

REV	ECN	DESCRIPTION	DATE	APPV'D
-		Initial release	10/27/15	J. BUONASERA
A		Updated with comments from Cygnacom	12/29/15	D. CUNNINGHAM
B		Updated with comments from Cygnacom	04/11/16 06/07/16	J. BUONASERA F. CORTES
C		Updates for NIST FIPS 140-2 Recertification	09/28/21	C. SCOTT
D		Incorporate comments from NIST prior to FIPS 140-2 Recertification	12/07/21	C. SCOTT

NON-PROPRIETARY


E-FILE/FOLDER NAME: 905-E6247-86.docx			MODEL NAME: ESRVIVR (HW VERSION: 1493200-3000)		
APPROVAL SIGNATURES			TITLE: eSRVIVR Cockpit Voice and Flight Data Recorder (CVFDR) Encryption Module Security Policy		
	NAME	DATE			
PREPARED BY	JOHN W. BUONASERA	06/08/16			
CHECKED BY	JOHN S. PATRICK	06/08/16			
ENGINEER	JOHN W. BUONASERA	06/08/16	DISTRIBUTION STATEMENT This document consists of general capabilities information that is not defined as controlled technical data under ITAR Part 120.10 or EAR Part 772. © Copyright 2015-2016 L-3 Communications Corporation. This document can be freely reproduced and distributed; but only whole and intact, including this copyright notice.		
APPROVED	ROBERT S. MORICH	06/08/16			
	L3 Aviation Products, Inc. 5353 52nd St SE Grand Rapids MI 49512 USA	SIZE	CAGE CODE	DWG. NO.	
		A	25583	905-E6247-86	
			SCALE NONE	SHEET 1 of 23	
ALL SHEETS ARE THE SAME REVISION					

Table of Contents

1.1. Purpose	4
1.2. Acronyms and Abbreviations	4
1.3. References	6
1.3.1. External References	6
1.3.2. L3 AP References	6
2. ENCRYPTION MODULE.....	7
2.1. Overview	7
2.2. Module Specification.....	8
2.3. Module Interfaces	12
2.4. Security Rules.....	12
2.4.1. FIPS 140-2 Imposed Security Rules	12
2.4.2. L3 AP Imposed Security Rules	13
2.5. Roles, Authentication and Services	14
2.5.1. Non Authenticated User Role	14
2.5.2. User and Crypto Officer Roles.....	14
2.5.3. Services.....	14
2.6. Physical Security	16
2.7. Operational Environment.....	17
2.8. Cryptographic Key Management.....	17
2.9. Self-Tests	18
2.10. EMI/EMC Compatibility.....	19
2.11. Design Assurance	20
2.12. Delivery and Operation.....	20
2.13. Guidance	20
2.14. Mitigation of Other Attacks	20
APPENDIX A	22
A.1 Password Strength.....	22

LIST OF FIGURES

FIGURE 1 – LOGICAL BOUNDARY OF L3 AP eSRVIVR® CRYPTOGRAPHIC MODULE 9
FIGURE 2 - L3 AP eSRVIVR® CRYPTOGRAPHIC BOUNDARY 10
FIGURE 3 - PHYSICAL BOUNDARY OF L3 AP eSRVIVR® CRYPTOGRAPHIC MODULE..... 11

LIST OF TABLES

TABLE 1 - SECURITY LEVEL PER FIPS 140-2 SECTION 8
TABLE 2 - FIPS 140-2 LOGICAL INTERFACES OF THE L3 AP eSRVIVR® CRYPTOGRAPHIC MODULE..... 12
TABLE 3 - ROLES AND REQUIRED IDENTIFICATION AND AUTHENTICATION..... 14
TABLE 4 - STRENGTHS OF AUTHENTICATION MECHANISMS 14
TABLE 5 - INSPECTION/TESTING OF PHYSICAL SECURITY MECHANISMS 17
TABLE 6 - LISTING OF MODULE SUPPORTED KEY AND CRITICAL SECURITY PARAMETERS 17
TABLE 7 - ACCESS TYPES LEGEND 17
TABLE 8 - CSP SERVICE VERSUS CSP ACCESS 18
TABLE 9 - MITIGATION OF OTHER ATTACKS 20

Introduction

1.1. Purpose

The Cryptographic Module Security Policy includes the rules derived from the requirements of the FIPS 140-2 standard (see FIPS 140-2 Appendix C) and the rules derived from any additional requirements imposed by L3 Aviation Products (L3 AP).

This is the Cryptographic Module Security Policy for the L3 AP eSRVIVR® Cockpit Voice and Flight Data Recorder (CVFDR) Encryption Module. This Security Policy describes how the L3 AP eSRVIVR® Cockpit Voice and Flight Data Recorder (CVFDR) Encryption Module meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — (Security Requirements for Cryptographic Modules)) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at <https://csrc.nist.gov/projects/cryptographic-module-validation-program/>.

The L3 AP eSRVIVR® Cockpit Voice and Flight Data Recorder (CVFDR) Encryption Module is referred to in this document as eSRVIVR®, eSRVIVR® cryptographic module, eSRVIVR® module, cryptographic module, crypto module, firmware cryptographic module, firmware module, or module.

