IMAG Technologies, Inc.

5270A IMPERIAL ST. BURNABY BC CANADA V5J 1E4 (604) 430-6460 FAX: (604) 430-6475

TIMAC Module Version 1.0

Security Policy

for

FIPS 140-2
Cryptographic Module

Level 3 Validation

by

Alex Jiang

January 18, 2005

Document Version 1.0

Table of Contents

List of Abbreviations

AES	Advanced Encryption Standard
CFB	AES Electronic Codebook mode
ECB	AES Cipher Block Chaining mode
CBC	AES Cipher Feedback mode
UART	Universal Asynchronous Receiver/Transmitter
I^2C SDA	Inter-Integrated Circuit Bus Serial Data Line
I^2C SCL	Inter-Integrated Circuit Bus Serial Clock Line
GND	Ground
SPI MISO	Serial Peripheral Interface Master-In Slave-Out
SPI MOSI	Serial Peripheral Interface Master-Out Slave-In
SPI CLK	Serial Peripheral Interface Clock
SPI /SS	Serial Peripheral Interface Slave Selection
PIN	Personal Identification Number
IV	AES Initial Vector
CSP	Critical Security Parameter
CO	Cryptographic Officer
UPIN	User role's Personal Identification Number
COPIN	Cryptographic Officer role's Personal Identification Number
EEPROM	Electrically-Erasable Programmable Read-Only Memory
CRC	Cyclic Redundancy Check

1. Module Overview

The TIMAC (P/N EM01-01 Rev. 1.1, FW Version 1.0) is a multi chip embedded cryptographic module targeted for FIPS 140-2 Overall Security Level 3. The primary purpose of this device is to provide inline encryption and decryption for serial communication data.

The physically contiguous cryptographic boundary is defined as the outer perimeter of a potted daughter board PCB that completely encapsulates the module's circuitry, an 8-pin and 9-pin connectors are exposed as interfaces. All of the TIMAC module's components are standard production grade. The image below depicts the cryptographic boundary and shows the interfaces:

Figure 1 – Image of the Cryptographic Module

2. Security Level

The TIMAC module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

The TIMAC module only supports an Approved mode of operation, and does not provide a non-FIPS mode. The Approved mode of operation indicator can be obtained through the "Get Status" service (described in Section 6 below) where the version number of the cryptographic module is returned along with a "FIPS Mode" string.

The TIMAC module supports a single cryptographic algorithm, the FIPS Approved Advanced Encryption Standard (AES) encryption algorithm. The AES algorithm can function in 3 modes with 128 bit key: Electronic Codebook mode (ECB), Cipher Block Chaining mode (CBC) and Cipher Feedback mode (CFB).

The mode of encryption is selected as part of the "Select Cipher Mode" service (described in Section 6 below).

4. Ports and Interfaces

The TIMAC module has one 8-pin connector and one 9-pin connector that support the following physical and logical interfaces:

Table 2: TIMAC module Interfaces and Pin Assignment

Interface pin #	Interface Type	Function
1	Data Input	UART 0 Data Input
2	Data Output	UART 0 Data Output
3	Status Indicator	Module status indicator
4	Power	GND (Ground)
5	Power	Vcc, supply voltage
6	Status Indicator	AES Mode indicator
7	Status Indicator	Fatal Error Alarm
8	Power	GND (Ground)
9	Data Output	UART 1 Data Output
10	Data Input	UART 1 Data Input
11	CSP Input	I^2C SDA
12	Control Input	I^2C SCL
13	Power	GND (Ground)
14	Status Output	SPI MISO
15	Control Input, Data Input	SPI MOSI
16	Control Input	SPI CLK
17	Control Input	SPI /SS

5. Identification and Authentication Policy

The TIMAC module enforces an Identity-based operator authentication before providing any of the TIMAC's security relevant services. The User or Cryptographic Officer must assert the desired role, and provide the correct username and 128 bit Personal Identification Number (PIN) to be authenticated by the TIMAC module. Re-authentication is required when the module's power is cycled.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Mechanism
User	Identity-based operator authentication	Username and 128 bit PIN
Cryptographic-Officer	Identity-based operator authentication	Username and 128 bit PIN

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and PIN	The probability that a random attempt will succeed or a false acceptance will occur is 1/ 2^128 which is far less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is (3*40) / 2^128, which is less than 1/100,000.

6. Access Control Policy

The TIMAC module supports both a User and a Cryptographic Officer role. An authenticated User is provided with all of the services necessary for secure data transport, while an authenticated Cryptographic Officer can command the TIMAC to zeroize the TIMAC's CSPs.

Table 5: Services Authorized for Roles

Role	Authorized Services
User	Authenticate Request: This service is used to gain authentication. Status Request: This service shows the status of the TIMAC module. Logout Request: This service unauthenticates the current User. Reload IV Request: This service sets the IV back to an initial value. Module Reset Request: This service performs a software reset, and executes the suite of TIMAC self-tests Mode Selection Request: This service configures the cipher mode to be used within AES (e.g. ECB, CBC, CFB). Baudrate Selection Request: This service selects the baud rate to be used for data communication. AES Encrypt: This service AES encrypts plaintext data passed into the TIMAC module using the TIMAC's AES key. AES Decrypt: This service AES decrypts the ciphertext data passed into the TIMAC module using the TIMAC's AES key. Flush Data Buffer Request: This service flushes the cryptographic module's data buffers.
Cryptographic Officer	Authenticate Request: This service is used to gain authentication. Status Request: This service shows the status of the TIMAC module. Logout Request: This service unauthenticates the current

	Cryptographic Officer. Zeroize Request: This service zeroizes the TIMAC's CSPs. Reset Request: This service performs a software reset and executes the suite of TIMAC self-tests.

