# Non-proprietary Security Policy

# Wavence Microwave radio cryptoModule

# Nokia XHAUL

9500 Microwave Packet Radio (MPR)

| | |
|---|---|
| Author | Nathalie Denizet |
| Owner | Nathalie Denizet |
| Organization | X-Haul Product Line |
| Approver | Michel Peruyero<br>Tom Loper |
| Document Type | Specification |
| Document ID | 3DB225000009DSZZA |
| Document Location | PDM |

Change History

| Version | Status | Date | Author | Owner | Reviewed by | Reviewed date | Approver | Approval date | Description of changes |
|---|---|---|---|---|---|---|---|---|---|
| 0.1 | Draft | 14-02-2018 | Nathalie Denizet | Nathalie Denizet | PCT | 15-02-2018 | Xavier Gaillard | 15-02-2018 | First Draft |
| 0.2 | Draft | 15-07-2019 | Nathalie Denizet | Nathalie Denizet | PCT | 17-07-2019 | Michel Peruyero | 15-02-2018 | Rework after first Workshop |
| 0.3 | Draft | 22-06-2020 | Nathalie Denizet | Nathalie Denizet | PCT | 22-06-2020 | Michel Peruyero | 22-02-2018 | Rework to align |
| 0.4 | Draft | 21-09-2021 | Nathalie Denizet | Nathalie Denizet | PMT | 21-07-2021 | Michel Peruyero | 21-07-2021 | Rework to align evolutions |
| 0.5 | Draft | 04-08-2021 | Nathalie Denizet | Nathalie Denizet | PMT | | | | Post testing review update<br>Version number update |
| 1.0 | Released | 18-12-2021 | Nathalie Denizet | Nathalie Denizet | PMT | 20-12-2021 | Fabien Mulot | 20-12-2021 | Final release |
| 2.0 | Released | 27-09-2022 | Nathalie Denizet | Nathalie Denizet | PMT | 27-09-2022 | Loper Tom | 28-09-2022 | Updated version for validation |
| 2.1 | Released | 29-11-2022 | Nathalie Denizet | Nathalie Denizet | PMT | 30-11-2022 | Loper Tom | 30-11-2022 | New Updated version for validation |
| 2.2 | Released | 04-01-2023 | Nathalie Denizet | Nathalie Denizet | PMT | 04-01-2023 | Loper Tom | 04-01-2023 | New Updated version for validation |
| 2.3 | Released | 18-01-2023 | Nathalie Denizet | Nathalie Denizet | PMT | 18-01-2023 | Loper Tom | 18-01-2023 | Updated listing of firmware components. |
| 2.4 | Released | 07-02-2023 | Nathalie Denizet | Nathalie Denizet | PMT | 08-02-2023 | Loper Tom | 31-01-2023 | Fixed missing image in Figure 9 and device part numbers. Update description of chassis. |

NOKIA

# Contents

# Index of figures



# Index of tables

# 1 Introduction

## 1.1 Overview

The Nokia Wavence product family includes a range of Microwave Packet Transport units (abbreviated as MPT in this document). These MPTs are integrated in the Nokia Network Services Platform to enable consistent operations across end-to-end packet microwave networks.

Another component of this overall system is the Wavence Microwave Service Switch (abbreviated as MSS in this document) which acts as a traffic aggregator, managing any kind of incoming traffic to be transported on any kind of microwave uplink.

The cryptographic module defined in this document is the MPT Wavence Microwave radio cryptoModule in version 1.0 by Nokia XHAUL (abbreviated as MPT-HLC in this document or referred to as cryptographic module). The cryptographic module is intended to establish an encrypted communication link over-the-air to another MPT-HLC. The encryption functionality is implemented in a dedicated FPGA as part of the cryptographic module.

On both sides, the MPT-HLC is connected to the MSS, which performs management functions of the cryptographic module. Both MSSs are connected to a key server providing keys for the over-the-air encryption. The communication between the MSS and the cryptographic module is protected by an IPsec channel (AES encryption and HMAC).

The cryptographic module is a MPT unit for long-haul applications and full-indoor configuration. To support long-distance, high-capacity, mission-critical applications, the cryptographic module comes in different configurations to offer flexibility, scalability, and reliability.

## 1.2 Identification

The cryptographic module consists of the following components:

| Type | Name | Version | Part Number | Additional Information |
|---|---|---|---|---|
| Hardware | MPT-HLC | 1.0 | See codes in Table 2 | N/A |
| Hardware | MPT-HLC Sub-Rack | 01 | 3EM22618AC | Chassis able to embed up to two MPT-HLC modules. |
| Hardware | MPT-HLC Sub-Rack Blank Filler Panel | 04 | 3EM22616AA | Blanking plate, used when only one MPT-HLC is inserted into the sub-rack. |
| Hardware | MPT-HLC Sub-Rack MA-Cover | 01 | 3DB76330AA | Installed at the rear of the MPT-HLC sub-rack to provide opacity. |
| Tamper-evident seals | Anti-Tampering Labels | N/A | 3DB76375AA | See Section 2.4 for details. |

| Type | Name | Version | Part Number | Additional Information |
|---|---|---|---|---|
| Firmware | BOMPT | V05.04.00 | N/A | Firmware used during the boot process. |
| Firmware | SWMPT | V25.02.41 | N/A | Firmware executed on the CPU for management services. |
| Firmware | FARPH | V06.05.07 | N/A | Firmware executed on the FPGA for traffic encryption/decryption. |
| Firmware | FM620 | V01.06.64 | N/A | Modem firmware. |
| Firmware | C2620 | V00.09.00 | N/A | Configuration file for the modem (configuration parameters). |
| Firmware | P2H24 | V00.04.05 | N/A | Configuration file for the modem (modem profiles). |
| Firmware | FLPAR | V01.00.12 | N/A | Configuration file for the radio shifters. |
| Firmware | HASH0 | V01.00.00 | N/A | Signed hash file listing the firmware components. |

*Table 1: Cryptographic module components*

The cryptographic module is very flexible and various frequency boards (analog boards) may be assembled in the MPT-HLC along with the digital boards defined below. The different product variants are all covered by this validation as they differ only in terms of excluded components. The firmware and hardware implementing the security functionality is therefore identical for all product variants listed in Table 2 below.

| Code | ICS | Designation | Frequency (GHz) | Transmitter Configuration | Receiver configuration |
|---|---|---|---|---|---|
| 3DB76123AA | 3 | TRANSCEIVER U4 GHz without DIVERSITY | 4U | Standard | Standard |
| 3DB76123BA | 3 | TRANSCEIVER U4 GHz with DIVERSITY | 4U | Standard | With Diversity |
| 3DB19060AA | 9 | MPT-HL 6L RT CUBIC STD | 6L | Standard | Standard |
| 3DB19060BA | 9 | MPT-HL 6L RT CUBIC SD | 6L | Standard | With Diversity |
| 3DB19060CA | 4 | TRANSCEIVER L6 GHz HP WITHOUT DIVERSITY | 6L | High Power | Standard |
| 3DB19060DA | 4 | TRANSCEIVER L6 GHz HP WITH DIVERSITY | 6L | High Power | With Diversity |
| 3DB19060EA | 1 | L6 MPT-HLC PLUS HIGH GAIN WITHOUT COMBIN | 6L | PLUS HIGH GAIN | Standard |
| 3DB19060FA | 1 | L6 MPT-HLC PLUS HIGH GAIN WITH COMBINER | 6L | PLUS HIGH GAIN | With Diversity |
| 3DB19060GA | 1 | L6 MPT-HLC PLUS STD WITHOUT COMBINER | 6L | PLUS Standard | Standard |
| 3DB19060HA | 1 | L6 MPT-HLC PLUS STD WITH COMBINER | 6L | PLUS Standard | With Diversity |
| 3DB76047AA | 9 | MPT-HL 6U RT CUBIC STD | 6U | Standard | Standard |
| 3DB76047BA | 9 | MPT-HL 6U RT CUBIC SD | 6U | Standard | With Diversity |
| 3DB76047CA | 4 | TRANSCEIVER U6 GHz HP WITHOUT DIVERSITY | 6U | High Power | Standard |
| 3DB76047DA | 4 | TRANSCEIVER U6 GHz HP WITH DIVERSITY | 6U | High Power | With Diversity |
| 3DB76047EA | 1 | U6 MPT-HLC PLUS HIGH GAIN WITHOUT COMBINER | 6U | PLUS HIGH GAIN | Standard |
| 3DB76047FA | 1 | U6 MPT-HLC PLUS HIGH GAIN WITH COMBINER | 6U | PLUS HIGH GAIN | With Diversity |
| 3DB76047GA | 1 | U6 MPT-HLC PLUS STD WITHOUT COMBINER | 6U | PLUS Standard | Standard |
| 3DB76047HA | 1 | U6 MPT-HLC PLUS STD WITH COMBINER | 6U | PLUS Standard | With Diversity |
| 3DB76048AA | 8 | MPT-HL 7Ghz RT CUBIC STD | 7 | Standard | Standard |
| 3DB76048BA | 8 | MPT-HL 7Ghz RT CUBIC SD | 7 | Standard | With Diversity |
| 3DB76048CA | 4 | TRANSCEIVER 7 GHz HP WITHOUT DIVERSITY | 7 | High Power | Standard |
| 3DB76048DA | 4 | TRANSCEIVER 7 GHz HP WITH DIVERSITY | 7 | High Power | With Diversity |
| 3DB76049AA | 8 | MPT-HL 8Ghz RT CUBIC STD | 8 | Standard | Standard |
| 3DB76049BA | 8 | MPT-HL 8Ghz RT CUBIC SD | 8 | Standard | With Diversity |
| 3DB76049CA | 4 | TRANSCEIVER 8 GHz HP WITHOUT DIVERSITY | 8 | High Power | Standard |
| 3DB76049DA | 4 | TRANSCEIVER 8 GHz HP WITH DIVERSITY | 8 | High Power | With Diversity |
| 3DB76078AA | 4 | TRANSCEIVER 10.5 GHz WITHOUT DIVERSITY | 10.5 | Standard | Standard |
| 3DB76078BA | 4 | TRANSCEIVER 10.5 GHz WITH DIVERSITY | 10.5 | Standard | With Diversity |
| 3DB76050AA | 4 | MPT-HL 11 GHz RT CUBIC STD | 11 | Standard | Standard |

