TriCipher, Inc.

TriCipher Armored Credential System™

(Hardware Version: 1000; 2000; Firmware Version: 3.1)

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation
Version 0.09
January 31, 2007

Table of Contents

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the TriCipher Armored Credential System™ (TACS) from TriCipher, Inc. This Security Policy describes how the TACS 1000 and 2000 firmware version 3.1, build 255 meets the security requirements of FIPS 140-2 and how to run the TACS in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the TACS.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/cryptval/.

The TACS 1000 and 2000 are referred to in this document as TACS, the Appliance, or the modules.

1.2 References

This document deals only with operations and capabilities of the TACS in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The TriCipher website (http://www.tricipher.com) contains information on the full line of products from TriCipher.
- The CMVP website (http://csrc.nist.gov/cryptval) contains contact information for answers to technical- or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to TriCipher. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to TriCipher and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact TriCipher.

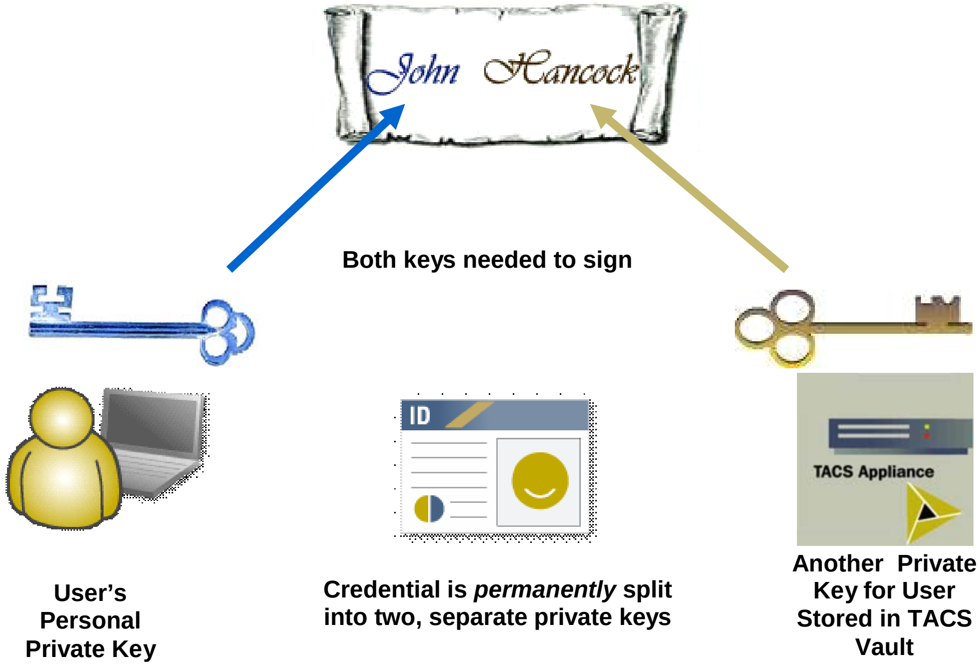
2. TRICIPHER ARMORED CREDENTIAL SYSTEM

2.1 Overview

Businesses and government agencies need a way to protect identity information and to perform secure authentication, and the TriCipher Armored Credential System provides the solution. Weak authentication, and inadequately protected identity data in on-line services are resulting in increasing instances of fraud. Organizations suffer reputational and financial losses and consumers loose confidence in on-line services. Organized criminal activity has just about started to move on-line, but is growing very fast. New attack vectors such as phishing have rapidly gained prominence in a matter of a few months. It is impossible to predict the nature of attack activity in 2006, let alone in 2007, 2008, and so on. Enterprises are faced with uncertainty about the nature of real cyberattacks, yet must make funding decisions today on how to improve their existing authentication infrastructure. Therefore solutions that allow adjustment of credential strength as needed are gaining prominence.

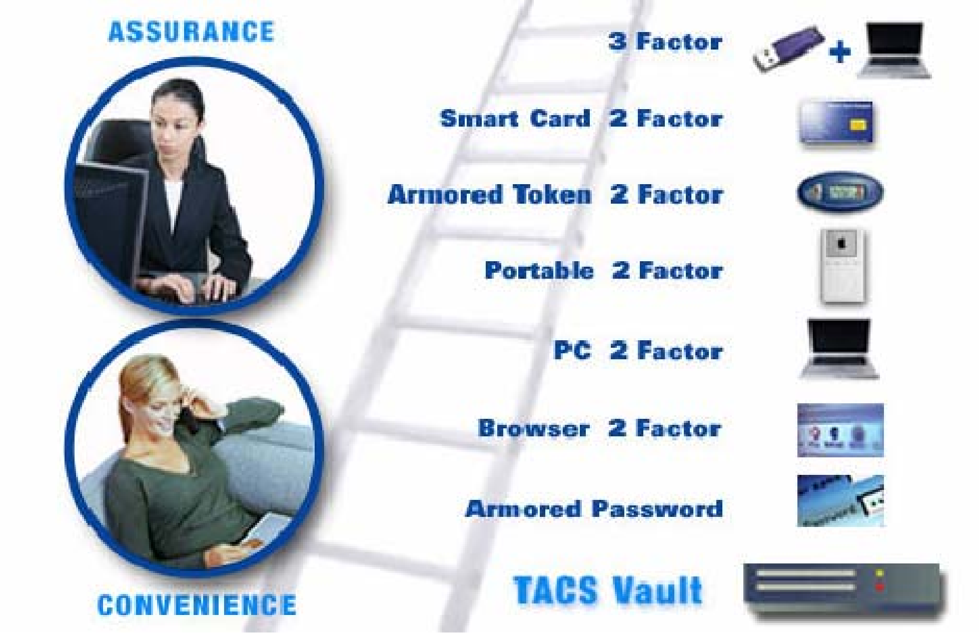
Most organizations require high-grade multi-factor authentication for their high-end users, yet few can justify the high cost for all their users. Flexible multi-factor authentication enables organizations to issue the appropriate grade of credential for each user class from a single reusable infrastructure, and make adjustments as needed.

The TriCipher Armored Credential System™ (TACS) provides a single platform that can issue and support a flexible range of credentials from a single infrastructure. The only system of its kind, the TACS Vault can be used to issue authentication credentials of many different types and can also serve as a vault for identity data (or encryption keys), providing a comprehensive solution to the problems of weak authentication and inadequately encrypted identity data. The TriCipher Armored Credential System (TACS) contains the TACS ID Vault hardware. The complete system consists of the following components: TACS ID Vault, Distributed Management, Distributed Deployment, and TACS Tools consisting of the Management Tool, User Administration Tool, Certificate Authority Utility and TACS ID Tool. The TACS ID Tool is an application installed on the user’s computer workstation.


John Hancock
Both keys needed to sign
ID
TACS Appliance
User's Personal Private Key
Credential is *permanently* split into two, separate private keys
Another Private Key for User Stored in TACS Vault

The above diagram illustrates Tricipher's non-Approved 3-key RSA algorithm. Using the 3-key RSA algorithm, the TACS splits the user's RSA private key in two parts. One part of the key is stored on the TACS Vault and never leaves it, and the other part is created on the user's local machine using a password chosen by the user (In contrast, conventional RSA uses a single private key known only to the user.) The original RSA private key is destroyed. The TACS keeps no record of the user's portion of the private key, and the user has no knowledge of the TACS portion of the private key.

Whenever the user is required to sign information, a partial signature is performed on the TACS, which is then completed on the user's local machine using the user's key, which is derived from his password. (This signature is different from the FIPS approved RSA digital signature used for TLS exchange.) However, the recipient need never know that the signature was computed using the TACS. Flexible multi-factor authentication is achieved by generating the user's personal private key from a variety of factors depending upon the credential strength.



The authentication ladder shows TACS issued credentials in increasing order of strength as we go up the ladder. This flexibility is achieved due to the use of 3-key RSA as the underlying cryptographic engine for all forms of authentication. The authentication ladder can be broken down into two categories based on the amount of credentials provided by the user in order to authenticate themselves. The two categories are: Single Credential and Multi-Part Credentials.

The simplest credential and only Single Credential is called Armored Passwords. Here, the user logs in as they always have, using a memorable password over SSL. A plug in at the web server computes a numeric “key” from the password, and then destroys the password. The password is never stored. The web server calls the TACS and authenticates using both the credential it created from the password and one stored on the TACS. No thief can crack a database of hashed passwords that doesn’t exist. The password, though, should still be chosen to resist social guessing.

While there is only one method of Single Credential there are several Multi-Part Credentials. Multi-Part Credentials can be divided into two categories of either 2 Factor or 3 Factor Credentials.

2 Factor Credentials consists of the following methods: Browser 2 Factor, PC 2 Factor, Portable 2 Factor, Armored Token 2 Factor, and Smart Card 2 Factor. As in Single Credentials, a 2 Factor Credential never stores the password. It can be seamless for the user, but does require a small piece of client side software, the TACS ID Tool. The Tool collects the user’s id and password, then signs (encrypts) the password using a key stored on the PC in the Intel® TPM or Windows® Key Store or in a removable device. This removable device can consist of any of the methods mentioned above in the diagram such as a cookie or certificate in a

browser, an armored token, a smart card, or some other portable device. This key is completely invisible to the user – to them; the login is completely familiar, only done through a special window. Once encrypted, the original password is destroyed, never stored. The Tool authenticates the user to the TACS which verifies that the user's credential is still valid, and then uses this authentication to prove the user's identity to the web server.

3 Factor Credentials works much the same as 2 Factor Credentials, except it requires a token that must be carried by the user. The user must plug in the token before logging on. When the TACS ID Tool signs the password, it does so with the key stored on the user's machine as well as the key from the token. In addition, the key in the token is regenerated after each use. If the token or its key is stolen and used, the user discovers the theft at the next logon and can reset their credentials.

The types of Single Credential and Multi-Part Credentials are summarized in the following bulleted list.

