SAAB ENCRYPTED AUTOMATIC IDENTIFICATION SYSTEM CRYPTOGRAPHIC MODULE (EAISCM)

VERSION NO: 1.0

FIPS 140-2 NON-PROPRIETARY SECURITY POLICY

FIPS SECURITY LEVEL: 1
DOCUMENT VERSION: 13

PREPARED FOR
SAAB Technologies

COMPILED BY
EWA-Canada, An Intertek Company

DATE
March 22, 2022

Issuing office: Electronic Warfare Associates – Canada, Ltd., An Intertek Company ("Intertek")

Disclaimer

This report has been prepared for the SAAB Encrypted Automatic Identification System Cryptographic Module (EAISCM) and should not be relied upon or used for any other project without an independent check being carried out as to its suitability and prior to obtaining the written authority of Intertek. Intertek accepts no responsibility or liability for the consequences of this document being used for a purpose other than for which it was commissioned. Any person using or relying on the document for such other purposes, agrees and will by such use or reliance be taken to confirm his agreement to indemnify Intertek for all loss or damage resulting therefrom. Intertek accepts no responsibility or liability for this document to any party other than the person by whom it was commissioned.

EWA-Canada Locations

OTTAWA, ON	ST. JOHN'S, NL
1223 Michael St. North, Suite 200 Ottawa, Ontario, Canada K1J 7T2 Tel (613) 230-6067 Fax (613) 230-4933	139 Water St., Suite 601 St. John's, Newfoundland, Canada A1C 1B2 Tel (709) 726-0667 Fax (709) 726-0668

Table of Contents

Table of Figures

Table of Tables

1 INTRODUCTION

1.1 Purpose

This non-proprietary Security Policy (SP) for the SAAB EAISCM describes how the module meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode.

This document was prepared as part of the Level 1 FIPS 140-2 validation of the module. The following table lists the module's FIPS 140-2 security level for each section.

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

Table 1 - FIPS 140-2 Section Security Levels

1.2 Background

Federal Information Processing Standards Publication (FIPS PUB) 140-2 – *Security Requirements for Cryptographic Modules* details the requirements for cryptographic modules. More information on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP), the FIPS 140-2 validation process, and a list of validated cryptographic modules can be found on the CMVP website:

http://csrc.nist.gov/groups/STM/cmvp/index.html

Additional information about SAAB can be found on the SAAB website:

https://www.saab.com/

1.3 Document Organization

This non-proprietary SP is part of the SAAB Encrypted Automatic Identification System Cryptographic Module 1.0 FIPS 140-2 submission package. Other documentation in the submission package includes:

- Product documentation
- Vendor evidence documents
- Finite state model
- Additional supporting documents

The SAAB EAISCM 1.0 is also referred to in this document as the cryptographic module, or the module.

2 MODULE OVERVIEW

The SAAB R5 SUPREME AIS Transponder (also referred to as the R5) is designed for all vessels that follow the Safety of Life at Sea (SOLAS) regulations and advanced applications such as Automatic Identification Systems (AIS). An AIS automatically provides information about a vessel to nearby vessels and coastal authorities.

Ships fitted with an AIS shall keep it operational at all times except where international agreements, rules or standards provide for the protection of navigational information.

SOLAS Chapter V "Carriage requirements for shipborne navigational systems and equipment" requires an AIS to be fitted aboard all vessels of 300 gross tonnage and upwards engaged on international voyages, cargo vessels of 500 gross tonnage and upwards not engaged on international voyages and all passenger vessels irrespective of size. The requirement became effective for all vessels as of 31 December 2004.

This regulation requires that an AIS shall:

- provide information - including the vessel's identity, type, position, course, speed, navigational status and other safety-related information - automatically to appropriately-equipped shore stations, other vessels and aircraft;
- automatically receive such information from similarly fitted vessels;
- monitor and track vessels; and
- exchange data with shore-based facilities.

The EAISCM 1.0 expands on the R5's capabilities by providing an AIS with the capability to transmit and receive encrypted data containing the information required by regulation.

