
# Thales Alenia Space Cryptographic Module for Microsemi RTG4 FPGA

## Non-proprietary FIPS 140-3 Security Policy

**Thales Alenia Space**

Version: 1.7

## CHANGES CONTROL

| Version | Date | Remark |
|---|---|---|
| 1.0 | 2022/06/17 | Initial Version |
| 1.1 | 2022/07/01 | Stable Version |
| 1.2 | 2022/07/20 | Quality Review |
| 1.3 | 2022/07/26 | Consistency with changes in the FSM |
| 1.4 | 2022/08/02 | The version of the module has been corrected |
| 1.5 | 2022/11/28 | Changes included:<br>• The version of the module has been updated<br>• Added CAVP Certificate<br>• Table 5 has been corrected to be more consistent with the physical ports of the cryptographic module<br>• Table 6 has been corrected to be more consistent with the cryptographic module design<br>• Table 7 has been corrected to be more consistent with the approved service indicator design<br>• Section 9 has been updated to be more consistent with the cryptographic module design<br>• Quality review |
| 1.6 | 2023/09/14 | Changes included:<br>• Some terms have been corrected to comply with FIPS 140-3<br>• Section 8 has been updated to indicate that it is not applicable for the cryptographic module<br>• Section 13 has been removed and its contents have been redistributed in Section 11.3<br>• Some sections have been updated to comply with SP 800-140B<br>• Quality review |
| 1.7 | 2024/01/26 | Changes included:<br>• Note added under Table 7<br>• Updated information under Table 3 |

| | | |
|---|---|---|
| | | • Quality review |

# Table of contents

1 General ..... 6
1.1 Overview ..... 6
1.2 Document Organization ..... 7
2 Cryptographic Module Specification ..... 8
2.1 Module Description and Cryptographic Boundary ..... 8
2.2 Modes of Operation and Security Functions ..... 10
2.3 Critical Security Parameters ..... 11
3 Cryptographic Module Interfaces ..... 12
4 Roles, Services, and Authentication ..... 16
4.1 Roles ..... 16
4.2 Services ..... 16
4.3 Authentication ..... 19
5 Software/Firmware Security ..... 20
6 Operational Environment ..... 21
7 Physical Security ..... 22
8 Non-Invasive Security ..... 23
9 Sensitive Security Parameters Management ..... 24
9.1 Random Bit Generator ..... 25
9.2 Security Sensitive Parameter Generation ..... 25
9.3 Security Sensitive Parameter Establishment ..... 25
9.4 Security Sensitive Parameter Entry and Output ..... 25
9.5 Security Sensitive Parameter Storage ..... 26
9.6 Security Sensitive Parameter Zeroization ..... 27
10 Self-tests ..... 28
10.1 Pre-operational Self-test ..... 28
10.2 Conditional Self-test ..... 28
11 Life-Cycle Assurance ..... 29

11.1 Configuration Management ..... 29
11.2 Configuration Items Identification Method ..... 29
11.3 Crypto Officer and User Guidance ..... 29
11.3.1 Operation Rules ..... 29
11.3.2 Secure Distribution ..... 30
11.3.3 Integrity and Confidentiality Assurance ..... 30
11.3.4 Installation and Initialization Instructions ..... 30
11.3.5 Secure Operation ..... 31
12 Mitigation of other Attacks ..... 32
13 Acronyms ..... 33
14 Document Reference ..... 34

# 1 GENERAL

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 01.00.00 (Module Version 46.04.00) which will also be referred to as "TASE-CM-VIPER" 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.

## 1.1 OVERVIEW

This cryptographic module has been developed by Thales Alenia Space and it has been implemented within the Ground Cryptographic Processor (GCP) placed on Earth and within the Volatiles Investigating Polar Exploration Rover (VIPER) 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-VIPER is the same for the GCP and for the VIPER transponder and can encrypt and decrypt indistinctly, in a real use case, the information will be encrypted in the GCP which will transmit it to the VIPER transponder where it will be decrypted and authenticated. The following image shows the communication process between the GCP and the VIPER transponder:

