AN/KRC-6 (ATCS-BBU) Non-Proprietary FIPS 140-3 Cryptographic Module Security Policy

Hardware Version: AN/KRC-6(v)1
Firmware Version: 1.1.1

Document Version 2.2
February 2025

Document prepared by

Lightship Security

www.lightshipsec.com

Contents

Tables

Figures

1. General

This is the non-proprietary cryptographic module security policy for the AN/KRC-6 (ATCS-BBU) *version 1* from *Ultra Electronics TCS Inc., (operating as Ultra Intelligence & Communications)*, hereafter referred to as "Ultra". This security policy was prepared as part of the validation of the module. This policy describes how the Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S. and Canadian government requirements for cryptographic modules. More information about the standard is available from csrc.nist.gov/projects/cryptographic-module-validation-program

This document also describes how to run the module in a secure Approved mode of operation.

The Module has been validated at the FIPS 140-3 section levels shown in the table below.

Table 1 – Security levels

ISO/IEC 24759 Section 6.	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A

The Module has an overall security level of 2.

2. Cryptographic Module Specification

The Base Band Unit (BBU) hereafter referred to as the "Module", is a multiband, point-to-point (PTP), point-to-multipoint (PMP) and Mesh radio system capable of providing at-the-halt communications across multiple echelons and on-the-move access capability. The system offers up to 400 Mbps throughput and operational flexibility. The Module operates as a component of the larger Amphibious Tactical Communications System (ATCS). The Module can also be referred to as the ATCS BBU.

Each module can communicate wirelessly with other devices using up to two waveforms. Each waveform can be configured for the local RF channel frequencies, polarization and topology (LBH, NBH or UNW). The Module operates in VHF (RF band 3+)

The Module offers encrypted digital communications over the TLS protocols, and management via SNMPv3 using HMAC-SHA-1 and AES-CFB-128. The Module can manage multiple VLANs. Each VLAN can be configured to be either encrypted or non-encrypted (see 4.7 Bypass Capability).

The Module is classified as a hardware module with a multiple-chip standalone embodiment and is designed to operate within a non-modifiable operational environment.

2.1 Cryptographic Boundary

The module's logical and physical boundaries are defined by the outer casing. This boundary encompasses the complete set of hardware and firmware components.

Figure 1 – AN/KRC-6 (ATCS BBU)

The block diagram below illustrates the principle physical components of the module.

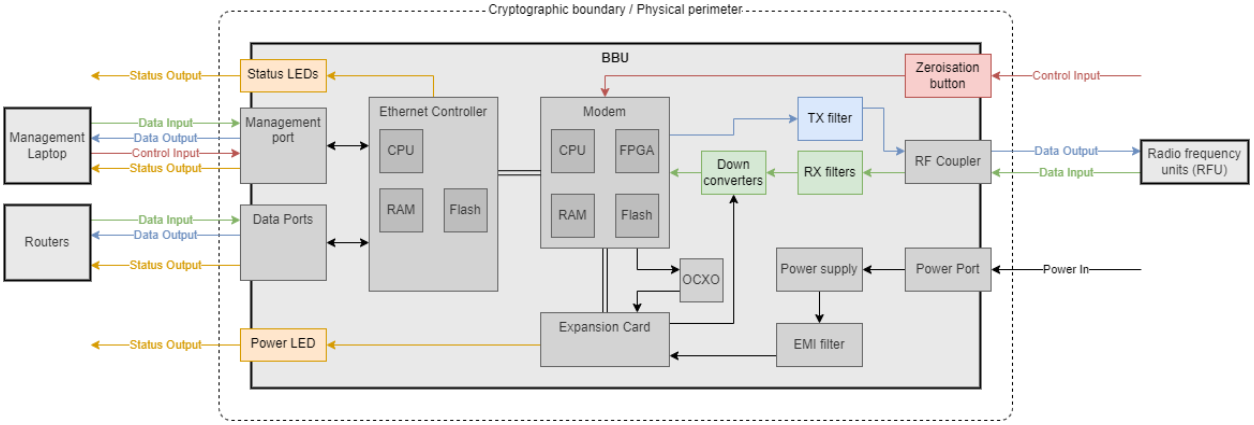

Figure 2 – Module Block Diagram and Cryptographic Boundary

The Module's firmware and operating system is executed primarily in the modem component. Secondary firmware related to the management of the physical ethernet ports is executed in the ethernet controller's independent CPU.

2.2 Tested Configurations

The Module was tested in the configuration listed below and was found to be compliant with FIPS 140-3 requirements.

Table 2 – Hardware Tested Configuration

Model	Hardware	Firmware Version	Distinguishing Features
BBU-B3	100-820001-000	1.1.1.0560	Rack mountable radio system.

2.3 Vendor Affirmed Configurations

The last four digits of the Module's firmware version listed in the Tester Configurations table above, is the build number of the firmware that was tested by the CSTL. From time to time, Ultra may recompile the module to address non-security relevant bug fixes, vulnerabilities or upon client request. For builds that preserve the same version: 1.1.1, Ultra affirms continued compliance with the FIPS 140-3 standard, but these builds will not have been tested by the CSTL. A security relevant change would be reflected in the version of the module, for example: 1.1.2.

Any firmware version of the module other than 1.1.1 is outside the scope of this security policy.

