RTL-TDEA Crypto Module
Security Policy

Document No. RTL-SP-TDEA

March 23, 2004
Revision 1.1

Prepared by:

RT Logic!

1042 Elkton Drive
Colorado Springs, CO 80907
(719) 598-2801
support@rtlogic.com
www.rtlogic.com

RT Logic!
Enabling Your Solutions

Revision History

Release Level	Release Date	Comments
1.0	December 10, 2003	Original release.
1.1	March 23, 2004	Security Policy updated to include description of the Non-Approved mode.

RT Logic!
Enabling Your Solutions

Table of Contents

Tables

Figures

1. Module Overview

The RTL-TDEA crypto module is a multi-chip embedded cryptographic module (Hardware Version 1, Firmware Version 1, tagged in CVS as version 1.0). The RTL-TDEA crypto module is a PCI card with two RS-422 ports (the data input port and the data output port), two RS-232 serial ports (a Crypto Control Port and a Key Control Port), and a power output port.

The RTL-TDEA crypto module takes user data from the data input port, processes it according to the mode specified through the "Set Mode" service, and then outputs the data via the data output port. All commands are issued through the crypto control port, and status is output via the crypto control port. The key control port is used only for the entry of keys that were manually established to the module. The module is provided power over the PCI interface, but it does not otherwise make use of this port in any way.

The RTL-TDEA crypto module is FPGA driven, with no general purpose processor or software. The crypto module is enclosed in a commercial grade hard metal enclosure that is sealed using tamper evident seals. The RTL-TDEA crypto module has a static, non-modifiable operational environment.

The crypto module's crypto boundary is established by the metal enclosure on the front side of the card and the PC board on the rear side of the card. The rear side of the PC board is a metal plane with no traces or signal vias. The enclosure encompasses the entire PCI card other than the PCI interface, the auxiliary power output port, and the RS-232 and RS-422 ports.

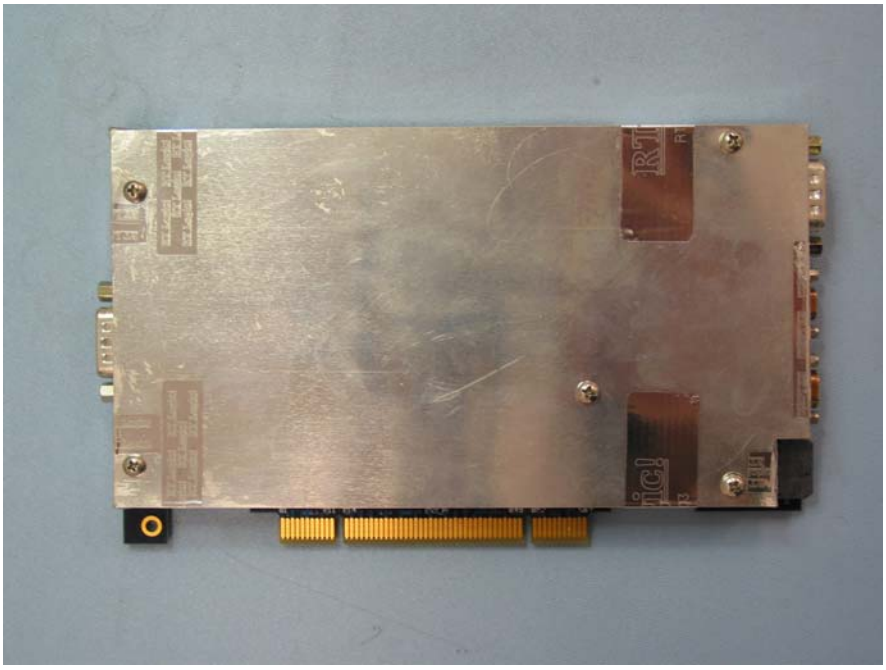

Figure 1-1. RTL-TDEA Crypto Module

2. Security Level

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

Table 2-1. Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module 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	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

3.1 Approved Mode of Operation

In FIPS mode, the crypto module only supports FIPS Approved algorithms as follows:

- Triple-DES (three key) for encryption (ECB, CBC, CFB64, OFB modes)
- Triple-DES (three key) for decryption (CFB64, OFB modes)

The crypto module has very simple behavior and key management: the crypto module can only have one key loaded at a time. All key establishment is accomplished through manually transported, electronically entered means through a port dedicated to key entry. All CSPs are stored in either FPGA registers, or within the module's NVRAM.

