



Thales Alenia Space

Thales Alenia Space Cryptographic Module for Microsemi RTG4 FPGA

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General.....	6
1.1 Overview	6
1.2 Security Levels.....	6
1.3 Additional Information.....	7
2 Cryptographic Module Specification.....	8
2.1 Description	8
2.2 Tested and Vendor Affirmed Module Version and Identification	11
2.3 Excluded Components	12
2.4 Modes of Operation.....	12
2.5 Algorithms	12
2.6 Security Function Implementations.....	13
2.7 Algorithm Specific Information	13
2.8 RBG and Entropy	14
2.9 Key Generation	14
2.10 Key Establishment.....	14
2.11 Industry Protocols.....	14
3 Cryptographic Module Interfaces	15
3.1 Ports and Interfaces	15
4 Roles, Services, and Authentication.....	18
4.1 Authentication Methods.....	18
4.2 Roles.....	18
4.3 Approved Services.....	18
4.4 Non-Approved Services.....	21
4.5 External Software/Firmware Loaded	21
5 Software/Firmware Security	22
5.1 Integrity Techniques	22
5.2 Initiate on Demand	22
6 Operational Environment	23
6.1 Operational Environment Type and Requirements	23
7 Physical Security.....	24
8 Non-Invasive Security.....	25
9 Sensitive Security Parameters Management.....	26
9.1 Storage Areas	26

9.2 SSP Input-Output Methods	26
9.3 SSP Zeroization Methods	27
9.4 SSPs	28
10 Self-Tests	29
10.1 Pre-Operational Self-Tests	29
10.2 Conditional Self-Tests	29
10.3 Periodic Self-Test Information	29
10.4 Error States	30
10.5 Operator Initiation of Self-Tests	30
11 Life-Cycle Assurance	31
11.1 Installation, Initialization, and Startup Procedures	31
11.2 Administrator Guidance	31
11.3 Non-Administrator Guidance	31
11.4 Design and Rules	31
12 Mitigation of Other Attacks	33

List of Tables

Table 1: Security Levels.....	7
Table 2: Tested Module Identification – Hardware.....	11
Table 3: Modes List and Description.....	12
Table 4: Approved Algorithms.....	13
Table 5: Security Function Implementations.....	13
Table 6: Ports and Interfaces.....	17
Table 7: Roles.....	18
Table 8: Approved Services.....	20
Table 9: Storage Areas.....	26
Table 10: Keys storage in EEPROM memory.....	26
Table 11: SSP Input-Output Methods.....	27
Table 12: SSP Zeroization Methods.....	28
Table 13: SSP Table 1.....	28
Table 14: SSP Table 2.....	28
Table 15: Conditional Self-Tests.....	29
Table 16: Conditional Periodic Information.....	29
Table 17: Error States.....	30

List of Figures

Figure 1: Communication process between the GCP and the NEOS transponder.....	6
Figure 2: Block Diagram.....	10
Figure 3: TASE-CM-NEOS Hardware Cryptographic Module.....	11
Figure 4: Top view of the TASE-CM-NEOS.....	24
Figure 5: Bottom view of the TASE-CM-NEOS.....	24
Figure 6: Key Uploading Environment.....	27

CHANGES CONTROL

Version	Date	Remark
1.0	2025/03/28	Initial Version

1 General

1.1 Overview

The purpose of this document is to define the non-proprietary FIPS 140-3 Security Policy of the Thales Alenia Space Cryptographic Module for Microsemi RTG4 FPGA (Module Version 01.00.00) which will also be referred to as “TASE-CM-NEOS” throughout this document.

This Security Policy specifies the security rules under which the cryptographic module should operate to meet FIPS 140-3 Security Level 1 requirements.

This cryptographic module has been developed by Thales Alenia Space and it has been implemented within the Near-Earth Object Surveyor (NEOS) transponder unit. The aim of this cryptographic module is to enable NASA to encrypt communications at the GCP, and decrypt and authenticate them at the transponder unit using AES-GCM. It is able to encrypt/decrypt and authenticate messages from 128 bytes to 1024 bytes of information in 128-bit blocks.

Although the TASE-CM-NEOS can encrypt and decrypt indistinctly, in a real use case, the information will be encrypted in the GCP which will transmit it to the NEOS transponder where it will be decrypted and authenticated. The following image shows the communication process between the GCP and the NEOS transponder:

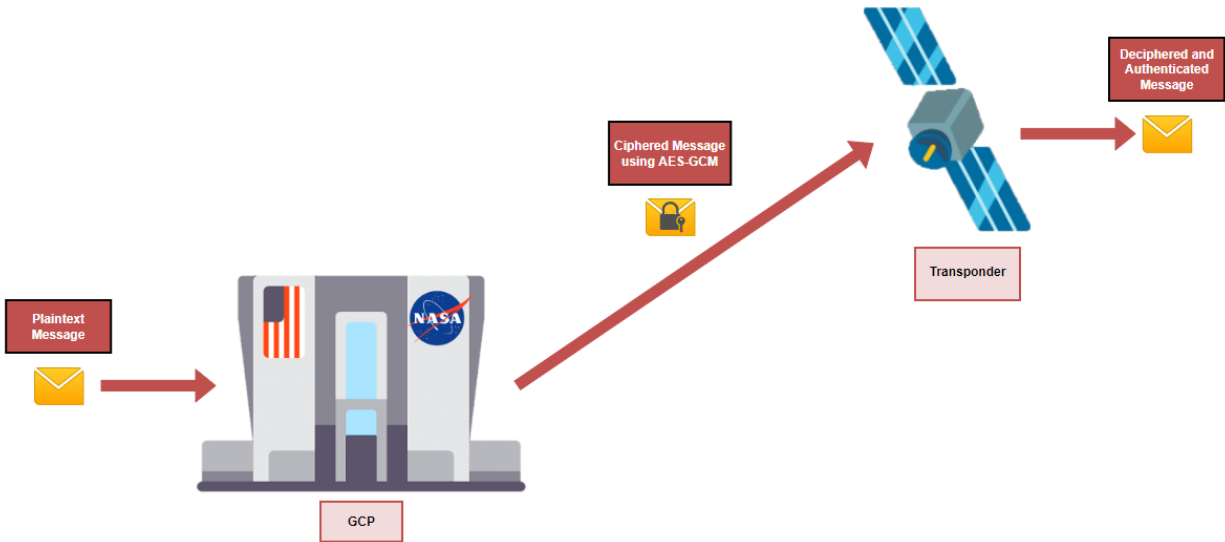


Figure 1: Communication process between the GCP and the NEOS transponder

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1

Section	Title	Security Level
5	Software/Firmware security	N/A
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

The module claims an overall Security Level of 1 with all individual sections at a Security Level 1. The module does not implement any non-invasive security mitigations or mitigations of other attacks and thus the requirements per these sections are not applicable.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The TASE-CM-NEOS is a hardware module based on a Microsemi RTG4 FPGA which implements two Helion IP cores for supporting AES-GCM encryption/decryption within the environment of the NEOS mission. This cryptographic module is classified by FIPS 140-3 as multiple-chip embedded.

In addition, the cryptographic module includes the telecommand (TC) and telemetry request (TMR) libraries necessary to control and monitor the cryptographic operations and communications between the GCP and the NEOS transponder.

Module Type: Hardware

Module Embodiment: MultiChipEmbed

Cryptographic Boundary:

The cryptographic boundary for TASE-CM-NEOS is composed of an FPGA which provides all the necessary to operate and interconnect the Helion IP cores (AES-GCM IP cores) to perform cryptographic operations, and the EEPROM memory to store all the AES-GCM keys and their CRCs.

The Microsemi RTG4 FPGA is composed of the following main elements:

- Two Helion IP cores for AES-GCM encryption/decryption and authentication.
- Other functional logic (green block) not related to the cryptographic operations, because its components functionality does not affect the security of the module.

Figure 2: Block Diagram depicts the cryptographic module block diagram specifying the cryptographic boundary for the TASE-CM-NEOS, showing all the input/output interfaces and the information flow described below:

- The plaintext is entered through the **data input** interface (**PDI**) into the TASE-CM-NEOS and it is ciphered by the Helion IP core before being output from the module through the **data output** interface (**CDO**).
- The ciphertext is entered into the TASE-CM-NEOS through the data input interfaces (**CDI**) and it is deciphered by the Helion IP core before being output from the module through the **data output** interface (**PDO**).
- All AES-GCM keys are entered into the TASE-CM-NEOS through the **data input** interface **KEYUART** by the Crypto Officer and, once the module calculates their CRCs and verifies that they match with the received CRCs through the same interface, both the keys and their CRCs are stored into the EEPROM memory.

- All the TCs and TMRs are entered into the TASE-CM-NEOS through the **control input** interfaces **HKUART** and **KEYUART**. Because for the encryption and decryption processes, the TCs associated with each operation (plaintext or ciphertext) are loaded through the **PDI** and **CDI** interfaces, these are also considered as **control input** interfaces. In addition, the cryptographic module implements a **Reset** pin used to perform the module reset operation, also considered as a **control input** interface.
- Because communication is established between the GCP and the NEOS transponder and ciphertext TCs are exchanged between both modules, the interface **CDO** is considered as **control output** interface.
- All the **status output** information related to the state of the cryptographic module is output from the TASE-CM-NEOS through the **HKUART** interface. The **status output** information related to the verification of each key CRC is output through the **KEYUART** interface. Moreover, the cryptographic module implements three **indicators** (Approved Service Indicator, Self-Test Indicator and Zeroization Indicator) to indicate the use of an approved security service, the successful completion of the self-test and zeroization services respectively, also considered as **status output**.
- Because the TASE-CM-NEOS requires power from the external power supply to the cryptographic boundary, it implements the **power input** interface.
- The frames are received through the **CDI interface** by the FPGA modulated, encoded and randomized by the RF system. The green block named "Other logic" is in charge of demodulating, decoding and derandomizing these input frames through the **ADC** interface to feed the cryptographic module through the **CDI logical** interface, which is used to enter the ciphertext to be deciphered into the TASE-CM-NEOS and consists of a data signal, a valid data signal and a frame completion signal that indicates when the complete frame has been finished. It is located into the same FPGA for power consumption purpose and all the functionality implemented by this block is operational with and without the cryptographic module. The information (green arrow) between this block and the UART I/F is because the **HKUART** interfaces allow configuring this block by using some TCs not related to the cryptographic operation of the module.