- Single Credential
        - Armored Password
- Multi-Part Credentials
    - 2 Factor Credentials
        - Browser 2 Factor
        - PC 2 Factor
        - Portable 2 Factor
        - Armored Token 2 Factor
        - Smart Card 2 Factor
    - 3 Factor Credentials
        - Armored Password + a key stored securely on the PC (Brower 2 Factor or PC 2 factor) + a removable token (Portable, Armored Token, or Smart Card 2 Factor)

The TACS Vault itself is specially designed to afford a very high degree of assurance. It is protected using three layers of defenses: (i) it has a locked down, dedicated hardened OS, (ii) all system and user administration is strictly compartmentalized on least privilege, need to know, basis, and (iii) it uses FIPS 140-2 Level 2 rated cryptography. It is also highly scalable and fault tolerant, running as a set of 2 or 3 load-balanced and failover appliances. Finally it is a high assurance platform which can act as a secure storage facility to protect identity data such as credit card numbers. Enterprises can choose to either store identity data directly on the TACS Vault, or else can choose to encrypt data in place, and use the TACS Vault as a key management facility. The data is only available to authorized users after successful strong authentication.

2.2 TACS Specification

The TriCipher Armored Credential System™ (TACS) 1000 and 2000 are multi-chip standalone modules that meet overall level 2 FIPS 140-2 requirements. The TACS 1000 is a 2U rack-mountable server, and the TACS 2000 is a 5U rack-mountable server. Both have tamper-evident labels affixed to the case in order to provide evidence of any attempts to tamper with the module's hardware (placement of these labels is described in Section 3, Secure Operation). The cryptographic boundary is defined by the outer case of the modules that encloses the complete set of hardware and software components.

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Table 1 – Security Level Per FIPS 140-2 Section

2.3 TACS Interfaces

The modules' designs separate the physical ports into four logically distinct and isolated categories. They are:

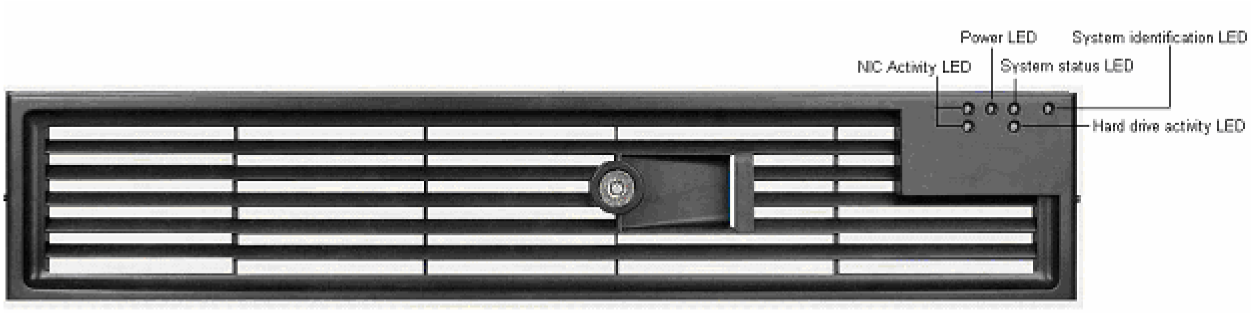
- Data Input
- Data Output
- Control Input
- Status Output

The modules' functionality is primarily accessed over the Ethernet ports. Operators log in via the Ethernet ports, accessing the module through an encrypted session. Other than tape backups for TACS 2000, all data input/output occurs over the Ethernet ports. The tape backup unit is an integral module device that connects internally via a SCSI interface.

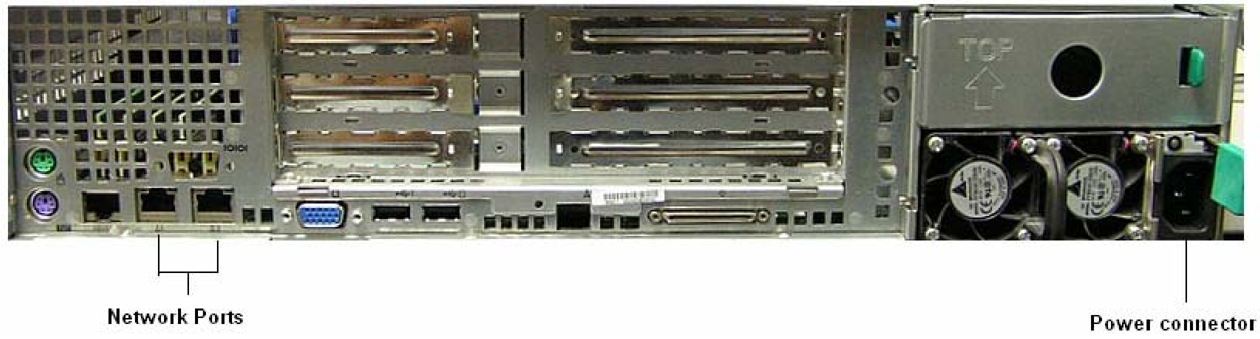
Data input/output are the packets utilizing the services provided by the module. These packets enter and exit the modules through the network ports.

Control input consists of data entered into the modules through the network ports and the input for the power connector.

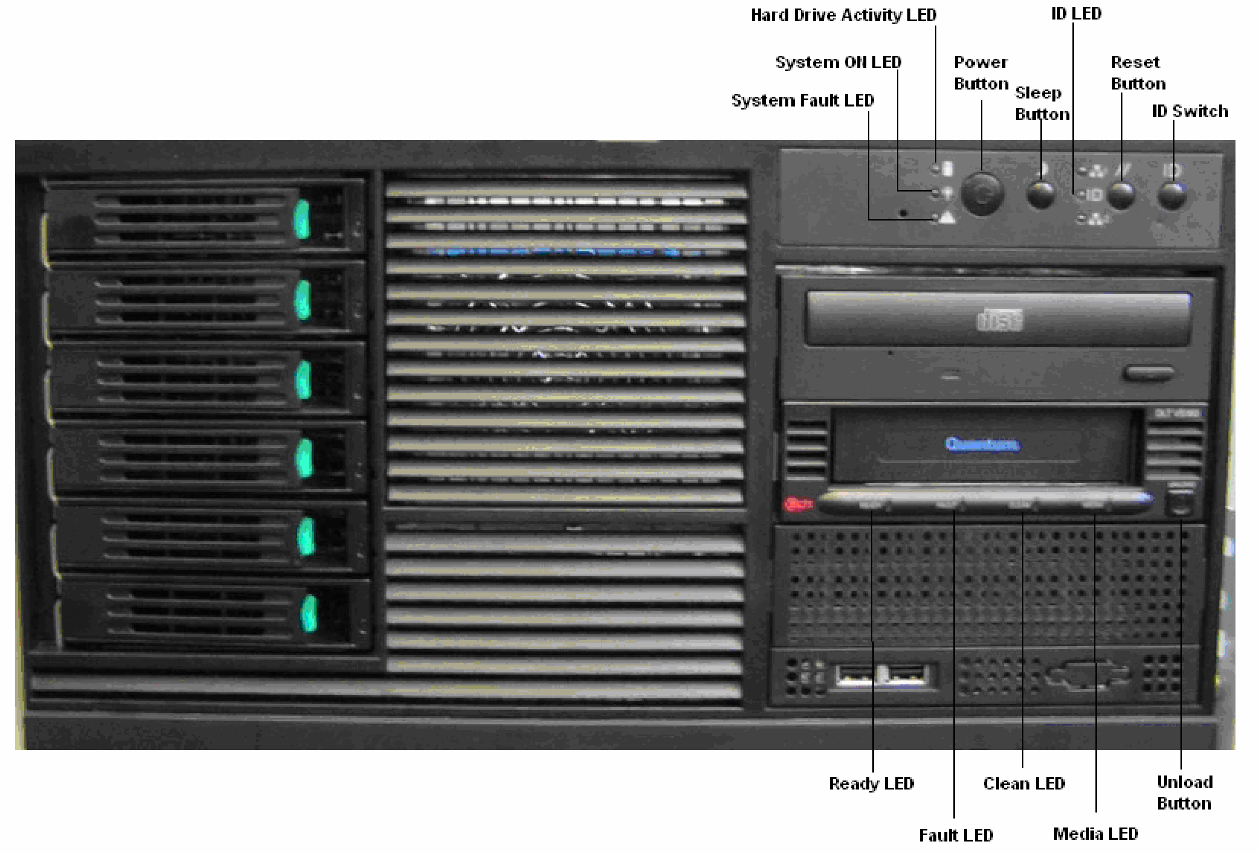
Status output consists of the status indicators displayed through the LEDs and log information output to the log servers. Additionally, the Crypto Officer has access to the user statistics.



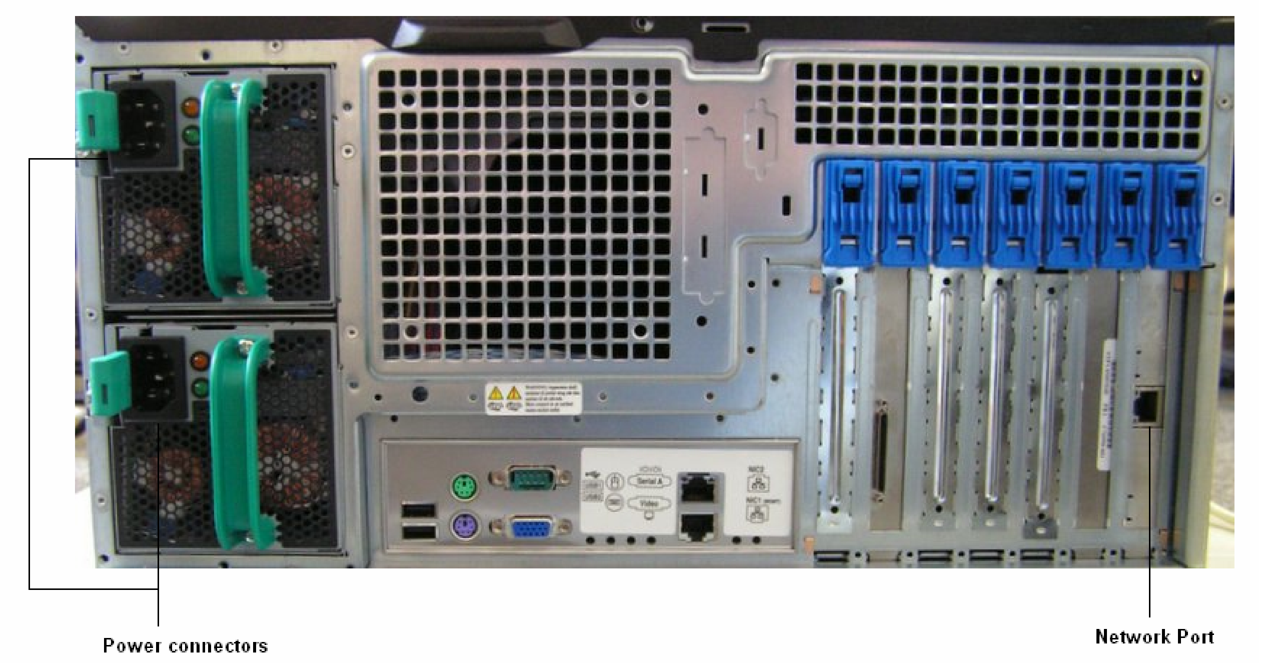
Front View of the TACS 1000 Physical Ports