2.4 Approved Algorithms

The Module implements the following algorithms:

Table 3 – Approved algorithms

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size / Key Strength	Use / Function
Modem (WolfSSL)				
A4734	AES [FIPS 197] [SP 800-38A]	CBC	128, 256	Encryption, decryption
A4734	AES [FIPS 197] [SP 800-38A]	CFB128	128	Encryption, decryption
A4734	AES [FIPS 197] [SP 800-38D]	GCM[1]	128, 256	Encryption, decryption
A4734	CVL [SP 800-135rev1] [RFC 7627]	TLS 1.2 KDF[2] with SHA2-256 / 384	-	Key derivation
A4734	CVL [SP 800-135rev1]	TLS 1.3 KDF[2] with SHA2-256 / 384	-	Key derivation
A4734	CVL [SP 800-135rev1]	SNMP KDF[2]	-	Key derivation
A4734	ECDSA [FIPS 186-4]		P-256	Key pair generation and verification during TLS
A4734	Hash_DRBG [SP 800-90Arev1]	SHA2-256	256	Deterministic random bit generation
A4734	HMAC [FIPS 198-1]	SHA-1, SHA2-256, SHA2-384	> 128	Message authentication
A4734	KAS-ECC-SSC[3] [SP 800-56Arev3]	ECC CDH ephemeral unified	P-256, P-384	Shared secret computation
A4734	PBKDF [SP 800-132]	SHA2-256	-	Password-based key derivation
A4734	SHS [FIPS-180-4]	SHA-1, SHA2-256, SHA2-384	-	Hashing
Ethernet Controller (WolfSSL)				
A4735	HMAC [FIPS 198-1]	SHA2-256	256	Message authentication

A4735	SHS [FIPS-180-4]	SHA2-256	-	Hashing
Hardware Acceleration (Freescale QorIQ P2020)				
A4738	AES [FIPS 197] [SP 800-38A]	CBC	128, 256	Encryption, decryption
A4738	HMAC [FIPS 198-1]	SHA-1	128	Message authentication
A4738	SHS [FIPS-180-4]	SHA-1	-	Hashing
Ultra IC Kernel				
A4155	SHS [FIPS-180-4]	SHA-1	-	Entropy Conditioning
Uboot Bootloader				
A4736	SHS [FIPS-180-4]	SHA2-256	-	Hashing

[1] AES-GCM is only used as part of TLS 1.2 GCM cipher suite. The module constructs the IV internally in compliance with IG C.H technique 1a. The IV is sourced entirely from the module's DRBG. The counter portion of the IV is set by the module within its cryptographic boundary. Per RFC 5246, when the nonce explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key.

[2] No parts of the TLS v1.2/v1.3, and SNMP protocols, other than the KDF, have been tested by the CAVP or CMVP.

[3] KAS-ECC-SSC is only used in the context of a key agreement schemes. The module's use of KAS-ECC-SSC is compliant with FIPS 140-3 IG D.F.

2.5 Allowed Algorithms

The module does not implement any allowed algorithms, with or without security claimed.

2.6 Non-Approved Algorithms

The Module can only operate in the Approved mode. There are no Non-Approved Algorithms.

2.7 Modes of Operation

The Module supports one mode of operation: Approved.

3. Cryptographic Module Interfaces

The following table lists the module's port and interfaces, both physical and logical.

Table 4 – Ports and interfaces

Physical port	Logical interface	Data that passes over port / interface
2 Data ports (Ethernet)	Data Input	Incoming network traffic
	Data Output	Outgoing network traffic
	Status Output	Status of the Module
Management port (Ethernet)	Data Input	Traffic encryption and authentication keys, management input data
	Data Output	Management output data
	Control Input	Commands to operate the Module
	Status Output	Status of the Module
Power LED	Status Output	Status of Module power supply
Power port	Power Input	None
Power switch	Control Input	None
RF Coupler	Data Input	Analog data received from RFUs. May or may not be encrypted
	Data Output	Analog data sent to RFUs. May or may not be encrypted
Status LED 1	Status Output	Status of waveform 1
Status LED 2	Status Output	Status of waveform 2
Status LED C	Status Output	Status of connectivity with other components in the ATCS
Status LED S	Status Output	Status of Module
Zeroisation button	Control Input	Command to invoke zeroisation and/or resetting

The Module acts as the manager of other hardware devices within the ATCS system. The module can issue control commands to the Dehydrator Unit (DU), the two Radio Frequency Units (RFU) and the Power Distribution Unit (PDU). However, none of these devices are classified as 'cryptographic modules'. Therefore, for the purposes of FIPS compliance: the Module does not support a control output interface.

The physical enclosure of the Module includes the additional 'LAN3' and 'BBU-Link' ports. These ports exist for a future version of the Module. In this version, these ports are not provisioned and are non-functional. When the Module is performing self-tests, or is in an error state, the data output interface is disabled.

4. Roles, Services and Authentication

The module's operations are managed by authorized users. Each user's account is assigned one of the following roles:

Crypto Officer (CO)

Referred to as the "Admin" role in Ultra documentation, users assigned this role are responsible for module configuration, which includes passwords, keys and certificates. The Crypto Officer has access to all services offered by the module.

Detailed Crypto Officer responsibilities are described in section 11.1 – Administrator Guidance.

Operator (OP)

A user assigned the Operator role has access to general security services, including cryptographic operations and other approved security functions. Detailed Operator responsibilities are described in section 11.4 – Non-administrator Guidance.

Monitor (MON)

A user assigned the Monitor role has read only access to all data, including non-security critical data.

Neither the Operator nor Monitor roles have permission to load keys or perform user management activities.

4.1 Concurrent Users

The Module supports concurrent users. Up to 10 users may be logged concurrently. The memory and process management features of the operating system maintain separation of users and corresponding services.

