Q-Net Security

Q-Box

Non-Proprietary FIPS 140-2 Security Policy

Version: 1.1

Date: December 8, 2022

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Q-Net Security (QNS) Q-Box module, hereafter denoted the Module. The module is a small device that secures precious data flowing between every endpoint in a network. Complete security is built directly into each module's silicon. Creating security directly in silicon avoids the use of vulnerable software and/or Operating Systems. The core of the hardware-enabled solution is AES-256 encryption and a novel symmetric key distribution that can provide a unique random key for each packet. QNS devices are placed in-line and nearby the endpoints to be secured. No external key management is necessary. Once deployed, the QNS devices never need to be upgraded or patched. QNS achieves superior security through a hardware security barrier that incorporates the True Random Number Generator (TRNG) delivering packet-level encryption. The QNS key management scheme monitors key entropy continuously to assure its randomness. This permits secure communications anywhere, even over public links including LTE and the Internet. The QNS approach removes all opportunities for an attacker to ever discover a security key, thereby thwarting many internal exploits as well as remote attacks.

Table 1– Cryptographic Module Versions

HW P/N and Version	FW Version
100211	2.2.2

The Module is intended for use by US Federal agencies, Energy Companies, Finance Industry, Gaming, or other markets that require FIPS 140-2 validated Level 2.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic 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	3
Mitigation of Other Attacks	N/A
Overall	2

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figures 1-3. The Module is a multi-chip standalone embodiment. The cryptographic boundary is comprised of the entire hardware module and consists of the hardware and firmware components.

The module is assembled by 4 threads at the bottom as seen in Figure 3

Figure 1 – Module Front Top View

Figure 2 – Module Side Top View

Figure 3 – Module Bottom View

1.2 Firmware and Logical Cryptographic Boundary

The block diagram below shows the hardware components in respect to the physical design. All cryptographic functions occur in the processing engine. The cryptographic boundary is marked by the red box.

