Altarus Corporation
Altarus Cryptographic Module version 1.0
FIPS 140-1 Level 1 Validation Security Policy

Author	**Title**
Adam Nelson	Chief Engineer/Architect
Ludge Olivier	Director of Client Services
Elizabeth Sellers	Technical Writer

Date: February 26, 2002

(Revised August 19, 2002)

(Revised December 17, 2002)

Table of Contents

1 INTRODUCTION

1.1 Purpose

This is a Non-Proprietary Federal Information Processing Standard (FIPS) 140-1 Security Policy for Altarus' Cryptographic Module (ACM). This Security Policy was produced as part of the FIPS 140-1 Level 1 validation of the ACM for the Altarus Enterprise Platform, software submission package.

The document is arranged in 3 main sections. The first section of this document provides an overview and introduction to the Altarus Cryptographic Module Security Policy while Sections 2 and 3 describe the module and how it may be operated securely in compliance with the requirements defined in the FIPS 140-1 Standard.

1.2 Altarus products

The Altarus offering provides a premier platform and rapid development tools for creating, extending, and deploying secure enterprise applications to the desktop, mobile devices, or handheld devices. Our product facilitates efficient data transfer while allowing for unprecedented real-time performance, mission critical reliability and security. Our product also enables companies to leverage existing IT resources – i.e., LAN or WAN, satellite, wired, or dial-up connection – while extending new information access methods.

Product features include:

- End-to-end application security
- Exponential increases in data transfer speeds
- Optimal wired and wireless application performance, via thick or thin clients
- Maximization of concurrent user capacity
- Dramatic reductions in bandwidth consumption
- High reliability and system availability
- Rapid integration and deployment
- Security enhancements: Network, Domain, Biometrics, Application, and Access Control

1.3 References

Altarus Corporation FIPS 140-1 Certification Documentation. (2002), Adam Nelson, Altarus Corporation, Virginia, U.S.A.

FIPS PUB 140-1 Security Requirements for Cryptographic Modules. (January 11, 1994), Federal Information Processing Standards Publication, U.S. Department of Commerce Technology Administration, National Institute of Standards and Technology.

FIPS PUB 180-1 Secure Hash Standard. (April 17 1995), Federal Information Processing Standards Publication, U.S. Department of Commerce Technology Administration, National Institute of Standards and Technology.

FIPS PUB 186-2, Digital Signature Standard (DSS). (May 19, 1994), Federal Information Processing Standards Publication, U.S. Department of Commerce Technology Administration, National Institute of Standards and Technology.

FIPS PUB 81 DES Modes of Operation. (December 2, 1980), Federal Information Processing Standards Publication, U.S. Department of Commerce Technology Administration, National Institute of Standards and Technology.

1.4 Glossary

API	Application Program Interface
ACM/CM	Altarus Cryptographic Module
CSP	Cryptographic Service Provider
3DES	Triple Data Encryption Standard (Triple DES)
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard
IC	Integrated Circuit(s)
RNG	Random Number Generator/Generation
RSA	Public key algorithm (created by Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman)
SHA-1	Secure Hash Algorithm
Triple DES	Triple Data Encryption Standard (3DES)

2 CRYPTOGRAPHIC MODULE

Altarus' Cryptographic Module is implemented as a software component of the Altarus Server architecture. The component is identical, at the source code level for all supported hardware platforms and operating systems. It is compiled into specific executable object code for each platform. All code which accesses or processes cryptographic keys, random number generation (RNG) internal state, etc. is contained within this code which can be further broken down into individual source files, which are listed in Appendix A of the Altarus Corporation FIPS 140-1 Certification Documentation.

The physical cryptographic boundary of the ACM is defined by the particular hardware configuration of the general-purpose personal computer (PC) upon which it is executed. The ACM is therefore considered to be a multi-chip standalone module for the purposes of FIPS 140-1.

The ACM's software does not contain any Integrated Circuits (IC), and its implementation means that the quality of the Integrated Circuit(s) that execute the module's functionality cannot be dictated in advance. However, the software is designed to execute on general-purpose personal computers, which are always mass-produced components with production-quality circuitry and ICs on a ceramic substrate.

2.1 Module Interfaces

The four main interfaces of the ACM are defined in terms of the API and consist of the Data Input, Data Output, Control Input, and Status Output interfaces. These interfaces are represented in the form of parameters, error and status codes in procedure calls on procedures exposed in the software. The table in Appendix C of the Altarus Corporation FIPS 140-1 Certification Document provides a complete list of each procedure exposed by the module, its parameters, and the logical interface category to which each of its parameters belongs. The physical interfaces of the ACM may be said to exist between the hardware components and peripheral devices constituting the configuration of the general purpose PC upon which the software is installed. The ACM does not provide a power interface, or a maintenance access interface.