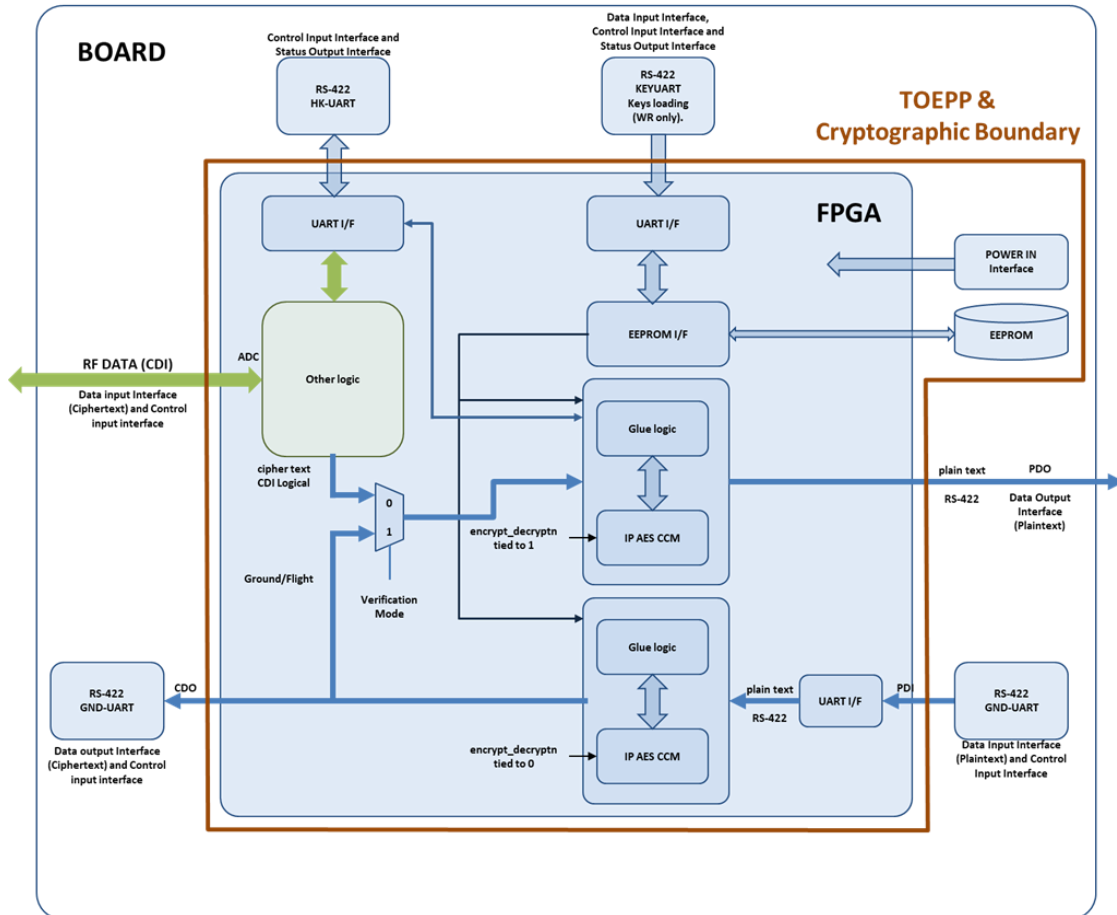


Figure 2: Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

The Tested Operational Environment's Physical Perimeter (TOEPP) is the combination of the FPGA and EEPROM memory.

