Mitsubishi Electric Corporation Kamakura Works

CRYP CARD

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document defines the FIPS140-3 non-proprietary security policy of Mitsubishi Electric FIPS140-3 CRYP CARD (hereinafter, referred to as “CRYP CARD” or “this module”). CRYP CARD provides various services which enable the operators to encrypt/decrypt or authenticate data with properly managed and protected keys.

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

CRYP CARD is designed to be used as an important building block in an embedded equipment. Operators can operate this module mainly via SpaceWire (SpW) [1] Interface. The primary functions are:

- Approved Security Functions
- Key Installation and Protection

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

Figure 1 shows the block diagram and the cryptographic boundary of CRYP CARD. All the components of this module are included within the cryptographic boundary. CRYP CARD is entirely contained within a metal enclosure that serves as a physical cryptographic boundary.

This module is equipped with four types of physical interfaces shown below. Four types of physical interfaces are provided by the connector.

- SpaceWire ch0 Interface
- SpaceWire ch1 Interface
- POWER Interface
- EIA-422 Interface

Most services are implemented by two FPGAs.

- CTRL FPGA: controls of the CALC FPGA, interfaces and SSPs.
- CALC FPGA: calculation of security functions.

Detailed specifications of logical interfaces and services are explained in Section 3 and 4.

Note: the CALC FPGA is the OE for the approved algorithms. The OE on the CAVP is labeled "CRYP CARD FPGA".