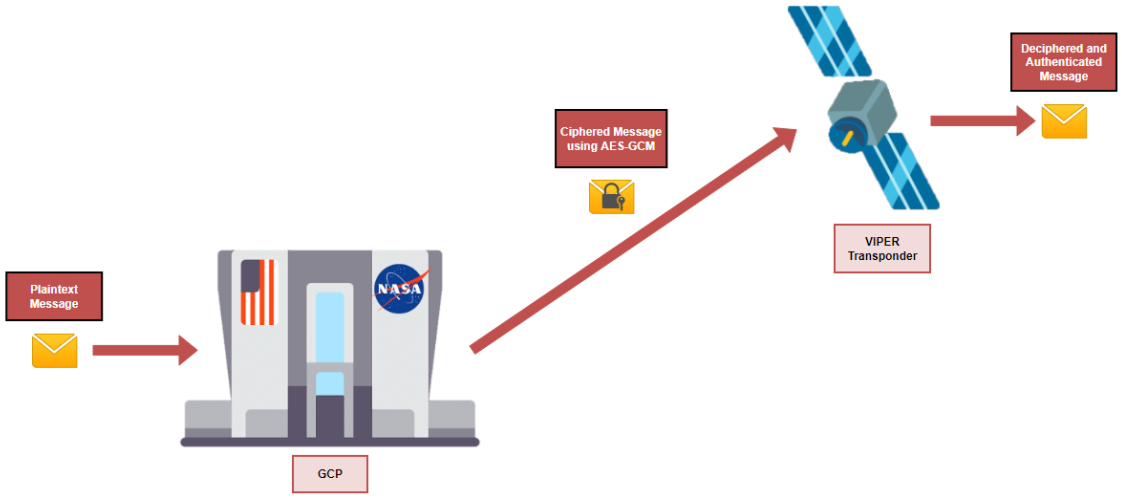


*Figure 1: Communication process between the GCP and the VIPER transponder*

The FIPS 140-3 security levels for the module are as follows:

| ISO/IEC 24759 Section 6. [Number Below] | FIPS 140-3 Section Title | Security Level |
|---|---|---|
| 1 | General | 1 |
| 2 | Cryptographic Module Specification | 1 |

| ISO/IEC 24759 Section 6. [Number Below] | FIPS 140-3 Section Title | Security Level |
|---|---|---|
| 3 | Cryptographic Module Interfaces | 1 |
| 4 | Roles, Services, and Authentication | 1 |
| 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*

## 1.2 DOCUMENT ORGANIZATION

This Security Policy is a part of the FIPS 140-3 submission package. The submission package contains:

- **FIPS 140-3 Security Policy:** this document.
- **FIPS 140-3 Algorithm Certificates:** see Section "2.2 Modes of Operation and Security Functions".
- **FIPS 140-3 Functional Specification and Design Documentation:** see Sections "2.1 Module Description and Cryptographic Boundary", "3 Cryptographic Module Interfaces" and **[TAS-FS]** document.
- **FIPS 140-3 User Guide:** see Section "11.3 Crypto Officer and User Guidance".
- **FIPS 140-3 Finite State Model:** see **[TAS-FSM]** document.
- **FIPS 140-3 Configuration Item List:** see **[TAS-CIL]** document.

# 2 CRYPTOGRAPHIC MODULE SPECIFICATION

The TASE-CM-VIPER 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 VIPER 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 VIPER transponder.

## 2.1 MODULE DESCRIPTION AND CRYPTOGRAPHIC BOUNDARY

The TASE-CM-VIPER 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 model of each component is specified in the table below:

| Model | Hardware | Firmware Version | Distinguishing Features |
|---|---|---|---|
| FPGA | Microsemi RTG4-CQ352 | N/A | N/A |
| IP core | Helion AES-GCM IP core | N/A | N/A |
| EEPROM | 28C010T 1 Megabit (128K x 8-Bit) | N/A | N/A |

*Table 2: Cryptographic Module Tested Configuration*

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. TASE-CM-VIPER Hardware Cryptographic Module*

***Figure 3: Cryptographic Boundary of TASE-CM-VIPER*** depicts the cryptographic module block diagram specifying the cryptographic boundary for the TASE-CM-VIPER, 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-VIPER 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-VIPER 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-VIPER 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-VIPER 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 VIPER 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-VIPER 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-VIPER 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-VIPER 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.