Rear View of the TACS 1000 Physical Ports



Front View of the TACS 2000 Physical Ports



Rear View of the TACS 2000 Physical Ports

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

TACS 1000 Physical Interface	TACS 2000 Physical Interface	FIPS 140-2 Logical Interface
Network ports	Network ports, Tape drive	Data Input Interface
Network ports	Network ports, Tape drive	Data Output Interface
Network ports	Network ports	Control Input Interface
Network ports, LEDs	Network ports, LEDs	Status Output Interface
Power connector	Power connector	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces

Note: Tamper-evident labels restrict access to the USB ports, SCSI ports, PS/2 ports (mouse and keyboard), serial ports, monitor port and CDROM drive for the modules in FIPS mode of operation.

2.4 Roles and Services

The TACS supports identity-based authentication. There are two roles in the TACS (as required by FIPS 140-2) that operators may assume: a Crypto Officer role and User role.

2.4.1 Crypto Officer Role (Identification and Authentication, Access Control)

The Crypto-Officer role is used to configure and maintain the modules. By default, this role is divided into six distinct sub-roles. In order to assume any of the six Crypto-Officer roles, you enter the account (user name) and activation code (password) associated with the role. If the account and activation code are correct you will be logged in under that role and you will have the services associated with that role available to you. These six sub-roles are:

1. **Super Manager**: Initializes the module and supervises managerial roles
2. **System Manager**: Sets system parameters
3. **Security Manager**: Sets security parameters and Appliance time server
4. **Super CSR**: Supervises Consumer Service Representative roles
5. **Create CSR**: Supervises consumer or end-user accounts
6. **Modify CSR**: Maintains consumer or end-user accounts

Sections 2.4.1.1 – 2.4.1.6 detail the services available to the Crypto-Officer role, separated according to sub-role. In addition to these services, the Crypto-Office role has the ability to access all services available to the User role.

2.4.1.1 Super Manager

The authenticated Super Manager has access to the following services:

Service	Description	Input	Output	CSP and Type of Access
Initialization	Initialize the module	Command and parameters	Command response	Appliance RSA key pair – read/write CA public key – read/write Appliance SSL RSA key pair – read/write
Role and record definition	Edit the role and record definition	Command	Command response	
Zero out appliance data	Destroys all data on the appliance	Command	Command response	All - Write
Appliance report	Generate and retrieve appliance report	Command	Command response	
IP address	Set the IP address for manager and user accounts	Command and parameters	Command response	
Mirror appliance	Configure mirror TACS servers	Command and parameters	Command response	Mirror public key - Read
Recovery	Recover from backup	Command	Command response	
Restart	Restart appliance processes	Command	Command response	
Shutdown	Shutdown or reboot the module	Command	Command response	
Update code	Upload and install the updates	Command	Command response	Upgrade RSA public key - Read
Create	Creates managerial accounts	Command and parameters	Command response	Operator activation code - Write
Read	Read managerial account information	Command	Command response	
Modify	Edit managerial account information	Command and parameters	Command response	
Suspend	Locks managerial accounts	Command	Command response	
Unsuspend	Unlocks managerial accounts	Command	Command response	
Revoke	Revoke managerial accounts	Command	Command response	Operator private key components - Write
Reset	Generate new activation code for a revoked account	Command	Command response	Operator activation code - Read
Delete	Destroy managerial account and information	Command	Command response	Operator RSA private key components - Write

Table 3 – Crypto Officer Services, Descriptions, CSPs

2.4.1.2 Security Manager

The authenticated Security Manager has access to the following services:

Service	Description	Input	Output	CSP and Type of Access
Security parameter	Set the security parameters for the module	Command and parameters	Command response	
Password management	Configure parameters for password management and authentication settings	Command and parameters	Command response	
External CA	Configure external CA to sign operator certificates	Command and parameters	Command response	
Certificate management	Configure the validity, hashing algorithm and extension for certificates	Command and parameters	Command response	
Security settings	Configure security setting for the module	Command	Command response	Roam tether questions - Read
User Statistics	Get user status	Command and parameters	Command response	

2.4.1.3 System Manager

The authenticated System Manager has access to the following services:

Service	Description	Input	Output	CSP and Type of Access
System parameter	Set the system parameters for the module	Command and parameters	Command response	
IP address	Set the IP address for manager and user accounts	Command and parameters	Command response	
LDAP	Configure LDAP server for publishing certificates	Command and parameters	Command response	LDAP password - Write
Logging	Set syslog server for logging	Command and parameters	Command response	
SNMP	Set SNMP for monitoring the appliance	Command and parameters	Command response	SNMP password - Write
Mirror appliance	Configure mirror TACS servers	Command and parameters	Command response	
Backup	Configure backup settings	Command and parameters	Command response	

2.4.1.4 Super CSR

The authenticated Super CSR has access to the following services:

Service	Description	Input	Output	CSP and Type of Access
Create	Create CSR accounts	Command and parameters	Command response	Operator activation code - Write
Read	Read CSR accounts	Command and parameters	Command response	
Modify	Modify CSR accounts	Command and parameters	Command response	
Suspend	Suspend CSR accounts	Command and parameters	Command response	
Unsuspend	Unsuspend CSR accounts	Command and parameters	Command response	
Revoke	Revoke CSR accounts	Command and parameters	Command response	Operator private key components - Write
Reset	Reset CSR accounts	Command and parameters	Command response	Operator activation code - Read
Delete	Delete CSR accounts	Command and parameters	Command response	Operator RSA private key components - Write

2.4.1.5 Create CSR

The authenticated Create CSR has access to the following services:

Service	Description	Input	Output	CSP and Type of Access
Create	Create consumer accounts	Command and parameters	Command response	Operator activation code - Write
Modify	Modify consumer accounts	Command and parameters	Command response	
Read	Read consumer accounts	Command and parameters	Command response	
Suspend	Suspend consumer accounts	Command and parameters	Command response	
Unsuspend	Unsuspend consumer accounts	Command and parameters	Command response	
Revoke	Revoke consumer accounts	Command and parameters	Command response	Operator private key components - Write
Reset	Reset consumer accounts	Command and parameters	Command response	Operator activation code - Read
Delete	Delete consumer accounts	Command and parameters	Command response	Operator RSA private key components - Write
Import a batch file	Import a batch file to create multiple consumer accounts	Command and parameters	Command response	Operators activation code - Read

2.4.1.6 Modify CSR

The authenticated Modify CSR has access to the following services:

Service	Description	Input	Output	CSP and Type of Access
Read	Read consumer accounts	Command and parameters	Command response	
Modify	Modify consumer accounts	Command and parameters	Command response	
Suspend	Suspend consumer accounts	Command and parameters	Command response	
Unsuspend	Unsuspend consumer accounts	Command and parameters	Command response	
Revoke	Revoke consumer accounts	Command and parameters	Command response	Operator private key components - Write
Reset	Reset consumer accounts	Command and parameters	Command response	Operator activation code - Read
Delete	Delete consumer accounts	Command and parameters	Command response	Operator RSA private key components - Write
Import a batch file	Import a batch file to create multiple consumer accounts	Command and parameters	Command response	Operators activation code - Read

2.4.2 User Role (Identification and Authentication, Access Control)

The User role accesses the end-user functionality of the module and does not have the ability to use any of the management functionality available to the Crypto-Officer. The services available to the User role include the ability to:

Service	Description	Input	Output	CSP and Type of Access
Activate	Activate account	Command and parameters	Command response	Operator activation code - Read
Login	Authenticate the user role	Command and parameters	Command response	Operator authentication components - Read
Logout	Logout the user	Command	Command response	TACS session keys - Write
Revoke	Permanently revoke user certificate	Command and parameters	Command response	Operator private key components - Write
Change password	Change the user password	Command and parameters	Command response	
Change profile	Change the user profile	Command and parameters	Command response	
Get certificate	Get user certificate	Command and parameters	Command response	Operator public key - Read
Logout and delete certificate	Logout and remove public certificate stored on the operator PC	Command	Command response	TACS session keys – Write Operator public key - Write
Logout and delete tethering credentials	Logout and remove tether data stored on the operator PC	Command	Command response	Operator tether data – Write
Register	Register computer for tethering information	Command and parameters	Command response	Operator tether data – Read
Sign	Sign and verify signatures	Command and parameters	Command response	Operator authentication data – Read
Decrypt	Decrypt data	Command and parameters	Command response	Operator authentication data – Read

Table 4 – User Services, Descriptions, Inputs and Outputs

2.4.3 Authentication Mechanisms (Identification and Authentication, Access Control)

The Crypto Officer can access the Appliance using the *TACS Manager* and *TACS CSR Utility* provided by TriCipher, or via a custom API application. The User can access the Appliance using the *TACS Identity Protection Tool* provided by TriCipher or via a custom API application. The Crypto Officer and User can only access the module over a TLS session. The operators authenticate via 3-Key RSA by signing the challenge sent by the TACS with the operator portion of the RSA private key component (which is constructed from a password, an optional tether key, and an optional two-factor key), and if present also with the Tether RSA private key and/or the Two Factor RSA private key. The TACS completes the signature with the TACS portion of the operator RSA private key component and verifies the challenge with the operator public key.