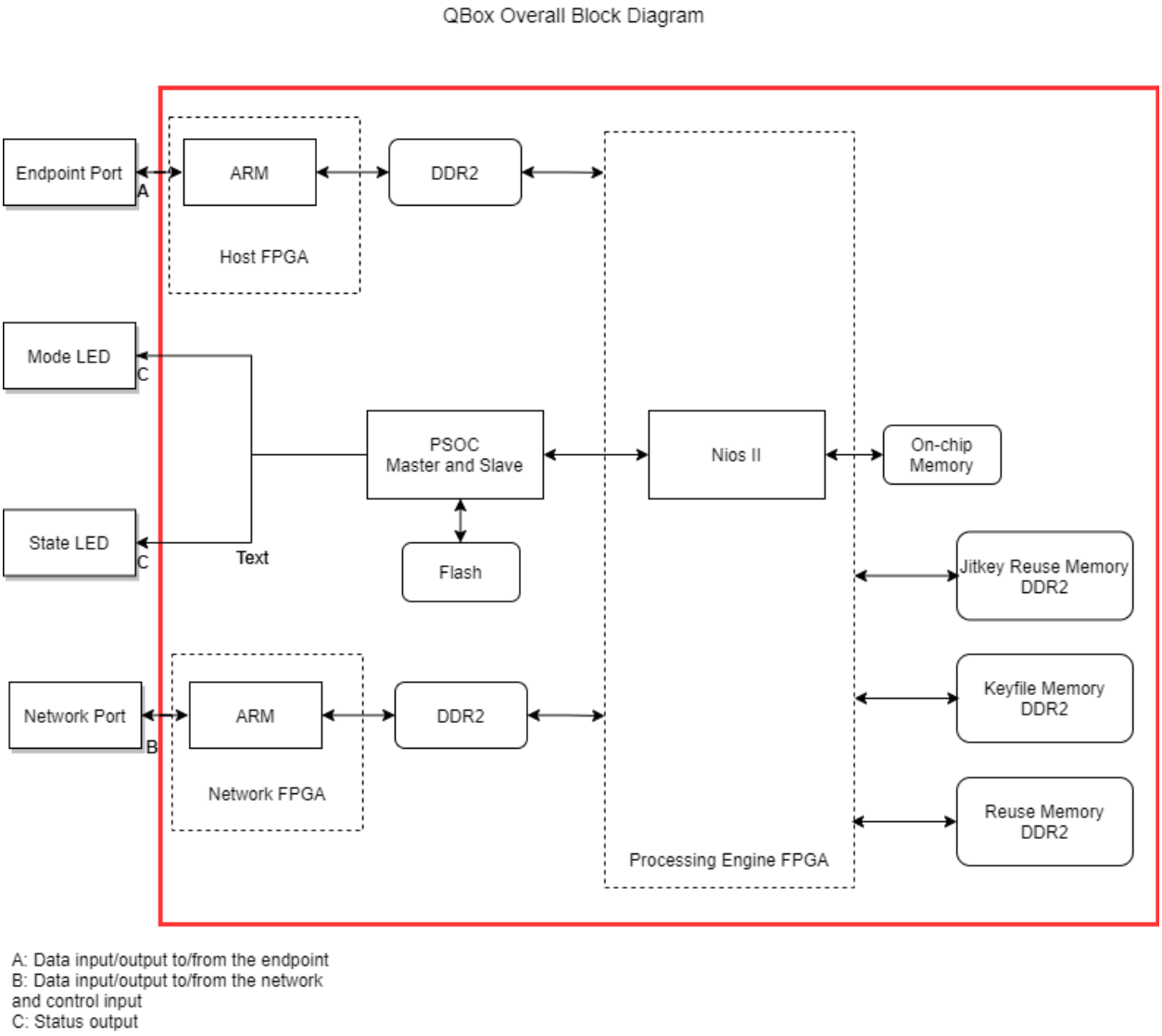

Figure 4 – The Q-Box Block Diagram

2 Ports and Interfaces

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
Power	Power input – 12v+ connection that powers the module.	Power In
Network	10/100 Mbps Ethernet Port – Plugs the module into the network (LAN/WAN).	Data input/output, Status Output, Control Input
Endpoint	10/100 Mbps Ethernet Port – Plugs the module into the Endpoint that sends packets.	Data input/output, Status Output
Mode Indicator	LED – Indicates the mode of the module.	Status output
State Indicator	LED – Indicates the operating state of the module.	Status output

3 Cryptographic Functionality

3.1 Mode of Operation

The Module has one Approved mode of operation and no non-Approved modes. Once power is supplied and the module is initialized for communication per Section 5, the module is always performing cryptographic security in a FIPS Approved mode of operation. Hardware and firmware versions for the module can be obtained through the QPM (Q-Net Policy Manager) in the devices section of the GUI.

3.2 Approved Cryptographic Functions

The Module implements the FIPS Approved cryptographic functions listed in Tables 4 below. There are no security relevant protocols used in FIPS mode.

Table 4 – Approved Algorithms

Algorithm	Mode	Description	Functions/Caveats	Cert
AES [197]	GCM [38D]*	Key Size: 256 Tag Len: 128	Authenticated encrypt, authenticated decrypt, and message authentication	#A1660
	ECB [38A]	Key Sizes: 256	Authenticated encrypt	#A1661
CKG [IG D.12]	[133r2] Section 6.2.2 Symmetric Keys Derived from a Pre-existing Key		Key Generation	Vendor Affirmed
DRBG [90A]	Hash	SHA (256)	Deterministic Random Bit Generation Security Strength = 256	#A1662

Algorithm	Mode	Description	Functions/Caveats	Cert
ENT (P) [90B]	Hardware based entropy source This cryptographic module has been validated for compliance with NIST SP 800-90B and IG 7.19.	Generated Entropy: 1920 bits of 1-bit entropy output. 0.269859 bits of entropy in each 1-bit output.	Used to generate the seed material for the FIPS Approved DRBG.	N/A
HMAC [198]	N/A	SHA (256)	Underlying hash for DRBG and KBKDF Security Strength = 256	#A1665
KBKDF [108]	Counter	HMAC-SHA (256)	Key Based Key Derivation	#A1666
KTS [D.9]	AES GCM	Key Size: 256	Key Wrapping	#A1660
SHA-256 [180]	N/A	SHA (256)	Underlying hash for KBKDF	#A1664
	N/A	SHA (256)	Underlying hash for DRBG	#A1663

* Note: The module's IV is generated internally by the module's Approved DRBG (Cert. #A1662). The DRBG seed is generated inside the module's physical boundary. The IV is 96-bits in length per NIST SP 800-38D, Section 8.2.2 and FIPS 140-2 IG A.5 scenario 2.