| Code | ICS | Designation | Frequency (GHz) | Transmitter Configuration | Receiver configuration |
|---|---|---|---|---|---|
| 3DB76050BA | 4 | MPT-HL 11 GHz RT CUBIC SD | 11 | Standard | With Diversity |
| 3DB76050CB | 1 | MPT-HLC High Power XCVR 11 GHz | 11 | High Power | Standard |
| 3DB76050DB | 1 | MPT-HLC High Power XCVR 11 GHz (with Combiner) | 11 | High Power | With Diversity |
| 3DB76050GA | 1 | MPT-HLC Plus XCVR 11GHz | 11 | PLUS Standard | Standard |
| 3DB76050HA | 1 | MPT-HLC Plus XCVR 11GHz with Combiner | 11 | PLUS Standard | With Diversity |

*Table 2: Validated configurations of the cryptographic module*

The module's firmware components are delivered as part of a combined package for the MSS and the MPTs of the overall system. The package containing the certified module is V08.09.1N. Please note that only the components listed in Table 1 are part of the validated module.

Customers can confirm they are running a validated configuration of the MPT-HLC by checking the following information:

- Comparing the part number of the MPT-HLC product identified on a label glued to the mechanical cover of the cryptographic module. The PNs and their corresponding MPT-HLC variants listed in Table 2 are covered by this validation. Note that the PN is identified in Table 2 as "Code".
- Comparing the hash value of the MPT parts of the overall firmware package (as listed in the HASH0 firmware component file) that is shown in the WebCT user interface of the MSS with the reference value reported in this document. The correct SHA-256 hash value for the of the validated module is:

  MPT SWP SHA-2 Hash
  Hash: 88A4D379598B3A9D97A5DB0EB1D5B9E75469797DFECD543182430EC7D2AF1D76

  Alternatively, the versions of the individual firmware components (called "units"), which are reported in the WebCT user interface, can be compared with the versions reported in Table 1.

See Section 2.10 for further details.

## 1.3 Purpose

This document covers the secure operation of the cryptographic module (i.e. the MPT-HLC) including initialization, roles, and responsibilities of operating the product in a secure, FIPS 140-2 compliant manner.

## 1.4 Document Organization

This Security Policy document is one part of the FIPS 140-2 Submission Package. This document outlines the functionality provided by the module and gives high-level details on the means by which the module satisfies FIPS 140-2 requirements.

The various sections of this document map directly onto the sections of the FIPS 140-2 standard and describe how the module satisfies the requirements of that standard.

## 1.5 Document Terminology

| Term | Description |
|---|---|
| AES | Advanced Encryptions Standard |
| API | Application Programming Interface |
| CAVP | Cryptographic Algorithm Validation Program |
| CMVP | Cryptographic Module Validation Program |
| CSP | Critical Security Parameters |
| DRBG | Deterministic Random Bit Generator |
| FIPS | Federal Information Processing Standard |
| GUI | Graphical User Interface |
| KAT | Known Answer Test |
| MPT | Microwave Packet Transport |
| MSS | Microwave/Multi Service Switch |
| OTA | Over-the-air |
| POST | Power-On Self-Test |
| RSA | An algorithm for public-key cryptography. Named after Rivest, Shamir and Adleman who first publicly described it. |
| RNG | Random Number Generator |
| SHA | Secure Hash Algorithm |
| SP | Security Policy |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| WebCT | Web Craft Terminal |
| WKAT | Well Known Answer Test |
| XPIC | Cross Polarization Interference Cancellation |

*Table 3: Acronym table*

## 1.6 Document References

| Reference | Description |
|---|---|
| [FIPS 140-2] | FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 25, 2001, CHANGE NOTICES (12-03-2002). http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf |
| [FIPS 140-2 DTR] | Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, January 4, 2011 Draft. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/fips1402DTR.pdf |

| Reference | Description |
|---|---|
| [FIPS 140-2 IG] | NIST, Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, last updated November 5, 2021 |
| [FIPS 197] | FIPS PUB 197, Advanced Encryption Standard (AES), FIPS Publication 197, November 26, 2001. |
| [PKCS#1] | PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002 |
| [SP 800-90Ar1] | NIST Special Publication 800-90A Revision 1, Recommendation for the Random Number Generation Using Deterministic Random Bit Generators (Revised), June 2015 |
| [SP 800-90B] | NIST Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018 |
| [FIPS 180-4] | FIPS PUB 180-4, Secure Hash Standard, FIPS Publication 180-4, August 2015 |
| [SP 800-38A] | NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation (December 2001) |
| [FIPS 186-4] | FIPS PUB 186-4, Digital Signature Standard (DSS), FIPS Publication 186-4, July, 2013 |
| [FIPS 198-1] | FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC). July 2008 |
| [SP 800-107r1] | NIST Special Publication 800-107 Revision 1, Recommendation for Applications Using Approved Hash Algorithms, August 2012 |
| [SP 800-77r1] | NIST Special Publication 800-77 Revision 1, Guide to IPsec VPN, June 2020 |
| [RFC3602] | The AES-CBC Cipher Algorithm and Its Use with IPsec (sept 2003) |
| [RFC4301] | Security Architecture for the Internet (2005) Protocol (V2 implementation) |
| [SP 800-133r2] | NIST, Recommendation for Cryptographic Key Generation (June 2020) |

*Table 4: Reference document table*

# 2 Wavence Cryptographic Module

## 2.1 Cryptographic Module Specification

### 2.1.1 Cryptographic Boundary

The cryptographic module (MPT-HLC) is shown in Figure 1 and is a **multiple-chip embedded hardware** cryptographic module that is covered with a commercial-grade chassis that includes components equipped for physical security and assurance of opacity. It belongs to the cryptographic module in the sense of FIPS 140-2 and is located within the cryptographic boundary and contributes to the physical security of the module.