Table 5 – Roles, Services, Input and Output

Role	Service	Input	Output
Crypto Officer	Account configuration	Command	Status
Crypto Officer	Account creation	New username, password and profile	Status
Crypto Officer	Account lock	Command	Status
Crypto Officer	Account removal	Command	Status
Crypto Officer	Account reset	New user password	Status
Crypto Officer	Account unlock	Command	Status
All roles	Change password	Existing password, New password	Status
Crypto Officer	Configure system	Command	Status
Crypto Officer	Configure Device MAC Filtering	Command	Status
Crypto Officer	Configure SNMP	SNMP Authentication key, SNMP Privacy key	Status
Crypto Officer	Configure NTP	Command	Status
Crypto Officer, Operator	Disable bypass mode	Command	Status
Crypto Officer, Operator	Enable bypass mode	Command	Status
Crypto Officer	Enter traffic authentication key	Traffic authentication Key	Status

Crypto Officer	Enter traffic encryption key	Traffic encryption Key	Status
All roles	Get state of encryption on RF interfaces	Command	Status
All roles	HTTPS Key Agreement	Command	TLS messages
All roles	Login	Existing Password	Status
All roles	Logout	Command	Status
Crypto Officer, Operator	Reboot (Via GUI)	Command	Status
Crypto Officer	Reset settings	Command	Status
Crypto Officer, Operator	System Self-test	Command	Status
All roles	SNMP Login	SNMP Authentication key	Internal ATCS network configuration and status
Crypto Officer, Operator	SNMP Editing	Command	Status
All roles	SNMP Viewing	Command	Status
All roles	Traffic authentication	Traffic authentication key, Traffic data, Traffic MACs	Status, validation ruling
All roles	Traffic decryption	Traffic encryption key, Encrypted traffic data	Plaintext traffic data
All roles	Traffic encryption	Traffic encryption key, Plaintext traffic data	Encrypted traffic data
All roles	Traffic MAC generation	Traffic authentication key, Traffic data	Traffic MACs
Crypto Officer, Operator	Upgrade firmware	Firmware image	Status
All roles	View status	Command	Status
Crypto Officer, Operator	View log	Command	Status
All roles	View information	Command	Status
Crypto Officer	Zeroise (via GUI)	Command	Status
All roles	Zeroise (via button)	Command	Status

4.2 Authentication

The Module supports role-based authentication using account names and passwords. Passwords are stored as keys using the Module's implementation of PBKDF with SHA2-256 as the PRF. The module uses an iteration count of 1,000.

Table 6 – Roles and Authentication

Role	Authentication Method	Authentication Strength
Crypto Officer	Role-based	A 256-bit key is generated from a password using PBKDF
Operator	Role-based	A 256-bit key is generated from a password using PBKDF
Monitor	Role-based	A 256-bit key is generated from a password using PBKDF

4.3 Authentication Strength Objective

The Module's authentication mechanism has been designed to meet the following objectives:

- the probability shall be less than one in 1,000,000 that a random attempt will succeed, and
- during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed.

4.4 Authentication Strength

Each user is authenticated using a password. Passwords must contain:

- at least 1 lowercase character (a to z)
- at least 1 uppercase character (A to Z)
- at least 1 numeral (0 to 9)
- at least 1 non-alphanumeric character (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

The Module requires that passwords be 16 to 30 characters long, drawn from the pool of 94 characters. The password strength is 1 in 1.52×10^{59}.

The Module also enforces the following:

- Passwords cannot be changed more than once in any 24-hour period.
- After their first login, users are required to change the default password assigned.
- After each failed login attempt, the Module imposes a 3 second timeout before another attempt can be made.
- After 3 unsuccessful login attempts, the user account is locked for 15 minutes.
- Passwords are valid for a maximum of 30 days. After which, users are prompted to change their passwords.
- The previous 5 passwords may not be reused.
- A user account that has been inactive for 35 days, is automatically disabled.
- After 10 minutes of inactivity, the Module requires the user to reauthenticate.

4.5 Approved Services

The following table lists the approved services available to Module operators.

Table 7 – Approved services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Account configuration	Change account profile	-	-	CO	-	-
Account creation	Creating a user account	PBKDF	User password key	CO	W	Implicit
Account lock	Disable a user account	-	-	CO	-	-
Account removal	Deleting a user account	-	-	CO	-	-
Account reset	Reset a user password	PBKDF	User password key	CO	W	Implicit
Account unlock	Enable a user account	-	-	CO	-	-
Change password	Change own account password	PBKDF	CO password key User password key	CO, OP, MON	W	Implicit
Reset settings	Restores the module configuration to factory settings	-	-	CO	-	-
Configure System	Configure the system, NTP, IP addresses, system logs, RF settings, bypass, allowed MAC addresses	-	-	CO	-	-
Configure Device MAC Filtering	Configure allowed MAC addresses	-	-	CO	-	-
Configure NTP	Configure NTP	-	-	CO	-	-
Configure SNMP	Modify of SNMP privacy and authentication passwords	SNMP KDF	SNMP Authentication key, SNMP Privacy key	CO	W	Implicit
Disable bypass mode	Configure an RF interface with an encrypted VLAN	HMAC-SHA2-256	Configuration integrity key	CO, OP	E	Implicit