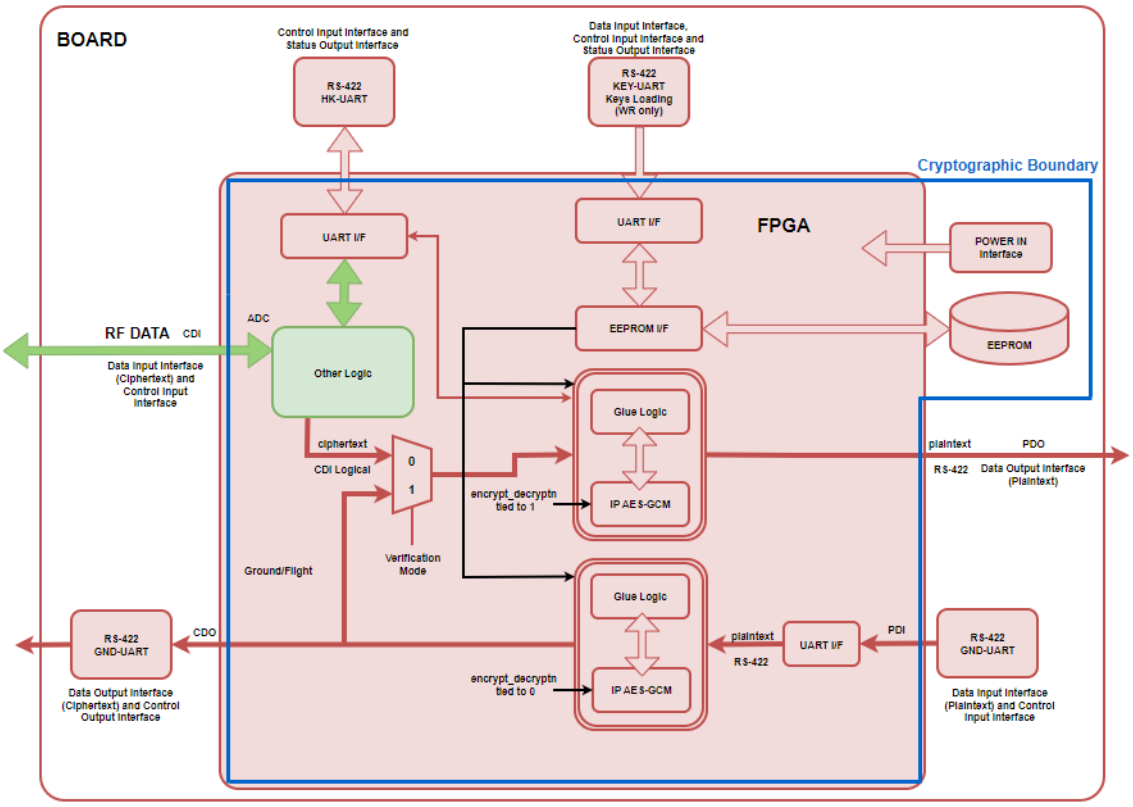


*Figure 3: Cryptographic Boundary of TASE-CM-VIPER*

## 2.2 MODES OF OPERATION AND SECURITY FUNCTIONS

The TASE-CM-VIPER can only operate in Approved mode. In 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.

Therefore, in this configuration, the cryptographic module supports the Approved security feature detailed in the table below:

| TASE-CM-VIPER Approved Algorithms | | | | |
|---|---|---|---|---|
| **CAVP Cert** | **Algorithm and Standard** | **Mode/Method** | **Description/Key Size(s)/ Strengths(s)** | **Use/Function** |
| **A2809** | AES [FIPS 197] | GCM [SP 800-38D] | 256 bits | Authenticated Encryption and Decryption |
| **A2809** | AES [FIPS 197] | ECB [SP 800-38A] | 256 bits | Encryption |

*Table 3: Approved Algorithms*

**Note:** AES-ECB is tested as the underlying algorithm for GCM. It is not independently invokable.

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 and 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.

The TASE-CM-VIPER 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.