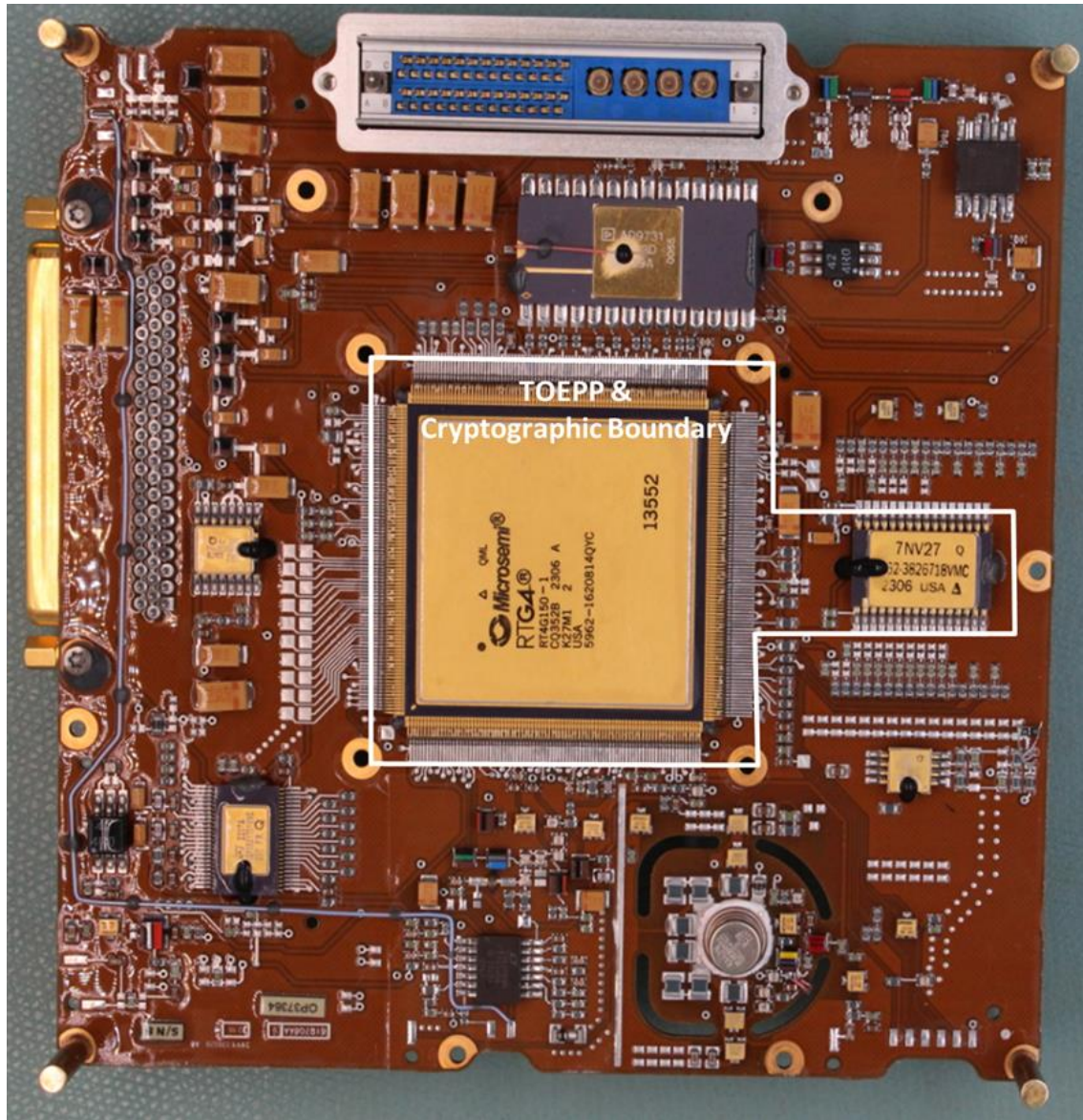


Figure 3: TASE-CM-NEOS Hardware Cryptographic Module

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
FPGA Microsemi RTG4-CQ352 & EEPROM 28C010T 1 Megabit (128K x 8-Bit)	01.00.00	N/A	N/A	N/A

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

No components have been excluded from the cryptographic boundary of the module.

2.4 Modes of Operation

Modes List and Description:

The table below details the Modes of Operation supported by the module.

Mode Name	Description	Type	Status Indicator
Approved Mode	The module can only operates in Approved mode. this mode, the cryptographic module receives the input plaintext/ciphertext which is processed by the IP core and the resultant ciphertext/plaintext is output from the module through the data output interfaces.	Approved	Approved Service Indicator (Pin 315)

Table 3: Modes List and Description

After passing all self-tests on start-up, the module automatically transitions to the Approved Mode.

Mode Change Instructions and Status:

The module implements only one mode of operation, the Approved Mode, in which the approved services are available. No configuration is necessary for the module to operate and remain in the Approved Mode.

Degraded Mode Description:

The module does not support a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

The table below lists all the Approved Algorithms supported by the module.

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A2809	Direction - Decrypt, Encrypt IV Generation - External Key Length - 256	SP 800-38D

Table 4: Approved Algorithms

The TASE-CM-NEOS is always operating in Approved mode; therefore, it does not support non-Approved mode nor degraded mode. In addition, it does not support non-Approved security functions nor vendor affirmed methods.

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

The table below lists the Security Function Implementations supported by the module.

Name	Type	Description	Properties	Algorithms
Authenticated Encryption	BC-Auth	Authenticated encryption of an entry plaintext		AES-GCM: (A2809)
Authenticated Decryption	BC-Auth	Authenticated decryption of an entry ciphertext		AES-GCM: (A2809)

Table 5: Security Function Implementations

2.7 Algorithm Specific Information

AES GCM

The cryptographic module properly manages the initialization vector of the AES-GCM according to the scenario 3 presented in FIPS 140-3 Implementation Guidance C.H H Key/IV Pair Uniqueness Requirements.

The cryptographic module uses a 96-bit external deterministic IV for the AES-GCM operations. The IV consists of:

- a 32-bit static field which contains a fixed value identifying the cryptographic module name. Therefore, the name construction allows for 2^{32} different names, fulfilling the requirement defined in FIPS 140-3 IG C.H.
- a 64-bit dynamic field containing a deterministic non-repetitive counter.

According to the [SP 800-38D] document, the maximum number of possible values for a given key of the deterministic non-repetitive counter is 2^{32} . When the counter part of the IV exhausts the maximum number of possible values for a given key, the cryptographic module will render this key unusable and will not accept any more frames with such key.

In case the module's power is lost and then restored, there will be a human operator who will reset the IV to the last one used.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

2.9 Key Generation

The TASE-CM-NEOS does not implement SSP generation algorithms.

2.10 Key Establishment

The TASE-CM-NEOS does not implement SSP establishment algorithms.

2.11 Industry Protocols

The TASE-CM-NEOS does not implement any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The table below details the module Ports and Interfaces.