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Enable bypass mode	Configure the RF interface with a nonencrypted VLAN	HMAC-SHA2-256	Configuration integrity key	CO, OP	E	Implicit
Enter traffic encryption key	Enter keys for traffic encryption	-	Traffic encryption Key	CO	W	-
Enter traffic authentication key	Enter keys for traffic authentication	-	Traffic authentication Key	CO	W	-
Get state of encryption on RF interfaces	Allows to view the configuration of the encrypted or nonencrypted VLAN on an RF interface	-	-	CO, OP, MON	-	-
HTTPS Key Agreement	Establish keys for secure communications	KAS-ECC-SSC CVL (TLS 1.2 / 1.3) ECDSA.KeyGen ECDSA.KeyVer	TLS session key, TLS session authentication key, ECDH Public key, ECDH Private key, TLS pre-Master secret, TLS Master secret, DRBG V value	CO, OP, MON	G E R	Implicit
Login	Used to log in to the module	PBKDF	CO password key, User password key	CO, OP, MON	R	Implicit
Logout	Logout of the module	-	-	CO, OP, MON	-	-
Reboot (via GUI)	Reboot the module	-	All SSPs stored in RAM	CO, OP	Z	-
System Self-test	Run hardware diagnostic tests	-	-	CO	-	-
SNMP Login	Access MIBs data	SNMP KDF	SNMP Authentication key	CO, OP, MON	R	Implicit
SNMP editing	Edit MIB data	AES-CFB-128	SNMP privacy key	CO, OP	E	Implicit
SNMP viewing	View MIB data	AES-CFB-128	SNMP privacy key	CO, OP, MON	E	Implicit
Traffic authentication	Authenticate network traffic	HMAC-SHA-1	Traffic authentication key	CO, OP, MON	E	Implicit
Traffic decryption	Decrypt network traffic	AES-CBC	Traffic encryption key	CO, OP, MON	E	Implicit

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Traffic encryption	Encrypt network traffic	AES-CBC	Traffic encryption key	CO, OP, MON	E	Implicit
Traffic MAC generation	Generated MAC for network traffic authentication	HMAC-SHA-1	Traffic authentication key	CO, OP, MON	E	Implicit
Upgrade Firmware	Upload new validated firmware	HMAC-SHA2-256	Configuration integrity key	CO, OP	E	Implicit
View Status	Shows system, VLAN, RF and waveform statistics	-	-	CO, OP, MON	-	-
View Log	Shows the system log	-	-	CO, OP	-	-
View Information	Shows general system identification and configuration	-	-	CO, OP, MON	-	-
Zeroise (via GUI)	Zeroise all SSPs	-	All SSPs	CO	Z	Implicit
Zeroize (via button)	Zeroise all SSPs	-	All SSPs	CO, OP, MON	Z	Implicit

Note: The module operates exclusively in the approved mode using approved security functions. The use of an approved security function is indicated implicitly by the completion of the corresponding service.

Access rights are indicated using the following notation:

- G – Generate: The module generates or derives the SSP.
- R – Read: The SSP is read from the module (e.g., the SSP is output).
- W – Write: The SSP is updated, imported, or written to the module.
- E – Execute: The module uses the SSP in performing a cryptographic operation.
- Z – Zeroize: The module zeroizes the SSP.

4.6 Non-Approved Services

The Module does not implement any non-approved services.

4.7 Bypass Capability

The Module supports a bypass capability. Each of the two Waveforms supported by the Module can be linked to one of the VLANs managed by the Module. Each VLAN can be configured to be either encrypted or non-encrypted (bypass). The Module can simultaneously output data in either a cryptographically protected or non-protected form – on separate VLANs or waveforms.

The bypass capability is enabled when the operator assigns a non-encrypted VLAN to a Waveform. A confirmation action will be required from the operator. Furthermore, a bypass alarm will remain active to inform the operator which waveform is set to accept an unencrypted VLAN, regardless of the administrative status of the Waveform.

The exit-bypass condition occurs when the operator assigns encrypted VLANs to both Waveforms.

The bypass capability is tested during the Module's boot sequence by the bypass self-test (see section 10.4).

5. Software Security

The module's firmware is comprised of two components: the bootloader and the firmware image. This latter component contains all firmware executed by the modem and ethernet controller. The integrity of both components is checked during the boot sequence by the module's bootloader.

The following three tests are performed:

- The bootloader performs a known-answer test (KAT) of its SHA2-256 implementation.
- The bootloader checks the integrity of itself using SHA2-256.
- The bootloader checks the integrity of the firmware image using SHA2-256.

Both hashes were created when the Module was compiled. They are stored in the Module and contained within the cryptographic boundary.

A user can invoke the integrity test on-demand by rebooting the Module.

If an integrity test fails, the Module will enter an error state, regardless of how the test was invoked (see section 10.5 Error Handling).

5.1 Firmware Loading

The Module supports the upgrading of the firmware image component. Firmware upgrades can be performed by a user assigned the *Operator or Crypto Officer* role. Upgrades are performed through the GUI of the management laptop.

Only firmware authenticated by Ultra can be loaded into the Module. See section 10.3 Firmware Load Test for a description of how the Module verifies the authenticity of firmware upgrades. If the module is unable to verify the authenticity of the firmware an error is raised (see 10.5 Error Handling). If the new firmware is determined to be authentic, the Module transfers the new firmware to non-volatile memory and invokes a reboot.

6. Operational Environment

This section is not applicable. A cryptographic module that has a physical security rating above 1, has no operational environment requirements.

The Module provides the following operational environments:

Table 8 – Operational Environments.

Module Component	Firmware Version	Processor	Implementation Description
Modem	WolfSSL 5.6.3 commercial FIPS	Freescale QorIQ P2020-Power PC	WolfSSL is a library which provides encryption and authentication services for HTTPS, SNMP and for digital signature within the Module.
Ethernet controller	WolfSSL 5.6.3 commercial FIPS	ARM Cortex-A5	The ethernet controller manages the physical ethernet ports within the Module. It uses the WolfSSL cryptographic library for hashing and message authentication.
Freescale QorIQ P2020	Freescale QorIQ P2020 - Security - SEC3.3	Freescale QorIQ P2020-P2020NXE2MHC	The Freescale QorIQ P2020 hardware accelerator provides encryption and authentication services for data traffic within the Module.
Ultra IC Kernel	Ultra IC Kernel v1.0	Freescale QorIQ P2020-Power PC	The Ultra IC kernel provides hash algorithm services for entropy source conditioning component within the Module.
Bootloader	169-820425-004	Freescale QorIQ P2020-Power PC	The bootloader provides integrity testing services to the modem component of the Module.

