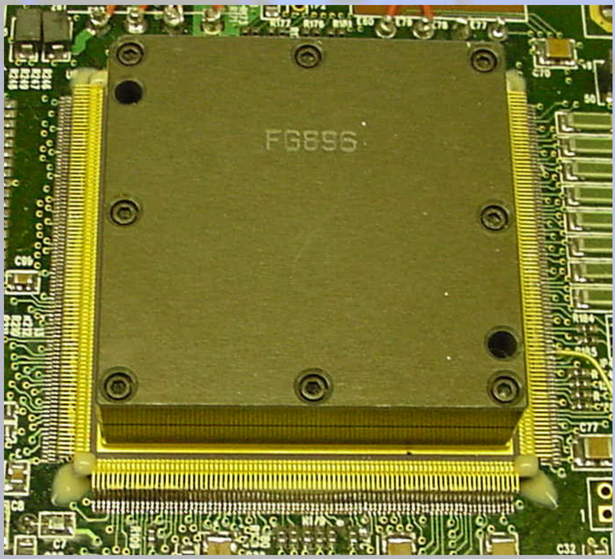
Document: 669506-1

AES-256 Encryption Core Security Policy



Revision A

July 24, 2006

Submitted To
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Prepared By
L-3 Communications
Cincinnati Electronics
7500 Innovation Way
Mason, OH 45040-9699

Revision History

Rev A (July 24, 2006)

Updated paragraph 1 with core FPGA part number
Added Appendix A for T-724 X-Band Mission Data Transmitter
Added Appendix B for T-725 X-Band Telemetry Transmitter

Table of Contents

Table of Contents - Continued

Table of Contents - Continued

Appendix A
T-724 X-Band Mission Data Transmitter PFGA Security Policy
L-3 CE PN 669515-1

Section Title Page

Table of Contents - Continued

Appendix A - Continued
T-724 X-Band Mission Data Transmitter PFGA Security Policy
L-3 CE PN 669515-1

Section Title Page

Table of Contents - Continued

Appendix B - Continued
T-725 X-Band Telemetry Transmitter PFGA Security Policy
L-3 CE PN 669517-1

Section Title Page

Table of Contents - Continued

Appendix B - Continued
T-725 X-Band Telemetry Transmitter PFGA Security Policy
L-3 CE PN 669517-1

Section Title Page

LIST OF TABLES

1 OVERVIEW

The AES-256 Encryption Core provides AES encryption as described in the Federal Information Processing Standards Publication (FIPS PUB) 197 Advanced Encryption Standard (AES) using a 256-bit cipher key. The Core meets the requirements for FIPS PUB 140-2 Security Requirements for Cryptographic Modules at security level 1. The programmed FPGA, L-3 Communications Cincinnati Electronics part number 669510-1, is considered a single-chip cryptographic module.

1.1 Purpose

This document provides the L-3 Communications Cincinnati Electronics AES-256 Encryption Core non-proprietary FIPS 140-2 Security Policy. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 1 requirements.

1.2 Reference Documents

FIPS 197 Advanced Encryption Standard (AES), November 26, 2001

FIPS PUB 140-2 Security Requirements for cryptographic modules, May 25 2001

Derived Test Requirements for FIPS PUB 140-2, Security Requirements for
Cryptographic Modules, March 24, 2004, Draft

NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation -
Methods and Techniques, December 2001

2 SECURITY LEVELS

The AES-256 Encryption Core single-chip cryptographic module meets the overall requirements of FIPS 140-2 security level 1.

3 FIPS 140-2 APPROVED OPERATIONAL MODE

The AES-256 Encryption Core approved security function is AES-256 encryption as described in FIPS PUB 197 using a 256 bit cipher key. The core provides Electronic Codebook (ECB) mode of operation as described in NIST Special Publication 800-38A. The module meets the overall security requirements of FIPS PUB 140-2 at security level 1. The module does not need any special configuration to operate in FIPS mode.

4 SECURITY RULES

4.1 Operating Environment

Not applicable.

4.2 Ports and Interfaces

4.2.1 Logical Interfaces

Logical interfaces allow input and output of data, CSPs and status.

4.2.1.1 Key Input Interface

The key interface is used to enter cipher keys.

4.2.1.2 Plaintext Data Input Interface

The plaintext data interface port provides the input path for the plaintext data.

4.2.1.3 Ciphertext Data Output Interface

The ciphertext data output port provides the output path for the ciphertext data.