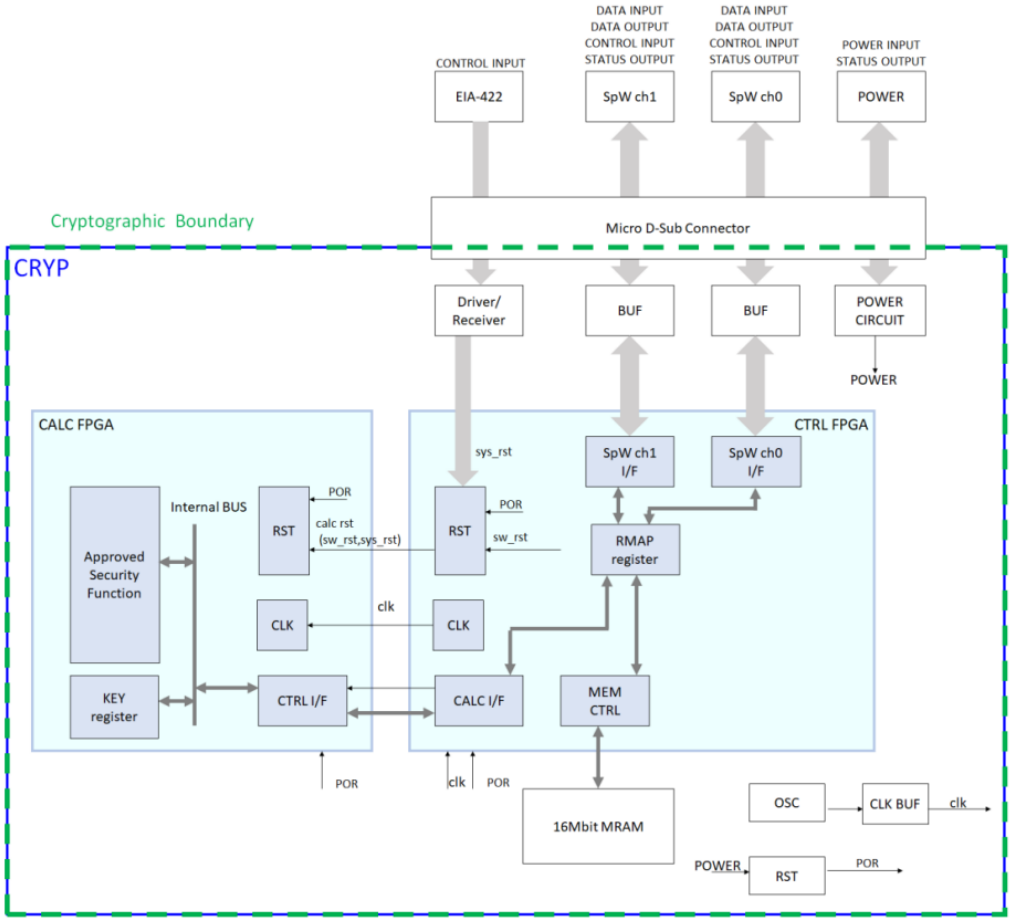

Figure 1: Block Diagram

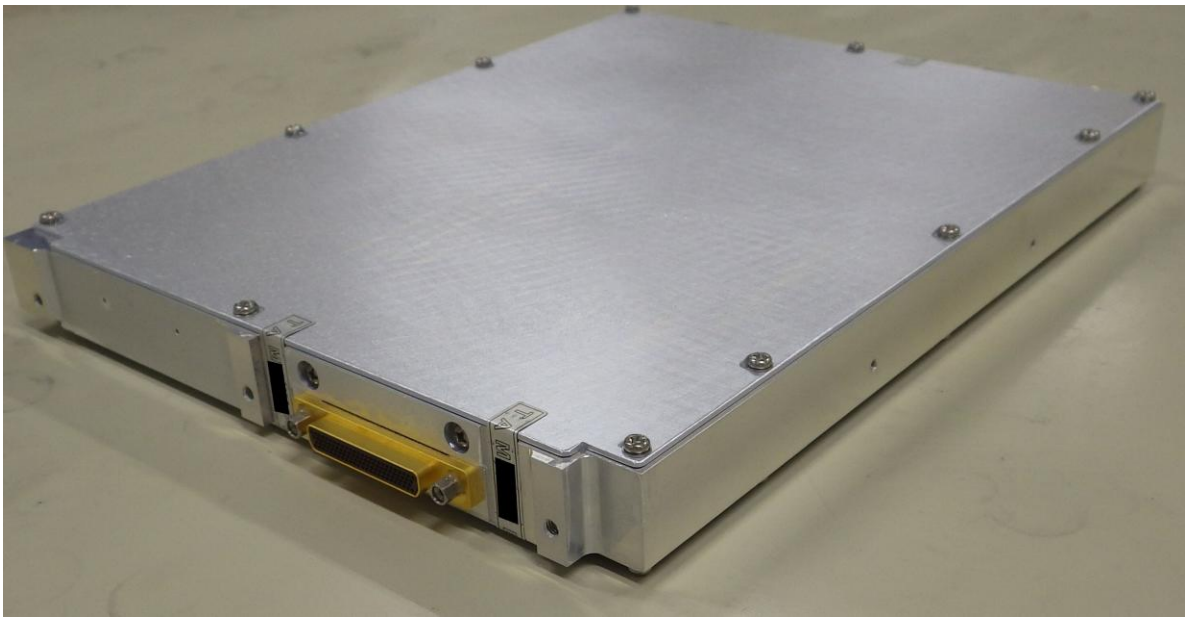

Figure 2: Module View

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Table 2 shows tested module configurations. The Module identifier and version of this module can be checked in the status register of RMAP registers.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
F7P4788-G03	1.0	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

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	All services are operated in this mode.	Approved	The successful completion of a service is an implicit indicator for the use of an approved service.

Table 3: Modes List and Description

As shown in Table 3, CRYP CARD has only the approved mode. All services in this module are performed in the approved mode.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A7719, A7720	Direction - Generation Key Length - 256	SP 800-38B
AES-CTR	A7719, A7720	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A7719, A7720	Direction - Encrypt Key Length - 256	SP 800-38A
AES-GCM	A7719, A7720	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D
SHA2-256	A7719, A7720	Message Length - Message Length: 0-8192 Increment 256	FIPS 180-4