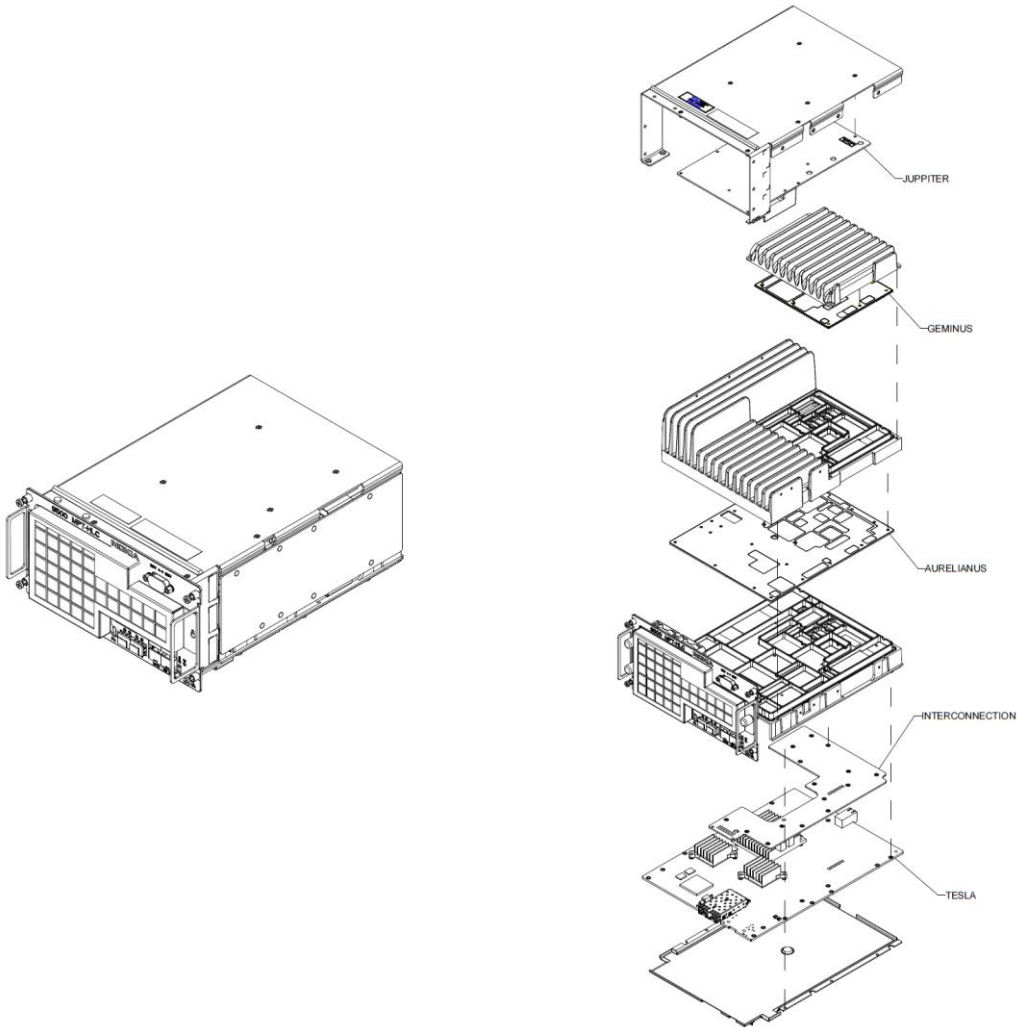


*Figure 1: MPT-HLC module: exploded view*

The MPT-HLC consists of the following components:

- One digital board named Tesla (frequency independent);

- One RF (Radio Frequency) board named Aurelianus for the main Transmitter and Receiver (frequency dependent);
- One RF board named Geminus for the diversity receiver (RxDiv) (frequency dependent and optional);
- One Interconnection board for connections between the digital and RF boards (frequency independent);
- One power supply board named Juppiter (frequency independent).

All boards composing the MPT-HLC are contained in a suitable sheet metal enclosure. RF boards are additionally protected by a die cast metallic enclosure.

The RF board Aurelianus, the RxDiv board Geminus and the power supply Juppiter are excluded components.

The cryptographic boundary is depicted in Figure 2 and includes the following items:

- the chassis (i.e. the sub-rack),
- a cover installed at the back of the chassis,
- one or two MPT-HLC modules contained in the chassis, and
- a blanking plate covering the empty slot of the chassis in case only one MPT-HLC is contained in the chassis.

The chassis physically hosts the transceivers (MPT-HLC modules) and provides from its rear side the RF connections. Also, a back-panel board is present on the rear side of the chassis. It hosts the connector for the HSB switch and makes some connections between the two transceivers in the chassis.

The following figures show the physical boundary in more detail.

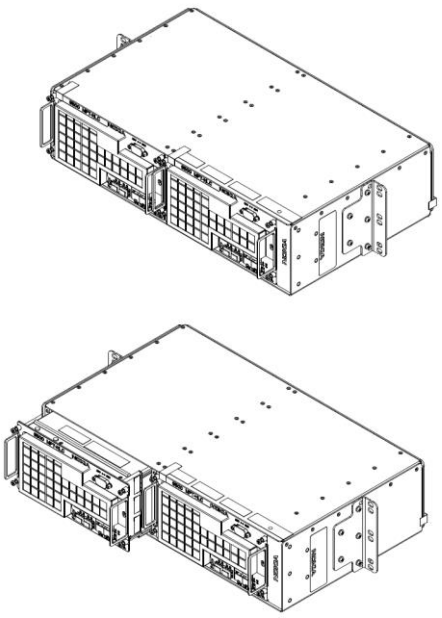

*Figure 2: Chassis with two MPT-HLC modules inserted*


*Figure 3: Front of the chassis with one MPT-HLC module inserted while the other slot is covered with a blanking plate*


*Figure 4: Front of the chassis with two MPT-HLC modules inserted*

*Figure 5: Rear view of the chassis*

### 2.1.2 Required External Component

The cryptographic module is intended to be operated as part of a Nokia Network Services Platform solution. This involves the usage of a MSS as an operator of the cryptographic module.

In order to operate the cryptographic module, different MSS configurations are available which are beyond this security policy.

The cryptographic module supports radio redundancy. Here, two MPT-HLC modules are inserted to the chassis while only one MPT-HLC module performs the cryptographic operations as specified in this document. The other MPT-HLC module acts as a transparent radio transceiver.

### 2.1.3 Mode of operation

The module only implements the approved mode of operation.

There are other firmware configurations available, however, only in case the firmware as identified in this document is running on the cryptographic module, the FIPS 140-2 requirements are satisfied.

### 2.1.4 Cryptographic Module Overview

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

| Section | Section title | Security level |
|---|---|---|
| 1 | Cryptographic Module Specification | 2 |
| 2 | Cryptographic Module Ports and Interfaces | 2 |
| 3 | Roles, Services, and Authentication | 2 |
| 4 | Finite State Model | 2 |
| 5 | Physical Security | 2 |
| 6 | Operational Environment | N/A |
| 7 | Cryptographic Key Management | 2 |
| 8 | EMI/EMC | 2 |
| 9 | Self-Tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | N/A |

*Table 5: Security Level Per FIPS 140-2 Section*

### 2.1.5 Cryptographic Algorithms

The following table provides details of the approved algorithms that are included within the module.

| Algorithm | CAVP certificate | Use | Notes |
|---|---|---|---|
| HMAC-SHA-512 | #A2009 | Within IPsec for management plane.<br>[FIPS 198-1] for HMAC and [FIPS 180-4] for SHA. (Key length is 512 bits) | Firmware implementation.<br>Note with reference to IG A.8: The module implements the HMAC-SHA-512 algorithm but truncates the output to 256 bits. |
| AES-256 CBC | #A2009 | Within IPsec for management plane<br>[FIPS 197] Advanced Encryption Standard algorithm<br>[SP 800-38A] for CBC mode<br>[RFC3602] for CBC in IPsec<br>The Module supports 256-bit key lengths CBC encrypt/decrypt modes. | Firmware implementation. |
| SHA-512 | #A2009 | - For SW/FW Integrity Test and SW/FW Load Test<br>- For Password storage<br>- For Database integrity check<br>- Conditioning component of the implemented ENT (NP)<br>[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms. The cryptographic module supports the SHA-2 (512-bit) | Firmware implementation. |
| RSA 4096 | #A2009 | - SW/FW Load Test (signature)<br>[FIPS 186-4] [PKCS#1] v1.5 and PSS RSA algorithms.<br>- Signature verification using 4096-bit keys. Note that RSA-PKCS#1 1.5 4096 verification and RSA-PKCS#1 PSS 4096 verification are available. RSA-PKCS#1 1.5 is present for legacy use only. | Firmware implementation. |
| AES-256 CTR | #A2009 | Payload encryption for data plane.<br>[FIPS 197] Advanced Encryption Standard algorithm. The Module supports 256-bit key lengths CTR encrypt/decrypt modes. | FPGA implementation. |
| CTR_DRBG | #A2009 | IPsec IV and key generation (management plane).<br>[SP 800-90Ar1] Deterministic Random Bits Generator (CTR_DRBG based on AES-256 with 256 bits of security strength, no derivation function is used) | Firmware implementation. |

| Algorithm | CAVP certificate | Use | Notes |
|---|---|---|---|
| CKG | Vendor affirmed | Generation of AES-256 and HMAC keys.<br>Please note that the implementation uses the 'direct generation' of symmetric keys specified in [SP 800-133r2].<br>With respect to Sec. 4 of [SP 800-133r2], the cryptographic module uses the output of the CTR_DRBG directly for key generation, i.e. no XOR is implemented. | Firmware implementation. |
| KTS | #A2009 | IPsec-based Key Transport Scheme using a combination of AES-256 in the CBC mode and HMAC-SHA-512 providing 256 bits of encryption strength:<br>KTS (AES Cert. #A2009 and HMAC Cert. #2009). | Firmware implementation. |
| ENT (NP) | N/A | [SP 800-90B]<br>Entropy source providing 512 bits of entropy. | Firmware implementation. |