Physical Port	Logical Interface(s)	Data That Passes
PDI: GNDUARTRX (PIN 272)	Data Input	This interface is used to enter the plaintext to be ciphered into the TASE-CM-NEOS.
CDI: ADCIN[0] (PIN 346), ADCIN[1] (PIN 347), ADCIN[2] (PIN 348), ADCIN[3] (PIN 349), ADCIN[4] (PIN 4), ADCIN[5] (PIN 5), ADCIN[6] (PIN 6), ADCIN[7] (PIN 7), ADCIN[8] (PIN 10), ADCIN[9] (PIN 11), ADCIN[10] (PIN 12), ADCIN[11] (PIN 13)	Data Input	This interface is used to receive the modulated, encoded and randomized input frame and is in charge of demodulating, decoding and derandomizing it to feed the cryptographic module through the CDI logical interface.
KEYUARTRX (pin 292)	Data Input	All AES-GCM keys to be used by the module in encryption/decryption operations are entered into the TASE-CM-NEOS through this interface.
CDO: GNDUARTTX (PIN 273)	Data Output	This interface is used to output the ciphertext from the TASE-CM-NEOS.
PDO: o_DATA_UPLINK (PIN 253), o_CLOCK_UPLINK (PIN254), TCENABLE (PIN 255)	Data Output	These interfaces are used to output the plaintext from the TASE-CM-NEOS.
PDI: GNDUARTRX (PIN 272)	Control Input	Besides of being used to enter the plaintext to be ciphered into the TASE-CM-NEOS, this interface is used to enter plaintext TMRs.
HKUARTRX (PIN 294)	Control Input	This interface is used to enter TCs and TMRs into the TASE-CM-NEOS.
CDI: ADCIN[0] (PIN 346), ADCIN[1] (PIN 347), ADCIN[2] (PIN 348), ADCIN[3] (PIN 349), ADCIN[4] (PIN 4), ADCIN[5] (PIN 5), ADCIN[6] (PIN 6), ADCIN[7] (PIN 7), ADCIN[8] (PIN 10), ADCIN[9] (PIN 11), ADCIN[10] (PIN 12), ADCIN[11] (PIN 13)	Control Input	This interface is used to receive the modulated, encoded and randomized input frame and is in charge of demodulating, decoding and derandomizing it to feed the cryptographic module through the CDI logical interface.
KEYCABLE[0] (PIN 298), KEYCABLE[1] (PIN 299), KEYCABLE[2] (PIN 300)	Control Input	If the harness is plugged (All these pins = 0) before turning on the TASE-CM-NEOS, the keys entry will start once the cryptographic module is turned on.
i_rst_async (PIN 305)	Control Input	This pin used to perform the module reset. The reset operation will not cause the AES-GCM counter to be

Physical Port	Logical Interface(s)	Data That Passes
		erased, so it can be performed without affecting the operation of the cryptographic module. During the operational lifetime of the module, it will be reset to perform self-tests on demand and to resume the normal operation after reaching error status.
CDO: GNDUARTTX (PIN 273)	Control Output	Besides of being used to output the ciphertext from the TASE-CM-NEOS, this interface is used to output the ciphertext TCs from the GCP to the NEOS transponder.
KEYUARTTX (PIN 293)	Status Output	The purpose of this interface is to output the TM related to the keys CRC checking during the key entry process.
HKUARTTX (PIN 297)	Status Output	This interface is used to output the TM related to the cryptographic error counter values and the status of the FSM.
o_selftest_indicator (PIN 311)	Status Output	This pin is used to indicate successful completion of the self-test service.
o_zeroization_indicator (PIN 312)	Status Output	This pin is used to indicate successful completion of the zeroization service.
o_service_indicator (PIN 315)	Status Output	This pin is used to indicate the execution of an approved security service.
VDD (PINS 14, 33, 51, 71, 86, 91, 105, 173, 179, 187, 199, 214, 215, 218, 237, 256, 276, 295, 313, 332 and 350)	Power	DC core supply voltage (1.2V)
VPP (PINS 28, 59, 96, 107, 164, 174, 201, 239, 290 and 327)	Power	Power supply for charge pumps (3.3V)
VDDI3 (PINS 258 and 267); VDDI4 (PINS 167, 181, 193, 206, 212, 224, 231, 244 and 250); VDDI5 (PINS 3, 8, 270, 282, 288, 301, 307, 319, 325, 338 and 344); VDDI6 (PINS 20, 26, 39, 45, 57, 64, 76, 82, 94 and 101)	Power	I/O Bank supplies
VDDPLL (PINS 1, 88, 89, 176, 177, 264, 265 and 352)	Power	Power for PLLs (3.3V)
VSS (PINS 2, 9, 15, 21, 27, 34, 40, 46, 52, 58, 65, 70, 77, 83, 87, 90, 95, 102, 106, 108, 111, 114, 117, 119, 122, 125, 129, 133, 136, 140, 144, 147, 150, 152, 155, 158, 161, 168, 175, 178, 180, 188, 194, 200, 207, 213, 219, 225, 232, 238, 245, 251, 257, 263, 266, 271, 277,	Power	Ground

Physical Port	Logical Interface(s)	Data That Passes
283, 289, 296, 302, 308, 314, 320, 326, 333, 339, 345 and 351)		
VDD_MONITOR (PIN 162); VSS_MONITOR (PIN 163)	Power	Internal power supply sense pins to monitor the device's VDD and VSS planes.
SERDES_PCIE_0_L01_VDDAPLL (PINS 109 and 130); SERDES_PCIE_0_L23_VDDAPLL (PINS 137 and 160)	Power	Analog power for SerDes lanes (2.5V).
SERDES_PCIE_0_L01_VDDAIO (PINS 110, 118 and 126); SERDES_PCIE_0_L23_VDDAIO (PINS 143, 151 and 159)	Power	TX/RX analog I/O voltage for SerDes lane (1.2V).
SERDES_VDDI (PINS 128 and 142)	Power	Power for SerDes reference clock receiver supply.
SERDES_VREF (PINS 127 and 141)	Power	External differential receiver reference voltage for SerDes Reference Clocks.

Table 6: Ports and Interfaces

When the module is performing self-tests or key zeroization processes, or is in an error state, all data output through the data output interfaces and all control output through the control output interface are inhibited. The inhibition of the data output and control output interfaces is performed in the source code by checking when the module enters in one of detailed states. In addition, the TASE-CM-NEOS does not require a maintenance interface because maintenance role is not supported.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

The module supports two roles that an operator may assume: Crypto Officer (CO) role and User role. Roles are assumed implicitly based on the service accessed. It is important to note that the cryptographic module does not allow concurrent operators to operate at the same time, as it is programmed to operate in sequential execution.

The table below lists the Roles supported by the module.