Table 4: Approved Algorithms

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

Name	Type	Description	Properties	Algorithms
KTS-UNWRAP	KTS-Unwrap	Unwrap a wrapped key	Standard:N/A IG D.G:Approved method from IG D.G	AES-GCM: (A7719) Direction: Decrypt
AES-GCM	BC-Auth	Authenticated AES Encryption and AES Decryption		AES-GCM: (A7719, A7720)
AES-CTR	BC-UnAuth	AES-CTR Encryption and AES-CTR Decryption		AES-CTR: (A7719, A7720)
AES-ECB	BC-UnAuth	AES-ECB Encryption and AES-ECB Decryption		AES-ECB: (A7719, A7720)
AES-CMAC	MAC	CMAC Message Authentication Code Generation		AES-CMAC: (A7719, A7720)
SHA2-256	SHA	Message Digest Generation		SHA2-256: (A7719, A7720)
Password Installation	BC-AuthDecrypt SHA	Password Installation		SHA2-256: (A7719) AES-GCM: (A7719) Direction: Decrypt
Role-based Authentication	SHA	Role-based Authentication		SHA2-256: (A7719)

Table 5: Security Function Implementations

All the algorithms shown in Table 5 are implemented as security function and can be performed by operators.

2.7 Algorithm Specific Information

AES-GCM encryption supports only the internal IV mode. The IV consists of concatenation of a 32-bit name field and a 64-bit counter field. The internal IV is stored in non-volatile memory (MRAM) and managed by this module so that it is incremented by 1 every time AES-GCM encryption is performed. Since data link rate of SpW between this module and user module is up to 20 [Mbps], the counter part of the IV never exhausts the maximum number of possible values.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

The module does not have or use an entropy source.

2.9 Key Generation

N/A for this module.

2.10 Key Establishment

The Key Transport Scheme (KTS) as specified in IG D.G implemented by the module is listed in Section 2.5 and 2.6.

2.11 Industry Protocols

N/A for this module.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
SpaceWire ch0	Data Input Data Output Control Input Status Output	Plain or encrypted SSPs and data. Module Status data. Control data.
SpaceWire ch1	Data Input Data Output Control Input Status Output	Plain or encrypted SSPs and data. Module Status data. Control data.

Physical Port	Logical Interface(s)	Data That Passes
POWER	Status Output Power	Power monitor. DC 5V +/- 0.25V Power.
EIA-422	Control Input	Reset.

Table 6: Ports and Interfaces

The module does not have any external input or output devices that can be used for data input, data output, status output, or control input.
The module does not implement control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password Authentication	128-bit PIN (Memorized secret)	SHA2-256	2^128< 1.0×10^12	3×2^128< 1.0×10^11

Table 7: Authentication Methods

CRYP CARD authenticates operators with role-based authentication. CRYP CARD takes as input a password from a purported operator, computes its HASH value, and compares it with the one which has been installed as legitimate. The strength of authentication mechanism that an illegitimate operator succeeds in impersonation is 1.0 × 10^-12 for each attempt and 1.0 × 10^-11 for multi attempt during a one-minute period, because CRYP CARD takes a preventive approach that it allows no more than three attempts in one minute.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	Password Authentication
User	Role	User	Password Authentication