## 2.3 CRITICAL SECURITY PARAMETERS

This section specifies the critical security parameter used by the TASE-CM-VIPER to be able to perform the security function detailed in section above.

| TASE-CM-VIPER Critical Security Parameters (CSPs) | |
|---|---|
| **CSPs** | **Description** |
| AES_EDK | AES 256-bit key used for AES-GCM authenticated symmetric encryption/decryption |

*Table 4: List of CSPs used by the module*

# 3 CRYPTOGRAPHIC MODULE INTERFACES

The following table summarizes the mapping between the logical interfaces required by FIPS 140-3 and the physical ports of the TASE-CM-VIPER:

| Logical Interface | Physical Port | | Data that passes over port/interface |
|---|---|---|---|
| Data Input | PDI | GNDUARTRX (PIN 272) | This interface is used to enter the plaintext to be ciphered into the TASE-CM-VIPER. |
| | CDI | ADCIN[0] (PIN 346)<br>ADCIN[1] (PIN 347)<br>ADCIN[2] (PIN 348)<br>ADCIN[3] (PIN 349)<br>ADCIN[4] (PIN 4)<br>ADCIN[5] (PIN 5)<br>ADCIN[6] (PIN 6)<br>ADCIN[7] (PIN 7)<br>ADCIN[8] (PIN 10)<br>ADCIN[9] (PIN 11)<br>ADCIN[10] (PIN 12)<br>ADCIN[11] (PIN 13) | 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) | | All AES-GCM keys to be used by the module in encryption/decryption operations are entered into the TASE-CM-VIPER through this interface. |
| Data Output | CDO | GNDUARTTX (PIN 273) | This interface is used to output the ciphertext from the TASE-CM-VIPER. |
| | PDO | o_DATA_UPLINK (PIN 253)<br>o_CLOCK_UPLINK (PIN 254)<br>TCENABLE (PIN 255) | These interfaces are used to output the plaintext from the TASE-CM-VIPER. |
| Control Input | PDI | GNDUARTRX (PIN 272) | Besides of being used to enter the plaintext to be ciphered into the TASE-CM-VIPER, this interface is used to enter plaintext TMRs. |
| | HKUARTRX (PIN 294) | | This interface is used to enter TCs and TMRs into the TASE-CM-VIPER. |
| | CDI | ADCIN[0] (PIN 346)<br>ADCIN[1] (PIN 347)<br>ADCIN[2] (PIN 348)<br>ADCIN[3] (PIN 349)<br>ADCIN[4] (PIN 4)<br>ADCIN[5] (PIN 5)<br>ADCIN[6] (PIN 6)<br>ADCIN[7] (PIN 7)<br>ADCIN[8] (PIN 10)<br>ADCIN[9] (PIN 11) | 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. |

| Logical Interface | Physical Port | | Data that passes over port/interface |
|---|---|---|---|
| | | ADCIN[10] (PIN 12)<br>ADCIN[11] (PIN 13) | |
| | KEYCABLE[0] (PIN 298)<br>KEYCABLE[1] (PIN 299)<br>KEYCABLE[2] (PIN 300) | | If the harness is plugged (All these pins = 0) before turning on the TASE-CM-VIPER, the keys entry will start once the cryptographic module is turned on. |
| | i_rst_async (PIN 305) | | This pin used to perform the module reset. The reset operation will not cause the AES-GCM counter to be erased, so it can be performed without affecting the operation of the cryptographic module.<br>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. |
| **Control Output** | CDO | GNDUARTTX (PIN 273) | Besides of being used to output the ciphertext from the TASE-CM-VIPER, this interface is used to output the ciphertext TCs from the GCP to the VIPER transponder. |
| **Status Output** | KEYUARTTX (PIN 293) | | The purpose of this interface is to output the TM related to the keys CRC checking during the key entry process. |
| | HKUARTTX (PIN 297) | | This interface is used to output the TM related to the cryptographic error counter values and the status of the FSM. |
| | o_service_indicator (PIN 315) | | This pin is used to indicate the execution of an approved security service (those listed in ***Table 7: TASE-CM-VIPER Approved Services***). |
| | o_selftest_indicator (PIN 311) | | This pin is used to indicate successful completion of the self-test service. |
| | o_zeroization_indicator (PIN 312) | | This pin is used to indicate successful completion of the zeroization service. |
| **Power Input** | VDD<br>(PINS 14, 33, 51, 71, 86, 91, 105, 173, 179, 187, 199, 214, 215, 218, 237, 256, 276, 295, 313, 332 and 350) | | DC core supply voltage (1.2V) |
| | VPP<br>(PINS 28, 59, 96, 107, 164, 174, 201, 239, 290 and 327) | | Power supply for charge pumps (3.3V) |
| | VDDI3<br>(PINS 258 and 267) | | I/O Bank supplies |