1.2. Acronyms and Abbreviations

AP / L3 AP	L3 Aviation Products
AES	Advanced Encryption Standard (FIPS PUB 197)
API	Application Program Interface
ASCII	American Standard Code for Information Interchange
CDF	Configuration Data File
CM	Crypto Module
CMS	Configuration Management System
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPM	Crash Protected Memory
CPU	Central Processing Unit
CRC	Cyclic redundancy check
CSP	Critical Security Parameter
CVFDR	Cockpit Voice and Flight Data Recorder
ECB	Electronic codebook mode
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
eSRVIVR	Encrypted SRVIVR Recorder
FAA	Federal Aviation Administration
FCC	Federal Communications Commission

FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
FPGA	Field-programmable gate array
FRAM	Ferroelectric Random Access Memory(Non Volatile RAM)
GHz	Gigahertz (10^9 Hertz) unit of frequency
GSE	Ground Station Equipment
KAT	Known Answer Tests (AES test vectors)
LRU	Line-Replaceable Unit
MHz	Megahertz (10^6 Hertz) unit of frequency
NIOS II	32-bit embedded-processor architecture for FPGAs.
NIST	National Institute of Standards and Technology
NVRAM	Non Volatile RAM
OFP	Operational Flight Program
OS	Operating System
RTOS	Real Time Operating System
RAM	Random Access Memory

1.3. References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

1.3.1. External References

ARINC 429-19	Mark 33 Digital Information Transfer System (DITS)
ARINC 717-14	Flight Data Acquisition and Recording System
IEEE STD 802.3	CSMA/CD Access Method and Physical Layer Specifications, Institute of Electrical and Electronic Engineers
MIL-STD-461(E)	Military standard requirements for EMI compatibility.
MIL-STD-810	Military Standard Tests for Environmental Conditions.
MIL-STD-1553	Dept. Of Defense Interface Standard for Digital Time Division Command/Response Multiplex Data
RS-422-A	Electrical Characteristics of Balanced Voltage Digital Interface Circuits, Electronic Industries Association
RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certification.
RTCA/DO-254	Design Assurance for Airborne Electronic Hardware.
CMVP website	(http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.

1.3.2. L3 AP References

L3Harris website	https://www.l3harris.com/ contains information on the full line of products from L3Harris Technologies, Inc.
8250029-1	Polysulfide sealant rubber per AMS 3281. Sealing compound,
8250029-2	Polysulfide, Class B-2 (CH), Vendor Part No. PR-1776M B-2, Mfr: PPG Aerospace - PRC DeSoto
8050417-2	Housing, Main, SRVIVR
8051587-2	LABEL, TAMPER-EVIDENT
8051599-1	LABEL, HARDWARE, ESRVIVR
AMS-3281	Sealing Compound, Polysulfide (T) Synthetic Rubber for Integral Fuel Tank and Fuel Cell Cavities, Low Density

2. Encryption Module

2.1. Overview

The eSRVIVR® CVFDR is a flight recorder that enables the storage of encrypted or plain text voice and flight data to a Crash Protected Memory (CPM). The eSRVIVR® cryptographic module is firmware code that performs encryption for the CVFDR. This data is recorded into a primary/backup pair of up to eight (8) physical and logical data partitions. The organization of the data and whether a partition is encrypted in the CPM is defined per partition pair via a factory-loaded Configuration Data File (CDF) that is developed by L3 AP to customer specifications. The CDF resides outside of the cryptographic module boundary and controls which data is encrypted by the cryptographic module and which data is recorded and stored into which partition. The CDF file is configurable, but it cannot be changed by a user. The CDF file and the OFP can only be uploaded at the factory.

The eSRVIVR® Ground Station Equipment (GSE) interface (*eSIS-2*) allows Application Interface Software operators to send commands to perform security functions related to loading and zeroizing keys used for encrypting, and provides methods of decrypting stored voice and flight data using the FIPS 197 certified AES encryption algorithm.

2.2. Module Specification

The encryption module (module version 1.0) is a firmware module composed of a set of functions for key management including loading, storage, authentication, diagnostics, and encryption. These functions are implemented entirely in the C programming language. The encryption module is a part of the eSRVIVR® firmware running on the processor contained in the CPU board. The cryptographic module is compiled into the generated software images and loaded onto the processor at boot time from the non-volatile memory.

Per FIPS PUB 140-2, the eSRVIVR® cryptographic module is classified as an embedded multi-chip firmware cryptographic module. The module meets overall Level 2 FIPS 140-2 requirements as detailed in Table 1.

The encryption module is enabled on the eSRVIVR® CVFDR on an as-defined basis for individual recording partitions as defined by the Configuration Data File (CDF) and can only operate in a single authorized mode (FIPS Mode). In this mode of operation, the Data recorder receives data that is not encrypted, then using the AES algorithm encrypts the data with the installed key for those CPM partitions that are defined to be encrypted. Operators can not alter whether partition data will be encrypted. This will be done at the factory only, as defined by the Configuration Data File.