The crypto module does not output any CSP in any form.

The crypto module can be operated in its Approved mode by selecting ECB (encrypt), CBC (encrypt), or CFB64 (encrypt or decrypt) modes and for the CBC, CFB64, and OFB modes specifying internally generated or externally provided IV mode through the "Set Mode" service.

Table 3-1. FIPS 140-2 Approved Modes of Operation

TDEA Mode	Encrypt/Decrypt Mode	IV Mode
ECB	Encrypt	N/A
CBC	Encrypt	Internally Created or Externally Provided
CFB64	Encrypt/Decrypt	Internally Created or Externally Provided
OFB	Encrypt/Decrypt	Internally Created or Externally Provided

The operator can determine if the crypto module is in FIPS mode by using the "Get Status" command and reviewing the Crypto Mode specified in the returned status.

3.2 Non-Approved Mode of Operation

In Non-FIPS Approved mode, the crypto module supports the following algorithms:

- Triple-DES (three key) for encryption (CTR)
- Triple-DES (three key) for decryption (ECB, CBC, CTR)

The crypto module control and behavior is the same in the Non-FIPS Approved 140-2 mode as it is in the Approved mode. The Non-Approved modes, CTR (encrypt or decrypt), ECB (decrypt), CBC (decrypt) are selectable through the "Set Mode" service . In the CBC (decrypt) mode the option to internally generate or use externally provided IV is selectable. In the CTR (encrypt or decrypt) mode only the internally generated IV option is available. The "Get Status" command provides status regarding Non-Approved mode of operation.

Table 3-2. Non-FIPS 140-2 Approved Modes of Operation

TDEA Mode	Encrypt/Decrypt Mode	IV Mode
ECB	Decrypt	N/A
CBC	Decrypt	Internally Created or Externally Provided
CTR	Encrypt/Decrypt	Internally Created

4. Ports and Interfaces

The RTL-TDEA crypto module provides the following physical ports and logical interfaces.

The RTL-TDEA crypto module provides six ports.

- Crypto Control Port (DE-9 male connector, RS-232 signaling)
- Key Control Port (DE-9 male connector, RS-232 signaling)
- Data Output Port (Micro D9P male connector, RS-422 signaling)
- Data Input Port (Micro D9S female connector, RS-422 signaling)
- Power Input Port (PCI 32 bit edge connector)
- Aux Power Output Port (4 pin MicroFit-3 male connector)

The six ports support the following FIPS interfaces:

- Data Input
- Data Output
- Control Input
- Status Output
- Power

Table 4-1. Relationship Between Ports and Interfaces

Interface	Port(s)
Data Input Interface	Data Input Port, Crypto Control Port, Key Control Port
Data Output Interface	Data Output Port, Key Control Port
Control Input Interface	Crypto Control Port
Status Output Interface	Crypto Control Port
Power Interface	Power Input Port, Aux Power Output Port

5. Identification and Authentication Policy

5.1 Assumption of Roles

The RTL-TDEA crypto module has two operator roles: User and Cryptographic Officer. Both of these roles have access to the same services, and use the same authentication information to authenticate. As such, they are referred to as a joint "User/Crypto-Officer Role" for the sake of brevity.

The User/Crypto-Officer role implicitly selects its role by invoking an authenticated service, in which the operator passes a 64 bit random value into the module. Each command that requires authentication is independently authenticated, so the operator "logs out" when the command is completed or the module is powered off.

Table 5-1. Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User/Crypto-Officer	Role Based Operator Authentication	Authentication Code

Table 5-2. Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Authentication Code	The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{64}$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is $1/2^{52}$ which is less than 1/100,000.