Table 8: Roles

CRYP CARD accepts two roles: Crypto Officer, and User. Table 8 shows the details of the roles and corresponding service commands that operators can input and output from CRYP CARD. Operators cannot take both roles simultaneously. After Power ON or reset, operators need to be authenticated with their role solely identified to proceed to perform applicable services. The role cannot be changed by any methods except for Power OFF or reset.
Operators can change their PINs using the password installation service. The default password shall be changed prior to the actual operation of CRYP CARD. Otherwise, the approved security function services (SHA2-256, AES-CMAC, AES-GCM, AES-CTR, and AES-ECB services), and the key services (Key Installation and Key Setting services) cannot be performed.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
SHA2-256	Used to generate a SHA2-256 message digest	Security Function output result of RMAP register: 'd2	Message	Message digest	SHA2-256	Crypto Officer User
AES-CMAC Generation	Used to generation a MAC using AES-CMAC	Security Function output result of RMAP register: 'd2	Message	MAC	AES-CMAC	Crypto Officer - AES Key: E - Temporary AES Key: E User - AES Key: E - Temporary AES Key: E
AES-GCM ENC	Used to perform authenticated symmetric encryption with AES-GCM	Security Function output result of RMAP register: 'd2	AAD, Plaintext	Ciphertext, Tag, AES GCM IV	AES-GCM	Crypto Officer - AES Key: E - Temporary AES Key: E - AES GCM IV: G,R,W,E User - AES Key: E - Temporary AES Key: E - AES GCM IV: G,R,W,E
AES-GCM DEC	Used to perform authenticated symmetric decryption with AES-GCM	Security Function output result of RMAP register: 'd2	Ciphertext, IV, AAD, Tag	Plaintext	AES-GCM	Crypto Officer - AES Key: E - Temporary AES Key: E User - AES Key: E - Temporary AES Key: E
AES-CTR ENC	Used to perform	Security Function	Plaintext, IV	Ciphertext	AES-CTR	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	symmetric encryption with AES-CTR	output result of RMAP register: 'd2				- AES Key: E - Temporary AES Key: E User - AES Key: E - Temporary AES Key: E
AES-CTR DEC	Used to perform symmetric decryption with AES-CTR	Security Function output result of RMAP register: 'd2	Ciphertext, IV	Plaintext	AES-CTR	Crypto Officer - AES Key: E - Temporary AES Key: E User - AES Key: E - Temporary AES Key: E
AES-ECB ENC	Used to perform symmetric encryption with AES-ECB	Security Function output result of RMAP register: 'd2	Plaintext	Ciphertext	AES-ECB	Crypto Officer - Temporary AES Key: E User - Temporary AES Key: E
Key Installation(KEK)	Installation of the KEK.	Key Installation status of RMAP register: 'd2	KEK, IV	N/A	KTS-UNWRAP	Crypto Officer - KEK: W - Default KEK: E
Key Installation(AES Key)	Installation of the AES key.	Key Installation status of RMAP register: 'd2	AES Key, IV	N/A	KTS-UNWRAP	Crypto Officer - KEK: E - AES Key: W
Key Installation(Temporary AES Key)	Installation of the Temporary AES Key.	Key Installation status of RMAP register: 'd2	Temporary AES Key	N/A	None	Crypto Officer - Temporary AES Key: W User - Temporary AES Key: W
Key Setting(AES Key)	Decryption and	Key Setting	Key number	N/A	KTS-UNWRAP	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	activation of AES Key for using in the approved security function service related to AES.	status of RMAP register: 'd2				- KEK: E - AES Key: R User - KEK: E - AES Key: R
Password Installation	Installation of its own role's password.	Password setting status of RMAP register: 'd2	PIN, IV	N/A	Password Installation	Crypto Officer - PIN: W - KEK: E User - PIN: W - KEK: E
Role-based Authentication	Authentication for Crypto Officer or User	Password Authentication status of RMAP register: 'd2	Role, PIN	N/A	Role-based Authentication	Unauthenticated - PIN: E
Self-test	Execution of the self-test by the device reset.	N/A	N/A	N/A	None	Crypto Officer User Unauthenticated
Reset	Zeroisation of Temporary AES by the device reset.	zeroize status of RMAP register: 'b1	N/A	N/A	None	Crypto Officer - Temporary AES Key: Z User - Temporary AES Key: Z Unauthenticated - Temporary AES Key: Z
Plain CSP Initialization	Zeroisation of KEK and PIN.	zeroize status of RMAP register: 'b1	zeroization code	N/A	None	Crypto Officer - KEK: Z - PIN: Z Unauthenticated - KEK: Z - PIN: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show status	Output CRYP CARD's status, information, and indicators.	N/A	N/A	CRYP CARD's status, information	None	Crypto Officer User Unauthenticated
Show version	Output CRYP CARD's versioning information	N/A	N/A	Module Identification and Version Information	None	Crypto Officer User Unauthenticated

Table 9: Approved Services

Details of the approved services are shown in Table 9. Operators are provided with all services excluding Self-test and Reset by RMAP access. The Self-test services are performed after Power OFF/ON via Power Interface or reset via EIA-422 or RMAP access.
If an unauthenticated operator performs the Plain CSP Initialization service, the entire MRAM area excluding the encrypted CSPs is zeroized. In contrast, if a CO operator performs the Plain CSP Initialization service, it is possible to specify the target CSP for zeroizing.
Table 9 uses acronyms defined below.

- 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 = Zeroise: The module zeroises the SSP.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

N/A for this module.