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

TABLE 1 - SECURITY LEVEL PER FIPS 140-2 SECTION

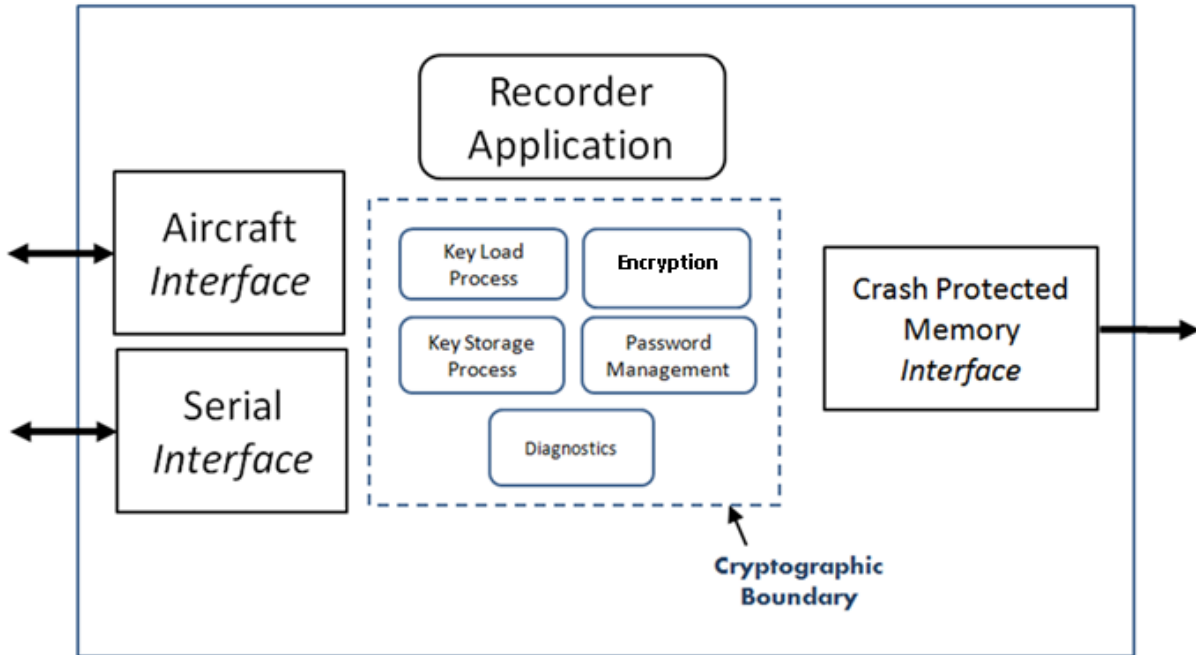


FIGURE 1 – LOGICAL BOUNDARY OF L3 AP eSRVIVR® CRYPTOGRAPHIC MODULE

FIGURE 1 above depicts the firmware and the logical boundary of the eSRVIVR® cryptographic module. The cryptographic module consists of the key load processes, key storage processes, password management, and AES Encryption Engine.

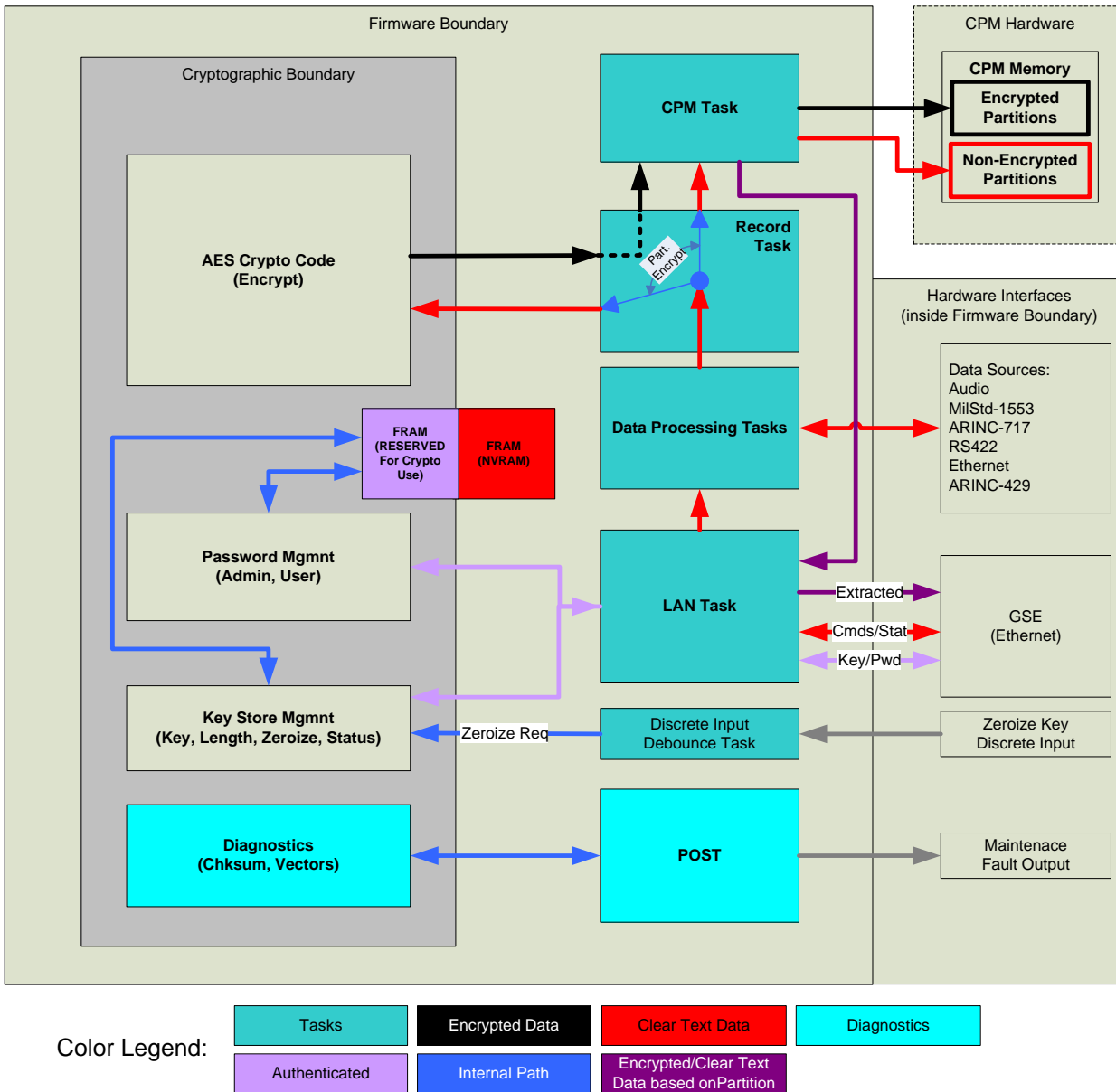


FIGURE 2 - L3 AP ESRVIVR® CRYPTOGRAPHIC BOUNDARY

FIGURE 2 above depicts the logical interfaces and the data flows of encrypted and plaintext data, keys, and CSPs related to the functional tasks of the eSRVIVR® cryptographic module.