3-Key RSA Authentication Component Type	Strength	Role
Password	Considering a case sensitive alphanumeric password with repetition, the total possible combinations for the password are 62^6. The probability for a random attempt to succeed is 1:62^6 or 1:56800235584, and, since this authentication attempt is additionally piped over an encrypted session, it is not possible to perform enough authentication attempts to reduce the 1:62^6 chance per attempt to 1:100,000 over a minute.	Crypto Officer, User
Tether, Two-factor key	When the tether and/or two factor RSA keys are used the authentication function is at least as strong as a 1024 bit RSA key. Using conservative estimates equating a 1024 bit RSA key to an 80 bit symmetric key, the probability for a random attempt to succeed is 1:2^80 or 1:1208925819614629174706176, and it is not possible for an operator to perform enough authentication attempts to reduce the 1:2^80 chance per attempt to 1:100,000 over a minute	Crypto Officer, User

Table 5 – User Services, Descriptions, Inputs and Outputs

2.5 Physical Security

TACS 1000 and 2000 are multi-chip standalone cryptographic modules enclosed in a hard, opaque metal case that completely encloses all of the internal components of the modules. There are only a limited set of vent holes provided in the case, and these are all obscured to prevent viewing of the internal components of the module. Tamper-evident labels are applied to the case of the 1000 and 2000 to provide physical evidence of attempts to remove the case or access any disabled ports of the modules. For instructions on the placement of the tamper evident refer to “Secure Operation” section below.

The TACS 1000 and 2000 components are of production-grade quality and were tested and found conformant 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).

Figure 1 and Figure 2 below are pictures of the screens that are installed in the TACS at the factory, which are used to obscure the ventilation holes.

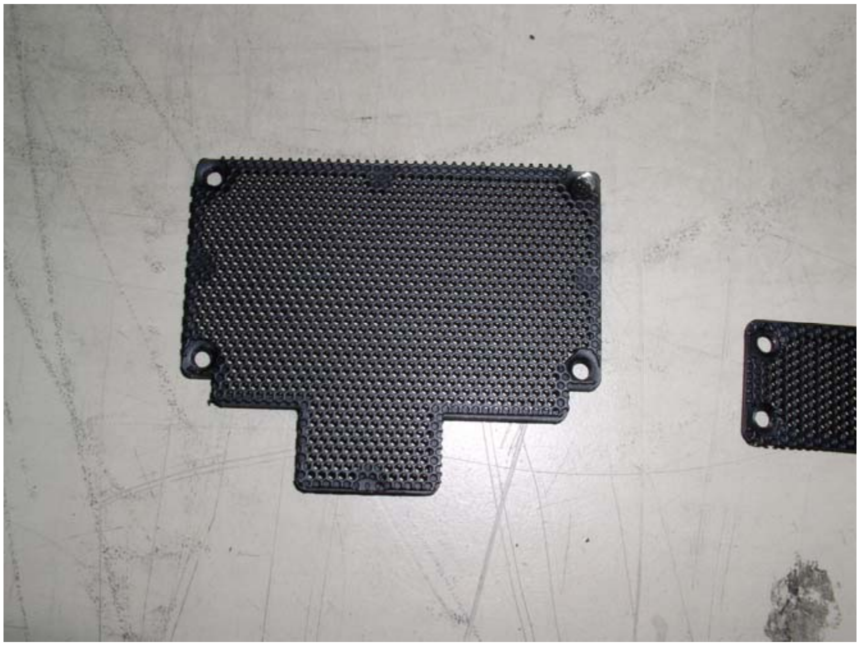


Figure 1 - Back Screen

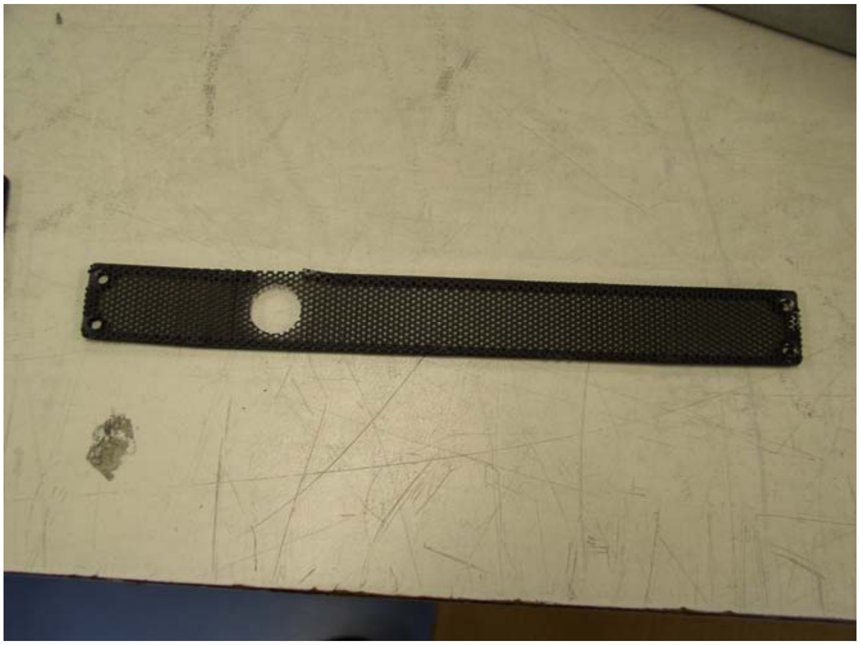


Figure 2 - Side Screen

Figure 3 and Figure 4 below show what the back and side of the TACS looks like with the screens installed. With the screens installed the inside of the TACS is obscured from view and probing tools.

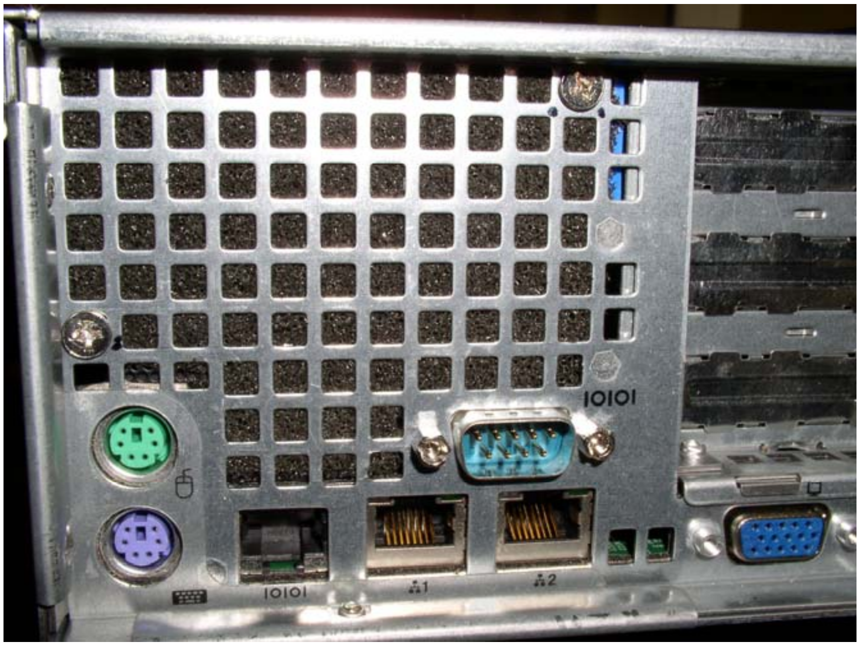


Figure 3 - Back Panel with Screen

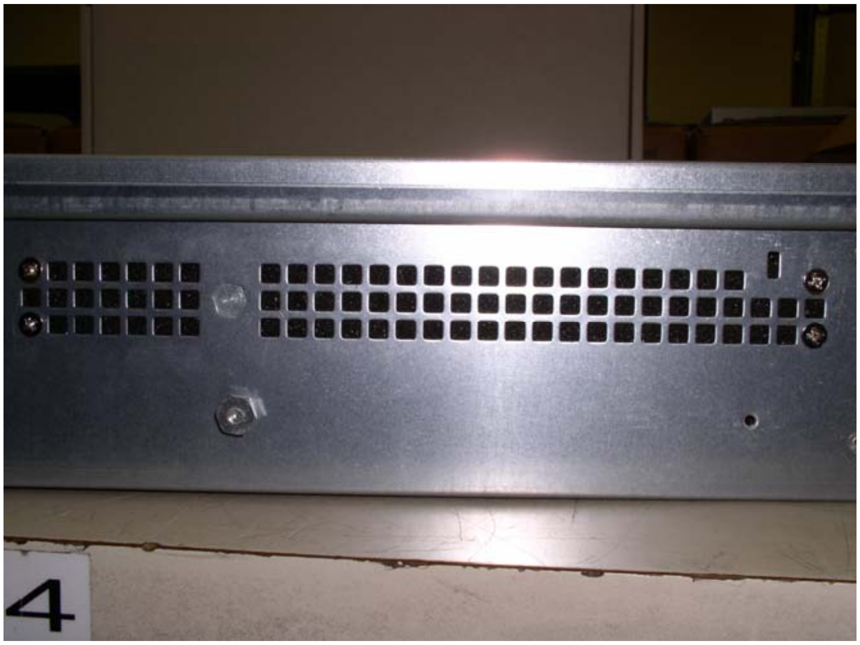


Figure 4 - Side Panel with Screen

2.6 Operational Environment

The operational environment requirements do not apply to the TACS 1000 and 2000. The modules do not provide a general purpose operating system and only allow firmware updating using digitally signed TriCipher firmware updates. Additionally, only updates validated to FIPS 140-2 may be activated, as described in the Crypto-Officer Guidance below.