4.2.1.4 Control Input Interface

The control input interface provides the control interface.

4.2.1.5 Status Output Interface

The status output interface provides indicators for the security features.

4.2.2 Physical Interfaces

Physical interfaces allow input and output of data, CSPs and status to the physical pins.

4.2.2.1 Input

The input interface is used to input cipher key, plaintext data and control.

4.2.2.2 Output

The output interface is used to output ciphertext data and status.

4.2.2.3 Clock Input

The clock input physical port provides a reference input clock.

4.2.2.4 Power on Reset Input

The power on reset input physical port is used to interface with an external reset signal.

4.2.2.5 Power Input

The power input physical port is used to supply power to the module.

5 IDENTIFICATION AND AUTHENTICATION POLICY

None

6 ACCESS CONTROL POLICY

6.1 Supported Roles

The AES-256 Encryption Core authorized roles are the crypto officer role and the user role.

6.2 Services

All services provided by the cryptographic module are approved.

6.3 Critical Security Parameters (CSP)

256-bit AES Cipher Key.

6.4 Services Authorized for Roles

Table 6-1. Services Authorized for Roles

Role	Authorized Service
Crypto Officer	Self-test/Key Zeroize
Crypto Officer	Cipher key load
User	AES-256 Encryption
User	Cryptographic Bypass

6.5 Access Rights within Services

Table 6-2. Access Rights within Services

Authorized Service	Cryptographic Keys And CSPs	Type of Access (e.g. Read, Write, Delete, Select)
Self-test/Key Zeroize	256-bit AES Key	Write
Cipher key load	256-bit AES Key	Write
AES-256 Encryption	256-bit AES Key	Read
Cryptographic Bypass	256-bit AES Key	Read

7 PHYSICAL SECURITY POLICY

The AES-256 Encryption Core is a single chip cryptographic module. The single chip is a production grade integrated circuit. The cryptographic module does not require maintenance therefore no maintenance access is required.

8 MITIGATION OF OTHER ATTACKS POLICY

None.

Appendix A
T-724 X-Band Mission Data Transmitter FPGA Security Policy
L-3 CE PN 669515-1

1 OVERVIEW

The T-724 is a high data rate X-Band transmitter used to downlink spacecraft mission data. The transmitter provides data processing modes consisting of AES-256 ECB encryption and additional data processing functions. The programmed FPGA, L-3 Communications Cincinnati Electronics part number 669515-1, is considered a single-chip cryptographic module.

1.1 Purpose

This appendix provides the L-3 Communications Cincinnati Electronics T-724 Mission Data Transmitter FPGA FIPS 140-2 Security Policy. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 1 requirements. Specifically, this appendix identifies the non-security related additions to the AES-256 Encryption Core FPGA.

2 SECURITY LEVELS

Same as AES-256 Encryption Core FPGA.

3 FIPS 140-2 APPROVED OPERATIONAL MODE

Same as AES-256 Encryption Core FPGA.
Note: The DES implemented within the T-724 FPGA is not FIPS compliant, and to operate the module in a FIPS Approved mode, the operator may not use DES encryption.

4 SECURITY RULES

4.1 Operating Environment

Same as AES-256 Encryption Core FPGA.

4.2 Ports and Interfaces

4.2.1 Logical Interfaces

Same as AES-256 Encryption Core FPGA.

4.2.1.1 Plaintext Key Input Interface

Same as AES-256 Encryption Core FPGA.

4.2.1.2 Plaintext Data Input Interface

Same as AES-256 Encryption Core FPGA.

4.2.1.3 Ciphertext Data Output Interface

Same as AES-256 Encryption Core FPGA.

4.2.1.4 Control Input Interface

Same as AES-256 Encryption Core FPGA.

4.2.1.5 Status Output Interface

Same as AES-256 Encryption Core FPGA.

4.2.2 Physical Interface

4.2.2.1 Command Input

The T-724 FPGA command interface permits selection of data processing modes and provides the key load interface.

4.2.2.2 Status Output

The T-724 FPGA status output provides the status of the transmitter and indicators for the security features.

4.2.2.4 Plaintext Data Inputs

The T-724 plaintext data interface provides the input path for plaintext data.

4.2.2.5 Modulator Ciphertext Data Output

The modulator ciphertext data output serializes the processed data outputs it to the modulator.

4.2.2.7 Oscillator Clock Interface

The T-724 FPGA oscillator clock input provides the reference clock input.