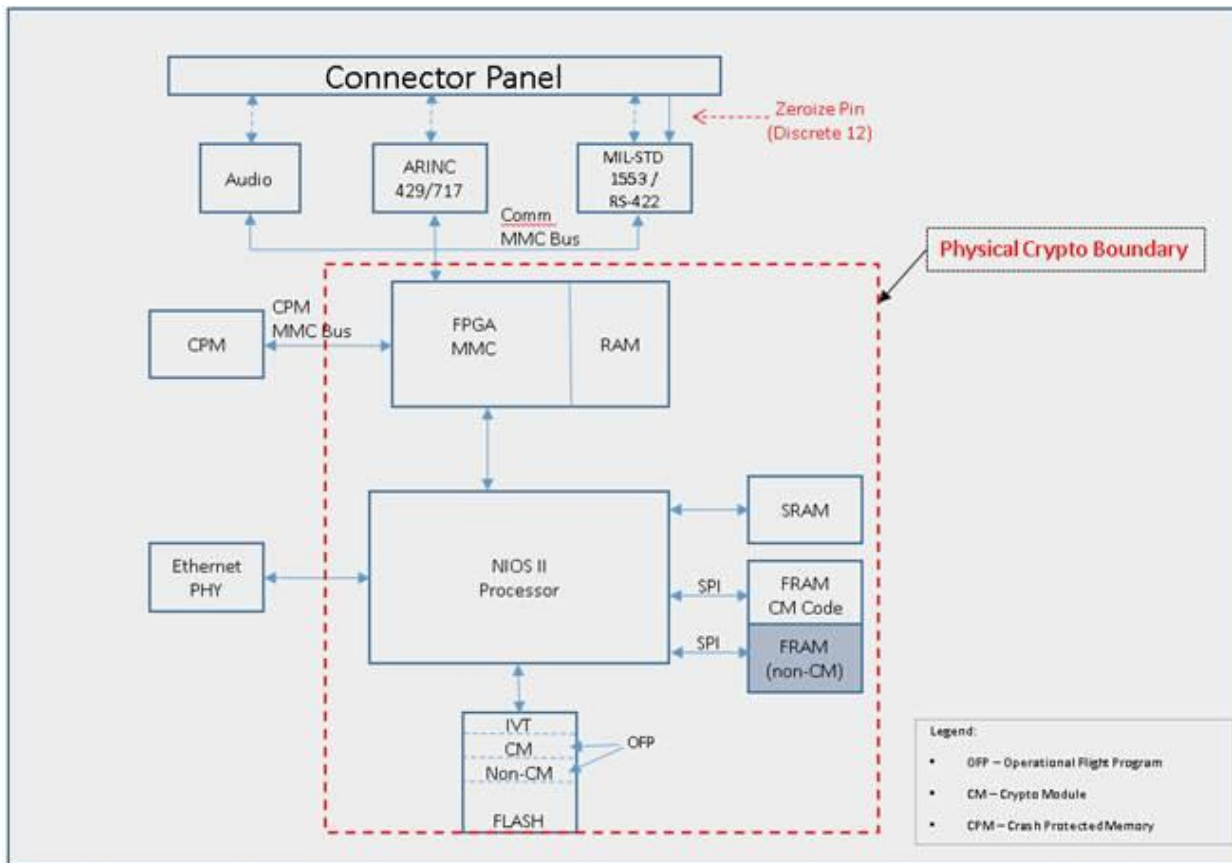


FIGURE 3 - PHYSICAL BOUNDARY OF L3 AP eSRVIVR® CRYPTOGRAPHIC MODULE

FIGURE 3 depicts the Processor card LRU and the physical boundary of the eSRVIVR® cryptographic module. Upon boot up, once the firmware integrity and Known Answer Tests are passed and a valid key is found, the cryptographic module becomes operational. If the startup tests fail or a valid encryption key is not available, the cryptographic module is disabled and the module discontinues all output (except status output) from the cryptographic module.

2.3. Module Interfaces

The cryptographic module’s physical interfaces of the embedded multi-chip module lie on its physical cryptographic boundary. They connect from the Module to the CVFDR’s Aircraft interfaces, GSE interfaces, and the Crash Protected Memory (CPM) memory interfaces which are physical connections of the CVFDR and not the Crypto Module’s interfaces.

A processor status word bit will be set when in the error state and it will be clear when in normal operation. The logical interface to the cryptographic module is the API (function calls) to the module.

All of the physical ports Table 2 are separated into logical interfaces defined by FIPS 140-2.

Logical Interface of the Module	Module Physical Port	FIPS 140-2 Logical Interface
Encryption API	Aircraft/Serial Interface (ARINC-429,MIL-STD 1553, A/D, Ethernet, RS-422)	Data Input Interface
Serial Messages API	Aircraft/Serial Interface (Ethernet/RS-422)	Data Input Interface
Serial Messages API	Serial Interface (Ethernet/RS-422)	Data Output Interface
Crash Protected Memory Interface	CPM Interface (CPM MMC Bus)	Data Output Interface
Serial Messages API	Aircraft/Serial Interface (Ethernet/RS-422)	Control Input Interface
Serial Messages API	Aircraft/Serial Interface (ARINC-429,MIL-STD 1553, A/D, Ethernet, RS-422)	Status Output Interface
Encryption API	Zeroize Input Discrete Pin	Control Input Interface
Encryption API	CVFDR Maintenance Output Pin	Status Output Interface
Not Applicable	Power pins in ‘Aircraft connector’ and external battery	Power Interface

TABLE 2 - FIPS 140-2 LOGICAL INTERFACES OF THE L3 AP ESRVIVR® CRYPTOGRAPHIC MODULE

2.4. Security Rules

The cryptographic module’s security rules are broken up into those imposed by FIPS 140-2, and those imposed by L3 AP.