7. Physical Security

The module is enclosed in a production-grade weatherproof aluminum alloy case that is opaque to the visible spectrum, which defines the cryptographic boundary of the module. There are no openings (slits and/or holes) in the enclosure to give any visual or physical access to internal components.

The module is classified as having a multi-chip standalone embodiment.

7.1 Tamper evident seals

The module's enclosure is sealed using four (4) tamper evident seals, that prevent the enclosure from being opened without signs of tampering.

The tamper evident seals shall be properly installed for the module to operate in the approved mode of operation.

The part number for ordering tamper evident seals is 612-990311-402.

7.1.1. Storage

Tamper evidence seals should be stored in a climate-controlled facility, that can maintain a maximum temperature of 90°F (32°C) and a relative humidity between 35% to 90%. Stored in this manner, the seals will remain viable for a minimum of 1 year. Cooler temperatures extend the shelf life.

The Crypto Officer is responsible for securing and having control at all times of any unused tamper evident seals.

7.1.2. Application

If the tamper evident seals have not been pre-applied by Ultra, the Crypto Officer is responsible for their application. The locations of the tamper evident seals are shown in Figure 3 – Placement of tamper evident seals.

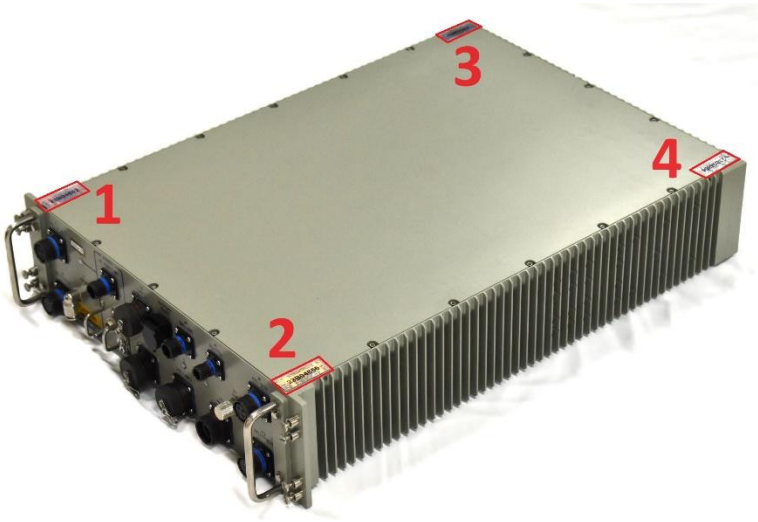

Figure 3 – Placement of tamper evident seals

The Crypto Officer shall prepare to apply tamper evident seals as follows:

- The Crypto Officer shall wash their hands prior to application, to minimize contamination from body oils.
- The application is to be done in a clean environment.
- The surface temperature of the Module shall be between 35°F (2°C) and 90°F (32°C).

- The surface of the Module shall be cleaned using 90% isopropyl alcohol and a clean paper towel. A second paper towel shall be used to dry the surface. Do not allow the alcohol to air dry as contaminants may remain on the surface.

It is critical that the application be performed in a manner that does not allow finger oils to transfer to the adhesive. The Crypto Officer shall apply tamper evident seals as follows:

- Peel back a portion of the liner (backer) to expose a portion of the adhesive side of the seal.
- Affix the exposed portion of the adhesive to the intended surface.
- Peel away the balance of the liner to fully affix the seal making sure that no bubbles or wrinkles are formed.

It is not possible to reposition a seal once applied. The seal will indicate tampering.

Seals shall be placed to cover two screws in each of the four corners of the module cover as shown in Figure 4. Seals do not need to contact the side panels of the module enclosure.

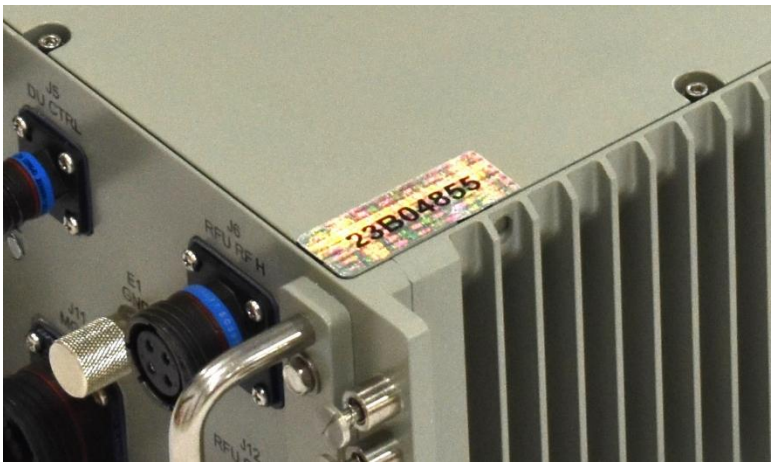

Figure 4 – Placement of tamper evident seal

7.1.3. Verification

The physical security of the Module shall be periodically verified per the table below:

Table 9 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper evident seals	During deployment or repositioning	Ensure that the tamper evident seals are not removed or damaged. If the Module shows any signs of tampering the Module shall not be put in operation and the Crypto Officer must be notified immediately.

8. Non-invasive Security

This section is not applicable. There are currently no approved non-invasive mitigation metrics defined at the time of writing. (Ref: ISO/IEC 19790:2012 Annex F)

9. SSP Management

The Module manages the SSPs, and keys listed in the following two tables.