2.2 Roles and Services

The ACM supports the two roles defined in the FIPS 140-1 standard, section 4.3.1, as the User role and the Crypto Officer role but does not implement any authentication or authorization of an operator, but assumes authorization by virtue of the ability of the operator to make calls into the ACM's functions. The ACM does not support concurrent operators, therefore only a single operator assuming one of these roles may operate the module at any one point in time. No means are provided to control access to the module prior to startup. The ACM reverts to the default role of Crypto Officer upon every startup and the operator's assumed role is changed from the Crypto Officer role to the User role when the Initialization service is completed. The User role remains active until the module is shutdown.

The ACM provides services to the operator, based on the operator's assumed role. In this respect, access to the Initialization service is restricted to operators assuming the Crypto Officer role. This service specifies the memory management functions to be used internally for memory allocation, and then initiates the power-up sequence for the module. Upon completion of the Initialization service, the current role is changed from the Crypto Officer role to the User role.

Service	Purpose/Function	Allowed In Role(s)
Encryption	Encrypt plaintext using a symmetric or asymmetric cipher. Encryption using 3DES, and RSA key exchange key pairs are supported. 3DES is the only FIPS-authorized encryption algorithm supported.	User
Decryption	Decrypt ciphertext using a symmetric or asymmetric cipher. Decryption using 3DES, and RSA key exchange key pairs are supported. 3DES is the only FIPS-authorized decryption algorithm supported.	User
Message Integrity	Verify the integrity of a message by computing and verifying a secure hash which is a product of both the message and a shared key. Message integrity with the SHA-1 secure hashing algorithm in combination with a 3DES key is supported (HMAC-SHA-1). HMAC-SHA-1 is the only FIPS-authorized message integrity verification method supported.	User
Key Decryption/Importation	Given an RSA key exchange key and an encrypted 3DES session key, internally decrypts the session key and provides a token which can be used to encrypt and decrypt data w/ the session key. Plaintext session key is never visible outside the module.	User
Key Encryption/Exportation	Given an RSA key exchange key and a 3DES session key token, encrypts the session key and produces a block of ciphertext suitable for transmission over an insecure transport. Plaintext session key is never visible outside the module.	User
Key Generation	Generation of 3DES, and RSA key exchange keys are supported. Generation is via a FIPS-approved SHA1-based RNG. Plaintext keys are never visible outside the module; only the tokens which provide internal references to the key data.	User
Key Destruction	Frees memory associated w/ a key token, and zeroizes the key data itself.	User
Random Number Generation	Generates an arbitrary series of pseudo-random bytes using a FIPS-approved SHA1-based RNG.	User
Show Status	Returns the current status of the module: error or ready.	User
Self-test	Initiates a self-test of the SHA1 and 3DES encryption algorithms, and the RNG.	User
Initialization	Specifies the memory management functions to be used internally for memory allocation, then initiates the power-up sequence for the module. Upon completion of the Initialization service, the current role is changed from Crypto Officer to User	Crypto Officer

Table 1: ACM Roles and Services

Self-tests are run by the module upon startup, when the Crypto Officer role is active. If the self-tests complete successfully, the module will transition to Ready state and the User role will be activated. In this state, cryptographic services are available to the operator assuming the User role. However, if any of the self-tests fail, the module will transition to Error state in which all cryptographic services will terminate.

Other services provided by the ACM include Message Integrity verification using the SHA-1 secure hashing algorithm in combination with a 3DES key (HMAC-SHA-1), Key Decryption/Importation, Key Encryption/Exportation, the Show Status service which advises the operator of the current module status which may be either Error or Ready, Key Destruction through zeroization and Self-Test services.

2.3 Cryptographic Key Management

The ACM contains several functions that can be combined to meet FIPS 140-1 Level 1 requirements for Cryptographic Key Management.

2.3.1 Key Generation

The ACM supports generation of 3DES and RSA key exchange public and private keys using a FIPS-approved RNG. The Cryptographic Module's RNG is an implementation of ANSI X9.17.

2.3.2 Key Distribution

The ACM provides functional building blocks for public key-based key exchange, which are used by Altarus software products to implement public key-based key exchange. For instances when key data is needed for transmission across a network, the module provides functions to export and import RSA public keys, (not considered sensitive), in clear text, and to export and encrypt and import and decrypt 3DES keys. The technique used to transmit 3DES keys is standard, accepted practice in commercial implementations, using public/private key encryption.