2.4.1. FIPS 140-2 Imposed Security Rules

1. The Cryptographic Module inhibits all data output whenever an error state exists and during self-tests.
2. The Cryptographic Module does not perform any cryptographic functions while in an error state.

3. The Cryptographic Module logically disconnects the data output path from the circuitry and all processes when performing key zeroization.
4. The Cryptographic Module enforces Role-Based authentication.
5. The Cryptographic Module supports 2 Authenticated Roles; a User role and a Crypto-Officer role.
6. The Cryptographic Module uses authentication for all commands that require authentication.
7. To help prevent brute-force attacks, the Cryptographic Module enforces a minimum password length of eight (8) ASCII printable characters.
8. To help prevent brute-force attacks, the Cryptographic Module enforces a maximum password length of fifteen (15) ASCII printable characters.
9. To help prevent brute-force attacks, the Cryptographic Module enforces a minimum number of character types required in the password. At least one each of the following character types are required:
 - A symbol character (!@#\$%^&*,...)
 - A number character (0-9)
 - An upper case character (A-Z)
 - A lower case character (a-z)

The probability of a successful random attempt is one in 3,025,989,069,143,040. See Appendix A for more details on how this probability is calculated.

10. To help prevent brute-force attacks, the Cryptographic Module enforces a hard ten (10) minute lockout after three (3) failed login attempts within a minute. The lockout will be persistent across hard or soft reboots. This ensures that random attempt success rate will be less than 1 in 100,000 in one (1) minute.
11. The Cryptographic Module protects keys from unauthorized disclosure, modification, and substitution.
12. The Cryptographic Module does not output Authentication data.
13. Key data is stored in a key record that includes a CRC over all of the fields to detect data corruption.
14. The Cryptographic Module denies access to the plaintext cryptographic key contained within the module.
15. The Cryptographic Module provides the capability to Zeroize the Cryptographic key stored in Non Volatile Memory within the module.

2.4.2. L3 AP Imposed Security Rules

1. The Cryptographic Module does not support multiple concurrent users.
2. The Cryptographic Module can only be reset to factory defaults by the Crypto Officer.
3. All other Cryptographic module services are suspended during key loading, including encryption.
4. Each command that requires authentication by the Cryptographic Module must be individually authenticated.

2.5. Roles, Authentication and Services

The module enforces operators to assume a role and supports two Authenticated Roles: a Crypto Officer role and an Authenticated User role. The cryptographic module implicitly assumes the Crypto Officer role to encrypt any data received from the aircraft as previously enabled by the Crypto Officer.

An operator assumes the User or Crypto Officer role based on the authentication process. For example: After startup, to load a new AES key, the operator is required to use the Crypto Officer password with the load key command and will assume the Crypto Officer role. Once this password is matched, the operator is designated as a Crypto Officer for the duration of the function's execution.

There are limits or requirements on password length (See Section 2.4.1, FIPS 140-2 Imposed Security Rules). Since this authentication is a FIPS level-2 compliant authentication, the passwords will be used for role based authentication and will not be assigned for identity based authentication. Descriptions and responsibilities for the Crypto Officer and User roles are described below.

Role	Type of Authentication	Authentication Data
Crypto Officer (GSE)	Role based Password (explicit)	95 ASCII printable characters, (see rules in Section 2.4.1)
User (GSE)	Role based Password	95 ASCII printable characters, (see rules in Section 2.4.1)

TABLE 3 - ROLES AND REQUIRED IDENTIFICATION AND AUTHENTICATION

Authentication Mechanism	Strength of Mechanism
Password (Random Attempt)	One in 3,025,989,069,143,040
Password (Random Attempt success rate)	Persistent Hard ten (10) minute lockout after a total of three (3) failed login attempts within a minute.

TABLE 4 - STRENGTHS OF AUTHENTICATION MECHANISMS

The values shown in TABLE 4 exceed the FIPS 140-2 requirements for each random attempt (1 in 1,000,000) and for multiple random attempts (1 in 100,000).

2.5.1. Non Authenticated User Role

Although some commands do not require authentication, there are no Non-Authenticated Roles.

2.5.2. User and Crypto Officer Roles

The User and Crypto Officer (Authenticated Users) can execute all commands transmitted via the Aircraft, Serial and GSE interfaces including API message IDs authenticated if a valid key has been loaded.

The User and Crypto Officer (Authenticated Users) can each set their own password.

Except for the "Zeroize Key" command, only the Crypto Officer can execute commands that change the security configuration of the L3 AP eSRVIVR® Cockpit Voice and Flight Data Recorder.

Once the AES key is loaded, the received data can utilize the cryptographic functionality of the eSRVIVR, which is assuming an implied Crypto Officer Role.

2.5.3. Services

Key zeroization will be performed when the Zeroize discrete pin generates an interrupt, or when a serial “Zeroize Key” command message is received. Key zeroization will also be performed when a “Reset to Factory” command message is received.

The “Zeroize Key” command is used to delete the current cryptographic key that is stored in the recorder. This command is not password protected and can be sent by any operator. The “Zeroize Key” command is unprotected by design. All of the recorder’s data encryption capability is disabled after this command is used. This command is intended for both Aircraft and GSE use.

The “Encrypt” command is used within the Data Recorder by the Crypto Officer Role Implicitly, if the unit is keyed. This command is not separately callable.

The “Set Crypto Key” command is used to set the cryptographic key that is required for data encryption. This command is intended to be used by the Crypto Officer. Therefore, the Crypto Officer password must be provided in order to use this command successfully. In addition, this command must be used at least once before any encryption can take place. This command is intended for GSE use.