3.3 Critical Security Parameters

All CSPs used by the Module are described in Table 5 below. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 5 – Critical Security Parameters (CSPs)

CSP	Description / Usage
DRBG-EI	1920 bits of 1-bit entropy input/Continuously feed Hash-DRBG. (518.13 bits of min-entropy input)
DRBG Nonce	960 bits of 1-bit entropy input/Instantiation Value for Hash-DRBG. (259.07 bits of min-entropy nonce)
DRBG Additional Data Vector	256 bits of 1-bit entropy input/Instantiation Value for Hash-DRBG used on generate and reseed.
DRBG-State	440-bit random vector for V and C/Used during generate to get key material
Key Buffer	½ AES GCM 256-bit key/Feeds keys to consumer module 128 bits at a time
Nios Buffer	32-bit DRBG output/Feeds the Enrollment Nonce, Enrollment IV, and PSK
IV Buffer	256 96-bit vectors/Feeds IV to consumer module

CSP	Description / Usage
Receive Keys	Up to 1,032,192 AES GCM 256-bit keys/Each key can be used for decryption 1 to 255 times
Transmit Keys	Up to 516,096 AES GCM 256-bit keys/Each key can be used for encryption 1 to 255 times
Enrollment Decryption Key	AES GCM 256-bit key/Decrypts a batch of initial Receive keys
Enrollment Encryption Key	AES GCM 256-bit key/Encrypts a batch of initial Transmit keys
HMAC keys	256-bit keys used in the underlying hash for DRBG and KBKDF
PSK (PSOC)	256 bits of DRBG output/Transferred to the Nios for use in the module upon power up and reset
PSK (Nios II)	256 bits of DRBG output/Used as the Input Key to generate Enrollment Keys

3.4 Public Keys

Not applicable.

4 Roles, Authentication and Services

4.1 Assumption of Roles

The module supports three (3) distinct operator roles; QPM Cryptographic Officer (MCO), Q-Box Cryptographic Officer (QCO) and the User role. The cryptographic module enforces the separation of roles used by the function being performed. Table 6 lists all operator roles supported by the module with services performed by that role, authentication of the role, and data used for authentication. The Module does not support a maintenance role or bypass capability.

The Module supports concurrent operators, and in some cases different services/functions can be accessed by different operators. For example, one connection may be performing enrollment as the MCO and another may be performing encryption as the QCO. Since roles are implied, there is no need to manage this separation explicitly. The module knows that the authenticated MCO role is performing enrollment and the QCO role is performing encryption/decryption.

Table 6 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
QPM CO (MCO)	The Cryptographic Officer role that registers, re-registers and enrolls the module.	Identity-based	Enrollment – PSK, Serial Number, and enrollment stage using KBKDF resulting in a 256-bit key
Q-Box CO (QCO)	The Cryptographic Officer role that performs Encryption and Decryption.	Identity-based	A 256-bit key (cipher text/plain text), a 96-bit IV, and a 128-bit GCM-AES tag. Resulting in an AES-GCM 256-bit key

Role ID	Role Description	Authentication Type	Authentication Data
User	User – Accesses reset, self-tests, show mode, and show state services.	Unauthenticated (power-up/Reset, self-tests, show mode and state)	N/A

4.2 Authentication Methods

Each authentication method used by the module is listed below. The corresponding probabilities and justification for its strength is listed in Table 7.

Identity-based authentication for Enrollment

PSK key agreement is used for authentication of the module via another device using a PSK, Q-Box serial number, and stage of enrollment. The PSK is a DRBG generated 256-bit value, the serial number is a 32-bit value, and there are 6 stages of enrollment. Limiting factor is twelve enrollment attempts per minute.

Identity-based authentication for Encryption/Decryption

Encryption/Decryption is authenticated with a 256-bit key (cipher text/plain text), a 96 bit IV, and a 128-bit GCM-AES tag. Limiting factor for authentications is 100 Mbps throughput.