The module has been tested on the following platform:

Tested Platform	Processor	Operating System
R5 SUPREME AIS Transponder	Texas Instruments OMAP-L138	non-modifiable OS

Table 2 – Tested Platform

2.1 Cryptographic Module Specification

The cryptographic module is a firmware module within a multi-chip standalone device. The physical boundary of the module is the R5 product boundary. The R5 contains the EAISCM as a component of its firmware image.

Front | Rear

Figure 1 – Physical: SAAB R5 SUPREME AIS Transponder

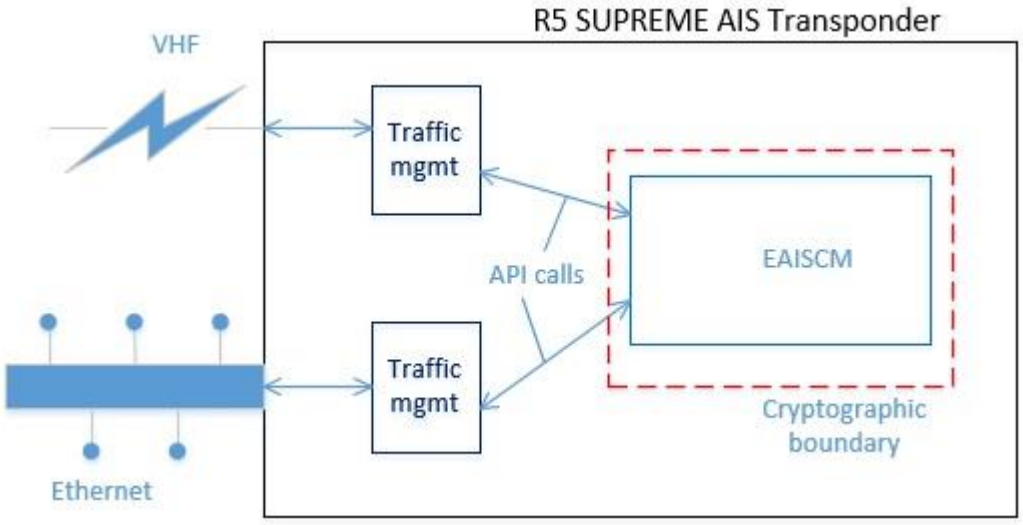

Figure 2 – Cryptographic Logical Boundary Within R5

2.2 Cryptographic Module Ports and Interfaces

As a component of the R5's firmware image, the module's ports and interfaces that are supported when operating in FIPS mode are as follows:

- Application Programming Interface (API) for input and output
- power from the R5

Table 3 shows how the module's physical interfaces map to the logical interfaces defined in FIPS 140-2.

FIPS 140-2 Interfaces	Physical Interface
Data Input	API
Data Output	API
Control Input	API
Status Output	API
Power	System bus

Table 3 – Module Interface Mappings

2.3 Roles and Services

2.3.1 Roles

The module has two operator roles: Crypto Officer (CO) and User.

The CO role is responsible for:

- loading the Advanced Encryption Standard (AES) key onto the R5 (outside the scope of this SP)
- purging the AES key from the R5 (outside the scope of this SP)
- passing plaintext data to the module via the API, and receiving ciphertext output from the API
- passing ciphertext data to the module via the API, and receiving plaintext output from the API

The User role is responsible for:

- passing plaintext data to the module via the API, and receiving ciphertext output from the API
- passing ciphertext data to the module via the API, and receiving plaintext output from the API

2.3.2 Services

The module permits multiple instances to call its APIs, but only one cryptographic function is executed at a time.

The following table provides a list of all of the module's services.