The “Set Password” command is used to set the password of the specified user (either Crypto Officer or User). Note that the Crypto Officer can set the password for either the Crypto Officer or the User, but the User can only set the password for the User. This command is password protected so a valid Crypto Officer password or valid User password must be provided for this command to be successful. This command is intended for GSE use.

The “Validate Password” command is used within other API calls that require authentication before it can execute. This command is not separately callable.

The “Get Crypto Status” command is used to get the status of various crypto items residing in the recorder. These items include the current encryption algorithm that is being used to encrypt the data, the version of the encryption algorithm, the total number of failed login attempts, and the total number of valid login attempts for all roles. This command is password protected so a valid Crypto Officer password or valid User password must be provided for this command to be successful. This command is intended for GSE use.

The “Reset to Factory” command is used to reset the cryptographic information in the recorder to the same state as it was when it was manufactured. This command will Zeroize the cryptographic key so that all further data encryption is disabled. A new key must be set using the “Set Crypto Key” command before encryption is enabled. It will also reset the Crypto Officer password and the User password to their factory defaults. This command is intended to be used by the Crypto Officer. Therefore, the Crypto Officer password must be provided in order to use this command successfully. After successful completion of this command, the default factory Crypto Officer password must be provided for any command that needs a Crypto Officer password. This command is intended for GSE use.

The “Perform Self-Tests” command forces the entire Recorder to restart and re-execute the Internal Built in Test (IBIT). This command is not password protected and can be sent by any operator. See the Self-Test section for a description of the test.

The “Retrieve File Segment Auth” command is used to access the audit data saved in the Crypto Log Information Partition. These items include the time logged events for: Encryption Start, Encryption Stop, Crypto Officer Login, Crypto Officer Login Fail, Crypto Officer Password Change, Crypto Officer Password Change Fail, User Login, User Login Fail, User Password Change, User Password Change Fail, Crypto Key Load, Crypto Key Load Fail, and Crypto Key Zeroize. This command is password protected so a valid Crypto Officer password must be provided for this command to be successful. This command is intended for GSE use.

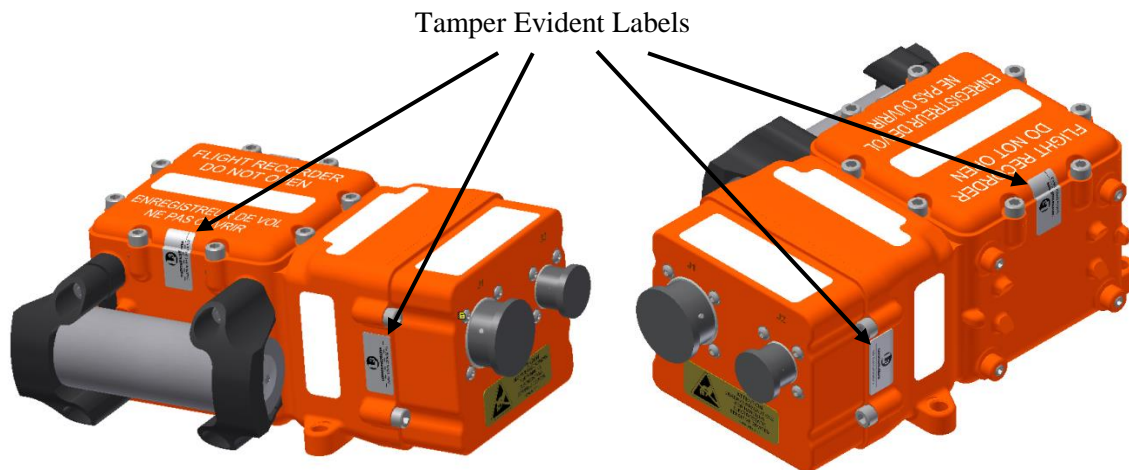
2.6. Physical Security

The physical embodiment of the firmware module, in FIPS terminology, is defined as a multi-chip embedded cryptographic module. The module's physical embodiment is made of all production-grade components and is enclosed in a stainless steel housing, Part Number: 8050417-3 (Housing, Main, SRVIVR), which surrounds all of the module's internal components, including all hardware and firmware.

The exterior components are painted to meet DO-160 or MIL-STD-810 environmental standards as applicable.

A polysulfide sealant rubber, per AMS 3281 will provide the ability to detect any physical tampering by sealing any entry points on the outside surface of the CSMU. The entire CSMU is environmentally sealed by the application of polysulfide around the perimeters of the front cover and top cover, including all seams, screws, and connectors, providing an environmentally seal around the entire CSMU housing thus blocking any fluids, humidity, sand and dust. In addition, the MIL-C-38999 Series III connectors environmentally seal the CSMU power and communication interfaces.

There will be four tamper evident labels (See Reference Documents 8501587-2 (LABEL, TAMPER-EVIDENT) and 8501599-1 (LABEL, HARDWARE, ESRVIVR) used to meet the tamper evidence requirements of FIPS 140-2 along with the environmental standards of DO-160 or MIL-STD-810 (as applicable).



The unit will often be installed in hard to access locations on aircraft that do not allow access other than at unit installation, or when maintenance is required. Therefore, inspection to look for signs of physical tampering will only be performed during product installation and maintenance.

The operator is never allowed to perform any maintenance that involves opening the case. All such maintenance shall be performed at the factory. Units that display evidence of tampering shall be declared defective, and returned to the factory. The investigation of tampering will be treated as a maintenance defect to be serviced by authorized personnel at the factory.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Stainless steel housing	Installation/Removal	Treat as a Maintenance Defect.

Polysulfide sealant rubber	Installation/Removal	Treat as a Maintenance Defect.
Tamper evident label	Installation/Removal	Treat as a Maintenance Defect.