4.2.2.8 Power On Reset Input

The power on reset input physical port is used to interface with an external active low reset signal.

4.2.2.9 Power Input

The power input physical port is used to supply power to the FPGA.

5 IDENTIFICATION AND AUTHENTICATION POLICY

Same as AES-256 Encryption Core FPGA.

6 ACCESS CONTROL POLICY

6.1 Supported Roles

Same as AES-256 Encryption Core FPGA.

6.2 Services

Same as AES-256 Encryption Core FPGA.

6.3 Critical Security Parameters (CSP)

Same as AES-256 Encryption Core FPGA.

6.4 Services Authorized for Roles

Same as AES-256 Encryption Core FPGA.

6.5 Access Rights within Services

Same as AES-256 Encryption Core FPGA.

7 PHYSICAL SECURITY POLICY

Same as AES-256 Encryption Core FPGA.

8 MITIGATION OF OTHER ATTACKS POLICY

Same as AES-256 Encryption Core FPGA.

Appendix B
T-725 X-Band Telemetry Transmitter FPGA Security Policy
L-3 CE PN 669715-1

1 OVERVIEW

The T-725 is a low data rate X-Band transmitter used to downlink spacecraft telemetry. The transmitter provides data processing modes consisting of AES-256 ECB encryption and additional data processing functions. The programmed FPGA, L-3 Communications Cincinnati Electronics part number 669715-1, is considered a single-chip cryptographic module.

1.1 Purpose

This appendix provides the L-3 Communications Cincinnati Electronics T-725 Telemetry Transmitter FPGA FIPS 140-2 Security Policy. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 1 requirements. Specifically, this appendix identifies the non-security related additions to the AES-256 Encryption Core FPGA.

2 SECURITY LEVELS

Same as AES-256 Encryption Core FPGA.

3 FIPS 140-2 APPROVED OPERATIONAL MODE

Same as AES-256 Encryption Core FPGA.
Note: The operator must zeroize and load a user key prior to encryption in order to operate the module in a FIPS Approved mode.

4 SECURITY RULES

4.1 Operating Environment

Same as AES-256 Encryption Core FPGA.

4.2 Ports and Interfaces

4.2.1 Logical Interfaces

Same as AES-256 Encryption Core FPGA.

4.2.1.1 Plaintext Key Input Interface

Same as AES-256 Encryption Core FPGA.

4.2.1.2 Plaintext Data Input Interface

Same as AES-256 Encryption Core FPGA.

4.2.1.3 Ciphertext Data Output Interface

Same as AES-256 Encryption Core FPGA.

4.2.1.4 Control Input Interface
Same as AES-256 Encryption Core FPGA.

4.2.1.5 Status Output Interface
Same as AES-256 Encryption Core FPGA.

4.2.2 Physical Interface

4.2.2.1 Command Input
The T-725 FPGA command interface permits selection of data processing modes and provides the key load interface.

4.2.2.2 Status Output
The T-725 FPGA status output provides the status of the transmitter and indicators for the security features.

4.2.2.4 Plaintext Data Input
The T-725 plaintext data interface provides the input path for plaintext data.

4.2.2.5 Modulator Ciphertext Data Output
The modulator ciphertext data output utilizes a Delta-Sigma D/A converter to output the I and Q channel Gaussian Filtered Offset Quadrature Phase Shift Key (GF-OQPSK) modulation waveform.

4.2.2.7 Oscillator Clock Interface
The T-725 FPGA oscillator clock input provides the reference clock input.

4.2.2.8 Power On Reset Input
The power on reset input physical port is used to interface with an external active low reset signal.

4.2.2.9 Power Input
The power input physical port is used to supply power to the FPGA.

5 IDENTIFICATION AND AUTHENTICATION POLICY

Same as AES-256 Encryption Core FPGA.

6 ACCESS CONTROL POLICY

6.1 Supported Roles

Same as AES-256 Encryption Core FPGA.

6.2 Services

Same as AES-256 Encryption Core FPGA.

6.3 Critical Security Parameters (CSP)

Same as AES-256 Encryption Core FPGA.

6.4 Services Authorized for Roles

Same as AES-256 Encryption Core FPGA.

6.5 Access Rights within Services

Same as AES-256 Encryption Core FPGA.

7 PHYSICAL SECURITY POLICY

Same as AES-256 Encryption Core FPGA.

8 MITIGATION OF OTHER ATTACKS POLICY

Same as AES-256 Encryption Core FPGA.