Table 10 – SSPs

Key / SSP Name / Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
CO password key (CSP)	256	PBKDF, SHA2-256 (A4734)	From CO password	-	-	Plaintext in Flash	Zeroisation service	Authentication
Configuration integrity key (CSP)	256	HMAC-SHA2-256 (A4734)	-	-	-	Embedded in FW image	During firmware upgrade by reimaging the flash memory	To authenticate configuration and bypass mechanism switch integrity. Authentication of firmware upgrades.
DRBG entropy input string (CSP)	196 bytes	Hash_DRBG (A4734)	Internally	-	-	Plaintext in RAM	Rebooting	Seeding DRBG
DRBG C Value (CSP)	55 bytes	Hash_DRBG (A4734)	Internally	-	-	Plaintext in RAM	Rebooting	Key agreement
DRBG V Value (CSP)	55 bytes	Hash_DRBG (A4734)	Internally	-	-	Plaintext in RAM	Rebooting	Key agreement
ECDH public key (PSP)	P-256	KAS-ECC-SSC (A4734)	Internally	Export in plaintext during TLS	-	Plaintext in RAM	Rebooting	For Key agreement session to establish TLS Pre-Master
ECDH private key (CSP)	P-256	KAS-ECC-SSC (A4734)	Internally	-	-	Plaintext in RAM	Rebooting	For Key agreement session to establish TLS Pre-Master
SNMP privacy key (CSP)	128	SNMP KDF, AES-CFB128 (A4734)	From SNMP privacy password	-	-	Plaintext in Flash	Zeroisation service	SNMP traffic encryption
SNMP Authentication key (CSP)	160	SNMP KDF, HMAC-SHA-1 (A4734)	From SNMP authentication password	-	-	Plaintext in flash	Zeroisation service	SNMP authentication
TLS Pre-master Secret (CSP)	48 bytes	KAS-ECC-SSC (A4734)	-	-	by ECDH Key agreement	Plaintext in RAM	Rebooting	Used to derive the TLS Master Secret and session keys

Key / SSP Name / Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
TLS Master Secret (CSP)	48 bytes	KAS-ECC-SSC (A4734)	-	-	using SP 800- 135 KDF TLS 1.2	Plaintext in RAM	Rebooting	Used in TLS connections to derive the session keys
TLS Session Key (CSP)	128, 256	AES-GCM (A4734, A4738)	Internally generated and derived using TLS protocol	-	-	Plaintext in RAM	Rebooting	Data encryption for TLS sessions
TLS Session Authentication Key (CSP)	256	HMAC-SHA2-256 (A4734)	Internally generated and derived using TLS protocol	-	-	Plaintext in RAM	Rebooting	Data authentication for TLS sessions
Traffic authentication key (CSP)	160	HMAC-SHA-1 (A4734)	-	Electronically imported through management GUI	-	Plaintext in Flash	Zeroisation service	Configure Hashing Keys for traffic data encryption
Traffic Encryption Key (CSP)	128, 256	AES-CBC (A4734)	-	Electronically imported through management GUI	-	Plaintext in Flash	Zeroisation service	Configure Keys for traffic data encryption
User password key (CSP)	256	PBKDF, SHA2-256 (A4734)	From user password	-	-	Plaintext in Flash	Zeroisation service	Authentication

A static ECDSA public/private key pair exists in the module firmware, but these keys are only used for testing the implementation of ECDSA. The module does not use these keys operationally.

9.1 Zeroisation

SSPs stored in volatile memory (RAM) are zeroized by powering down or rebooting the Module. SSPs stored in non-volatile memory (Flash) can be zeroized using either of the following two methods:

- invoking the zeroise command from the web interface, or
- holding the zeroisation push button for 30 seconds.

Both methods will result in the zeroisation of all SSPs stored in the module, returning the Module to the factory-state. The zeroisation of SSPs stored in Flash memory involves reformatting the entire memory with zeroes.

Upon completion of the zeroisation service, the Module automatically reboots which zeroizes SSPs stored in volatile memory.

The Module does not overwrite an unprotected SSP with another. This approach ensures that sensitive data cannot be recovered.

9.2 Transitions

The Module does not implement any algorithms / keys that will transition from approved to non-approved before the validation expires.

The Module's digital signature, block cipher, hashing and key establishment algorithms are compliant to the requirements of CNSA 1.0.

9.3 RBG [Random Bit Generator] and Entropy

The following entropy sources are available to the module and have been tested to NIST SP800-90B.

Table 11 – Non-Deterministic Random Number Generation Specification

Entropy Source	Minimum number of bits of entropy	Details
Ultra IC Entropy Source	The Ultra IC Entropy Source provides 0.9 bits of entropy per output bit.	ESV #E88

10. Self-tests

The Module performs both pre-operational and conditional self-tests. Once invoked, the Module will perform no functions or services until the self-test(s) has been completed.

10.1 Pre-Operational Self-tests

Pre-operational self-tests are performed automatically after the Module has been powered up. No action from the operator is required. In its pre-operational state, the Module performs the Cryptographic Algorithm Self-Test (CAST) that is required for the subsequent firmware integrity test.

Once the integrity test has passed, the Module performs a suite of cryptographic algorithm tests pre-operationally.

All tests must be passed for the Module to transition to an operational state. If any test fails, the Module transitions to an error state (see section 10.5 Error Handling).

While the pre-operational self-tests are being performed, the data output interface is inhibited.

The module performs the following pre-operational self-tests:

Table 12 – Pre-operational self-tests

Algorithm	Properties	Type	Details
Bootloader integrity	SHA2-256	KAT	Integrity test of the bootloader image
Firmware integrity	SHA2-256	KAT	Integrity test of the compressed firmware image.
Bypass	-	-	Verify the correction routing of encrypted and non-encrypted packets.