*Table 6: Approved cryptographic algorithms*

Non-compliant but allowed algorithms with no security claim:

| Algorithm | Use |
|---|---|
| PBKDF | Used to derive a key from a string. This key is used to encrypt the IPsec keys for persistent storage with AES-256-CBC.<br>This implementation is not compliant with [SP 800-132].<br>From a security perspective, IPsec keys are stored in the cryptographic module in plaintext. |

*Table 7: Non-compliant but allowed cryptographic algorithms*

Non-FIPS approved algorithm not to be used in FIPS mode: **none.**

## 2.2 Cryptographic port and interface

The device can come with one or two MPT-HLC modules mounted. The description below refers to the case of having a single cryptographic module available.

The cryptographic module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the cryptographic module are mapped to four FIPS 140-2-defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following tables.

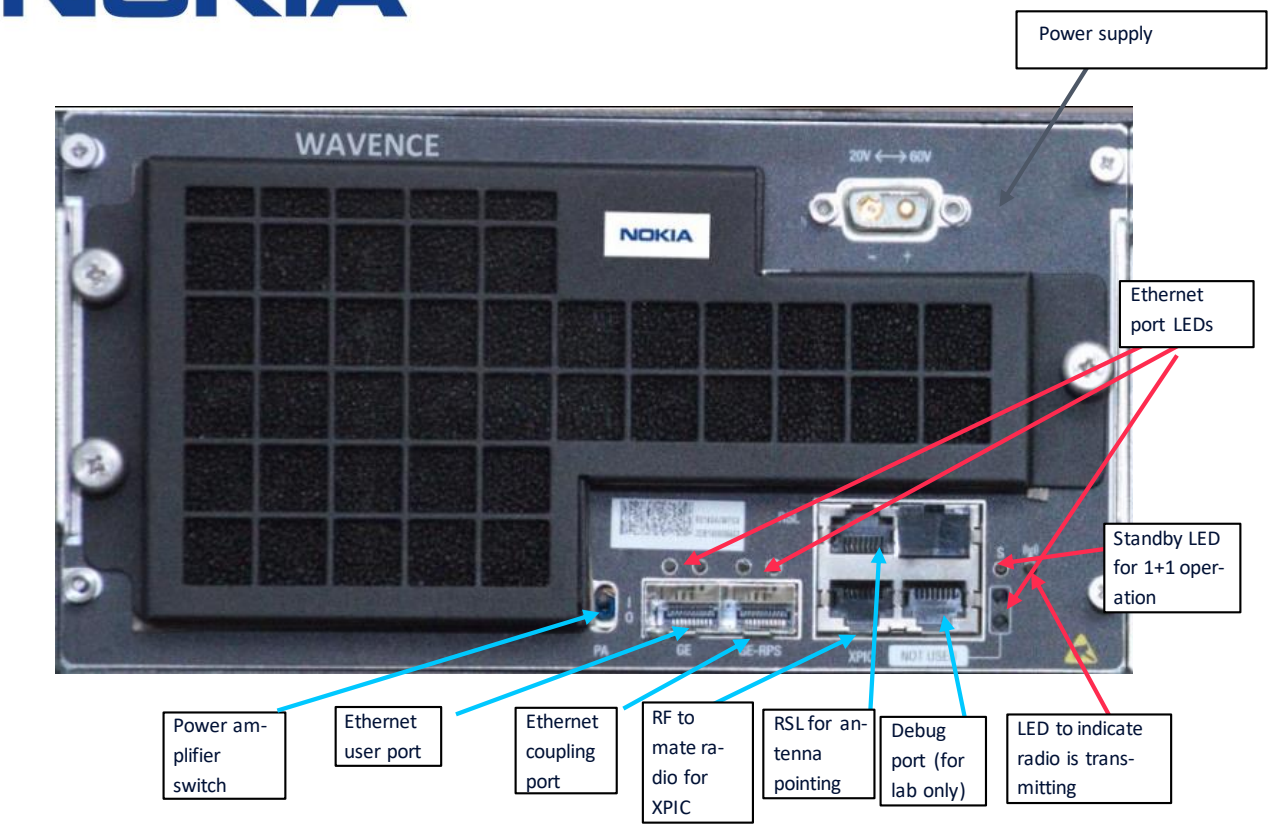


*Figure 6: MPT-HLC ports and interfaces on front plane*


*Figure 7: MPT-HLC ports and interfaces on Backplane*

| FIPS Interface | Physical Interface |
|---|---|
| Data Input | Ethernet user port<br>Ethernet coupling Port<br>RF port from Antenna (Rx)<br>RF port from Antenna (Rx-div)<br>RF port from mate XPIC RF port |
| Data Output | Ethernet user port<br>Ethernet coupling port<br>RF port to antenna (Tx) |

| FIPS Interface | Physical Interface |
|---|---|
| | RF port to mate XPIC RF port |
| Control Input | Ethernet user port<br>Debug port (for lab only) |
| Status Output | Ethernet user port<br>Ethernet port LEDs<br>Standby LED for 1+1 operation<br>LED to indicate radio is transmitting<br>RSL for antenna pointing |
| Power interface | Power amplifier switch<br>Power supply port |

*Table 8: Module interfaces*

## 2.3 Roles, Service and Authentication

The following sections provide details about the roles supported by the module, how they are authenticated, and which services they are authorized to access.

### 2.3.1 Authorized Roles

The encryption module supports two roles, the Crypto Officer and the User role. Some services are also available without authentication (see Table 11). Configuration of the module occurs over a single interface, to which a single entity can be connected in a point-to-point manner.

The module has two phases:

- The personalization phase (first commissioning), where a key generation request can be sent from a PC over Telnet using the “key_admin” user account. Logging into this account requires a role-based authentication. After successful authentication, the “key_admin” operator assumes the Crypto Office role.
- The operational phase, where module management is performed via the MSS, which acts as the operator. After a role-based authentication using IPsec, the MSS has the complete access to configure and manage the module and simultaneously assumes the following two roles:
  - The Crypto Officer role for all activities relative to the key during operational life of the product.
  - The User role to configure and manage the module and establish the remote peer secure connection.

After start-up and MSS authentication, it is the MSS’s responsibility to check the type and version of the cryptographic module.