5 Software/Firmware Security

5.1 Integrity Techniques

Software/Firmware Security requirement is not applicable to this module because it incorporates NO software, firmware, or FPGA configuration data within its memory chips. This module is equipped with antifuse-based FPGAs whose circuits are programmed during manufacturing at the vender’s factory and never reprogrammed again.

5.2 Initiate on Demand

N/A for this module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Metal removable cover		Periodically compare the current condition of the enclosures with the previous record.
Tamper seals		Periodically compare the current condition of the tamper seals with the previous record.

Table 10: Mechanisms and Actions Required

CRYP CARD is multiple-chip embedded hardware module contained within a metal removable cover sealed with tamper-evident seals. Figure 3 indicates the precise placement of tamper seals.

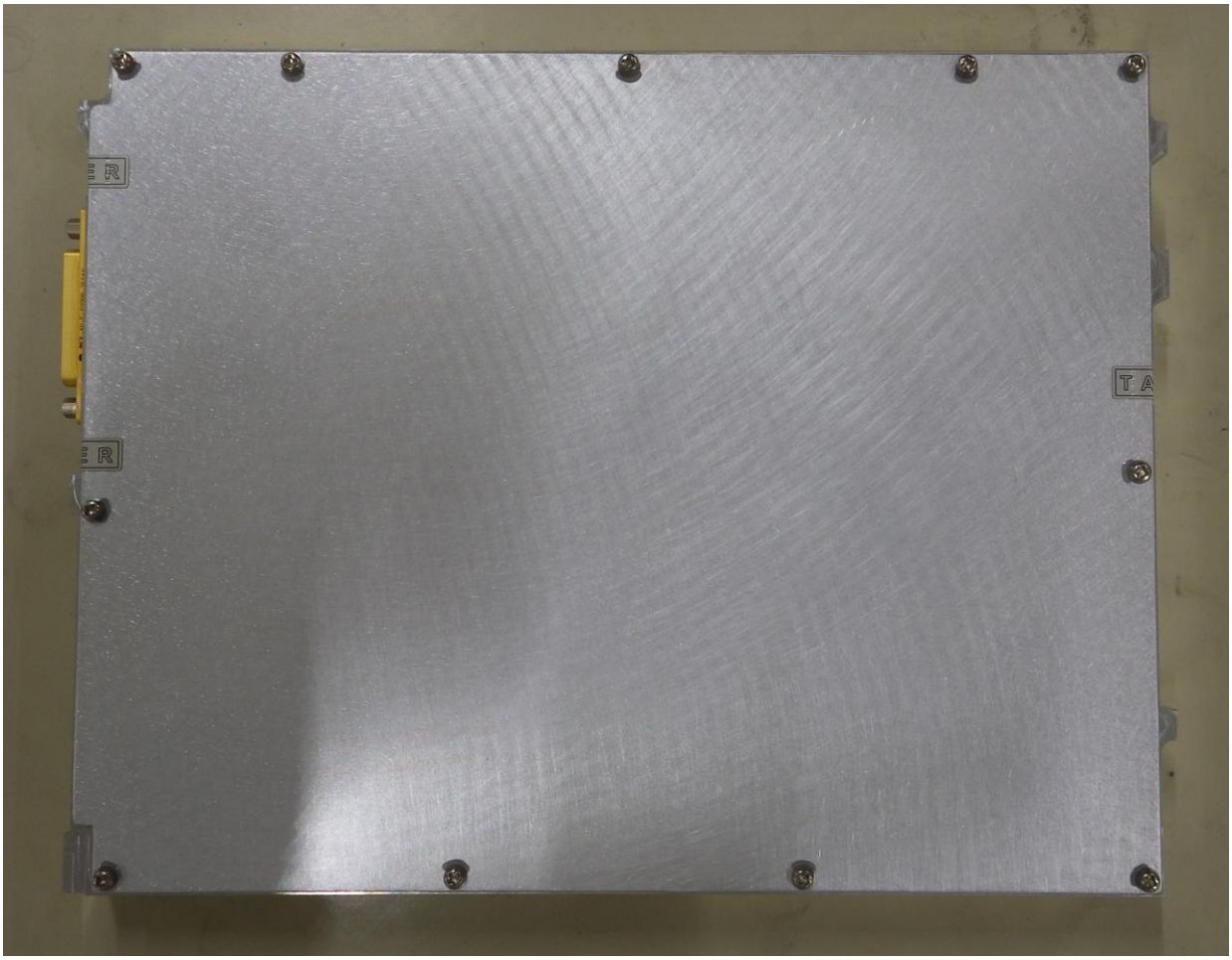

Figure 3: Tamper seals

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
MRAM	Non-volatile memory that is zeroised by the plain CSP initialization service.	Static
Registers or BRAMs in FPGA	Volatile memory that is zeroised by the reset service.	Dynamic
OTP in FPGA	Hardcoded in FPGA.	Static

Table 11: Storage Areas

As shown in Table 11, SSPs (excluding the default KEK) are stored in MRAM memory. Also, they are stored temporarily in registers or BRAMs of FPGA. The default KEK is hard-coded into the anti-fuse FPGA, i.e. it is stored in the OTP in the FPGA.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Key Installation	Outside the module	MRAM	Encrypted	Manual	Electronic	KTS-UNWRAP
Password Installation	Outside the module	MRAM	Encrypted	Manual	Electronic	Password Installation
Temporary Key Installation	Outside the module	Registers or BRAMs in FPGA	Plaintext	Manual	Electronic	
AES GCM IV output	Registers or BRAMs in FPGA	Outside the module	Plaintext	Manual	Electronic	

Table 12: SSP Input-Output Methods

This module does not support CSP output methods.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Plain CSP Initialization	0x00 is written to each memory to cell three times.	The SSPs are overwritten by 0x00.	By calling the Plain CSP Initialization service(input the zeroisation code by RMAP Write Commands).