Service	Operator	Description	Input	Output	CSP
Encrypt	CO, User	Encrypt traffic coming into the transponder	Plaintext traffic	Ciphertext traffic	Traffic Key
Decrypt	CO, User	Decrypt traffic coming into the transponder	Ciphertext traffic	Plaintext traffic	Traffic Key
Zeroize	CO, User	Delete Traffic Key from module memory	None	Result of deletion	Traffic Key
Get Status	CO, User	Get current status of module (works even in error state)	None	Current status of module	None

Table 4 – Services

2.4 Authentication Mechanisms

The module does not make use of authentication at Level 1.

2.5 Physical Security

The module is firmware, present as a component of the firmware running on the R5 as a multi-chip standalone device.

2.6 Operational Environment

The module operates in a non-modifiable operational environment as part of the R5 system image.

2.7 Cryptographic Key Management

2.7.1 Algorithm Implementations

A list of FIPS-Approved algorithms implemented by the module can be found in the following table.

Algorithms and Modes	Key Sizes	Certificate #
AES (ECB)	128-bit, 192-bit, 256-bit	A1075
SHA-512	N/A	A1075

Table 5 – FIPS-Approved Algorithm Implementations

SHA-512 is used solely to verify a fresh hash of the module's binary against a hash saved in the R5 system image.

2.7.2 Key Management Overview

The access rules for the module are given in Table 7 below.

R – read access W – write access X – execute access

CSP	Type / Size	Usage (Service)	Storage	Generation	Zeroization	(R,W,X) Access by Role (CO, User)
Traffic Key	AES 128/192/256 bits	Encrypt Decrypt	External to module	external	Power-cycle and fips_set_key API Call	CO (RWX) User (RX)

Table 6 – Cryptographic Keys, Key Components, and CSPs

2.7.3 Key Generation and Input

No keys are generated by the module.

The Traffic Key is entered separately into the module's physical boundary (the R5) electronically by the CO. This is considered a key that is manually distributed via electronic entry. It is then only loaded into the module's logical boundary after successfully completing the self-tests. More details on how the Traffic Key is managed can be found in the Crypto Officer Guidance in Section 3.2 of this SP.

2.7.4 Key Output

No keys are output from the module.

2.7.5 Storage

Only the Traffic Key is stored in the module's memory, and only while the module is operational.

2.7.6 Zeroization

In normal operation, the Traffic Key is stored in Random Access Memory (RAM) and is ephemeral, so it is deleted if the host system loses power. The module has a zeroization function that overwrites the Traffic Key with zeros if invoked.

2.8 Electromagnetic Interference / Electromagnetic Compatibility

The cryptomodule conforms to the Federal Communications Commission (FCC) Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC) requirements in 47 Code of Federal Regulation, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A.

2.9 Self Tests

2.9.1Power Up Self Tests

The module performs the following tests upon power up:

- Self-tests for all validated algorithms:
  - SHA-512
  - AES-128 encryption / decryption
- SHA-512 firmware integrity test (compare against saved value)

In order to manually initiate self-tests, the module must be restarted / rebooted.

2.10 Design Assurance

Source Code

The module's source code is managed in a software repository (GIT) where the configuration of a release is tagged with a corresponding version number.

The module's compiled binary is stored in a Windows file repository and given a part number and a revision number.

Configuration Management

The compiled binary is considered a Configuration Item (CI) and is referenced from a Configuration Item Data List (CIDL) document, together with the location and the version of the source code as well as any update history and corresponding dates.

The specific CIDL part number and version is in turn referenced from the CIDL of the entire R5 AIS Transponder Firmware package, as the binary is included in the total R5 AIS Firmware package.

> **NOTE:** A CIDL is a SAAB design document defining a product (or part of product) identifiable by a 7000 xxx-series SAAB part number, which may be an assembly of different CIs.

A CIDL is updated to a new revision when the configuration of a CI within the CIDL is changed.

Document Versions

Documentation version control is manual, and each document is a CI. For example:

7000 118-123, A1, Example Document Name.docx

- *7000 118-123* is the part number
  - *7000* for Saab TransponderTech
  - *118* for "R5 product" items
  - *123* a unique identifier for the CI
- *A1* is the revision (each update has its own revision)
- *"Example Document Name"* is the Cf's Name, as assigned in the corresponding part number series registry file.