Note: * - For Inspection/Test Guidance, see the Installation/Maintenance manual.

TABLE 5 - INSPECTION/TESTING OF PHYSICAL SECURITY MECHANISMS

2.7. Operational Environment

The operational environment is non-modifiable and thus not applicable to FIPS 140-2, section 4.6.1 for this firmware module. The cryptographic module in the eSRVIVR® Cockpit Voice and Data Recorder (Hardware version: 1493200-3000) runs on an embedded Nucleus Plus 1.15.6 Real-Time Operating System (RTOS) by Mentor Graphics.

2.8. Cryptographic Key Management

The module implements the following FIPS-approved algorithms:

- AES-128, AES-192, AES-256 (ECB mode, encryption only) – FIPS 197 Validation #3754.

The module does not implement any non-approved algorithms.

CSP	Key Type	Generation	Storage	Use
AES Key	128, 196, 256 bit AES key	Externally generated and electronically loaded via the SRVIVR GSE Interface.	Held in volatile memory in plaintext. Stored in non-volatile memory and retrieved on reboot.	Encrypts voice and/or flight data per configuration, and is not output from the module.
User/Crypto-Officer Password	8-15 character ASCII password	Entered into the module SRVIVR via the GSE over the Serial Interface.	Stored in non-volatile memory as plaintext.	Used for User & CO Role Authentication.

TABLE 6 - LISTING OF MODULE SUPPORTED KEY AND CRITICAL SECURITY PARAMETERS

Crypto Access Type	Description
x - Role	Applies to specified role.
s - Store	Storage in volatile and non-volatile memory.
u - Use	Uses Key and CSPs internally for encryption / decryption services.
z - Zeroize	Zeroizes the AES Key.

TABLE 7 - ACCESS TYPES LEGEND

Service (API Calls)	CSP	Role	Type of Access to CSP
---------------------	-----	------	-----------------------

	AES Key	User Password	Crypto-Officer Password	User Role	Crypto-Officer Role	No Role Required	
Validate Crypto-Officer Password (used within other API calls)			u		x		(R)ead Password
Set Password (Crypto Officer)			u,s		x		(W)rite Password
Validate User Password (used within other API calls)		u		x	Not Used ¹		(R)ead Password
Set Password (User)		u,s	u ¹	x	x		(W)rite Password
Set Crypto Key	s		u		x		(W)rite Key
Zeroize Key	z					x	(W)rite Key
Encrypt	u				x ²		(E)xecute
Reset to Factory	z		u		x		(W)rite Password and Key
Perform Self-Tests						x	(R)ead Key (internally)
Get Crypto Status		u	u	x	x		(R)ead Password
Retrieve File Segment Auth			u		x		(R)ead Password

Notes:

1 – The Crypto Officer password is validated when the Crypto Officer changes the user password.

2 – All CM encryption falls under the Crypto Officer Role Implicitly, if the unit is keyed.

TABLE 8 - CSP SERVICE VERSUS CSP ACCESS

2.9. Self-Tests

If any of the self-tests fail, the module will output an error indication on the CVFDR Maintenance pin or the Data Fault pin (see below) and the Crypto Module in the eSRVIVR® will stop all cryptographic operations and discontinue operating in normal mode (encryption of voice and flight data halts and no data designated for an encrypted data partition is recorded).

The eSRVIVR® Crypto Module performs the following self-tests:

1. Conditional tests
 - There are not applicable conditional tests.
2. Power up and on-demand tests

- Cryptographic Algorithm Known Answer Tests (KAT): The algorithms (AES-128, AES-192, and AES-256 in ECB mode) are tested by using a known key, known plaintext data, and known encrypted data. The plaintext data is then encrypted and compared with the known encrypted data; the test passes if the final encrypted data matches the known encrypted data, otherwise it fails. If the Cryptographic Algorithm Known Answer Tests (KAT) fail, the eSRVIVR® Crypto Module asserts a status bit (for the Report Status command) which will drive the CVFDR Maintenance pin. The module then transitions to the non-recoverable error state.
- Firmware Integrity Test: Upon startup the cryptographic module performs a 16-bit CRC of the program memory where it resides and any associated constants stored in memory as part of its self-tests. A failure of the cryptographic module's CRC value compared to the expected CRC value will assert a status bit (for the Report Status command) which will drive the CVFDR Maintenance pin. The module then transitions to the non-recoverable error state. The eSRVIVR uses an industry standard CRC-16 (CCITT) polynomial ($X^{16} + X^{12} + X^5 + 1$) for authentication of Crypto module code and constant data. The CRC-16 algorithm is implemented via a table lookup method.
- Key CRC Test: Any failure that occurs while trying to validate the cryptographic key will cause an assertion of a status bit (for the Report Status command) which will drive the Data Fault pin. The module then transitions to the recoverable error state.

Once the module is in the power off state, powering the unit on will initiate the power-on self-tests. All of the power-on self-tests are run as soon as possible after the system has been initialized. This occurs before any of the data collection tasks that use the crypto module are running. None of the self-tests require any inputs or actions by the operator.