| Logical Interface | Physical Port | Data that passes over port/interface |
|---|---|---|
| | 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) | |
| | VDDPLL (PINS 1, 88, 89, 176, 177, 264, 265 and 352) | 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, 283, 289, 296, 302, 308, 314, 320, 326, 333, 339, 345 and 351) | Ground |
| | VDD_MONITOR (PIN 162) | Internal power supply sense pins to monitor the device's VDD and VSS planes |
| | VSS_MONITOR (PIN 163) | |
| | SERDES_PCIE_0_L01_VDDAPLL (PINS 109 and 130) | Analog power for SerDes lanes (2.5V) |
| | SERDES_PCIE_0_L23_VDDAPLL (PINS 137 and 160) | |
| | SERDES_PCIE_0_L01_VDDAIO (PINS 110, 118 and 126) | TX/RX analog I/O voltage for SerDes lane (1.2V) |
| | SERDES_PCIE_0_L23_VDDAIO (PINS 143, 151 and 159) | |
| | SERDES_VDDI (PINS 128 and 142) | Power for SerDes reference clock receiver supply |
| | SERDES_VREF (PINS 127 and 141) | External differential receiver reference voltage for SerDes Reference Clocks |

*Table 5: TASE-CM-VIPER 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-VIPER does not require a maintenance interface because maintenance role is not supported.

# 4 ROLES, SERVICES, AND AUTHENTICATION

## 4.1 ROLES

The TASE-CM-VIPER supports the roles of User and Crypto Officer. 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.

| Role | Service | Input | Output |
|---|---|---|---|
| User | Power-up | This service does not require any input. | This service does not provide any output. |
| User | Show Status | This service requires the TMR ***"Show Crypto-Status"*** as input. | This service outputs the status of the FSM and the four Crypto Counters values. |
| User | Show Module Versioning | This service requires the TMRs ***"Show Module Version"*** and ***"Show Module Identifier"*** as inputs. | This service outputs the module version and identifier. |
| User | Self-test | This service does not require any input. | This service outputs the Self-Test Indicator (Pin 311). |
| User | Encrypt | This service requires the key, IV and plaintext data as inputs. | This service outputs the ciphertext data. |
| User | Decrypt | This service requires the key, IV and ciphertext as inputs. | This service outputs the plaintext data. |
| Crypto Officer | Key Entry | This service requires the key and its CRC as inputs. | This service outputs the key ID, and key status. |
| Crypto Officer | Key Zeroization | This service does not require any input. | This service outputs the Zeroization Indicator (Pin 312). |

*Table 6: Roles, Service Commands, Input and Output*

The TASE-CM-VIPER 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.

## 4.2 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 access types to keys are denoted as follows:

- **G = Generate:** The module generates or derives the SSP.

- **R = Read:** The SSP is read from the module.
- **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 = Zeroise:** The module zeroizes the SSP.