Name	Type	Operator Type	Authentication Methods
User	Role	User	None
Crypto Officer	Role	CO	None

Table 7: Roles

The TASE-CM-NEOS does not support maintenance role because it does not need logical or physical maintenance services. Moreover, the cryptographic module does not implement the bypass capability.

4.3 Approved Services

Once module installation has been performed successfully, each role (User and Crypto Officer) can use the services and keys detailed in the table below depending on its type of access by using a specified API TC/TMR.

The table below lists all Approved Services supported by the module. The abbreviations of the access rights to keys and SSPs have the following interpretation:

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.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Power-Up	Used to power-up the TASE-CM-NEOS. When the module is powered on, it operates automatically in Approved operation mode.	N/A	This service does not require any input.	This service does not provide any output.	None	User
Show Status	Used to obtain the current status of the TASE-CM-NEOS. The status of the module can be obtained through the HKUART interface as a response for the TMR "Show Crypto-Status".	Approved Service Indicator (Pin 315)	This service requires the TMR "Show Crypto-Status" as input.	This service outputs the status of the FSM and the four Crypto Counters values.	None	User
Show Module Versioning	Used to obtain the identifier and the current version of the TASE-CM-NEOS. The module version and identifier can be obtained through the HKUART interface as a response for the TMRs "Show Module Version" and "Show Module Identifier".	Approved Service Indicator (Pin 315)	This service requires the TMRs "Show Module Version" and "Show Module Identifier" as inputs.	This service outputs the module version and identifier.	None	User
Self-Test	Used to perform the self-test. The self-test is executed automatically when TASE-CM-NEOS is powered on. Therefore, it can be executed on demand by resetting or rebooting the cryptographic module.	Approved Service Indicator (Pin 315) and Self-Test Indicator (Pin 311)	This service does not require any input.	This service outputs the Self-Test Indicator (Pin 311).	None	User
Authenticated Encryption	Used to perform the authenticated encryption of an entry plaintext using AES-GCM with the desired AES 256-bit key.	Approved Service Indicator (Pin 315)	This service requires the key, IV and plaintext data as inputs.	This service outputs the ciphertext data.	Authenticated Encryption	User - AES_EDK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Authenticated Decryption	Used to perform the authenticated decryption of an entry ciphertext using AES-GCM with the desired AES 256-bit key.	Approved Service Indicator (Pin 315)	This service requires the key, IV and ciphertext as inputs.	This service outputs the plaintext data.	Authenticated Decryption	User - AES_EDK: E
Key Entry	Used to enter the AES keys into the TASE-CM-NEOS. To enter the keys into the cryptographic module, the CO must follow these steps: - Step 1: The CO must plug the harness for key uploading to the KEYUART interface. - Step 2: The CO must wait until the self-test and key zeroization processes are completed successfully. - Step 3: Once the TASE-CM-NEOS is in Key-Uploading state, the CO can enter up to 64 keys into the cryptographic module verifying that the load is successful using this command for each key: 1) TC "Load New Key"; 2) "TMR "Key-Status"	Approved Service Indicator (Pin 315)	This service requires the key and its CRC as inputs.	This service outputs the key ID, and key status.	None	Crypto Officer - AES_EDK: W
Key Zeroization	Used to zeroize the EEPROM memory pages where the AES keys are stored. The zeroization is performed automatically before the CO proceeds with the new keys loading as it is indicated in Section "9.3 SSP Zeroization Methods".	Approved Service Indicator (Pin 315) and Zeroization Indicator (Pin 312)	This service does not require any input.	This service outputs the Zeroization Indicator (Pin 312).	None	Crypto Officer - AES_EDK: Z

Table 8: Approved Services

Note: The approved indicator follows Scenario #2 Global Indicator for modules that have approved service only from Section “2.4.C Approved Security Service Indicator” of the [140IG] document. The service indicator is identifiable as a positive pulse on Pin 315.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

FIPS 140-3 Software/Firmware requirements are not applicable because the module satisfies the requirements identified in *FIPS 140-3 Implementation Guidance 5.A Non-Reconfigurable Memory Integrity Test*, and therefore the implementation can be considered hardware.

5.2 Initiate on Demand

As stated in the paragraph above, the module does not implement any software/firmware security test that can be initiated on-demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

The TASE-CM-NEOS is a multiple-chip embedded cryptographic module which encompasses an FPGA and an EEPROM memory used to store the AES-GCM keys and their CRCs. Its operational environment corresponds with the cryptographic module hardware and is classified as non-modifiable operational environment. Since the cryptographic module is an FPGA that sequentially executes a single process, there are no concurrent operators.

7 Physical Security

The TASE-CM-NEOS consists of production grade components protected by polymer conformal coating as a standard passivation technique and it is classified by FIPS 140-3 as a multiple-chip embedded cryptographic module.

Moreover, the physical security is enhanced because in the case of the module placed in the NEOS transponder there is no possibility of having physical access to it. Regarding the GCP module, it is placed in a secure room in NASA facilities and it is always used and managed under the supervision of the CO.



Figure 4: Top view of the TASE-CM-NEOS



Figure 5: Bottom view of the TASE-CM-NEOS

8 Non-Invasive Security

FIPS 140-3 Non-invasive Security requirements are not applicable because the TASE-CM-NEOS is not designed to implement non-invasive attack mitigation techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
EEPROM	Up to 64 keys are stored together with its CRC value using the Triple Modular Redundancy (TMR) methodology.	Static

Table 9: Storage Areas

Once the Crypto Officer has completed the key uploading process depicted above, the keys are stored in the EEPROM memory. Due to the inhospitable space conditions, the module has several methods to ensure the correctness of the stored keys.

