module has no access to the SRDI.

Module SRDI/Role/Service Access Policy	Security Relevant Data Item	User Password	Secure Server Password	Security Log Pass Phrase	RNG Seed, RNG Seed Key	DH private exponent, DH Shared	Database AES Key	Package Public Key, Package Pass	Trap Listener Password	SNMPv3 Auth Key, Private Key	SSH RSA private key, DSA private	SSH session key, session auth key	TLS CA public key, private key	TLS Server public key, private key	TLS premaster secret, session key
Role/Service															
Unauthenticated Services															
Bootloader factory default		d	d	d	d	d	d		d	d	d	d	d	d	d
Bootloader switch code banks															
Power on/off					d	d						d			d
User role															
Oper Role		w x			x	x				w	x	x		x	x
Config Role		w x	x		x	x				w	x	x		x	x
Crypto-officer Role															
Admin Role		w x d	w x d	w x	x	x	x d	x	w x d	w x d	x d	x	d	x	x

Table 11 SRDI Access

8. Electromagnetic Interface/Electromagnetic Compatibility

The iQ1000 conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

9. Self Tests

The module contains the following power up self tests. All of the tests shown in section 9.1 execute at power-up without user input. Failure of any power-up self-test is a system fault and therefore will transition the module into the error state as defined by the FSM.

9.1. *Power-Up Self Tests*

1. *Cryptographic algorithm test*
   OpenSSL provides:
   - AES KAT encrypt
   - AES KAT decrypt
   - Triple-DES KAT encrypt
   - Triple-DES KAT decrypt
   - DSA pair-wise consistency test (sign/verify)
   - RSA KAT sign
   - RSA KAT verify
   - PRNG KAT
   - HMAC-SHA-1 KAT
   - HMAC-SHA-224 KAT
   - HMAC-SHA-256 KAT
   - HMAC-SHA-384 KAT
   - HMAC-SHA-512 KAT
   - OpenSSL internal integrity HMAC-SHA-1

   sshd provides:
   - AES-CTR KAT

2. *Software/firmware integrity test*
   File Integrity Test:
   - SHA-256 checksum verification of individual security relevant files.

3. *Critical functions test-*
   - N/A

9.2. *Conditional Self tests*

The module contains the following conditional self tests.

1. *Pair-wise consistency test (for public and private keys)*
   OpenSSL provides:
   - RSA pair-wise consistency

2. *Software/firmware load test*
   Software Package Test:
   - Signed by RSA 2048 bit private key
   - Symmetrically Encrypted with AES-256
   - SHA-256 digest

   During software download the package is checked against the SHA-256 digest which is also downloaded to the target system. This only serves to confirm uncorrupted download of the package. The package is then unencrypted using symmetrical AES-256 and the password which is already stored on the target. The decrypted package consists of a tarball and the signed SHA-256 of the

tarball. The private key used in the signature is of type RSA-2048. If the signed hash cannot be validated (using the locally stored public key), the package will not be installed and the upgrade fails. The status of each step of the upgrade process is displayed on the GUI-interface and is also appended to the system log.

3. *Manual key entry test*
    - N/A

4. *Continuous random number generator test*
   OpenSSL provides:
    - PRNG continuous test
    - Per Implementation Guide section 9.8, continuous test of the NDRNG is not required because its output is only used once after module power-on and not used again until the module is power cycled off.

5. *Bypass test*
    - N/A

10. Mitigation of Other Attacks

- N/A