6. Access Control Policy

6.1 Roles and Services

Table 6-1. Services Authorized for Roles

Role	Authorized Services

User/Crypto-Officer:
This role shall provide all of the services necessary for protecting the confidentiality of input data, and related key management functions.
	• **Set Mode:** Specifies the mode for the crypto module. The mode selected either zeroizes the crypto module (in which case no user data can be encrypted or decrypted until a new key is loaded) or specifies a cryptographic mode (which directs the module to process user data). This service can:
	  • Set the cryptographic mode for the crypto module, both Approved and Non-Approved FIPS modes, including the mode of use for the TDEA algorithm (ECB, CBC, CFB64, OFB and CTR encrypt/decrypt), the IV mode (internally created or externally provided), and the requested key's label.
	  • Zeroize all keys
	  • Zeroize all CSPs
	• **Self Test:** This service initiates the crypto module's cryptographic algorithm test. All power-up self-tests can be re-run by power cycling the crypto module.
	• **Authenticate:** This service allows the crypto module to verify the authentication code provided by the operator, but does not otherwise affect the module.

6.1.1 Unauthenticated Services

The RTL-TDEA crypto module supports several unauthenticated services. These services do not affect the crypto module's CSPs or use security functions.

The RTL-TDEA crypto module supports the following unauthenticated services:

- **Reset:** This service resets the crypto module's state machines. If there is a key currently loaded, this key is left unmodified, and the crypto module can continue to process user data. The crypto module's message count and block count are reset.
- **Get Status:** This service causes the crypto module to output its current status.
- **Enable:** This service enables the data input to the crypto module after it has been disabled through the "Disable Command."
- **Disable:** This service shuts off the data input port and data output port until the "Enable Command" service is run.

Table 6-2. Specification of Service Inputs and Outputs

Service	Control Input	Data Input	Data Output	Status Output
Set Mode	Header info, crypto mode, IV mode, encrypt/decrypt mode	Authentication Code, Plaintext data or Ciphertext data (depending on mode), key selection, key tag, key	Plaintext data or Ciphertext data (depending on mode)	Success/failure error code
Self Test	Header info	Authentication Code	N/A	Success/failure error code
Authenticate	Header info	Authentication Code	N/A	Success/failure error code
Reset	Header info	N/A	N/A	Success/failure error code
Get Status	Header info	N/A	N/A	Current crypto mode, IV mode, enabled/disabled, current error code, message counter, block count, hardware revision, firmware revision/failure error code
Enable	Header info	N/A	N/A	Success/failure error code
Disable	Header info	N/A	N/A	Success/failure error code

6.2 Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the crypto module:

- **Loaded Key:** This is the TDES key used to encrypt or decrypt user data.
- **Authentication Code:** This is a random 64 bit value that is loaded at the factory and cannot be changed.
- **IV Seed:** This is a 64 bit value used in internal IV creation. The IV Seed is loaded at the factory and cannot be changed.

6.3 Definition of CSPs Modes of Access

Table 6-3 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- **Use Loaded Key:** This operation uses the loaded key in the selected TDES mode of operation to process user provided data.
- **Create IV:** This operation uses the IV Seed to create an Initialization Vector that is used to initialize the encryption algorithm just prior to encrypting data.
- **Verify Authentication Code:** This operation compares the provided authentication code with the stored authentication code.
- **Load Key:** This operation replaces the Loaded Key with another key from the Key Control Port.
- **Zeroize Loaded Key:** This operation zeroizes the Loaded Key.
- **Zeroize All CSPs:** This operation zeroizes the Loaded Key, the Authentication Code and the IV Seed.

Table 6-3. CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
User/Crypto-Officer	Unauthenticated		
X		Set Mode	Load Key, Zeroize Loaded Key, Zeroize All CSPs, Use Loaded Key, Create IV, Verify Authentication Code
X		Self Test	Verify Authentication Code
X		Authenticate	Verify Authentication Code
	X	Reset	N/A
	X	Get Status	N/A
	X	Enable	N/A
	X	Disable	N/A

7. Operational Environment

The FIPS 140-2 Operational Environment requirements are not applicable because the RTL-TDEA crypto module is a limited operational environment.