Table 9 provides more information for the roles available in each of the two phases.

| Phase | Operator | Type of Authentication | Type of Authentication | Authentication Data |
|---|---|---|---|---|
| Personalization | key_admin | Crypto Officer | Role-based | Password (via Telnet) |
| Operational | MSS | Crypto Officer and User | Role-based | IPsec datagram with HMAC |

*Table 9: Roles and required identification and authentication*

### 2.3.2 Authentication mechanisms

The module supports role-based authentication in the personalization and the operational phase. Module operators must authenticate to the module before being allowed access to services, which require the assumption of an authorized role. The module employs the authentication methods described in the table below:

| Operator | Authentication Mechanism | Strength of Mechanism |
|---|---|---|
| MSS<br>(Crypto Officer and User role) | Keys | The IPsec keys are generated using the DRBG, which provides 256 bits of entropy (full entropy). A correct authentication relies on the HMAC key as well as on the usage of the correct encryption key.<br>Therefore, both need to match which leads to 2^(2*256) combinations for a single authentication attempt. The probability of a successful single random authentication attempt is one in 2^(2*256)=1.341E154 which is meeting the requirement (< 1 in 1,000,000).<br>For the probability of a successful authentication with random attempts in one minute, 6 attempts per minute are possible. Therefore, the probability of a successful authentication is 1-(1-1/(2^512))^6 which corresponds to one in 2.23463E153 which is meeting the requirement (less than one in 100,000). |
| key_admin<br>(Crypto Officer role) | Password | The password shall be changed during initialization.<br>The password length is 8 up to 25 characters (all alpha numerical upper/lower case sensitive w/o 'space'). Therefore, 26 lowercase characters +26 uppercase characters +10 digits +31 special characters are available for each character.<br>In case of a password length of 8 characters only, the probability of a successful single random authentication attempt is one in 93^8 = 5.595E15 which is meeting the requirement (< 1 in 1,000,000).<br>The probability of a successful authentication with random attempts in a one-minute period shall be less than 1 in 100,000. Here, the number of authentication attempts is limited to three in one minute. Therefore, the probability of a successful authentication is 1-(1-1/(93^8))^3 which corresponds to one in 1.865E15 which also meets the requirement (less than one in 100,000). |

*Table 10: Strengths of authentication mechanisms*

### 2.3.3 Services

The approved services that require operators to assume an authorized role (Crypto Officer or User) as well as unauthenticated services are listed in the table below. The cryptographic module does not implement non-approved services. Please note that the keys and Critical Security Parameters (CSPs) listed below use the following indicators to show the type of access performed by the respective service:

- **R (Read):** The CSP is read.
- **W (Write):** The CSP is established, generated, or modified.
- **Z (Zeroize):** The CSP is zeroized.

| Service | Operator | Role | Description | Input | Output | Key/CSP Access |
|---|---|---|---|---|---|---|
| Connect to key_admin | key_admin | Unauthenticated | Open a Telnet console to authenticate as key_admin and perform the key_admin services. Change the default password for the key_admin account at first connection or the default account | Commands: Open a Telnet console with telnet telnet-init<br>Then type : >Connect to key-admin + pwd | Prompt in the key_admin space | key_admin Pwd (R)<br><br>Or<br><br>key_admin Pwd (R/W) at first connection |
| Change key_admin password | key_admin | Crypto Officer | Change the password for the key_admin account after authentication | CLI Command: >Password Change | Command response: Success/fail | key_admin Pwd (R/W) |
| Logout from key_admin | key_admin | Crypto Officer | Exit from the key_admin CLI | CLI command: >Exit | None | None |
| Generate IPsec keys | key_admin | Crypto Officer | Generate IPsec keys (one for authentication and one for encryption) to use for IPsec | CLI Command: >ipseckey generate | The cryptographic module outputs the generated IPsec keys via the control output interface of the physical user Ethernet interface to the external Telnet client PC in plaintext. | IPsec AES key (W/R)<br><br>IPsec HMAC key (W/R)<br><br>DRBG entropy input (R)<br><br>DRBG key (R)<br><br>DRBG V (R) |
| Module restart | key_admin | Crypto Officer | Restart the module | CLI Shell command: >Restart Cold Restart of the module zeroizes the OTA encryption keys stored in the FPGA. | Restart of the module | OTA AES key A/B (Z)<br><br>DRBG entropy input (Z)<br><br>DRBG key (Z)<br><br>DRBG V (Z) |
| | MSS | User | Restart the module | Proprietary notification message via MSS Restart of the module zeroizes the OTA encryption keys | Restart of the module | Cold reset only: OTA AES key A/B (Z)<br><br>Warm and cold reset: |

| Service | Operator | Role | Description | Input | Output | Key/CSP Access |
|---|---|---|---|---|---|---|
| | | | | stored in the FPGA.<br>The MSS can call a cold reset or a warm reset. In case of a warm reset, the FPGA operation is not stopped and OTA AES keys are not zeroized. | | DRBG entropy input (Z)<br><br>DRBG key (Z)<br><br>DRBG V (Z) |
| Perform self-tests on demand | - | Unauthenticated | Used to initiate on demand self-tests via power-cycle. | Manual power cycle operation | Restart of the module | None |
| Equipment start | MSS | Unauthenticated | When the module starts, MSS needs to recover some information to properly start the module. | Proprietary Telemetry message via MSS | Command responses:<br>MPT type, firmware version, remote inventory,<br>Map version(protocol) | None |
| Get start-up self-test status | MSS | Unauthenticated | Provide the readiness of the module to go for authentication mode with self-test results. | Proprietary Telemetry message via MSS | Self-test results | None |
| Configure module | MSS | User | Configure the module, radio parameters, Ethernet parameters, alarm notifications as well as monitor the performance of the module. | Proprietary telecommand message via MSS | Commands response | IPsec AES key (R)<br><br>IPsec HMAC key (R) |
| Enable over-the-air payload encryption | MSS | Crypto Officer | Although only a Crypto Officer may configure a secure data link, they may enable and disable encryption. | Proprietary telecommand message via MSS | Commands response | IPsec AES key (R)<br><br>IPsec HMAC key (R) |
| Disable over-the-air payload encryption | MSS | Crypto Officer | Although only a Crypto Officer may configure a secure data link, they may enable and disable encryption. | Proprietary telecommand message via MSS | Commands response | IPsec AES key (R)<br><br>IPsec HMAC key (R)<br><br>OTA AES key A/B (Z) |
| Set over-the-air encryption keys | MSS | Crypto Officer | MSS is propagating keys to the module to use for the link encryption.<br>Afterwards, the keys can be used when the command “Switch over-the-air AES key” is received.<br>Keys are imported to the cryptographic module via an IPsec tunnel, | Proprietary telecommand message via MSS | Commands response | OTA AES key A/B (W) |

| Service | Operator | Role | Description | Input | Output | Key/CSP Access |
|---|---|---|---|---|---|---|
| | | | i.e. in an encrypted and authenticated manner. | | | |
| Switch over-the-air AES key | MSS | Crypto Officer | The MSS instructs the module to activate the newly set OTA encryption key used for over-the-air encryption. | Proprietary tel-ecommand message via MSS | Commands re-sponse | OTA AES key A/B (R) |
| Transmit/re-ceive data | MSS | User | Encrypt/Decrypt data (AES-CTR) passing through the module (FPGA). | Data | Encrypted/de-crypted data | OTA AES key A/B (R) |
| MSS identifi-cation using IPsec | MSS | Unauthenti-cated | Crypto Officer authenti-cated locally by the module. Crypto Officer authenticated permits the MSS to manage crypto services. Each request/command | IPsec datagram from MSS con-taining the au-thentication di-gest | Success/fail<br><br>IPsec secure tunnel set-up success or fail-ure | IPsec AES key (R)<br><br>IPsec HMAC key (R) |
| IPsec keys ze-roization | MSS | Crypto Officer | Delete the IPsec keys and key_admin Pwd CSPs from the module. | Proprietary tel-ecommand message via MSS | IPsec keys and key_admin password are removed from the crypto-graphic mod-ule. | IPsec AES key (Z)<br><br>IPsec HMAC key (Z)<br><br>key_admin Pwd (Z) |
| Change IPsec keys | MSS | Crypto Officer | Request the crypto-graphic module to gen-erate new IPsec keys and change them. MSS recovers these keys through the on-going IPsec tunnel. | Proprietary tel-ecommand message via MSS | Generate new IPsec keys, send them to MSS. Reboot and re-setup IPsec session with the new IPsec keys, Old Keys are zero-ized using ser-vice IPsec keys zeroization. | IPsec AES key (R/W/Z)<br><br>IPsec HMAC key (R/W/Z) |
| Firmware up-grade | MSS | User | Upgrade the firmware of the module. If the firmware loading is suc-cessful, loads the new firmware units into module and reboots the module to allow the new firmware to become operational. If the firmware upgrade fails, then the new firmware is not loaded to the module the | Proprietary tel-ecommand message via MSS | Success/Fail<br><br>The crypto-graphic module is running the new SwP if the proof of origin is passed.<br><br>No new SwP is downloaded to the crypto-graphic module if the proof of origin fails. | None |

| Service | Operator | Role | Description | Input | Output | Key/CSP Access |
|---|---|---|---|---|---|---|
| | | | module remains operational with the old firmware. | | Activation happens only on successful firmware download | |

*Table 11: Services authorized for roles and access rights within services*

Please note that the firmware update service results in a new version of the cryptographic module. The firmware update should only be performed with FIPS validated firmware images.