On the one hand, each key is stored with its own CRC, which will be used before an authenticated encryption/decryption process to guarantee the key validity.

On the other hand, the key storage is performed using the Triple Modular Redundancy (TMR) methodology in order to protect the information against Single Event Effects (SEE) that can disrupt the keys and their CRC content. Therefore, the result is that each ID, key and CRC will be stored three times in one page of EEPROM memory.

ID	CRC	KEY	Redundancy 1			Redundancy 2		
0	CRC 0	Key 0	0	CRC 0	Key 0	0	CRC 0	Key 0
1	CRC 1	Key 1	1	CRC 1	Key 1	1	CRC 1	Key 1
2	CRC 2	Key 2	2	CRC 2	Key 2	2	CRC 2	Key 2
3	CRC 3	Key 3	3	CRC 3	Key 3	3	CRC 3	Key 3
.
.
.
63	CRC 63	Key 63	63	CRC 63	Key 63	63	CRC 63	Key 63

Table 10: Keys storage in EEPROM memory

When a key stored in the EEPROM is selected, the TASE-CM-NEOS applies majority voting system for each of its bytes using the three possible stored values. The CRC over this key is calculated and it is compared with the CRC stored in the EEPROM, applying again the majority voting system.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Key Uploading	External	EEPROM	Plaintext	Manual	Electronic	

Table 11: SSP Input-Output Methods

All keys used by the TASE-CM-NEOS to perform approved security functions (authenticated encryption and decryption operations) must be entered into the cryptographic module. The module is able to store up to 64 AES-GCM keys and their CRCs identifying them using a unique ID from 1 to 63 (plus one key with id 0 which is used for the self-test).

In order to perform the secure key entry, the CO is responsible of completing the following steps to comply with the FIPS 140-3 standard:

1. Firstly, the cryptographic keys are entered (via USB) into the PC (non-networked) used to load the keys into the module.
2. Secondly, the CO must plug the harness to the *KEYUART* interface prior to powering on the TASE-CM-NEOS.
3. Once the harness is connected, the CO must power on the cryptographic module.
4. After the cryptographic module is powered-up and the self-tests are passed completed successfully, the cryptographic module will detect that the harness is plugged and start with the key zeroization process.
5. When the key zeroization is completed, the key uploading process starts and the CO can upload up to 64 keys in total by using the scheme depicted in the image below and the following sequence of TC and TMR:
 - a. TC **“Load New Key”** à This TC is used to load the new key into the TASE-CM-NEOS.
 - b. Enter the new key generated externally in plaintext form via software using a PC.
 - c. TMR **“Key-Status”** à This TMR is used to check the CRC of the last uploaded key.

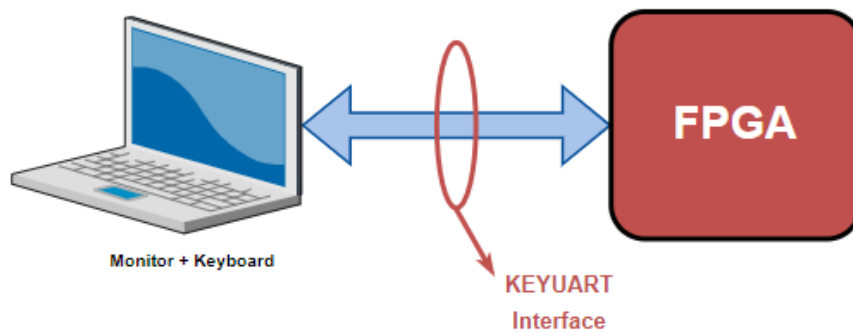


Figure 6: Key Uploading Environment

The upper limit is 64 keys, but the Crypto Officer can enter a lower number of keys into the TASE-CM-NEOS.

Regarding the SSPs output, the cryptographic module does not support SSP output operations, because it does not allow access to the keys from outside the cryptographic boundary.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
EPPROM Zeroization	Key and CRC are zeroized automatically prior the key uploading process.	The 64 memory pages where the AES-GCM keys (AES_EDK) and their CRCs are stored are zeroized.	By starting the key uploading process.

Table 12: SSP Zeroization Methods

The key zeroization process will be performed automatically prior the key uploading process as it is specified in above section. During this process, the TASE-CM-NEOS will only erase the 64 memory pages where the AES-GCM keys (AES_EDK) and their CRCs are stored because these are the only memory pages which contain keys and CSPs.

During the key zeroization process, all data output interfaces are inhibited in order to prevent inadvertent disclosure of sensitive information as the plaintext cryptographic keys or CSPs.

The cryptographic module indicates the successful completion of the zeroization process via the Zeroization Indicator (Pin 312).

9.4 SSPs

The following table summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES_EDK	AES-GCM key used for authenticated encryption and decryption.	256 bits - 256 bits	Symmetric Key - CSP	Other		Authenticated Encryption Authenticated Decryption

Table 13: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES_EDK	Key Uploading	EEPROM:Plaintext		EPPROM Zeroization	

Table 14: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

N/A for this module.

Since the cryptographic module does not implement firmware/software component, the bypass capability nor critical functions, it does not perform pre-operational self-tests. Therefore, the cryptographic module directly performs the conditional self-tests.