Table 7 – Authentication Description

Authentication Method	Probability	Justification
Identity-based authentication for Enrollment	1/2^256	1/2^256 is significantly less than 1/1,000,000 per attempt. There are 12 enrollment attempts allowed in a minute, so 12 x 1/2^256 is much less than the probability of 1/100,00.
Identity-based authentication for Encryption/Decryption	1/2^256	1/2^256 is significantly less than 1/1,000,000 per attempt. Maximum system throughput is 100Mbs and the smallest allowed packet is 84 bytes (672 bits). 100,000,000 (bits/s) x 60s/672 bits = 8,928,571 attempts. 8,928,571 x 1/2^256 is much less than the probability of 1/100,000.

4.3 Services

All services implemented by the Module are listed in Table 8 and 9 below.

Table 8 – Authenticated Services

Services	Description	MCO	QCO
Enrollment	Derives two AES256 keys that are used to encrypt/decrypt batches of keys for communication to the QPM.	X	
Encryption	Receives input from the Keyfile and DRBG Services, as well as performs AES256 GCM encryption and associates with the correct cipher tag per packet.		X
Decryption	Receives input from the Keyfile Service, gets the expected tag from the prior encryption, and decrypts the packets.		X

All authenticated services are operated in one of the crypto officer roles indicated in Table 8 above, which is implied by the service being accessed by the module.

Table 9 – Unauthenticated Services

Service	Description
Self-tests	Performs all self-tests when the unit is power cycled, or a reset command is received.
Registration	Through the QPM, allows reading the module serial number and receives a PSK from another device. Also allows the overwriting of the PSK (PSOC) on re-registration.
Reset	Destroys all CSPs (excluding the PSK (PSOC)) and resets the module.
Show Mode	Monitors and indicates the modes of the module and displays them through an LED.
Show State	Monitors and indicates the states of the module and displays them through an LED.

All unauthenticated services, except registration* are operated in the user role, which is implied by the service being accessed by the module.

* Registration is performed as a part of the initialization and module set up per Section 5

Table 10 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The service generates the CSP.
- O = Output: The service outputs the CSP.
- E = Execute: The service uses the CSP in an algorithm.
- I = Input: The service inputs the CSP.
- Z = Zeroize: The service zeroizes the CSP.

Table 10 – Security Parameters Access by Service

Service	CSP											
	DRBG EI	DRBG Nonce	DRBG-State	Key Buffer	Nios Buffer	IV Buffer	Receive Keys	Transmit Keys	Enrollment Decryption Key	Enrollment Encryption Key	PSK (PSOC)	PSK (Nios)
Registration	-	-	-	-	-	-	-	-	-	-	G, Z*	G, O
Enrollment	-	-	-	-	-	-	-	-	I**	G	-	E
Encryption	-	-	-	E	E	E	-	O**	-	-	-	-
Decryption	-	-	-	E	E	E	I**	-	-	-	-	-
Self-tests	E	E	E	-	-	-	-	-	-	-	-	-
Reset	Z	Z	Z	Z	Z	Z	Z***	Z***	Z	Z	-	Z
Show Mode	'	-	-	-	-	-	-	-	-	-	-	-
Show State	-	-	-	-	-	-	-	-	-	-	-	-

* Rewrites the key on re-registration

** Performs the action on the encrypted version of the key.

*** Zeroizes the plaintext version of the key.

5 Installation and Module Initialization

The Q-Box must be set up and initialized by registering the module with the Q-Net Policy Manager (QPM) using the QPM CO role.

Installation

1. Remove a Q-Box from the packaging.
2. Plug an approved power supply into a standard 120V outlet and the other end into the power port (marked with a +12V power symbol) on the Q-Box as illustrated. Screw the silver ring clockwise to lock the power connector in place.
3. Within 1 second the Mode LED on the left should start to slow blink. The LED will continue to blink while the Q-Box loads its internal firmware. Within 10 seconds the Mode LED will light solid. **Note:** A fast blinking Mode LED indicates a critical error. The module will restart itself to attempt to clear the error. If the light continues to fast blink, please contact Q-Net Security support.
4. Plug one end of a Cat 5 cable into the Endpoint port on the Q-Box.
5. Plug the other end into the Registration port of the QPM (Q-Net Policy Manager)
6. Log into the QPM using the QPM username and password
7. After login, the QPM CO will land on the Devices list page
8. Click the Registration button at the top right (which only appears when a device is connected to the registration port) to start the registration process.
9. Enter Registration Information
   9.1 Enter a device name
   9.2 Choose whether to Auto Discover the Endpoint. If “No” is chosen, enter the Endpoint IP and Endpoint MAC.
   9.3 Use a Local or External QPM IP (if available). Make sure the Gateway IP and Network mask are correct
   9.4 Click Save
10. Upon successful Registration, a notification will be seen at the top of the screen (highlighted in green).
    If the device fails to register, a failed message will receive at the top the screen in red.
11. Once registration is complete, remove the Cat 5 cable from the Endpoint port and remove power.