2.7 Cryptographic Key Management

The TACS 1000 and 2000 implement the following FIPS-approved algorithms:

- RSA (1024 bits) – RSA key generation, PKCS#1(sign/verify) (certificate 120)[1]
- Triple DES-CBC (168 bits) – FIPS 46-3 (certificate 413)
- FIPS 186-2 PRNG – Appendix 3.1 of FIPS 186-2 [(x-Original); (SHA-1)] (certificate 170)
- SHA-1 – FIPS 180-2 (certificate 430)
- HMAC SHA-1 (key length: 24 bytes; MAC length 20 bytes) – FIPS 198 (certificate 159)

Apart from the algorithms the module uses the following mechanisms in FIPS mode of operation:

- TLS v1 for all the operator communication
- SCP for backup and recovery (SSHv2)
- SFTP for recovery (SSHv2)

Additionally, the module utilizes the following non-FIPS-approved algorithm implementation:

- RSA (key wrapping; key establishment methodology provides 80-bits of encryption strength) (not Approved but can be used in FIPS mode)
- Operating System RNG – for seeding the FIPS-approved deterministic RNG (not Approved but can be used in FIPS mode)
- PKCS #5 for password based key expansion (cannot be used in FIPS mode)
- MD5 for TLS (cannot be used in FIPS mode)

The module disables the following protocols when running in FIPS mode:

- SSL V3.0

The module supports the following critical security parameters:

[1] Key wrapping, key establishment methodology provides 80-bits of encryption strength.

Table 6 - TriCipher Detailed Key/CSP Table

Key	Key type	Generation/Input	Output	Storage	Zeroization	Use
Appliance RSA private key	RSA key (1024 bits)	Generated internally using ANSI X9.31 RSA key generation	Not output from the TACS	Stored on disk	Zeroized by generating a new key pair	Sign Operator RSA public key (in certificate) and during login protocol; or for authentication during mirror operation
Appliance RSA public key	RSA key (1024 bits)	Generated internally using ANSI X9.31 RSA key generation; Input as signed digital certificate during initialization	Output with certificate chain or by CO	Stored on disk	Zeroized by generating a new key pair	Used by the Client to verify appliance signature and operator certificate verification; or for authenticating the mirror TACS
CA public key	RSA public key (1024 bits)	Externally generated according to the generating CA's procedures and input into the TACS during initialization	Output with certificate chain	Stored on disk	Zeroized by importing a new CA certificate	Sign the Appliance public key certificate
TLS RSA private key	RSA key (1024 bits)	Externally generated by a CA (e.g., Verisign) and input during initialization	Not output from the TACS	Stored on disk	Zeroized by importing new SSL certificate	Public key-based key exchange during TLS handshake
TLS RSA public key	RSA key (1024 bits)	Externally generated and input during initialization	Output during SSL handshake or by CO	Stored on disk	Zeroized by importing new TLS certificate	Public key-based key exchange during TLS handshake
TACS session keys (R12)	2 TDES keys (168 bits), 2 HMAC keys (192 bytes)	Negotiated during TACS session establishment	Not output from the TACS	Stored on disk in SKD database	Zeroized when not needed or when the TACS is powered down	Secure TACS session traffic
TLS session keys	TDES keys (168 bits)	Negotiated during TLS session establishment	Not output from the TACS	Volatile memory only	Zeroized when not needed or when the TACS is powered down	Further secure TACS session traffic
Activation Code	Alphanumeric string (minimum of 8 characters)	Entered into TACS over an encrypted TACS session; or generated by the TACS when the operator account is reset	Output from the TACS when the operator account is reset	Stored on disk as hash in SKD database	Zeroized when the account is activated or reset	Used for activating the Crypto Officer and Users accounts

Key	Key type	Generation/Input	Output	Storage	Zeroization	Use
Operator Password	Alphanumeric string (minimum of 8 characters)	Entered over a TLS session.	N/A	N/A	Zeroized when the password is updated with a new one	Used for generating the authentication data
Tether RSA public key	RSA key (1024 bits)	Entered into TACS over an encrypted TACS session	Not output from the TACS	Stored on disk in PKD database	Zeroized when the operator is revoked	Used for verifying the tether data
Tether RSA private key	RSA key (1024 bits)	If roam tether is enabled then tether components are entered into the TACS over an encrypted TACS session	If roam tether is enables tether components are output during register protocol over an encrypted TACS session	TDES encrypted components of key pair are stored in PKD	Zeroized when the operator is revoked	Used for generating the authentication data
Roam Tether questions	Alphanumeric string	Hardcoded in the TACS binaries	If roam tether is enabled, output during operator key generation and register protocols	Stored on disk	Zeroized when the Appliance is zeroized	Used for verifying the operator when registering on a new machine
Roam Tether secret response	Alphanumeric string	If roam is enabled then it is created by the operator during activation and entered over an encrypted TACS session if roam tether is enabled	Not output from the TACS	Stored on disk	Zeroized when the operator is revoked	Used for verifying the operator when registering on a new machine
Two Factor private key	RSA key (1024 bits)	N/A	N/A	N/A. Stored outside the TACS	N/A	Used to generate authentication data for operators with two factor authentication
Two Factor public key	RSA key (1024 bits)	If two-factor is enabled then it is generated externally by the FIPS-validated Windows CSP or the FIPS-validated OpenSSL library (for UNIX systems)	Not output from the TACS	Stored in the TACS in PKD	Zeroized when the operator is revoked or when the password is updated with a new one	Used to authenticate operators with two factor authentication data

Key	Key type	Generation/Input	Output	Storage	Zeroization	Use
		Entered into TACS over an encrypted TACS session				
Rolling private key (d_2F_rolling)	RSA key (1024 bits)	If two-factor rolling is enabled then two-factor rolling components are entered into the TACS over an encrypted TACS session	N/A	N/A. Stored outside the TACS	Zeroized when a new rolling key pair is generated on each login	Used to encrypt Two Factor private key on the Client two factor device
Rolling public key (e_2F_rolling)	RSA key (1024 bits)	If two-factor rolling is enabled then it is generated externally by the FIPS-validated Windows CSP or the FIPS-validated OpenSSL library (for UNIX systems)Entered into TACS over an encrypted TACS session	Not output from the TACS	Stored in the TACS in PKD	Zeroized on each login by the operator or when the operator is revoked	Used to decrypt Two Factor private key on the Client two factor device
Operator RSA public key (e)	RSA key (1024 bits)	Generated internally using ANSI X 9.31 RSA key generation when operator key pair is generated on the TACS;or entered into the TACS over an encrypted TACS session when operator key pair is generated by the Client	Output form the TACS when the operator certificate is requested and optionally to the external LDAP database	Stored on disk and optionally in external LDAP database	Zeroized when the operator is revoked or password changed	Used to verify RSA digital signatures
Operator RSA private key (d)	RSA key (1024 bits)	Generated internally using ANSI X 9.31 RSA key generation when operator key pair is generated on the TACS	Not output from the TACS when operator key pair is generated on the TACS; Or does not enter the TACS when operator key pair is	Temporarily stored in volatile memory when operator key pair is generated on the TACS	Zeroized after generating Authentication key component2 (dauth2) and Persistence key component2 (dpersistence2) when operator key pair is generated on the TACS	Used to generate Authentication key component2 (dauth2) and Persistence key component2 (dpersistence2) when operator key pair is generated on the TACS

Key	Key type	Generation/Input	Output	Storage	Zeroization	Use
			generated on the Client			
Authentication key component1 (dauth1)	RSA 1024 bit private key component	Generated externally and entered into TACS over an encrypted TACS session (PKCS5 of authentication data and salt) when "Authentication key component2 (dauth2)" is generated by the TACS; Or does not enter the TACS when "Authentication key component2 (dauth2)" is generated on the Client	Not output from the TACS	Volatile memory only when operator key pair is generated by the TACS	Zeroized after computing the Authentication key component2 when operator key pair is generated on the TACS	Used to authenticate operator
Authentication key component2 (dauth2)	RSA 1024 bit private key component	Calculated internally (dauth1 * dauth2 = d mod n); Or entered into the TACS over an encrypted TACS session when "Authentication key component2 (dauth2)" is generated by the Client	Not output from the TACS	Stored on disk	Zeroized when the operator is revoked	Used to verify the authentication of the operator
Persistence key component1 (dpersistence1)	RSA 1024 bit private key component	Generated externally and entered into TACS over an encrypted TACS session (PKCS5 of authentication data and modified salt) when "Persistence key component2 (dpersistence2)" is generated by the TACS; Or does not enter the TACS when "Persistence key component2 (dpersistence2)" is generated on the Client	Not output from the TACS	Volatile memory only when operator key pair is generated on the TACS	Zeroized after computing the Persistence key component2 when operator key pair is generated on the TACS	Used to compute operator portion of sign and decrypt data

Key	Key type	Generation/Input	Output	Storage	Zeroization	Use
Persistence key component2 (dpersistence2)	RSA 1024 bit private key component	Calculated internally (dpersistence1 * dpersistence2 = d mod n); Or entered into the TACS over an encrypted TACS session when "Persistence key component2 (dpersistence2)" is generated by the Client	Not output from the TACS	Stored on disk	Zeroized when the operator is revoked	Used to compute TACS portion of sign and decrypt data
Login session private key (d_loginsession)	RSA key (1024 bits)	Generated outside the TACS and does not enter the TACS	N/A	N/A	N/A	Used on the client to extract persistence keys to complete the sign operation
Login session public key (e_loginsession)	RSA key (1024 bits)	Generated externally and entered into TACS over an encrypted TACS session	Not output from the TACS	Stored on disk in SKD	Zeroized when no longer used or the TACS reboots	Used to encrypt persistence keys for storage in volatile memory on the client
Kiosk Authentication key component1 (dauth1kiosk)	RSA 1024 bit private key component	Generated externally and entered into TACS over an encrypted TACS session (PKCS5 of password and salt) when "Kiosk Authentication key component2 (dauth2kiosk)" is generated by the TACS; Or does not enter the TACS when "Kiosk Authentication key component2 (dauth2kiosk)" is generated on the Client	Not output from the TACS	Volatile memory only when operator key pair is generated by the TACS	Zeroized after computing the Kiosk Authentication key component2 when operator key pair is generated by the TACS	Used to authenticate operator in kiosk mode
Kiosk Authentication key component2 (dauth2kiosk)	RSA 1024 bit private key component	Calculated internally (dauth1kiosk * dauth2kiosk = d mod n); Or entered into the TACS over an encrypted TACS session when "Kiosk	Not output from the TACS	Stored on disk	Zeroized when the operator is revoked	Used to verify the authentication of the operator in kiosk mode