In addition, the TIMAC module provides the following unauthenticated services that do not disclose, modify, substitute CSPs, use an Approved security function, or otherwise affect the security of the module:

Status Request: This service shows the status of the TIMAC module.

Reset Request: This service performs a software reset, and executes the suite of TIMAC self-tests

6.1. Definitions of Critical Security Parameters (CSPs)

The TIMAC module contains 3 Critical Security Parameters (CSPs) summarized in Table 6. All of the CSPs are 128 bits long, are factory set, and do not change once the TIMAC module leaves the factory.

Table 6: Critical Security Parameters

Critical Security Parameters (CSPs)	Function
AES Key	The AES key used for encryption and decryption.
User personal identification number (UPIN)	The User role's authentication PIN.
Cryptographic Officer personal identification number (COPIN)	The Cryptographic Officer role's authentication PIN.

6.2 Definition of CSP Modes of Access

Authenticate (A): use the CSP within an identity based authentication scheme.

Encrypt (E): use the CSP to encrypt data.

Decrypt (D): use the CSP to decrypt data.

Reinitialize (R): set the parameter back to an initial value.

Zeroize (Z): actively destroy the CSP.

Table 7 – CSP Access Rights within Roles & Services

Role		Service			
C.O.	**User**		**AES Key**	**UPIN**	**COPIN**
X	X	Authenticate Request		A	A
	X	AES Encrypt	E		
	X	AES Decrypt	D		
	X	Select Mode Request			
	X	Select baud rate Request			
	X	Reinitialize IV Request			
X	X	Logout Request			
X		Zeroize Request	Z	Z	Z
X	X	Status Request			
X	X	Reset Request			
	X	Flush Data Buffer Request			

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the TIMAC module does not contain a modifiable operational environment.

8. Security Rules

The following describes the security rules enforced by the TIMAC module to implement the security requirements specified by FIPS 140-2 Level 3.

1. The cryptographic module shall provide one User role and one Cryptographic Officer role.

2. The cryptographic module shall provide identity-based authentication. The User must possess the correct name and UPIN to be able to obtain authorization. The Cryptographic Officer must possess the correct name and COPIN to be able to obtain authorization.

3. The cryptographic module shall not support a maintenance role, maintenance interface, or maintenance state.

4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.

5. The cryptographic module shall only use Approved security functions, and shall not support a non-FIPS mode of operation.

6. The cryptographic module shall encrypt message traffic using the AES algorithm.

7. The cryptographic module shall perform the following Power up Self-Tests:

    a. Cryptographic algorithm tests – AES Known Answer Test

    b. Software Integrity Test using an error detection code (16-bit CRC)

    c. Critical Function – EEPROM Integrity Test (16-bit CRC)

8. The cryptographic module shall distinguish between data and control for input and data and status for output.

9. Data output shall be inhibited during initialization, self-tests, zeroization, and error states.

10. The cryptographic module shall not support the output of CSPs in any form.

11. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

12. The module shall not support concurrent operators.

13. The module shall enforce a timed-access protection to prevent brute force attacks on the PINs.
14. The cryptographic module shall provide a zerorization process that immediately actively destroys all CSPs contained within the cryptographic boundary.
15. The cryptographic module shall not support a bypass capability.
16. When the cryptographic module is powered off and subsequently powered on, the results of previous authentications shall not be retained.
17. The cryptographic module shall not permit an operator to change roles without re-authenticating.
18. The cryptographic module shall not provide a feedback mechanism that weakens the strength of the authentication mechanism.
19. The cryptographic module shall require explicit role selection during the authentication process.
20. Upon entering the error state, the cryptographic module shall inhibit all data output, cryptographic functions, and shall provide status of the error.
21. The cryptographic module shall provide physical security mechanisms that provide a hard, opaque, tamper evident enclosure. It shall not be possible to remove the potting without destroying the cryptographic module circuitry.
22. The cryptographic module shall not provide the ability to modify the operational environment.
23. The cryptographic module shall protect all CSPs from disclosure, modification and substitution.
24. The cryptographic module shall provide key to entity association for key storage.
25. The cryptographic module shall conform to the applicable requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.
26. The cryptographic module does not mitigate any specific attacks beyond the scope of FIPS 140-2.

9. Physical Security Policy

The device is a multi chip embedded cryptographic module that is potted with hard, opaque, tamper evident, epoxy. The hard potting material encapsulates the module's circuitry such that, with high probability, removal and penetration attempts destroy the device. This enclosure has no removable doors, cover, or any vents or openings that need to be protected against probing.

9.1. Operator Required Actions

The operator is required to periodically inspect the potting for visible signs of tampering.

Table 8 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard, opaque, tamper evident potting	To be determined by the security policy and internal procedures enforced by the acquiring agency.	To be determined by the security policy and internal procedures enforced by the acquiring agency.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate specific attacks outside of the scope of FIPS 140-2.

Table 9 – Mitigation of Other Attacks

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

11. References

- FIPS PUB 140-2
- FIPS PUB 197