The cryptographic module implements the WKAT mechanism, which automatically checks if OTA keys are identical on both ends of the communication channel. This is implemented as a known-answer test. Both keys are synchronized by transmitting the generated WKAT ciphertext via the encryption line. In case of a mismatch, the MSS triggers the generation and establishment of a new set of keys. The WKAT mechanism is not considered a security service and the WKAT plaintext or ciphertext are not considered CSPs.

The cryptographic module does not support bypass functionality.

## 2.4 Physical Security

The module is entirely encased by a thick steel chassis (called sub-rack). The back of the chassis has vent holes to allow air to flow across components within the module to provide cooling and prevent overheating. Internally, it has a backplane into which up to two MPT-HLC modules may be inserted.

Figure 8 shows the chassis with two MPT-HLC modules inserted. In case the second MPT-HLC is missing, the corresponding slot in the chassis shall be covered by a blanking plate (part number: 3EM22616AA; see Figure 3).

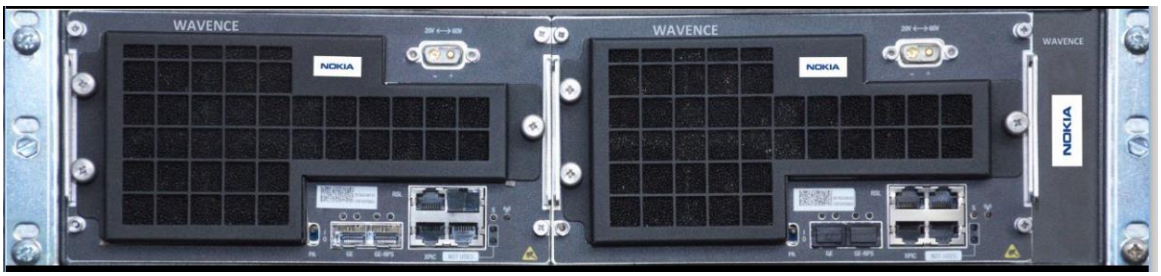


*Figure 8: Two MPT-HLC modules inserted into the chassis*

For the module to operate in the FIPS-approved mode of operation, a total of eight anti-tampering labels shall be applied to the MPT-HLC module(s), the MPT-HLC Sub-Rack MA-Cover, and, if applicable, the blanking plate, such that for each item that borders the chassis there is a label joining the item to the chassis. Figure 9 shows the placement of the four front-side labels depending on whether one or two MPT-HLC modules are inserted into the chassis. Two labels shall be used per inserted item. The four back-side labels shall be installed as shown in Figure 10. Before delivery to the customer, the ordered MPT-HLC module(s), the MPT-HLC Sub-Rack MA-Cover, and, if applicable, the blanking plate are mounted in the chassis at the factory and an initial set of anti-tampering labels is applied as specified above.

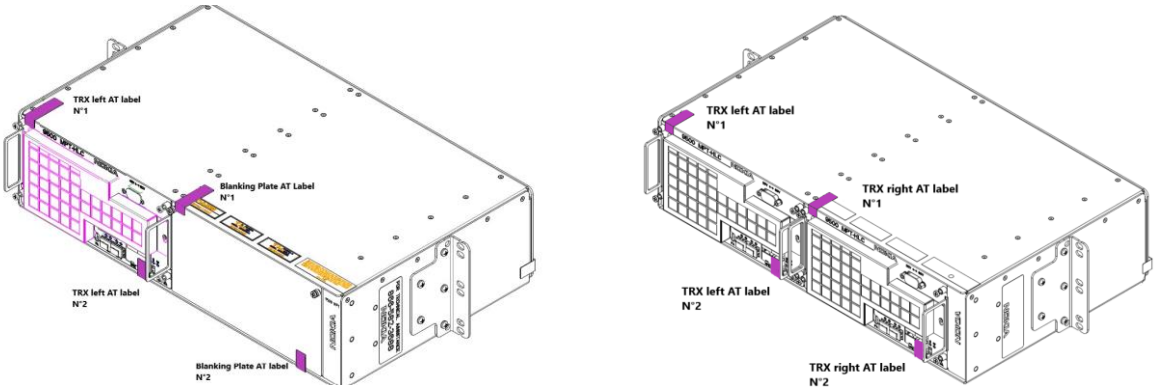


*Figure 9: Anti-tampering label placement at the front-side of the cryptographic module (left: one MPT-HLC module and blanking plate on empty slot; right: two MPT-HLC modules)*

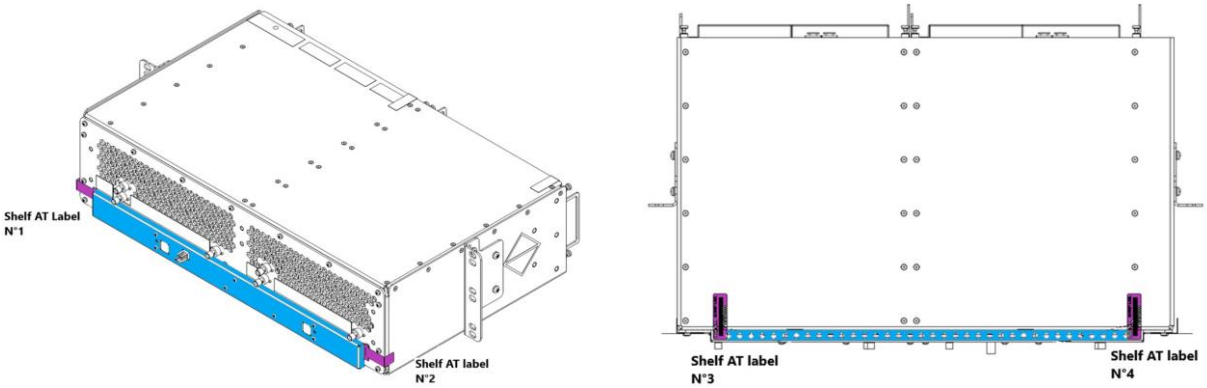


*Figure 10: Anti-tampering label placement at the back-side of the cryptographic module (top view and underside)*

The following graphics illustrate the tamper-evident labels. Figure 11 illustrates a tamper-evident label with no evidence of tampering.


*Figure 11: Tamper-evident label: intact*

Figure 12 illustrates a tamper-evident label that shows signs of tampering. Figure 13 is a magnified view of the broken label.


*Figure 12: Tamper-evident label: broken (normal view)*


*Figure 13: Tamper-evident label: broken (close-up view)*

**Anti-tampering labels**

Anti-tampering labels (part number: 3DB76375AA) are adhesive seals being destroyed in case of any attempt of removal.

Each label is serialized in a unique mode not permitting any unwanted replacement

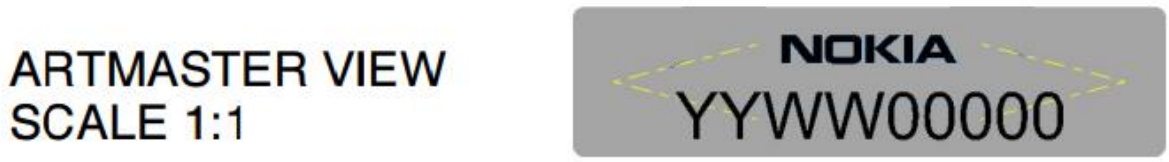


*Figure 14: Anti-tampering label design*

YY and WW are respectively the year and week of label production, while the five-digit numeric field gets a sequential value from 00001 to 99999. It resets at any year/week change.

**Apply Labels**

When applying Anti-Tamper labels, ensure that:

- The surface temperature to be sealed is at minimum +10°C
- The surface to be sealed is dry. Moisture of any kind can cause a problem. Wipe the area with a clean paper towel.
- Clean the surface with 100% isopropyl alcohol (*). Wipe the area with a cloth or paper towel alcohol dry with clean dry cloth or paper towel
- Wait 48 hours for the adhesive to cure

When an anti-tampering label must be removed:

- peel it out
- remove the label residuals cleaning the area with a cloth or paper towel soaked with 100% isopropyl alcohol (*)
- Note (*): Avoid using rubbing alcohol; it can leave an oily coating that will interfere with adhesion of the label.

**Inspect labels**

The Crypto Officer is also responsible for inspecting the anti-tampering labels on the shelves at least every three months. If any evidence of tampering is observed on the tamper-evident seals, the module shall be considered as being in a non-compliant state. Upon such discovery, the Admin shall decommission the module and return to the vendor.