Key	Key type	Generation/Input	Output	Storage	Zeroization	Use
		Authentication key component2 (dauth2kiosk)" is generated by the Client				
Kiosk Persistence key component1 (dpersistence1kiosk)	RSA 1024 bit private key component	Generated externally and entered into TACS over an encrypted TACS session (PKCS5 of password and modified salt) when "Kiosk Persistence key component2 (dpersistence2kiosk)" is generated by the TACS; Or does not enter the TACS when "Kiosk Persistence key component2 (dpersistence2kiosk)" is generated on the Client	Not output from the TACS	Volatile memory when operator key pair is generated by the TACS	Zeroized after computing the Kiosk Persistence key component2 when operator key pair is generated by the TACS	Used to compute operator portion of sign and decrypt data in kiosk mode
Kiosk Persistence key component2 (dpersistence2kiosk)	RSA 1024 bit private key component	Calculated internally (dpersistence1kiosk * dpersistence2kiosk = d mod n); Or entered into the TACS over an encrypted TACS session when "Kiosk Persistence key component2 (dpersistence2kiosk)" is generated by the Client	Not output from the TACS	Stored on disk	Zeroized when the operator is revoked	Used to compute TACS portion of sign and decrypt data in kiosk mode
Symmetric session key (R1)	TDES (168 bits), HMAC (192 bits)	Generated externally and entered into the TACS over TLS session	Not output from the TACS	Volatile memory only	Zeroized when not used	Used to encrypt dpersistence1
Symmetric kiosk session key (R1)	TDES (168 bits), HMAC (192 bits)	Generated externally and entered into the TACS over TLS session	Not output from the TACS	Volatile memory only	Zeroized when not used	Used to encrypt dpersistence1kisok
SCP session key	TripleDES (168 bits)	Negotiated during SSH session establishment (Not used in FIPS	Not output from the TACS	Volatile memory only	Zeroized when not used or the TACS is powered down	Used to encrypt/MAC the SCP sessions for backup and

Key	Key type	Generation/Input	Output	Storage	Zeroization	Use
		mode)				recovery
SFTP session key	TripleDES (168 bits)	Negotiated during SFTP session establishment	Not output from the TACS	Volatile memory only	Zeroized when not used or the TACS is powered down	Used to encrypt/MAC the SFTP sessions for recovery
LDAP Password	Alphanumeric string (minimum of 8	Entered into the TACS over an encrypted TACS session	Not output from the TACS	Stored on disk	Zeroized when the password is updated with a new one	Used for authentication during operator certificate access in LDAP
SNMP Password	Alphanumeric string (minimum of 8	Entered into the TACS over an encrypted TACS session	Not output from the TACS	Stored on disk	Zeroized when the password is updated with a new one	Used for authentication for SNMP services
Backup key	TripleDES (168 bits)	Generated internally by FIPS 186-2 PRNG	Encrypted with Backup key 2	Volatile memory only	Zeroized when no longer used or backup data is zeroized	Encrypt/decrypt backup data
Backup key 2	TripleDES (168 bits)	Generated internally when the super manager key pair is generated by the TACS; or generated externally and entered into the TACS over an encrypted TACS session when super manager key pair is generated by the Client	Not output from the TACS	Stored on disk in PKD	Zeroized when no longer used or the CO password is changed	Encrypt/decrypt backup key
Firmware upgrade key	RSA public key (1024 bits)	Externally generated predetermined value	Not output from the TACS	Non-volatile memory (hard drive – plaintext) in TACS binaries	Zeroized when the appliance zero-out is performed	Verify signatures on firmware upgrades
FIPS 186-2 PRNG Seed	SHA-1 hash of entropy	Generated internally from various entropy sources	Not output from the TACS	Volatile memory only	Zeroized when no longer used	Used by FIPS 186-2 PRNG
FIPS 186-2 PRNG Seed key	160 bits	Generated internally by gathering the system entropy	Not output from the TACS	Volatile memory only	Zeroized when no longer used	Used by FIPS 186-2 PRNG

The modules use the FIPS Approved FIPS 186-2 PRNG to obtain the initial values used in the key establishment process.

2.8 Self-Tests

The TACS performs the following self-tests at power-up:

- Firmware integrity check – The modules verify that their firmware has not been modified by verifying a SHA-1 hash over their firmware
- Known Answer Tests (KATs) – The modules perform cryptographic algorithm tests at power-up to verify the correct operation of the following FIPS-approved algorithm implementations:
    - Triple-DES KAT
    - SHA-1 KAT
    - HMAC SHA-1 KAT
    - FIPS 186-2 PRNG KAT
    - RSA pairwise-consistency check

The TACS performs the following conditional self-tests:

- Continuous Random Number Generator Tests for FIPS 186-2 PRNG – This test is run upon generation of random data by the modules' FIPS 186-2 PRNG to detect failure to a constant value.
- Continuous Random Number Generator Tests for seeding the FIPS 186-2 PRNG – This test is run upon generation of a seed for the modules' FIPS 186-2 PRNG to detect failure to a constant value.
- RSA Pair-wise Consistency Tests (sign/verify) – This test is run upon generation of a new RSA key pair to verify the correct operation of the newly generated key pair.
- Firmware load test – This test is run upon downloading an update for the modules firmware. A digital signature is verified over the firmware update to ensure the integrity of the firmware update.

The power-up tests do not require any inputs from or actions by the operator. Power-up self tests occur when the module is powered up before the TACS provides any services. Power-up self-tests can be called on demand by the CO by power cycling or rebooting the module. The conditional self-tests are performed when the applicable security function or operation is invoked and do not require any additional inputs from or actions by the operator. Conditional self-tests can be executed by invoking the applicable security function or operation.

If any of the power-up self-tests or the conditional self-tests fails, the module enters an error state and outputs an error indicator. The error indicator is in the form an output to the console interface stating that the load failed. The module fails to the error state and discontinues the loading operation. In this state the module does not provide any services. The module's power has to be recycled to clear the error. If the firmware upgrade test fails then the module deletes the downloaded firmware. The module will then revert to the previous version.

2.9 Design Assurance

TriCipher uses CVS for configuration management of source code, hardware components and related documentation. The CVS system provides access control, versioning, and logging.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 is used to provide configuration management for the TACS' FIPS documentation. This software provides access control, versioning, and logging.

2.10 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 level 2 requirements for this validation.

3. Secure Operation

The TACS 1000 and 2000 meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-approved mode of operation.

3.1 Crypto-Officer Guidance

3.1.1 Initial setup

The TACS 1000 and 2000 are available from TriCipher through shipping using a bonded carrier. TriCipher provides the customer with the shipment package check list which includes a detailed list of the hardware components, release notes, Client software. The Crypto-Officer is responsible for inspecting the module and its packaging upon receipt for signs of tampering. If any sign of damage to the packaging or the module are found the Customer should contact the TriCipher sales support desk for assistance.

The TACS 1000 and 2000 require that a fine mesh ventilation hole screen be installed in order for the TACS to operate in FIPS-approved mode. These screens are not user-servicable and must be installed at the factory by the TriCipher manufacturing team.

The Crypto-Officer must apply tamper-evident labels to the TACS 1000 or 2000. The following steps detail the label application procedure:

- TACS 1000 and 2000 Label Application Procedure:

1. Clean the areas of the module’s chassis where the tamper-evident labels will be applied to remove any grease, dirt, etc. Alcohol-based cleaning pads are recommended for this purpose. Labels must be applied indoors in an ambient temperature of 55F to 85F. Ensure that the equipment has had sufficient time to adjust to the ambient temperature before applying the label.