Reset	Electrically reset and overwritten by default value of each register or BRAM in FPGAs.	Volatile memory used by the module is zeroised when power is removed or reset.	By performing the device reset by Power OFF/ON, EIA-422, or RMAP access.

Table 13: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KEK	Key encryption key	256 bits - 256 bits	Symmetric Key - CSP		KTS-UNWRAP	KTS-UNWRAP
AES Key	AES key used for encryption, decryption,	256 bits - 256 bits	Symmetric Key - CSP		KTS-UNWRAP	AES-GCM AES-CTR AES-CMAC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	and computing MAC.					
Temporary AES Key	Temporary AES key used for encryption, decryption, and computing MAC.	256 bits - 256 bits	Symmetric Key - CSP			AES-GCM AES-CTR AES-ECB AES-CMAC
Default KEK	Default KEK used for installation of the operator's KEK and PIN.	256 bits - 256 bits	Symmetric Key - CSP			KTS-UNWRAP
PIN	authentication data for role-based authentication	128 bits - 128 bits	Authentication data - CSP			Role-based Authentication
AES GCM IV	IV((Initialization vector) used in AES-GCM ENC service	96 bits - N/A	IV - PSP			AES-GCM

Table 14: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KEK	Key Installation	MRAM:Plaintext		Plain CSP Initialization	AES Key:Wraps AES Key:Unwraps Default KEK:Wrapped by
AES Key	Key Installation	MRAM:Encrypted		N/A	KEK:Wrapped by
Temporary AES Key	Temporary Key Installation	Registers or BRAMs in FPGA:Plaintext	From input to zeroization.	Reset	
Default KEK		OTP in FPGA:Plaintext		N/A	KEK:Unwraps
PIN	Password Installation	MRAM:Obfuscated		Plain CSP Initialization	
AES GCM IV	AES GCM IV output	MRAM:Plaintext		Plain CSP Initialization	

Table 15: SSP Table 2

Table 14 and Table 15 show Keys and other SSPs in this module. Zeroisation is not applicable to AES Keys because they are encrypted and authenticated with KEK and are protected CSPs. It is also not applicable to the default KEK, since it is only used to protect and input the KEK when it is not stored.

10 Self-Tests

10.1 Pre-Operational Self-Tests

N/A for this module.