**Opacity**

The chassis has vent holes at the back. In correspondence to the digital board, the vent holes are covered by a dedicated cover (part number: 3DB76330AA) that prevents line of sight view of any internal components (see Figure 15). The cover also makes the back-panel board inaccessible except for its HSB switch connector.

*Figure 15: Cover on the rear side of the chassis for opacity of the digital board and protection of the back panel board*

## 2.5 Operational Environment

Section 4.6.1 of the FIPS 140-2 standard is not applicable. The module is a hardware module with a limited modifiable operational environment embedded firmware.

## 2.6 Cryptographic Key Management

For an algorithm implementation to be listed on a cryptographic module validation certificate as an Approved security function, the algorithm implementation shall meet all the requirements of FIPS 140-2 and shall successfully complete the cryptographic algorithm validation process.

The following table identifies each of the CSPs associated with the cryptographic module. For each CSP, the following information is provided:

- The name of the CSP/Key
- The type of CSP and associated length
- A description of the CSP/Key
- Storage of the CSP/Key
- The zeroization for the CSP/Key

Please note that the public RSA keys used for the SW/FW integrity test are not considered as CSPs. The same applies to other keys used only for self-testing purposes and the keys derived using the non-compliant PBKDF implementation.

| Key/CSP | Size | Description | Storage | Generated/Entry/Output | Zeroization |
|---|---|---|---|---|---|
| DRBG entropy input | 384 bits | This is the entropy following [SP 800-90B] for the CTR-DRNG following [SP 800-90Ar1]. | RAM | **Generated** using entropy source validated per [SP 800-90B]. | Module restart |
| DRBG key | 256 bits | DRBG key for the CTR_DRBG as defined in [SP 800-90Ar1] for AES256. | RAM | **Generated** as part of the CTR_DRBG instantiation as specified in [SP 800-90Ar1] Sec. 12.2.1.3. | Module restart |
| DRBG V | 128 bits | Internal V value used as part of the DRBG following [SP 800-90Ar1]. | RAM | Instantiated/updated based on the DRBG's entropy input. | Module restart |
| IPsec HMAC key | 512 bits | HMAC-SHA 512. It authenticates the IPsec packet. | EEPROM | **Generated** at commissioning or at renewal request. | Zeroization service and overwritten after renewal |
| IPsec AES key | 256 bits | This is the CO configured key used to protect transmission of session keys. Algorithm used is AES-CBC. | EEPROM | **Generated** at commissioning or at renewal request. **Output** in plaintext as the response to the IPsec key generation process initiated by the key_admin operator. **Output** via the IPsec KTS as the response to the IPsec key generation process initiated by the MSS operator. | Zeroization service and overwritten after renewal |
| OTA AES key A/B | 256 bits | Key used to encrypt and decrypt data traffic. Algorithm used is AES-CTR. Two alternative keys A and B can be configured, but only one key is active. | Stored in write-only device registers in FPGA | **Imported** across encrypted IPsec link from MSS. | Module restart and "Disable over-the-air payload encryption" service. |
| key_admin Pwd | Password with 8 to 25 characters (see Sec. 2.3.2) | Password for key_admin authentication. | Flash | **Imported** across encrypted IPsec link from MSS. Never exits the module. | Zeroization service |

*Table 12: Cryptographic keys and CSPs*

As stated in Section 2.3.3, the WKAT plaintext for key synchronization between both ends of the OTA communication channel are not considered CSPs.

### 2.6.1 Random Number Generators

The module contains an approved SP 800-90Ar1 CTR_DRBG seeded by a non-physical entropy source ENT (NP) compliant to [SP 800-90B]. The entropy source provides an output of 512 bits containing full entropy. This entropy pool is used for seeding the CTR_DRBG.

### 2.6.2 Key Generation

The module generates symmetric keys for IPsec tunnel in compliance with requirements of FIPS 140-2 standard using output of the FIPS approved SP 800-90Ar1 DRBG. Please see Table 12 for details. The cryptographic module implements the direct generation of symmetric keys as specified in [SP 800-133r2].

### 2.6.3 Key Entry/Output

Please see Table 12 for details. All keys are entered into or output from the module in a secure manner. Besides the key input and output listed in Table 12, no key input or output is implemented.

The Cryptographic module receives the over-the-air AES keys in encrypted form via the IPsec channel established with the MSS. This corresponds to a key transport scheme with a security strength of 256 bits.

### 2.6.4 Zeroization procedure

Please see Table 12 for details.

IPsec keys as well as the key_admin password can be zeroized using the key zeroization service. This is a Crypto Officer service requiring Crypto Officer authentication.

Over-the-air AES keys as well as DRBG CSPs are zeroized by performing a power cycle.

The Over-the-air AES keys can be also zeroized using the “Disable over-the-air payload encryption” service.

## 2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

The module is classified as intentional radiators. It is conforming to FCC part 101.

## 2.8 Self-Tests

Self-tests are health checks that ensure that the cryptographic algorithms within the module are operating correctly. The self-tests identified in FIPS 140-2 fall within two categories:

1. Power-up Self-Tests
2. Conditional Self-Tests

### 2.8.1 Power-up Self-Tests

The cryptographic module performs known answer tests and critical functions tests at power up without any further user interaction. See table:

| Self-test performed in | Algorithm | Description |
|---|---|---|
| CPU (warm and cold reset) | DRBG | KATs of the instantiate, generate, and reseed functions. |
| | Repetition Count Test and Adaptive Proportion Test | As per [SP 800-90B] for 1024 samples. |
| | HMAC | KAT (512-bit key) |
| | AES-CBC | Encrypt and decrypt KAT (256-bit key) |
| | RSASSA-PKCSS1-v1.5<br>RSA-PSS | Signature verification KAT |
| | Firmware integrity test | RSA signature verification for firmware package proof of origin and integrity. |
| FPGA (cold reset only) | AES-CTR | Encrypt KAT (256-bit key) |

*Table 13: Power-up self-tests*

### 2.8.2 Conditional Self-test

The cryptographic module performs the following conditional self-tests:

| Test | Description |
|---|---|
| Firmware load test | Integrity and RSA signature verification.<br>Condition: Firmware loading |
| Repetition count test and adaptive proportion test from [SP 800-90B] | For FIPS approved noise source.<br>Condition: Continuous health testing of the noise source. |

*Table 14: Conditional self-tests*

As per IG 9.8, the CTR_DRBG and the ENT (NP) do not implement a continuous random-number generator test (CRNGT) as specified in AS.07.04 and AS.09.41 of the FIPS 140-2 standard.

### 2.8.3 Self-test error handling

If any of the identified POSTs (Power-On Self-Test) fail, the module will not enter an operational state and will instead provide an error message. The module will then be placed in an error state.

If the SW/FW Load Test fails, the new firmware is not loaded. In this case, the module does not enter an error state, it but goes back to operation.

If either of the RBG health test fails, the module raises an alarm to warn about the lack of randomness of the DRBG, an error message is provided and the module performs a power cycle, which includes full self-testing.

Please note that the cryptographic module implements a cold reset and a warm reset (see service Module restart in Section 2.3.3). In case of the cold reset, the complete module is reset (CPU and FPGA). In case of a warm reset, only the CPU-part is reset while the FPGA keeps running. Self-tests executed as part of a partial module restart resulting from a warm reset do not prevent FPGA output as the FPGA is considered to remain in a self-tested state. A warm reset also does not trigger a self-test of the FPGA. Both during execution of the self-tests (except in the aforementioned conditions) and while in an error state, data output is inhibited.

## 2.9 Design Assurance

Nokia employs industry standard best practices in the design & development, configuration Management, documentation, and delivery of the Wavence products, including the Encryption module.

Nokia has a TL 9000 Certified Quality Management System.

### 2.9.1 Design and Development

The design and development of the cryptographic module is based on the "Nokia MN CREATE" product Life Cycle (PLC).

The PLC consists of Phases separated by Program Milestones. A Program Milestone is the synchronization point between all stakeholders. At a Program Milestone, the results of the preceding phase and the conditions to proceed to the next phase are assessed, and the decision is made whether to approve successful completion of the preceding phase and to proceed to the next phase. A Program Milestone ensures alignment with business strategy and portfolio management process and requires management approval. Decision Reviews ensure visibility of product/project status across the corporation.

