GENERAL DYNAMICS
Decision Systems

Assembly

Crypto Module

FIPS 140-2 Non-Proprietary
Security Policy

Level 2 Validation

November 2003

Table of Contents

List of Tables

List of Figures

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Assembly Crypto Module (ACM) (HW P/N 01-P35200T004 Version E001, FW Revision C) from General Dynamics Decision Systems. This security policy describes how the Assembly Crypto Module meets the security requirements of FIPS 140-2. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

This document deals with the capabilities, protection, and access rights provided by the ACM.

Overview

The ACM is designed to meet the overall requirements applicable to Security Level 2 as defined in FIPS PUB 140-2. The individual security levels are listed in Table 1 below.

Security Area for FIPS 140-2	Level
Cryptographic Module	2
Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	N/A
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 1: Validation Level

The ACM performs the following FIPS Approved algorithm:
- Triple-DES

Module Interface

The cryptographic boundary of the ACM is defined as the metal case enclosing all of the system components. The module is accessible through one connector partitioned into four separate quadrants. Figure 1 shows the ACM.

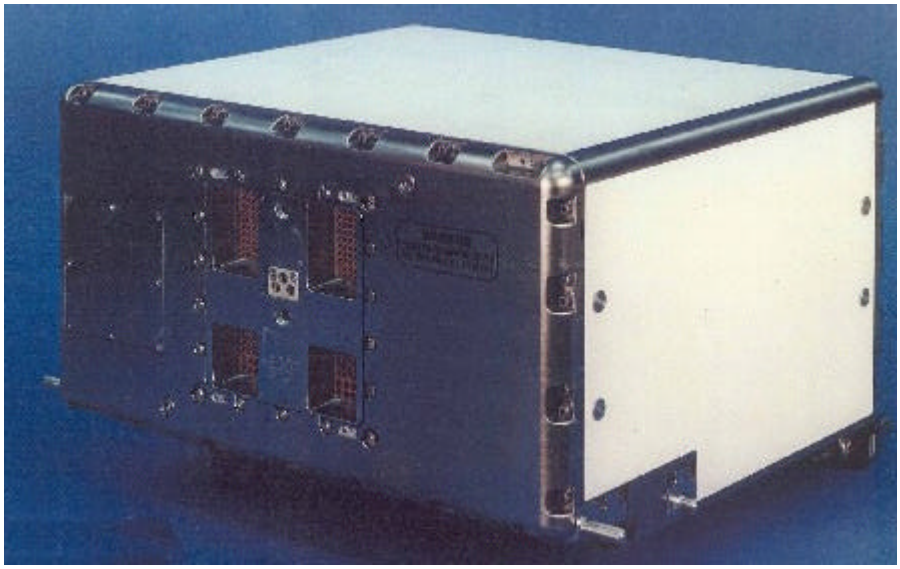

Figure 1: Assembly Cryptographic Module (ACM)

Roles, Services and Authentication

The ACM supports a Crypto Office Role and a User Role. Role-based authentication is used for both roles.

Role	Type of Authentication	Authentication Data
Crypto Officer	Role Based	Password
User	Role Based	TDES Key

Table 2: Roles and Required Identification and Authentication

The Crypto Officer accesses the module via the external connector by commands used only by the Crypto Officer. The Crypto Officer authenticates with a password and is able to configure the module.

The User role accesses the module via the external connector by command. The User authenticates with encrypted data.

The module has non-authenticated services that do not affect any critical security parameters, and these services are available to all roles. The non-authenticated services include polling for ACM status and the ability to command the ACM to perform a self-test and report the results.

Role	Authorized Services
User	Decryption
Crypto Officer	Initialize Zeroize Update CSPs
Non-Authenticated Services	Enable/Disable Decryption Key Index Status Self-Test

Table 3: Services Authorized for Roles

Role/Service	Cryptographic Keys and CSPs	Types of Access
User/ Decryption	TEK KEK Password	None None None
Crypto Officer/ Initialize	TEK KEK Password	None Write Write
Crypto Officer/ Zeroize	TEK KEK Password	None None None
Crypto Officer/ Update CSPs	TEK KEK Password	None None Write
Non-Authenticated Services/ Enable/Disable Decryption Key Index Status Self-Test	TEK KEK Password	None None None

Table 4: Access Rights within Services

Authentication Mechanism	Strength of Mechanism
Password	64 bits
TDES Key	112 bits

Table 5: Strengths of Authentication Mechanisms

Physical Security

The ACM is a multi-chip standalone cryptographic module designed to meet the Level 2 physical security requirements as defined in FIPS PUB 140-2. The module is an opaque sealed container made of hardened aluminum alloy. The front and rear box covers are attached with screws that are staked with epoxy, providing tamper evidence. One external connector provides access to the module. The unit has no doors or removable covers.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Epoxy on Screws	Yearly	Check to ensure epoxy on the box screws is completely intact, undisturbed, and securely bonded to the chassis

Table 6: Inspection/Testing of Physical Security Mechanisms

Mitigation of Other Attacks

This module does not implement mechanisms to mitigate any other specific attacks.

Acronyms

ACM	Assembly Crypto Module
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
TDES	Triple Data Encryption Standard