2. Apply labels as depicted in Figures 1, 2 and 3 for TACS 1000 and Figures 4 and 5 for TACS 2000.

3. Record all the serial numbers of the labels applied to the system in a security log.

4. Allow a minimum of 12 hours for the labels to cure.

5. Do not expose the labels to outdoors conditions or to extreme temperatures (outside the range 55F to 85F).

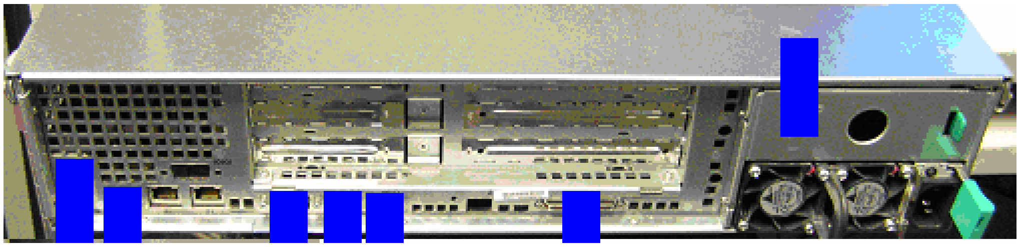


Figure 1: TACS 1000 tamper evident labels on the rear panel

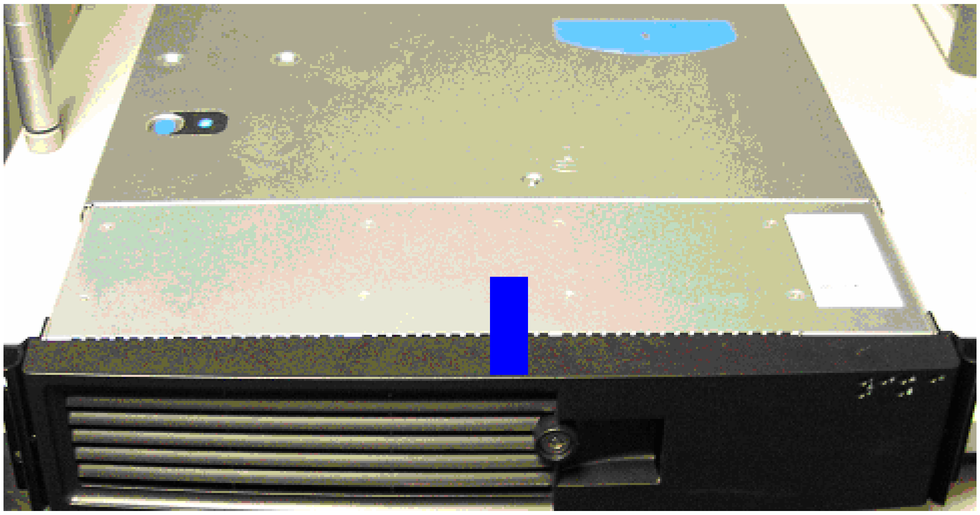


Figure 2: TACS 1000 tamper evident labels on the front top side

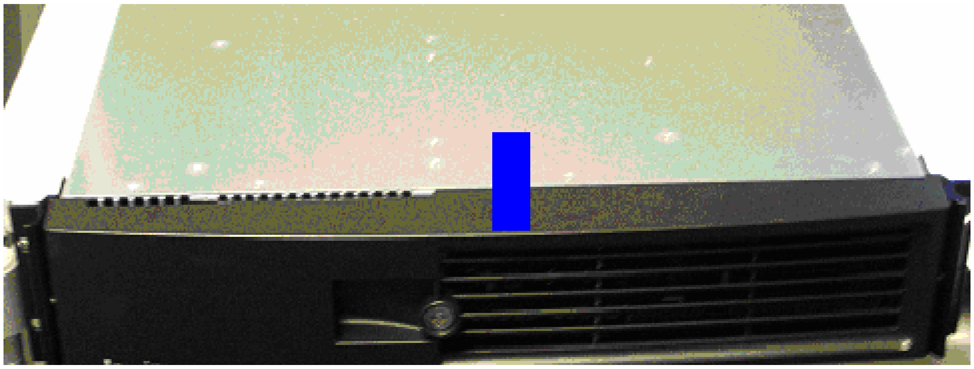


Figure 3: TACS 1000 tamper evident labels on the front bottom side

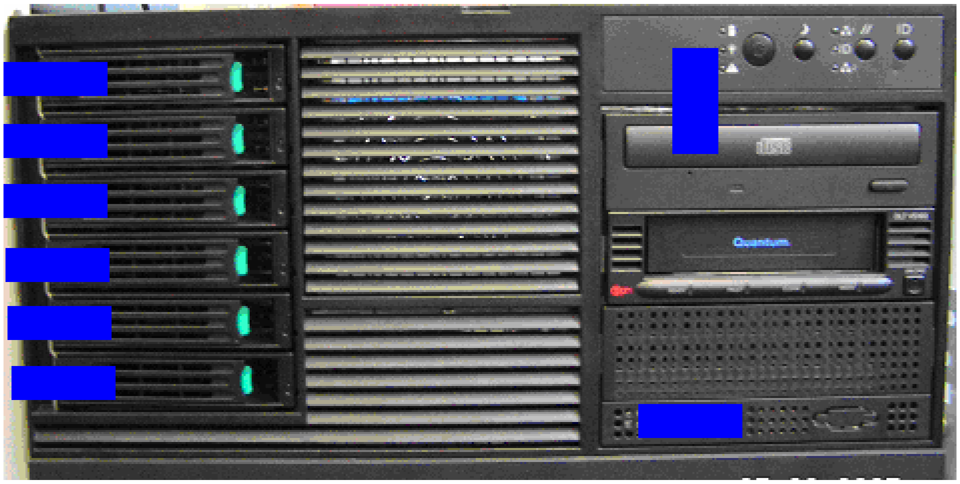


Figure 4: TACS 2000 tamper evident labels on the front panel

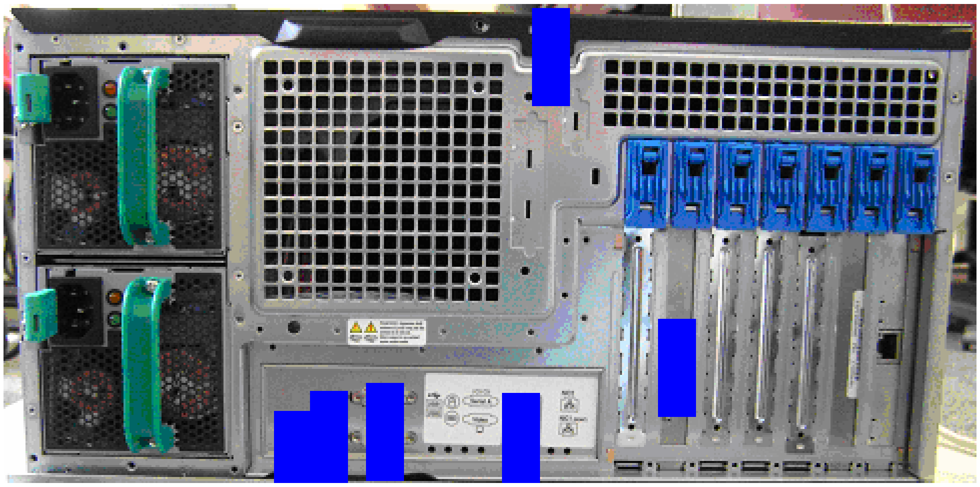


Figure 5: TACS 2000 tamper evident labels on the rear panel

3.1.2 Initialization

The Appliance ships with a default Crypto Officer account, the Super Manager, with its default password for this account. The Crypto Officer must complete the “TACS Initialization” process which consists of the following steps:

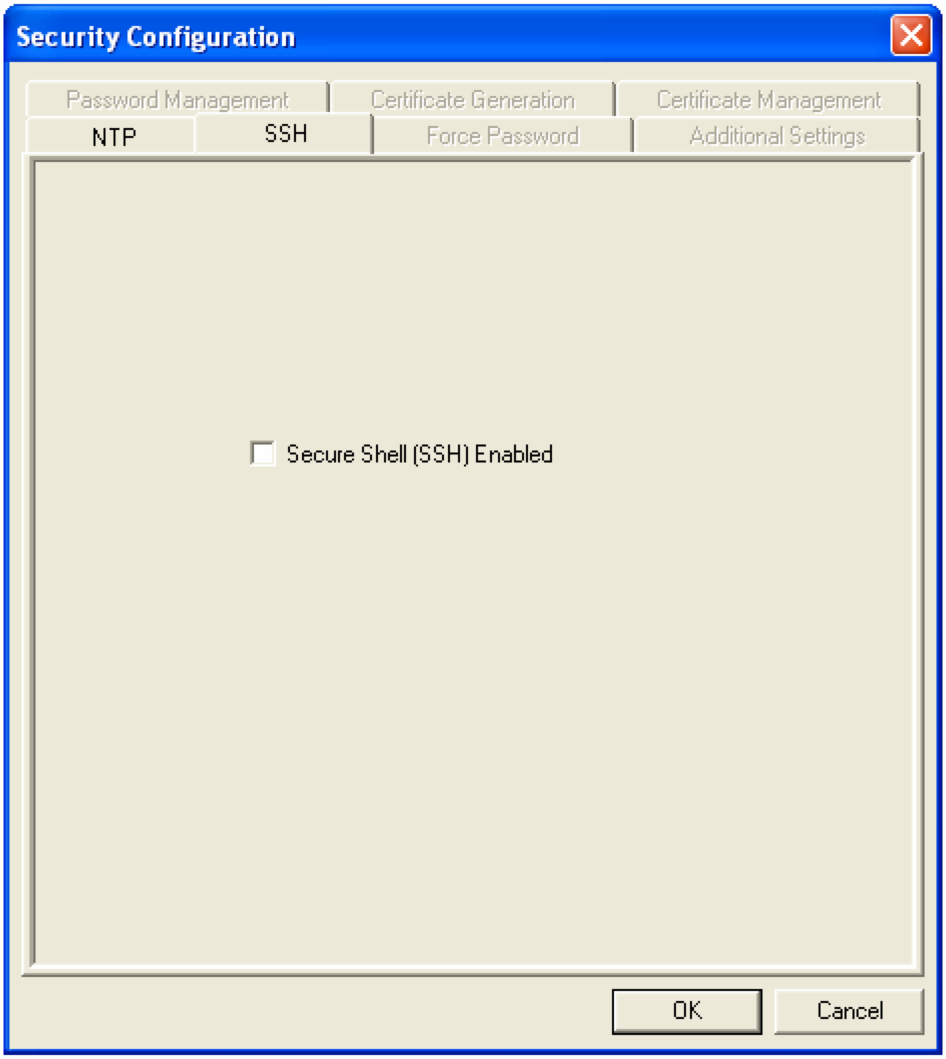
1. The Super Manager Account must be activated.
2. New appliance keys must be generated to replace the factory-installed appliance keys for the first unit.
3. New appliance keys must be generated to replace the factory-installed appliance keys for the second unit (if used, for a mirrored pair).

4. New appliance keys must be generated to replace the factory-installed appliance keys for the third unit (if used, for a triad).
5. The Super Manager must set TLS Keys.
6. The Super Manager must add the root certificates for chaining.
7. The Super Manager must change his password (this resets his user keys), and generate a new certificate.

Refer to the *TACS Operation Guide* by TriCipher for more information on the "TACS Initialization" process. The following additional configurations must be set by the Crypto Officer in order to put the Appliance into the FIPS mode of operation:

The ability to use SSH to access the modules must be disabled. This can be accomplished by the following procedure:

1. Select *Security Management -> Configuration* and open the **SSH** tab (as depicted in Figure 6).
2. Uncheck the **Secure Shell Enabled** checkbox on the **SSH** tab.
3. Click **OK**.