While operating in the pre-operational state, the Module also performs its suite of cryptographic algorithm self-tests (CASTs) and health checks for the DRBG's Generate / Instantiate / Reseed functions as specified in section 11.3 of NIST SP 800-90Arev1.

Pre-operational self-tests can be invoked on-demand by rebooting the module.

10.2 Conditional Self-tests

Conditional self-tests are performed by the Module during operation when specific conditions occur.

The Module performs the following conditional self-tests:

Table 13 – Conditional self-tests

Algorithm	Properties	Type	Details	Condition
Modem (WolfSSL)				
AES	CFB128	KAT	Encrypt and decrypt	On power up
AES	CBC	KAT	Encrypt and decrypt	On power up
AES	GCM	KAT	Encrypt and decrypt	On power up
ECDSA	P-256	KAT	SigGen and SigVer	On power up
HMAC	SHA-1 SHA2-256 SHA2-384	KAT	-	On power up

Hash_DRBG	SHA2-256	KAT	Instantiate, Generate, Reseed health tests	On power up
KAS-ECC-SSC	P-256	KAT	Shared secret calculation	On power up
ECDSA	SHA2-256	PCT	SigGen and SigVer	On generation of ECDH key pair
PBKDF	SHA2-256	KAT	Derive master key: 384, 400 and 512 bits	On power up
TLS 1.2 KDF	SHA2-256	KAT	-	On power up
TLS 1.3 KDF	SHA2-256	KAT	-	On power up
SNMP KDF	SHA-1	KAT	-	On power up
Firmware	HMAC-SHA2-256	-	-	On firmware upgrade
Hash_DRBG	-	CHT	verify that the output of the DRBG is not the same as the previous value	On instantiate, generate and reseed
-	-	RCT	Verify that the noise source has not gotten stuck on a single value	On power up, and each time entropy is requested (every 10ms)
-	-	APT	Verify that no value is occurring more frequently than expected over any group of512 consecutive samples	On power up, and Continuously (every 10ms)
Bypass	HMAC-SHA2-256	KAT	Verify the integrity of the configuration file	On power up
Ethernet Controller (WolfSSL)				
HMAC	SHA2-256	KAT	-	On power up
SHS	SHA2-256	KAT	-	On power up
Hardware Acceleration				
AES	CBC	KAT	Encrypt and decrypt, 128 and 256-bit keys	On power up
HMAC	SHA-1	KAT	-	On power up
SHS	SHA-1	KAT	Message lengths: 8, 16, 128, 256, 360, 384 bits	On power up
Ultra IC Kernel				
SHS	SHA-1	KAT	-	On power up
UBoot Bootloader				
SHS	SHA2-256	KAT	-	On power up

Upon failure of the conditional bypass self-test, the module will transition to the soft error state. The failure of any other self-test will induce a transition to the hard error state. The Crypto Officer will be required to take the actions described in section 10.5 Error Handling.

10.3 Firmware Load Test

Upon receiving a firmware upgrade request, the Module invokes its firmware load test. This test entails the Module computing the expected MAC of the new firmware image using HMAC-SHA2-256 and its embedded configuration integrity key. This MAC is compared to the MAC of the firmware image received. If the MACs match, the Module accepts the new firmware and copies it into the non-volatile memory.

10.4 Bypass self-test

Each Waveform can be connected to either an encrypted data path or a non-encrypted data path. The configuration of each Waveform is stored in a single configuration file for the entire module. Whenever the user makes *any* change to the configuration of the module, this file is updated *and* the module calculates a new message authentication code (MAC) of the entire configuration file, using HMAC-SHA2-256 and the configuration integrity key. The new configuration file MAC is stored in a non-volatile memory location.

During the boot process, the module performs both a pre-operational bypass self-test and a conditional bypass self-test.

The conditional test is performed first. This test involves calculating a MAC of the existing configuration file and comparing it to the previously calculated MAC. The bypass test fails if the MACs do not match. When this occurs, the module raises a configuration alarm and transitions into a soft error state where cryptographic and traffic operations are inhibited. The user must invoke the "Reset settings" service to clear the error condition.

The pre-operational test involves assigning each Waveform to the non-encrypted data path followed by the encrypted data path. For each assignment, a test packet is sent through the module's transfer switch and hardware encryption engine. The module then checks the transmitted packet counts for each Waveform. If the counts are not what is expected, the test fails causing the Module to transition to the hard error state.

10.5 Error Handling

If the bypass self-test fails, the module enters the "soft error state". If any other self-test fails, the module enters the "hard error state". When the module enters any error state it automatically stops transmitting by shutting off the waveform interfaces. This is to ensure any data output via the data output interface is inhibited.

The user can recover from the soft error state by invoking the "Reset settings" service (see section 10.4 Bypass self-test). To recover from a hard error state, the Module must be power cycled.

In either case, an error message is logged in the module System Log. A service status is shown for the Crypto Officer through the WebGUI for review.

11. Life-cycle Assurance

The following sections describe how to install, configure, operate and eventually dispose of the Module.

Additional information and recommended replacement Modules can be found on *Ultra's* website or by contacting customer service at *514 855 6363*.

11.1 Administrator Guidance

The Crypto Officer is responsible for the initialization, configuration, and management of the Module. The Crypto Officer can receive the Module from the vendor via trusted delivery courier including but not limited to DHL, UPS, and FedEx. The Crypto Officer can also arrange for pick up directly from Ultra.

Upon receipt of the Module, the Crypto Officer should check the package for any irregular tears or openings. Upon opening the package, the Crypto Officer should inspect the tamper-evident seals. If there is suspicion of tampering, the Crypto Officer shall contact Ultra immediately.