Since CRYP CARD implements none of software, firmware, bypass capabilities, and critical functions, this module does not perform pre-operational self-tests. Instead of them, conditional cryptographic algorithm self-tests shown in Table 16 are performed.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A7719)-Encrypt	AES-GCM Encryption KAT using 256 bits key	KAT	CAST	self test status of RMAP register: 'd2	AES Encryption	Performed when the module is powered on
AES-GCM (A7719)-Decrypt	AES-GCM Decryption KAT using 256 bits key	KAT	CAST	self test status of RMAP register: 'd2	AES Decryption	Performed when the module is powered on
AES-GCM (A7720)-Encrypt	AES-GCM Encryption KAT using 256 bits key	KAT	CAST	self test status of RMAP register: 'd2	AES Encryption	Performed when the module is powered on
AES-GCM (A7720)-Decrypt	AES-GCM Decryption KAT using 256 bits key	KAT	CAST	self test status of RMAP register: 'd2	AES Encryption	Performed when the module is powered on
AES-CMAC (A7719)	MAC Generation KAT	KAT	CAST	self test status of RMAP register: 'd2	MAC Generation	Performed when the module is powered on
AES-CMAC (A7720)	MAC Generation KAT	KAT	CAST	self test status of RMAP register: 'd2	MAC Generation	Performed when the module is powered on
SHA2-256 (A7719)	SHA2-256 Message Digest KAT	KAT	CAST	self test status of RMAP register: 'd2	Message Digest	Performed when the module is powered on

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A7720)	SHA2-256 Message Digest KAT	KAT	CAST	self test status of RMAP register: 'd2	Message Digest	Performed when the module is powered on

Table 16: Conditional Self-Tests

Table 16 shows conditional cryptographic algorithm self-tests (CAST) that this module supports. CRYP CARD does not support any other conditional self-tests because it contains NO pair-wise keys generation, software/firmware load, manual entry services, bypass capabilities, and critical functions.
AES-CTR (encryption and decryption) and AES-ECB (encryption) are not included in the CAST target list because they are significantly simpler than AES-GCM (encryption and decryption).

10.3 Periodic Self-Test Information

N/A for this module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A7719)-Encrypt	KAT	CAST	On demand	Manually
AES-GCM (A7719)-Decrypt	KAT	CAST	On demand	Manually
AES-GCM (A7720)-Encrypt	KAT	CAST	On demand	Manually
AES-GCM (A7720)-Decrypt	KAT	CAST	On demand	Manually
AES-CMAC (A7719)	KAT	CAST	On demand	Manually
AES-CMAC (A7720)	KAT	CAST	On demand	Manually
SHA2-256 (A7719)	KAT	CAST	On demand	Manually
SHA2-256 (A7720)	KAT	CAST	On demand	Manually

Table 17: Conditional Periodic Information

Operators can manually initiate CAST on demand by the device reset.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	Cannot perform any services except for the status output service and the reset service.	Failure of the conditional self-test	The only method to clear this error state is to reset the module.	current state of RMAP register: 'hFF

Table 18: Error States

Table 18 shows the error state defined in this module. When KATs returned to an error, this module enters the error state. The indicator is the current state of RMAP register; by RMAP Read access to the register, operators can recognize entering the error state. No services are available in the error state except for the status output service and the reset service. Instead, by resetting CRYP CARD, the self-tests are performed automatically after general initialization process.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

This module accepts no additional installation of software and firmware throughout its life cycle. Before or after integration into another embedded modules or systems, CRYP CARD can be initiated by the steps shown below. Details are given in Section 11.2 and 11.3.

- Password Installation
- Key installation

11.2 Administrator Guidance

This section describes guidance for Crypto Officer (CO).

Interfaces and Services for CO:
All Interfaces shown in Table 6 are available for CO, and services for CO are listed in Table 9.

Distributing by CO:
It is necessary to maintain security when distributing this module that tamper seals and enclosures shall be verified at least at the beginning and end of distribution.