| Service | Description | Approved Security Functions | Keys and/or SSPs | Role | Access Rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| Power-up | Used to power-up the TASE-CM-VIPER. When the module is powered on, it operates automatically in Approved operation mode. | N/A | N/A | User | N/A | N/A |
| Show Status | Used to obtain the current status of the TASE-CM-VIPER. The status of the module can be obtained through the *HKUART* interface as a response for the TMR "***Show Crypto-Status"***. | N/A | N/A | User | N/A | Approved Service Indicator (Pin 315) |
| Show Module Versioning | Used to obtain the identifier and the current version of the TASE-CM-VIPER. 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"***. | N/A | N/A | User | N/A | Approved Service Indicator (Pin 315) |
| Self-Test | Used to perform the self-test. The self-test is executed automatically when TASE-CM-VIPER is powered on. Therefore, it can be executed on demand by resetting or rebooting the cryptographic module. | N/A | N/A | User | N/A | Approved Service Indicator (Pin 315) and Self-Test Indicator (Pin 311) |
| Authenticated Encryption | Used to perform the authenticated encryption of an entry plaintext using AES-GCM with the desired AES 256-bit key. | AES- GCM [SP 800-38D]<br>AES-ECB [SP 800-38A] | AES_EDK | User | E | Approved Service Indicator (Pin 315) |
| Authenticated Decryption | Used to perform the authenticated decryption of an entry ciphertext using AES-GCM with the desired AES 256-bit key. | AES- GCM [SP 800-38D]<br>AES-ECB [SP 800-38A] | AES_EDK | User | E | Approved Service Indicator (Pin 315) |

| Service | Description | Approved Security Functions | Keys and/or SSPs | Role | Access Rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| Key Entry | Used to enter the AES keys into the TASE-CM-VIPER.<br>To enter the keys into the cryptographic module, the CO must follow these steps:<br>- **Step 1:** The CO must plug the harness for key uploading to the *KEYUART* interface.<br>- **Step 2:** The CO must wait until the self-test and key zeroization processes are completed successfully.<br>- **Step 3:** Once the TASE-CM-VIPER is in Key-Uploading state, the CO can enter up to 32 keys into the cryptographic module verifying that the load is successful using this command for each key:<br>・ TC "***Load New Key"***<br>・ TMR ***"Key-Status"*** | N/A | AES_EDK | CO | W | Approved Service Indicator (Pin 315) |
| 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 "9.6 Security Sensitive Parameter Zeroization". | N/A | AES_EDK | CO | W | Approved Service Indicator (Pin 315) and Zeroization Indicator (Pin 312) |

*Table 7: TASE-CM-VIPER 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.

For the Authenticated Encryption service, the TASE-CM-VIPER requires the input of the TMR ***"Load Header Information"*** which contains the header of the frame and will output the associated TM to indicate if an error encryption has been occurred. If no error encryption has been occurred, the module requires the input of the TMR ***"Load Plaintext Data"*** which contains the plaintext information and will output the TM ***"Output Ciphertext Data"*** containing the ciphertext frame.

For the Authenticated Decryption service, the TASE-CM-VIPER requires the input of the TC ***"Load Ciphertext Frame"*** which contains the ciphertext frame and will output the plaintext data information.

## 4.3 AUTHENTICATION

The TASE-CM-VIPER does not implement authentication mechanisms, therefore, an operator can select a role implicitly based on the service accessed by the module.

# 5 SOFTWARE/FIRMWARE SECURITY

FIPS 140-3 Software/Firmware requirements are not applicable because the TASE-CM-VIPER is completely hardware and does not contain software or firmware components.

# 6 OPERATIONAL ENVIRONMENT

The TASE-CM-VIPER 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-VIPER 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 VIPER 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-VIPER*

*Figure 5: Bottom view of the TASE-CM-VIPER*

# 8 NON-INVASIVE SECURITY

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

# 9 SENSITIVE SECURITY PARAMETERS MANAGEMENT

This section specifies the Sensitive Security Parameters used by the TASE-CM-VIPER to be able to perform the module approved security functions.

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

| TASE-CM-VIPER Sensitive Security Parameters (SSPs) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Key/SSP Name/Type** | **Strength** | **Security Function and Cert. Number** | **Generation** | **Import/Export** | **Establishment** | **Storage** | **Zeroization** | **Use & related keys** |
| **AES_EDK** | 256 bits | AES- GCM [SP 800-38D] Cert#A2809<br>AES-ECB [SP 800-38A] Cert#A2809 | Generated externally | The CO is responsible for performing the electronic key entry process.<br>The module does not support SSP export. | N/A | Each key is stored with its own CRC into the EEPROM using the TMR methodology. | EEPROM zeroization is performed automatically prior the key uploading process. | AES 256-bit key is used for authenticated symmetric encryption/decryption operations. |

*Table 8: SSPs*

## 9.1 RANDOM BIT GENERATOR

The TASE-CM-VIPER does not support random bit generation.