8. Security Rules

8.1 Rules Specified By the FIPS 140-2 Standard

1. The crypto module restricts all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the crypto module.
2. The crypto module interfaces are logically distinct from each other.
3. The crypto module distinguishes between data and control for input and data and status for output.
4. All input data entering the crypto module via the "data input" interface only passes through the input data path.
5. All output data exiting the crypto module via the "data output" interface only passes through the output data path.
6. The crypto module does not perform manual key entry or key generation.
7. The output data path is logically disconnected from processes while performing key zeroization.
8. The crypto module does not output plaintext cryptographic keys or CSPs.
9. The crypto module does support multiple concurrent operators. The module internally maintains the separation of roles assumed by each operator and each corresponding service.
10. The crypto module supports role based operator authentication.
11. The crypto module does not allow operators to perform physical or logical maintenance.
12. The crypto module does not implement a bypass capability.
13. The crypto module allows the user/crypto-officer to implicitly select their role.
14. The crypto module does not maintain the results of previous authentications between power cycles.
15. The crypto module contains authentication required to authenticate the operator for the first time the crypto module is accessed.
16. For each attempt to use the crypto module's authentication mechanism, there is less than a 1/1,000,000 chance that a false acceptance will occur.
17. For multiple attempts within a one minute time period, the probability is less than 1/100,000 that a false acceptance will occur.
18. The crypto module does not provide any feedback to the operator during authentication.
19. The crypto module employs physical security mechanisms in order to restrict unauthorized physical access to the module and to deter unauthorized modification to the crypto module. All hardware and firmware components within the crypto-boundary are protected.
20. The crypto module is classified as a multi-chip embedded cryptographic module.
21. Unauthorized attempts at physical access, use, or modification have a high degree of being detected subsequent to an attempt by leaving visible signs of tamper.
22. The crypto module does not have a maintenance role and is not designed to permit access to the contents of the crypto module.
23. The crypto module consists of production grade components, including standard passivation techniques and a production grade enclosure.
24. The crypto module provides evidence of tampering when physical access to the module is attempted.
25. The crypto module is contained within an opaque tamper evident enclosure.
26. The crypto module is classified as a limited operational environment.
27. Secret keys and CSPs are protected within the crypto module from unauthorized disclosure, modification, and substitution.
28. Key establishment (key transport) is accomplished only through manual methods.
29. Keys are entered into the crypto module using electronic methods.
30. Cryptographic keys entered into the crypto module are associated with the entity (role) to whom they are assigned.
31. Secret keys are manually established and entered into the module in plaintext.
32. Cryptographic keys stored within the crypto module are stored in plaintext form.
33. The crypto module associates all cryptographic keys stored within the crypto module with the correct entity to which the key is assigned.

34. The crypto module provides a method to zeroize all plaintext secret cryptographic keys and CSPs within the crypto module.
35. The crypto module conforms to the 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)
36. If the crypto module fails a self-test, the module enters an error state and outputs an error indicator via the status output interface.
37. The crypto module does not perform any cryptographic operations while in an error state.
38. All data output via the data output interface is inhibited when an error state exists.
39. Power-up tests are performed by the crypto module when power is applied to the crypto module.
40. The power-up tests are initiated automatically and do not require operator intervention.
41. When the power-up tests are completed, the results are output via the "status output" interface.
42. All data output via the data output interface is inhibited when the power-up tests are performed.
43. The operator can initiate the crypto algorithm test by running the Self Test service, or can re-run all of the power-up self-tests by restarting the crypto module.
44. The crypto module includes the following Power-On Self-Tests:
    a. Triple DES KAT (CFB64, encrypt mode)
    b. Firmware integrity test (16 bit CRC)