There are two ways to check for the success or failure of the self-tests:

- 1) Output Pin Interface – Two pins provide an electrical means of checking for self-test failures:
 - a. CVFDR Maintenance Pin – Pin 18 of the J-1 connector can be used to check for the success or failure of the Known Answer Test and the Firmware Integrity Test. Pin 18 will be at the standard ground voltage level (i.e. asserted) if the Known Answer Test or the Firmware Integrity Test has failed. Pin 18 will be open/not connected (i.e. not asserted) if the Known Answer Test and the Firmware Integrity Test have passed. Note that this pin is used to report the success or failure of crypto-specific self-tests as well as the non-crypto self-tests so an assertion on this pin doesn't necessarily mean that only the Known Answer Test or the Firmware Integrity Test has failed.
 - b. Data Fault Pin – Pin 19 of the J-1 connector can be used to check for the success or failure of the Key Load Test. Pin 19 will be at the standard ground voltage level (i.e. asserted) if the Key Load Test failed. Pin 19 will be open/not connected (i.e. not asserted) if the Key Load Test passed. Note that this pin is used to report the success or failure of crypto-specific self-tests as well as the non-crypto self-tests so an assertion on this pin doesn't necessarily mean that only the Key Load Test has failed.
- 2) Report Status Command – The “Report Status” GSE command can be used for a detailed report of the success or failure of the self-tests. The crypto-specific self-test results are part of the “Processor” status word. Results are given for the following tests:
 - a. Crypto Algorithm (Known Answer Test) Failure
 - b. Crypto CRC Failure
 - c. Crypto Key Load Failure

2.10. EMI/EMC Compatibility

The eSRVIVR® Data Recorders meets MIL Standard 461F emissions requirements that are more stringent than the level 2 - EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use)

The L3 AP encryption module meets all applicable FCC requirements by similarity to the MIL-STD-461F radiated emissions (RE102) testing.

The applicable FCC Emissions requirement (for radio) specifies that the radiated coverage runs from 30 MHz to 1 GHz which aligns with the much broader limits of MIL-STD 461F in that spans the frequency range 10 kHz – 18 GHz.

2.11. Design Assurance

Microsoft Visual SourceSafe CMS is used as the configuration management system to control the source code versions and releases of the L3 AP eSRVIVR® cryptographic module. The CMS automatically records modifications made to the source code set, noting the date and time. The system retains all intermediate versions of the source code back to the original implementation. Each file checked into the CMS has a version number that is initialized to 1. This version number is incremented by 1 each time the file is revised (by first checking out the file, revising the file, and then checking the file back into CMS). The information tracked by the CMS allows the engineering team to identify the specific version of each file that is required to build an executable configuration. The CMS system has facilities for restricting or completely eliminating modifications to controlled items, which are used to control configurations. This mechanism, combined with a regular backup routinely administered by systems administration staff, ensures the ability to retrieve and build any given firmware configuration.

The hardware drawings and circuit schematics are maintained in a separate archive. This archive keeps tracks of the version number and date of each hardware drawing and schematic. Every new file (drawing or schematic) is assigned a unique version number. The version number starts at 1 and is incremented when newer versions are added to the archive. All versions of a file are kept in the archive and are never deleted. The access to the archive is limited to a few authorized personnel that can retrieve files and add to the archive. Once stored in the archive, a file cannot be modified and stored with the same version number.

The Project-level Integrated Compliance Management System is used as the primary interface between the Project Team, Customer and/or the FAA for the L3 AP eSRVIVR® cryptographic module. This Web-based system is comprised of a SecureWeb Management System, Problem Reporting Management System, Document Review Management System, Meeting and Action Item Management System, Requirements Traceability Management System and Coverage Analysis Management System. All systems were specifically developed to show compliance with the objectives of DO-178B and DO-254.

The Microsoft SharePoint web application platform is used for editing and tracking changes to documents. A SharePoint database record is kept for each document; it also provides a hyperlink to the document. The system maintains and keeps track of separate versions of every file that is stored in the database.

2.12. Delivery and Operation

The L3 AP eSRVIVR® CVFDR is delivered with all necessary firmware installed and configured for proper operation. The operator is required to turn the Data Recorder on and follow the operating instructions from the user's guide to operate the device.

2.13. Guidance

Administration and maintenance of the L3 AP eSRVIVR® CVFDR is accomplished via the commands listed in section 2.5. The L3 AP GSE software package (eSIS-2) provides an easy way for the Crypto Officer or the User to execute these commands. Details of the wiring needed to power, run, and monitor the L3 AP eSRVIVR® CVFDR is given in the user's guide.

2.14. Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

TABLE 9 - MITIGATION OF OTHER ATTACKS

The eSRVIVR® cryptographic module does not employ security mechanisms to mitigate specific attacks.

APPENDIX A

A.1 Password Strength

The strength of the passwords used to gain access to the Crypto-Officer role or the User role is calculated as shown below. To calculate the probability of a successful random attempt, we find cardinality of the union of n sets:

- 1) Start with 95 ASCII printable characters for the principle of inclusion–exclusion (95^8)
- 2) Next, exclude (subtract):
 - a. All passwords with no lowercase characters (69^8)
 - b. All passwords with no uppercase characters (69^8)
 - c. All passwords with no digit characters (85^8)
 - d. All passwords with no special characters (62^8)
- 3) Next, include (add):
 - a. All passwords with no lowercase characters AND no uppercase characters (43^8)
 - b. All passwords with no lowercase characters AND no digit characters (59^8)
 - c. All passwords with no lowercase characters AND no special characters (36^8)
 - d. All passwords with no uppercase characters AND no digit characters (59^8)
 - e. All passwords with no uppercase characters AND no special characters (36^8)
 - f. All passwords with no digit characters AND no special characters (52^8)
- 4) Next, exclude (subtract):
 - a. All passwords with only lowercase characters (26^8)
 - b. All passwords with only uppercase characters (26^8)
 - c. All passwords with only digit characters (10^8)
 - d. All passwords with only special characters (33^8)
- 5) Result: $95^8 - (69^8 + 69^8 + 85^8 + 62^8) + (43^8 + 59^8 + 36^8 + 59^8 + 36^8 + 52^8) - (26^8 + 26^8 + 10^8 + 33^8) = 3,025,989,069,143,040$

The probability of a successful random attempt is one in 3,025,989,069,143,040.