The ACM supports electronic key distribution/entry of RSA key exchange public keys and 3DES keys. Keys are exported by Cryptographic Modules on other machines, and then imported by the ACM.

2.3.3 Key Storage

The ACM does not store any CSPs, including keys, in any permanent or non-volatile storage area/mechanism. All CSPs are stored in memory only, and zeroized prior to release.

2.3.4 Key Destruction

All keys supported by the ACM, including RSA public and private keys and 3DES keys are zeroized when they are no longer required. Key data is zeroized prior to releasing the memory associated with the keys to ensure that it may not be recovered later when the freed memory is reassigned to another process. The ACM does not maintain sensitive internal security parameters other than cryptographic keys and key archiving is not supported.

2.3.5 Key Protection

Keys are protected from exposure, unauthorized modification and substitution, at run-time by limiting access to the actual key data to within the logical boundary of the ACM defined under Section 2 Cryptographic Module . All secret keys are encrypted prior to output. Private keys are never output for any reason. In the case of the 3DES keys, unauthorized modification and substitution are also prevented by providing access to the key data in ciphertext form only. All intermediate key generation states are restricted to the module's cryptographic boundary and are therefore inaccessible.

External modules that use the ACM for cryptographic services are assigned key tokens to represent each key the module is using. The external module does not have any knowledge of the meaning of this token, and therefore cannot convert it into the actual key data required to perform cryptographic operations with the key. In order to use the key token for cryptographic services, the external module must call the appropriate function in the ACM, passing the key token as a parameter. This ensures that key data is never exposed.

2.3.6 Cryptographic Algorithms

The ACM supports both FIPS-approved and non FIPS-approved algorithms. 3DES and HMAC-SHA-1 are the FIPS-approved encryption algorithm employed by the Altarus Cryptographic Module, and SHA-1 is the FIPS-approved secure hashing algorithm employed by the ACM. The cryptographic module also uses the SHA-1 secure hashing function as the basis for the HMAC function. By convention, the HMAC implementation that uses SHA-1 is referred to as HMAC-SHA-1. Therefore ACM supports the HMAC-SH1 algorithm. The Non FIPS-approved algorithm supported by the ACM is the RSA public key algorithm.

Cryptographic Algorithms	
FIPS Approved:	
	TDES CBC Cert# 99
	SHA-1 Cert# 88
	HMAC/SHA-1 (Cert#88: vendor affirmed)
Non-FIPS Approved:	
	RSA

Table 2: FIPS Approved and Non-FIPS Approved Cryptographic Algorithms supported by ACM.

2.4 Self-Tests

The ACM implements a number of self-tests to verify correct functioning of the module. This includes power-up self-tests (which are also callable on-demand) and conditional self-tests.

2.4.1 Power-up Self-Tests

Power-up tests are executed automatically upon initialization of the module and therefore do not require any operator intervention. Tests performed upon module initialization include Module Integrity tests, Known answer tests of the FIPS-approved cryptographic algorithms (3DES and SHA-1), and RNG seeding verification. These power-up tests can be initiated manually by calling CryptoSelfTest, and as with the automatic execution of these tests, any failure immediately transitions to the Error state.

2.4.2 Conditional Self-Tests

Pair-wise consistency tests are performed on test data blocks encrypted with the RSA public key, then decrypted with the RSA private key. Failure of this test immediately transitions to the Error State.

In the RNG Conditional Self-Test, as random data is generated with the RNG, each 32-bit block is compared with the previous 32-bit block. If any two contiguous blocks are found to be identical, the RNG is said to be “stuck”, and the module state transitions to the Error state. In this state, all cryptographic operations are suspended until the module is powered down and restarted.

3 MODULE OPERATION SECURITY

The ACM is linked with a number of Altarus products at build time. Thus, the compiled ACM is embedded within the compiled code for Altarus’ software products. This is the only form of the ACM that Altarus distributes externally, thus users do not have any access to scrutinize or modify the source code. The ACM is also compiled with a SHA-1 hash of its code segment. During power-on self-tests, this hash is compared with the hash of the module the caller has loaded. If these hashes do not match, indicating the potential for module corruption, the power-on self-test, and thus initialization, fails and the module transitions to the Error state. No cryptographic operations may be performed while the module is in the Error state.

The ACM has been validated to be used with one or more Altarus applications as a shared Windows DLL.