8.2 Rules Specified by the Vendor

1. Each RTL-TDEA crypto module has a unique serial number.
2. The eight tamper evident seals on the RTL-TDEA crypto module all bear the "RT Logic!" logo.
3. The two largest seals on the crypto module additionally have a unique serial number printed on the seal.
4. The Authentication Code and IV Seed are specified during manufacturing, and cannot be changed in the field.
5. The crypto module firmware is programmed during manufacturing, and cannot be changed in the field.
6. If the "Zeroize All" mode of the "Set mode" service is selected, the crypto module becomes non-functional, and can only be rendered functional by returning it to the factory.
7. The Key Control Port may only be used to support a manual key establishment mechanism.
8. The crypto module keeps a count of the total number of messages and blocks sent since the previous power up or reset command.
9. The crypto module is completely initialized at the factory, and does not require further operator initialization or start-up procedures.
10. The RTL-TDEA crypto module is installed in a larger RT Logic product. This entire product is normally provided to the end customer, though it is possible to send only the crypto module in the case where system maintenance on a pre-existing system is necessary. The crypto module (and the product that it is enclosed in) is shipped through a commercial carrier, and requires signature verification upon delivery. In all cases, pictures of the crypto module and the crypto module serial number and its tamper evident label serial numbers are provided to the end customer through a separate channel, so the customer can confirm that the crypto module that was shipped is the same module that was received.

9. Physical Security Policy

9.1 Physical Security Mechanisms

The RTL-TDEA crypto module has the following physical protections:

- Production-grade components and production-grade opaque enclosure with tamper evident seals.
- All eight tamper evident seals bear the "RT Logic!" logo.
- Two of the eight tamper evident seals bear a unique serial number.

9.2 Operator Required Actions

The operator is required to periodically inspect tamper evident seals.

Table 9-1. Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	Upon initial delivery. Thereafter, each 18 months	Verify that all seals are present and intact. Verify that no seal shows a change in the seal pattern. Verify that there is no tamper evidence left on the enclosure. Verify that all seals bear the "RT Logic!" logo. Verify that the seals with serial number bear the same serial number as previous inspections.

10. Mitigation of Other Attacks Policy

The RTL-TDEA crypto module is not designed to mitigate attacks not specified by FIPS 140-2.

11. References

1. FIPS 140-2, Security Requirement for Cryptographic Modules, 12-03-2002

2. FIPS 46-3, Data Encryption Standard (DES) 10-25-1999

3. NIST SP 800-38A, Recommendations for Block Cipher Modes of Operation, 2001

4. ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation

5. EIA/TIA-232-E, Interface between Data Terminal Equipment and Data Circuit-Termination Equipment Employing Serial Binary Data Interchange

6. RS-422, specified by EIA

12. Acronyms

Acronym	Meaning
CBC	Cipher Block Chaining
CFB	Cipher Feed Back
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
ECB	Electronic Code Book
EMI/EMC	Electro-Magnetic Interference/Electro-Magnetic Compatibility
FCC	Federal Communications Commission
FPGA	Field Programmable Gate Array
IV	Initial Vector
KAT	Known Answer Test
NVRAM	Non-Volatile Random Access Memory
OFB	Output Feed Back
PC board	Printed Circuit Board
PCI	Peripheral Component Interconnect
RS-232	Recommended Standard 232, specified in EIA/TIA-232
RS-422	Recommended Standard 422, specified in EIA standard RS-422
TDES	Triple DES

Reader Comment Form

RT Logic welcomes your comments and questions regarding our software and documentation. Please help us improve the quality and usefulness of our products by filling out and returning this form to:

RT Logic!

1042 Elkton Drive
Colorado Springs, CO 80907
Attention: Director, Product Development
support@rtlogic.com

Title of Document:	**RTL-TDEA Crypto Module Security Policy**
Document #:	RTL-SP-TDEA
Name/Title:	
Firm:	
Address:	
Telephone:	

I used this manual ...

- ❒ As an introduction to the subject
- ❒ as an aid for advanced training
- ❒ to instruct a class
- ❒ to learn operating procedures
- ❒ as a reference manual
- ❒ other:

I found this material ...

	Yes	No
accurate and complete	❒	❒
written clearly	❒	❒
well illustrated	❒	❒

Please indicate below any other comments you may have regarding this material or software as well any errors you may have encountered, listing page numbers where appropriate.