For each new product or solution development, a dedicated multi-competences team is created to manage the Program called a Program Management Team (PMT). The PMT is responsible for the proper implementation of the PLC.

### 2.9.2 Configuration Management

The purpose of Configuration Management (CM) is to establish and preserve the integrity of all work products throughout their life cycle.

Work products are uniquely identified, their version and status are maintained, changes to released work products are formally controlled, dependencies between work products are maintained, and problems are registered and traced to their solution.

The Configuration Management process identifies the items that form the configuration that will be developed for the project, baselines these items, and manages changes to the items.

This CM process is implemented in the Product Data Management database ("PDM").

Other dedicated tools are used to manage Requirements, Tests, fault Reports, Change requests.

### 2.9.3 Guidance documents

This encompasses all the manuals needed for the end users to install, commission, and operate the Wavence product family.

The inputs are provided by the persons in the development activities having the best knowledge of each subject to be addressed in the manuals. These inputs are provided to the Customer Documentation Team who inserts them in the user manuals in the most appropriate format and at the right place.

Reviews are performed to check and validate the evolutions before publishing.

For the Wavence radio secure mode, the guidance documents are made of:

- The standard set of Wavence user manuals, associated to the firmware package (see Section 1.2).
- The specific secure mode user manual. Guidance appropriate to an operator's role is provided with the module and provides all of the necessary assistance to enable the secure operation of the module by an operator, including the approved security functions of the module.

## 2.10 Delivery

The cryptographic module is protected with security labels as shown in Section 2.4 above. These labels shall be checked by the Crypto Officer before performing initialization tasks.

Additionally, to identify a validated product, users shall check the part number printed on a sticker glued to the enclosure. Besides that, the hash or the version information of the installed firmware units as part of the firmware package shall be checked. Please see Section 1.2 for details.

### 2.10.1 SW elements delivery.

The SW streaming strategy is organized around a single Mainstream, avoiding feature branches. This simple streaming strategy relies on the Continuous Integration (CI) chain to guaranty the Quality of the Mainstream.

The features development is iterative and incremental.

Each iteration allows moving forward on feature development adding new functionality on top of existing ones until the full feature is complete and delivered for the final tests.

Then, as part of the CI chain, Non-Regression Tests (NRT) are executed.

If no issues are observed, the SW is promoted to Release Candidate status with:

1. SW Package version and date of creation,
2. List of components and component versions making up the SW package delivery.

### 2.10.2 Product Release and SWP identification

The Secure mode is supported by the Product Release Wavence 20A (Commercial Naming).

A Revision number is used when maintenance versions are published. The first publication is Rev 01.

The SWP associated to the Product Release is identified by a SW Package version.

The list of the SW components in the SW package version with their identifications and versions is displayed in the Customer Release Note (CRN).

This list can be verified in the Cryptographic Module via the Craft Terminal.

There is a specific Wavence 20A secure mode SW package.

A µSD master image is then created and archived in the technical database (PDM) under a dedicated code.

### 2.10.3 Secure mode solution delivery

The Secure Mode SWP is loaded in the station via a µSD memory: The Secure Mode SWP µSD master image is retrieved by the factory from the PDM database.

Then the factory:

- Assembles the complete station in a rack, including the cryptographic module shelf and the Microwave Service Switch shelf fully equipped,
- Powers up the station. During this process, the secure mode SW is downloaded to the cryptographic module.
- Runs the station commissioning process.
- Runs the station tests.
- When all the station tests are done and OK, the MPT-HLC Sub-Rack MA-Cover is installed and all required anti-tampering labels are applied.

Delivery of the complete station, including the cryptographic module and some replacement anti-tampering labels, to customers from the vendor is done via third party forwarders.

Customers can order the following replacement kits:

| Name | Part number | Contents (see Table 1) |
|---|---|---|
| HLC sub-rack anti-tampering kit | 3DB76333AA | 1 MPT-HLC Sub-Rack MA-Cover (part number: 3DB76330AA)<br>8 Anti-Tampering Labels (part number: 3DB76375AA) |
| FIPS maintenance kit | 3DB19786AA | 1 MPT-HLC Sub-Rack Blank Filler Panel (part number: 3EM22616AA)<br>8 Anti-Tampering Labels (part number: 3DB76375AA) |

*Table 15: Replacement kits*

## 2.11 Mitigation of Other Attacks Policy

The module does not claim to mitigate any other attacks beyond those specified in FIPS 140-2.

# 3 Configuring the MPT-HLC for Secure Operation

The following steps are required to put the Module into a FIPS approved mode of operation.

## 3.1 Installation

The MPT-HLC is a subsystem belonging to the Wavence product. It cannot operate in a standalone manner in this configuration.

To run in FIPS mode of operation, MPT-HLC is delivered with a FIPS flag hard coded in the firmware version.

The MSS acting as the master sub-system shall drive the MPT-HLC into the FIPS mode operation.

MSS is also delivered to run in a secured mode of operation from factory.

The Crypto Officer must verify at installation that the MPT-HLCs tamper-evident seals have not been altered.

1) Connect MPT-HLC with PC in 192.168.100.XXX VLAN 4080 through RJ45 / optical converter to user access MPT-HLC 192.168.100.1
2) Power up the MPT-HLC
3) Open a Telnet console with following credential telnet telnet-init
4) Connect to key_admin shell with following command:
   - connect to key-admin
     then enter the default password: key_admin
5) After authentication with the default password, a new key_admin password shall be entered
6) To generate CSP keys type the following command:
   - ipseckey generate

     The cryptographic module then returns the Authentication Key and Encryption Key as shown in the following figure:

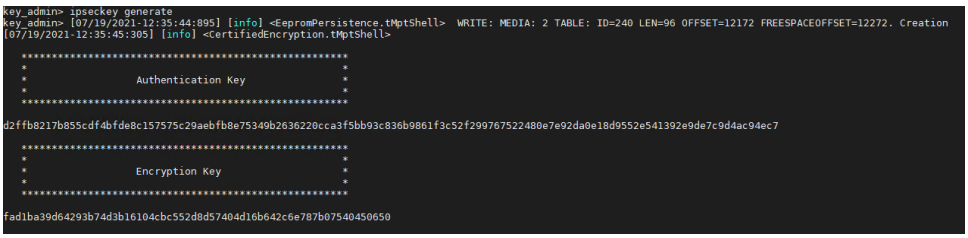


*Figure 16: Example of the returned data for the ipseckey generate command*

7) Copy/Paste the 2 lines of parameters
8) Type "**exit**" to exit the shell
9) Unplug the PC from MPT-HLC
10) Power the MSS

11) Login as administrator with WebCT to configure the MPT-HLC on the MSS. (see user's manual for details)
12) Login as Crypto Officer with WebCT (MPT-HLC already defined in MSS).
13) Configure the MPT-HLC IPsec parameters previously copied on WebCT MPT-HLC radio panel associated to the MPT-HLC
14) Connect the MPT-HLC to the MSS with the Ethernet cable as defined in the WebCT user's manual.
15) Power cycle the MPT-HLC

**Important**:

The Crypto Officer shall make sure the generated IPsec keys shown on screen shall be kept confidential. In addition, the Crypto Officer should make sure that key values do not remain in the PCs clipboard as keys are entered to the MSS using copy & paste.

## 3.2 Initialization

When MPT-HLC and MSS start the communication, the IPsec stack is initialized with the keys entered at commissioning (installation phase). MSS is authenticated into MPT-HLC automatically based on the IPsec authentication capability.

In case provisioning was not properly done, alarms are displayed to the operator.

The IPsec Keys can be updated using the WebCT configurator of MSS.

MPT-HLC will regenerate a new set of IPsec parameter that will be exchanged on the secure link.

Then the IPsec connection will be closed, key zeroized, and reinitialized with the new set of parameters.

The use of the MSS in "secure mode" locks out the use of non-approved algorithms on MPT-HLC and performs all the authentication needed for the MSS/MPT-HLC communication.

## 3.3 Initialization of encryption keys

Wavence uses Advanced Encryption Standard (AES)-256 keys to encrypt client traffic over the radio link. Encryption keys are zeroized by any of the following actions, resulting in a loss of traffic:

Zeroization of cryptographic keys is detailed in Table 11.
Disabling encryption for a radio direction. This action zeroizes the encryption key for the MPT-HLC.
Decommissioning the system. This action zeroizes all encryption keys on the system.
Restarting the system or the MPT-HLC sub system.