Initialization and startup steps for CO:

Step 1: Power on.
Step 2: Before initialization, CRYP CARD is set to use the default KEK and CO's PIN. No KEK, AES Keys or CO's PIN are stored in MRAM. To confirm that these SSPs are not changed after manufacturing, CO should check the key installation information or other configuration information by the status output service via RMAP Read Commands after Power on.
Step 3: For installation of CO's CSPs, the operator shall perform the role-based authentication service via RMAP Write Commands. The Default CO's PIN for the first role authentication is a default value, which are separately notified by the vender.
Step 4: After authenticating CO's role, a new PIN shall be installed. In the installation process, the new PIN and the default PIN are input via RMAP Write Commands. While the default PIN is input as plaintext, the new PIN shall be encrypted and authenticated by AES-GCM using the default KEK. Details of the encryption procedure and the default KEK are also separately notified by the vender.
Step 5: CO's own KEK shall be installed by the key installation service via RMAP Write Commands. The new KEK shall be encrypted and authenticated by AES-GCM using the default KEK.

Step 6: (Optional) CO can install AES Keys for the approved security function services related to AES.
. These keys shall be encrypted and authenticated by AES-GCM using the CO's KEK. This step is applicable even when the module is in operation.
Step 7: Power off.

Operation for CO:
After being authenticated as CO, and confirming configurations of CRYP CARD through RMAP accesses, CO can perform any services listed in Table 9.

Sanitization for CO:
To sanitize all plain CSPs, Plain CSP Initialization service shall be performed. In case of sanitization of all encrypted CSPs, destruction of this module is needed.

11.3 Non-Administrator Guidance

This section describes guidance for User.

Interfaces and Services for User:
All Interfaces shown in Table 6 are available for User, and services for users are listed in Table 9.

Distributing by User:
It is necessary to maintain security when distributing this module that tamper seals and enclosures shall be verified at least at the beginning and end of distribution.

Initialization and startup steps for User:
initialization and startup steps for User must be performed after CO's initialization.

Step 1: Power on.
Step 2: When User first uses the module for initialization, CRYP CARD does not contain User's operational PIN in MRAM and accepts only the User's default PIN. Prior to initialization, User should verify the key installation state by using the status output service provided by RMAP Read Commands.
Step 3: User shall perform the role-based authentication service by using RMAP Write Commands to install a new PIN. The default PIN is separately notified by the vender.
Step 4: After authenticating User's role, installation of a new PIN shall be performed. RMAP Write Commands takes as input both the default PIN (as plaintext) and the new PIN (as encrypted and authenticated using AES-GCM with KEK, where KEK is installed by CO). It depends on the operators' standard whether CO or User encrypts the new PIN. Note that CO needs to notify KEK when the new PIN is encrypted by User.
Step 5: Power off.

Operation for User:
User can perform all the services in Table 9 when authentication succeeds and configurations of CRYP CARD are verified as appropriate.

12 Mitigation of Other Attacks

N/A for this module.

Appendix A. Glossary

SpW	Space Wire. A High-speed serial communication protocol used in spacecraft and satellite systems.
RMAP	Remote Memory Access Protocol. A Communication protocol used in embedded systems of spacecraft to access and control remote memory locations or registers. RMAP defines a standardized procedure for RMAP Write Command and RMAP Read Command.
BRAM	Block RAM. A type of memory embedded and used in FPGAs.
MRAM	Magnetoresistive Random Access Memory. A non-volatile memory technology that uses magnetic elements to store data.
EIA-422	Also Known as RS-422. A standard for serial communication that defines the electrical characteristics and signaling and uses differential signaling.
PIN	Personal Identification Number. A password used to authenticate CO's or User's role. In this module, PINs are defined as a hex number fixed at 128-bit.

Appendix B. References

[1] ECSS, "ECSS-E-ST-50-12C Rev.1 SpaceWire - Links, nodes, routers and networks," 15 May 2019.

[2] NIST, "FIPS197 Advanced Encryption Standard (AES)," 9 May 2023.

[3] NIST, "NIST SP 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," November 2007.

[4] NIST, "NIST SP 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques," December 2001.

[5] NIST, "NIST SP 800-38B Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication," 10 June 2016.

[6] NIST, "FIPS PUB 180-4 Secure Hash Standard (SHS)," August 2015.

[7] ECSS, "ECSS-E-ST-50-52C SpaceWire - Remote memory access protocol," 5 February 2010.

[8] NIST, "FIPS140-3 Security Requirements for Cryptographic Modules," 22 March 2019.