## 9.2 SECURITY SENSITIVE PARAMETER GENERATION

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

## 9.3 SECURITY SENSITIVE PARAMETER ESTABLISHMENT

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

## 9.4 SECURITY SENSITIVE PARAMETER ENTRY AND OUTPUT

All keys used by the TASE-CM-VIPER 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 32 AES-GCM keys and their CRCs identifying them using a unique ID from 1 to 32.

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-VIPER.
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 32 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"*** → This TC is used to load the new key into the TASE-CM-VIPER.
    b. Enter the new key generated externally in plaintext form via software using a PC.
    c. TMR ***"Key-Status"*** → This TMR is used to check the CRC of the last uploaded key.

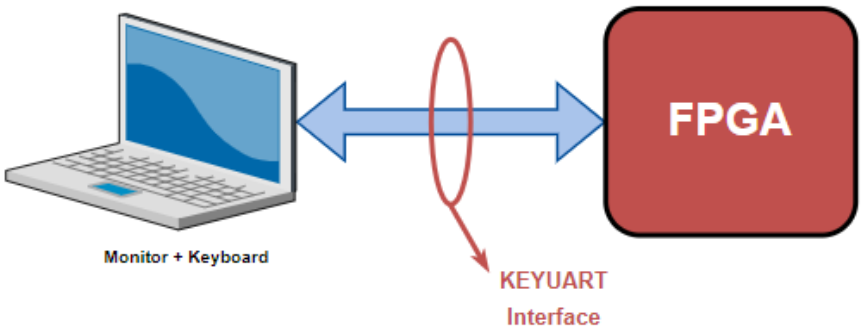


*Figure 6: Key Uploading Environment*

The upper limit is 32 keys, but the Crypto Officer can enter a lower number of keys into the TASE-CM-VIPER.

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.

## 9.5 SECURITY SENSITIVE PARAMETER STORAGE

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 | | |
|---|---|---|---|---|---|---|---|---|
| **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 |
| . | . | . | . | . | . | . | . | . |
| . | . | . | . | . | . | . | . | . |
| . | . | . | . | . | . | . | . | . |
| **32** | CRC 32 | Key 32 | **32** | CRC 32 | Key 32 | **32** | CRC 32 | Key 32 |
| **0** | 0 | 0 | **0** | 0 | 0 | **0** | 0 | 0 |
| **0** | 0 | 0 | **0** | 0 | 0 | **0** | 0 | 0 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| . | . | . | . | . | . | . | . | . |
| . | . | . | . | . | . | . | . | . |

*Table 9: Keys Storage in EEPROM memory*

When a key stored in the EEPROM is selected, the TASE-CM-VIPER 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.

## 9.6 SECURITY SENSITIVE PARAMETER ZEROIZATION

The key zeroization process will be performed automatically prior the key uploading process as it is specified in Section “9.4 Security Sensitive Parameter Entry and Output”. During this process, the TASE-CM-VIPER will only erase the 32 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).

# 10 SELF-TESTS

## 10.1 PRE-OPERATIONAL SELF-TEST

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-TEST

The TASE-CM-VIPER 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-VIPER 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.

In addition, the User can perform an on-demand conditional self-test by resetting the TASE-CM-VIPER. The KAT applies for the Approved algorithm detailed in the table below:

| TASE-CM-VIPER Conditional Algorithm Self-test | |
|---|---|
| **Algorithm** | **Description** |
| **AES-GCM** | Known Answer Test (KAT). By performing encryption/decryption and authentication. |

*Table 10: Conditional Algorithm Self-test*

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).

# 11 LIFE-CYCLE ASSURANCE

## 11.1 CONFIGURATION MANAGEMENT

The configuration management list is composed of configuration item version control, change control, flaw remediation tracking and source code review, which are managed by Thales Alenia Space in a private Git repository with write access restricted to authorized developers.

## 11.2 CONFIGURATION ITEMS IDENTIFICATION METHOD

The internal versioning of the VHDL source code is performed by Git automatically and the assigned version and revision are used internally to control the code development, so that it must not be confused with the final released version of the VHDL that is appended manually to the name of the VHDL code file using the following format “release-XX_YY_ZZ”, where XX is the version number, YY is the revision number and ZZ is associated with bug fixing.