10.2 Conditional Self-Tests

The TASE-CM-NEOS is a hardware cryptographic module based on an FPGA and does not contain software or firmware components as specified in Section 5 Software/Firmware Security, so it is not necessary to implement the software/firmware loading test. In addition, the module does not generate cryptographic keys, does not allow the manual key entry, and does not implement bypass capability nor critical functions. Therefore, during the conditional self-test the TASE-CM-NEOS only performs the KAT (Known Answer Test) to verify the correct operation of the AES-GCM, performing the encryption/decryption and authentication of known information.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A2809) Encrypt	256-bit key	KAT	CAST	Self-Test Indicator (Pin 311)	Encrypt KAT	Module power-up
AES-GCM (A2809) Decrypt	256-bit key	KAT	CAST	Self-Test Indicator (Pin 311)	Decrypt KAT	Module power-up

Table 15: Conditional Self-Tests

The module will be in Operative state once the conditional self-test is passed successfully (status code of the module is set to 101) and if the harness for key uploading is not plugged. Until this moment, the outputs are inhibited to prevent inadvertent disclosure of the key components or CSPs, so the module cannot output any cryptographic data or perform cryptographic operations.

Moreover, if the conditional self-test fails, the module will reach the error state, not allowing to perform any cryptographic operation and keeping all data and control outputs inhibited. After an error, the cryptographic module resumes normal operation by means of a reset (Pin 305).

10.3 Periodic Self-Test Information

N/A for this module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A2809) Encrypt	KAT	CAST	On-Demand	Manually module rebooting
AES-GCM (A2809) Decrypt	KAT	CAST	On-Demand	Manually module rebooting

Table 16: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	The module's error state	CAST failure	Module reboot	Status Code = 111

Table 17: Error States

10.5 Operator Initiation of Self-Tests

The User can perform the on-demand conditional self-test by resetting the TASE-CM-NEOS.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Secure Distribution

The module is shipped only to NASA via certified courier service by Thales Alenia Space, and it is shipped in Thales boxes with Thales adhesive. Therefore, the recipient will be able to notice if it is tampered.

In addition, it is not possible to modify the module, notwithstanding, once the module is installed, it is possible to verify that the module identifier and version are correct as it is detailed in section "Installation and Initialization Instructions" below.

Integrity and Confidentiality Assurance

The integrity and confidentiality of the cryptographic module is assured by following the secure distribution methodology specified above and verifying the module version and identifier after following the steps to initialize the module in a secure manner as is specified in the section below.

Installation and Initialization Instructions

When NASA receives the cryptographic module, the Crypto Officer will be the one in charge of interconnecting and anchoring the support in the GCP and the NEOS transponder. Then, the module can be initiated in a secure manner by following the steps below:

1. **Step 1:** Once the TASE-CM-NEOS is installed and interconnected in a secure manner, it does not contain any AES-GCM key to operate. Therefore, the first step is to proceed with the key entry into the cryptographic module. The Crypto Officer, that is responsible for the CSPs and keeping them into the module, must follow the steps described in Section 9.2 SSP Input-Output Methods to insert up to 64 keys into the module and to store them into the EEPROM memory.
2. **Step 2:** After the keys are entered and stored into the cryptographic module, the Crypto Officer must power off the TASE-CM-NEOS and unplug the harness from the KEYUART port.
3. **Step 3:** Finally, it is necessary to verify the correct module version and identifier by using the TMRs "Show Module Version" and "Show Module Identifier", after powering on the module.

11.2 Administrator Guidance

When the module has been configured and the AES-GCM keys stored in a secure manner by the Crypto Officer, the TASE-CM-NEOS can be powered on to be used by or User role by using the TCs and TMRs and the procedures specified in 4.3 Approved Services.

11.3 Non-Administrator Guidance

Once the self-tests are passed successfully, the data encryption and decryption operations can be performed without additional security measures, because the module is always operating in Approved mode. In addition, the module does not return any private secret, key component or CSP through the output data interface.

11.4 Design and Rules

When the module is powered on, it is initialized to operate in Approved mode, which is its only mode of operation, complying with the following rules:

1. The cryptographic module is initialized in Approved mode of operation automatically after the self-test are completed successfully.
2. The replacement or modification of the module by unauthorized users is prohibited.
3. During the operational lifetime of the module, it will never be shut down.
4. The cryptographic module does not need to implement pre-operational self-test.
5. Conditional self-test does not require any operator action to be executed.
6. Data output interfaces are inhibited during the key entry, conditional self-test, zeroization and error states.
7. Any input interface will ignore any incomplete incoming TC or TMR.
8. Status information does not contain CSPs or sensitive data.
9. Zeroization affects the 64 EEPROM memory pages which contain the possible 64 keys to be stored.
10. The cryptographic module does not support the maintenance interfaces or role. Moreover, the cryptographic module does not implement bypass capability.
11. The cryptographic module does not implement authentication mechanisms because it is not required for Security Level 1.
12. The cryptographic module does not support manual key entry.
13. The keys are entered into the TASE-CM-NEOS in plaintext form via software.
14. The cryptographic module does not output CSPs, secret or private keys from the module.
15. According to the [SP 800-38D] document, the maximum number of invocations for each key is 2^{32} .
16. There will be a human operator who will reset the IV to the last one used in case the module's power is lost and then restored.
17. All keys are stored into an EEPROM memory with a unique identifier which allow the user to operate with them without having access to their content or value.
18. The Crypto Officer is the one in charge of performing the key zeroization and uploading of the new keys to be stored into the EEPROM memory.
19. If the TASE-CM-NEOS is in Error state, it will not be able to perform cryptographic operations. To resume normal operation mode, the cryptographic module must be reset.

12 Mitigation of Other Attacks

The TASE-CM-NEOS is not designed to mitigate other attacks which are outside of the scope of FIPS 140-3 standard.