11.2 Initialization

The Crypto Officer is responsible for the initialization of the module through the Web Interface. The Crypto Officer must login to the module using the default username "CryptoOfficer" and password "CryptoOfficer11!".

Once first-time authentication has been completed, the Crypto Officer is forced to create a new password respecting the password restrictions enforced by the Module as defined in section 4.4 .

The following steps are required to enable the secure operation of the Module:

- The Crypto Officer must change the default authentication password upon first-time login,
- The Crypto Officer must verify that the installed firmware version number is listed in the certificate. Only a CMVP validated version is allowed to be used.
- The Crypto Officer must rename the default "CryptoOfficer" username,
- The Crypto Officer may choose to add users with Operator or Monitor profiles (optional). The Operator profile is equivalent to the User role per FIPS definitions.
- The Crypto Officer must configure an encrypted VLAN by selecting the traffic encryption key length (128 or 256 bits) and entering the encryption key.
- The Crypto Officer may enable traffic authentication mode and enter the traffic authentication key (optional).
- The Crypto Officer must assign one of the two previously configured encrypted VLANs to the wireless interface. By default, the wireless interfaces are in bypass mode.
- The Crypto Officer must ensure that the module does not show any FIPS alarm.
- The Crypto Officer must enter the SNMP privacy and authentication passwords, if required by policy.
- The module is ready for configuration of non-security related parameters.

For additional initialization guidance, please reference the "ATCS Technical Manual".

11.3 Management

The Crypto Officer can configure and monitor the Module via the secure Web-based GUI. The Crypto Officer should check the System Status and System Logs frequently for errors. If the Module ceases to function normally, contact Ultra customer support.

11.4 Non-administrator Guidance

The Module's web-based interface and configuration options available to a user assigned the Operator or Monitor profile are a subset of the interface and configuration options available to the Crypto Officer. Refer to Section 11.1 – Administrator Guidance for details.

The Operator has access to the same web-based interface and configuration options as the Crypto Officer, except for the following.

The Operator cannot:

- Perform any user management action such as add or delete users,
- Change any other user's password,
- Add, modify, or delete any encryption keys,
- Enable, modify parameters, or disable SNMP,
- Enable, modify parameters, or disable NTP.

The Monitor profile grants the user read-only access to non-security-related parameters within the Module.

11.5 Maintenance

The internal components of the Module cannot be replaced on the field. In case of hardware malfunction or defect, the Crypto Officer shall:

- zeroize the unit if possible, and
- send the Module to the maintenance facility for repair via a trusted delivery courier.

11.6 Common Vulnerability and Exposures

There are no known CVEs with this module.

11.7 End of life

The Module is expected to last for the duration of the validation certificate. If the validation certificate has expired and no new validated firmware upgrade has been made available, the Module is considered void and must no longer be used. The Crypto Officer must arrange for disposal of the module hardware in accordance with regulation: DFARS 252.245-7005 Reporting, Reutilization, and Disposal.

https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS_252.245-7004

12. Mitigation of Attacks

The module does not claim mitigation of attacks.

Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
API	Application Programming Interface
APT	Adaptive Proportion Test
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CHT	Continuous Health Test
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CSTL	Cryptographic and Security Testing Laboratory
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
EC DH	Elliptic Curve Diffie-Hellman
ECC	Elliptic Curve Cryptography
ECC CDH	ECC Cofactor Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	Hash-Based Message Authentication Code
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KAS	Key-Agreement Scheme

Acronym	Meaning
KAT	Known Answer Test
MAC	Message Authentication Code
MIB	Management Information Base
MON	Monitor
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OE	Operational Environment
OP	Operator
OS	Operating System
PBKDF	Password Based Key Derivation Function
PCT	Pair-Wise Consistency Test
PKCS	Public Key Certificate / Cryptography Standard
POST	Pre-Operational Self-Test
PRF	Pseudorandom Function
PSP	Public Security Parameter
RBG	Random Bit Generator
RCT	Repetition Count Test
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SP	Security Policy or Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	Sensitive Security Parameter
TLS	Transport Layer Security

Document History

Version	Date	Author	Description
1.0	9 May 2023	Brent Hyde	Initial Draft
1.1	30 May 2023	James Ramage	First round of comments
1.2	31 May 2023	Brent Hyde	Addressing comments
1.3	1 Jun 2023	Brent Hyde	Ultra styles added. Self-tests updated based on source code
1.4	22 Jun 2023	James Ramage	Second round of comments
1.5	29 Jun 2023	Brent Hyde	Addressing comments
1.6	12 Jul 2023	Brent Hyde	Integrating feedback from Ultra
1.7	26 Jul 2023	Audy Louis-Jacques	Comments
1.8	31 Jul 2023	Brent Hyde	Addressing comments
1.9	25 Aug 2023	Brent Hyde	Added PBKDF and ECDSA, other minor tweaks
1.10	22 Sep 2023	Brent Hyde	Bypass testing updates. Adding bootloader integrity test and algorithms.
1.11	16 Nov 2023	Brent Hyde	Module photo added, control output interface removed, authentication changed to role-based, bootloader integrity finalized, processor names adjusted for consistency with ACVP, tamper seal placement defined, bypass testing finalized, end-of-life finalized, unused acronyms removed.
1.12	27 Nov 2023	Brent Hyde	ECDSA keys removed. Version numbers added. CAVP certs added.
1.13	6 Dec 2023	Brent Hyde	Authentication strength updated
1.14	20 Dec 2023	James Ramage	Entropy section completed, ECDH peer key removed.
1.15	22 Dec 2023	Brent Hyde	Addressing QA observations, physical security inspection reformatted as a table.