Documentation Storage and Access

All documents are stored in a product-categorized Windows file repository that is backed up nightly, with access controlled by per-project group policies, using Microsoft Active Directory (AD).

Released product document PDFs are stored in: `\\Records\Product\Product documents\`

- The R5 documentation is stored in: `…\Product documents\7000 118; R5\`
- The Word source files are stored separately under: `…\7000 118; R5\_source`

2.11 Mitigation of Other Attacks

The module does not claim to mitigate any attacks outside the requirements of FIPS 140-2.

3. SECURE OPERATION

The module automatically starts up in FIPS mode when the R5 starts up, and there is no non-FIPS mode.

3.1 Initialization

The module automatically performs the following upon startup:

- self-tests (AES-128 and SHA-512)
- generation of a fresh SHA-512 hash on its image, and comparison of that against a saved value

Should any of these tests fail, then the module will halt in an error state. Only `fips_getstatus` will work when the module is in the error state, otherwise data output is inhibited.

3.2 Crypto Officer Guidance

With reference to the definitions given in Figure 2 – Cryptographic Logical Boundary Within R5; the interface between the CO and the R5 Transponder FW application (across the physical boundary) is external to the EAISCM (cryptographic logical boundary). All interfaces across the cryptographic logical boundary to the EAISCM is done through API calls as described in Table 9 – Module APIs

The following information is applicable for key management of the Traffic Key across the physical boundary.

3.2.1 Loading the Traffic Key from a source external to the R5 physical boundary

To load a new traffic key, or to update the traffic key, a new key using the below formatting must be used. If the R5 Transponder FW accepts the command, this will result in a *fips_set_key* API call from the R5 Transponder Firmware application to the EAISCM. The transponder physical interface is conformant to IEC 61162-1/2/450.

$PSTT,13F,x,h-h,x,x,h-h*hh<CR><LF>

FIELD	FORMAT	NAME	RANGE	NOTE
1	13F	Sentence Id	13F always	
2	x	Authorization Level	Authorization level: 0 = User 1 = Administrator	
3	h-h	Password	Password string in ASCII hexadecimal form	
4	x	Link Type	1 = BFT 2 = STEDS	
5	x	Encryption Algorithm	***0 = AES** always*	
6	h-h	Encryption Key	32, 48 or 64 HEX characters, representing a 128, 192 or 256 bit key.	

Table 7 – External System Set key command

3.2.2 Removing the Traffic Key from a source external to the R5 Supreme transponder

To remove a traffic key, a command using the following format must be used. If correctly formatted, this will result in a zeroization API call to the EAISCM. The transponder physical interface is conformant to IEC 61162-1/2/450.

$PSTT,12B,h-h*hh<CR><LF>

FIELD	FORMAT	NAME	RANGE	NOTE
1	12B	Sentence Id	12B always	
2	h-h	Code	52454D4F5645414C4C4B455953 always	

Table 88 – External System Remove key command

3.3 User Guidance

Both the CO and the User access the module using APIs.

API Call	Description
`fips_encrypt`	Encrypts a block of data
`fips_decrypt`	Decrypts a block of data
`fips_getstatus`	Shows the current status of the module
`fips_set_key`	Updates the Traffic Key (0 length = zeroize)

Table 9 – Module APIs

4. ACRONYMS

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
AIS	Automatic Identification System
API	Application Programming Interface
CBC	Cipher Block Chaining
CI	Configuration Item
CIDL	Configuration Item Data List
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CCCS	Canadian Centre for Cyber Security
CSP	Critical Security Parameter
EAISCM	(SAAB) Encrypted Automatic Identification System Cryptographic Module
ECB	Electronic Codebook
EMI/EMC	Electromagnetic Interference / Electromagnetic Compatibility
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
RAM	Random Access Memory
SHA	Secure Hash Algorithm
SOLAS	Safety of Life at Sea

Table 10 – Acronym Definitions