Regarding each associated module documentation, they are manually versioned by appending the version and revision on their filename as follow: Document-X.Y. The assigned version number is stated as part of the file name with the following naming convention:

- **Naming:** Name-X.Y, where Name is the unique name of the related document, and X.Y are the version and revision of the document. Every new document is named with version v1.0.
- **Version Update:** When the document is modified and this modification implies major changes, the ‘X’ number must be changed. However, if changes and modifications imply minor changes, then the ‘Y’ number must be changed.

The configuration item list can be consulted in **[TAS-CIL]** document.

## 11.3 CRYPTO OFFICER AND USER GUIDANCE

### 11.3.1 OPERATION 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 32 EEPROM memory pages which contain the possible 32 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-VIPER 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-VIPER is in Error state, it will not be able to perform cryptographic operations. To resume normal operation mode, the cryptographic module must be reset.

### 11.3.2 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 "11.3.4 Installation and Initialization Instructions".

### 11.3.3 INTEGRITY AND CONFIDENTIALITY ASSURANCE

The integrity and confidentiality of the cryptographic module is assured by following the secure distribution methodology specified in the previous section 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.

### 11.3.4 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 VIPER transponder. Then, the module can be initiated in a secure manner by following the steps below:

**Step 1:** Once the TASE-CM-VIPER 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 "9.4 Security Sensitive Parameter Entry and Output" to insert up to 32 keys into the module and to store them into the EEPROM memory.

**Step 2:** After the keys are entered and stored into the cryptographic module, the Crypto Officer must power off the TASE-CM-VIPER and unplug the harness from the *KEYUART* port.

**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"***, detailed in the **[TAS-FS]** document, after powering on the module.

### 11.3.5 SECURE OPERATION

When the module has been configured and the AES-GCM keys stored in a secure manner by the Crypto Officer, the TASE-CM-VIPER can be powered on to be used by or User role by using the TCs and TMRs detailed in **[TAS-FS]** document and the procedures specified in “4 Roles, Services, and Authentication”.

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.

# 12 MITIGATION OF OTHER ATTACKS

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

# 13 ACRONYMS

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **CO** | Crypto Officer |
| **CRC** | Cyclic Redundancy Check |
| **CSP** | Critical Security Parameter |
| **ECB** | Electronic CodeBook |
| **EEPROM** | Electrically Erasable Programmable Read-Only Memory |
| **FPGA** | Field Programmable Gate Arrays |
| **FSM** | Finite State Model |
| **GCM** | Galois/Counter Mode |
| **GCP** | Ground Centre Processor |
| **ID** | Identifier |
| **IV** | Initialization Vector |
| **KAT** | Known Answer Test |
| **RF** | Radio Frequency |
| **SEE** | Single Events Effects |
| **SSP** | Security Sensitive Parameter |
| **TASE-CM-VIPER** | Thales Alenia Space VIPER Cryptographic Module |
| **TC** | Telecommand |
| **TM** | Telemetry |
| **TMR** | Telemetry Request |
| **TMR** | Triple Modular Redundancy |
| **UART** | Universal Asynchronous Receiver-Transmitter |
| **VIPER** | Volatiles Investigating Polar Exploration Rover |

# 14 DOCUMENT REFERENCE

| | |
|---|---|
| **[TAS-CIL]** | Thales Alenia Space FIPS 140-3 - Configuration Item List v1.7 |
| **[TAS-FS]** | Thales Alenia Space FIPS 140-3 - Functional Specification v1.7 |
| **[TAS-FSM]** | Thales Alenia Space FIPS 140-3 - Finite State Model v1.7 |
| **[TAS-SP]** | Thales Alenia Space FIPS 140-3 - Security Policy v1.7 |
| **[FIPS 197]** | Advanced Encryption Standard (AES) |
| **[SP 800-140F]** | CMVP Approved Non-Invasive Attack Mitigation Test Metrics |
| **[SP 800-38A]** | Recommendation for Block Cipher Modes of Operation: Methods and Techniques |
| **[SP 800-38D]** | Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC |
| **[140IG]** | Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program |