Enrollment

Connect the module’s Network port to the network and the Endpoint port into an Endpoint/Host and reconnect power. The MCO will enroll the module automatically if configured properly, with access to the QPM. Once enrollment is complete, the module is in FIPS Approved mode.

6 Self-Tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power-up self–tests are available on demand by power cycling the module or sending an internal reset signal. The module performs no critical functions tests.

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptography by the Module. If any of the KATs fail, the Module enters the critical error state and indicates critical error mode by fast blinking the mode LED. Otherwise, successful completion is indicated by a solid mode LED.

The module performs the following algorithm KATs on power-up.

- AES-GCM-256 Generation KATs (implicitly tests underlying ECB)
- SP 800-90A Hash DRBG KAT tests instantiate, Generate and Reseed (implicitly tests the underlying SHA-256 (Cert # A1663)
- KBKDF KAT
- HMAC-SHA-256 KAT (Cert # A1665)
- SHA-256 KAT (Cert # A1664)

The module performs the following ENT (P) health tests on power-up.

- RCT Integrity Test
- APT Integrity Test
- RCT BIST per SP800-90B over 2048 consecutive samples
- APT BIST per SP800-90B over 2048 consecutive samples

The module performs the following algorithm FW Integrity tests on power-up.

- FPGA/Nios II 32-bit CRC integrity check
- PSOC 16-bit CRC integrity check
- ARM 16-bit CRC integrity check

The module performs the following ENT (P) conditional self-tests continuously during module operation.

- RCT per SP800-90B
- APT per SP800-90B

7 Physical Security Policy

The module is contained in a completely opaque aluminum box sealed by threaded inserts that can only be removed by cutting or drilling.

Table 11 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Thick Aluminum box sealed with tamper evident threaded inserts.	Periodically	Look for signs of tampering. Remove from service if tampering found.

8 Operational Environment

The Module has a non-modifiable operational environment under the FIPS 140-2 definitions. Firmware versions validated through the FIPS 140-2 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

9 Mitigation of Other Attacks Policy

None

10 Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-2.

1. The module provides three (3) distinct operator roles: QPM Cryptographic Officer (MCO), Q-Box Cryptographic Officer (QCO) and the User.
2. The module does not require any user actions for physical security.
3. The module provides role-based and identity-based authentication (see Table 7).
4. The module clears previous authentications on power cycle.
5. An operator does not have access to any cryptographic services prior to assuming an authorized role.
6. The module allows the operator to initiate power-up self-tests by power cycling power or resetting the module.
7. Power up self-tests do not require any operator action.
8. Data outputs are inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The only restriction on which keys or CSPs are zeroized by the Reset Service is the PSK, which can be over-written by the Registration Service.

11. The module does support concurrent operators.
12. The module does not support a maintenance interface or role.
13. The module does not support manual key entry.
14. The module does have a proprietary external input/output device used for entry/output of data.
15. The module does not output plaintext CSPs.
16. The module does not output intermediate key values.
17. The module does not provide bypass services or ports/interfaces.

11 References and Definitions

The following standards are referred to in this Security Policy.

Table 12 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program (November 5, 2021)*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 2 *March 2019*
[133r2]	*NIST Special Publication 800-133 Revision 2, Recommendation for Cryptographic Key Generation, June 2020*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[202]	*FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018*

Table 13 – Acronyms and Definitions

Acronym/Term	Definition
Jitkey	Just-in-time Key used for encryption/decryption
Keyfile	Used to track and monitor Jitkeys
Nios II	Embedded processor designed for an FPGA
PSoC	Programmable System on a Chip

Acronym/Term	Definition
Q-Box	Module to which this policy applies
QNS	Q-Net Security
QPM	Q-Net Policy Manager