☐ Secure Shell (SSH) Enabled

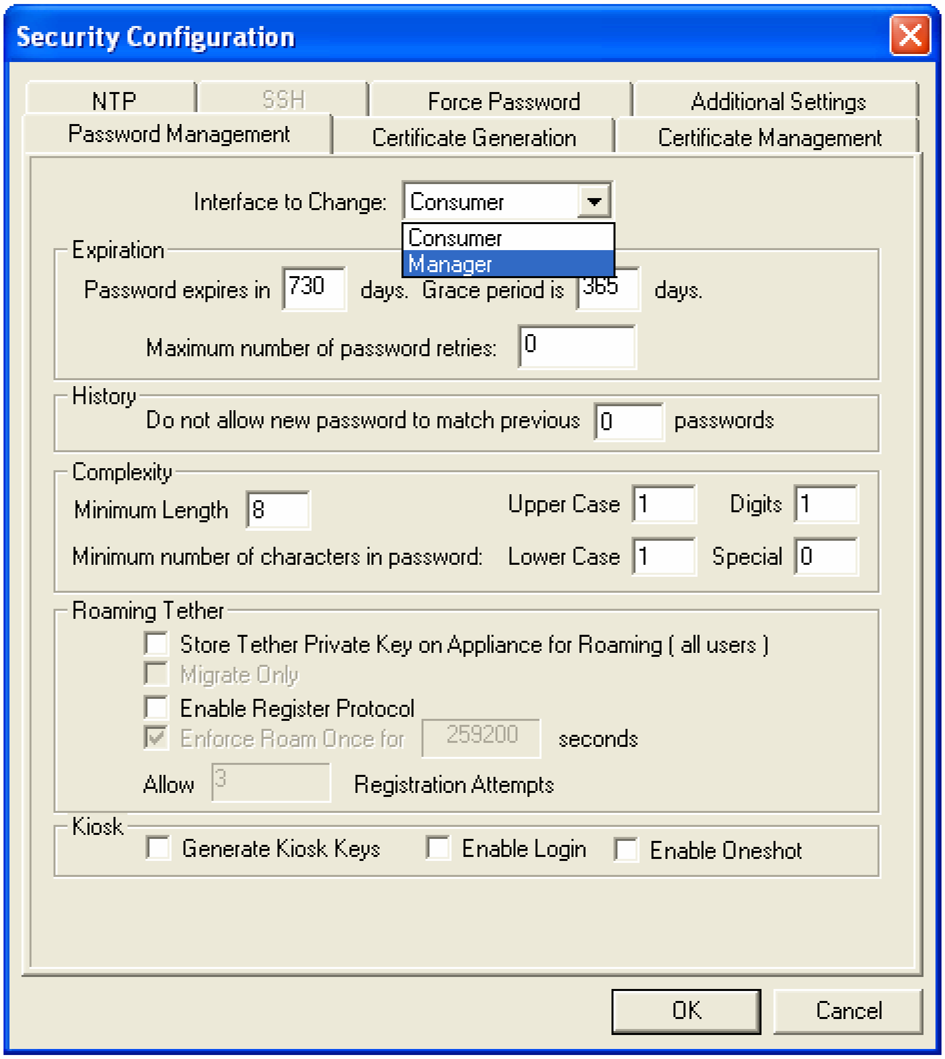
Figure 6 – Disable SSH

All operator passwords must be a minimum of 8 characters in length. This option can be configured by the following procedure:

1. Select *Security Management -> Configuration* and open the **Password Management** tab (as depicted in figure 7).
2. Select **Consumer** in the drop-down menu for **Interface to Change**
3. Enter **8** for Minimum Length under Complexity.
4. Click **OK**
5. Select *Security Management -> Configuration* and open the **Password Management** tab (as depicted in figure 7).
6. Select **Manager** in the drop-down menu for **Interface to Change**

7. Enter **8** for Minimum Length under Complexity.

8. Click **OK**



Interface to Change: Consumer
Consumer
Manager

Expiration
Password expires in 730 days. Grace period is 365 days.
Maximum number of password retries: 0

History
Do not allow new password to match previous 0 passwords

Complexity
Minimum Length 8 Upper Case 1 Digits 1
Minimum number of characters in password: Lower Case 1 Special 0

Roaming Tether
□ Store Tether Private Key on Appliance for Roaming (all users)
□ Migrate Only
□ Enable Register Protocol
☑ Enforce Roam Once for 259200 seconds
Allow 3 Registration Attempts

Kiosk
□ Generate Kiosk Keys □ Enable Login □ Enable Oneshot

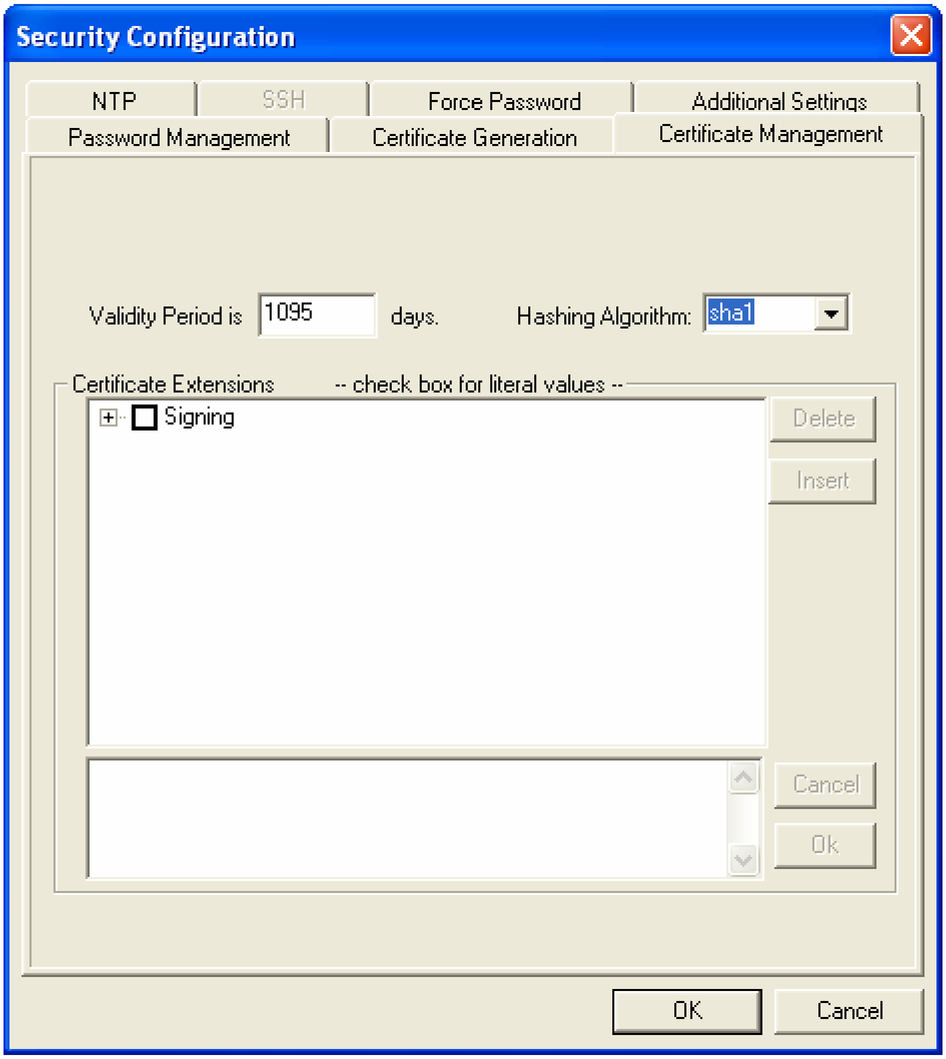
Figure 7 – Setting Minimum Password Length for User and Crypto Officer

All Certificate Hashing algorithm should to set to use SHA-1. This can be accomplished by the following procedure:

1. Select *Security Management -> Configuration* and open the **Certificate Management** tab (as depicted in figure 8).

2. Select **Hashing Algorithm** as **SHA-1** on the **Certificate Management** tab

3. Click **OK**



Validity Period is 1095 days.

Hashing Algorithm: sha1

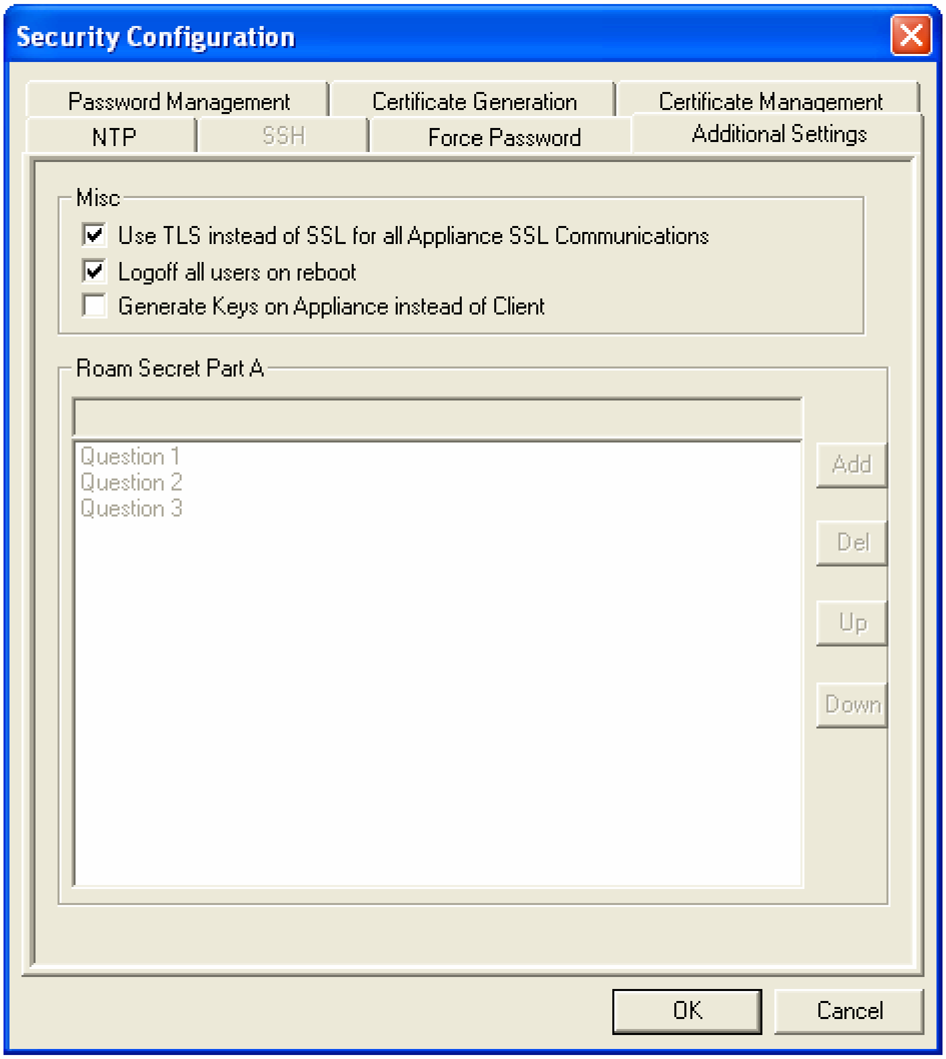
Certificate Extensions -- check box for literal values --

□ Signing

Figure 8 – Select Hashing Algorithm for use in Certificates

All operators must be logged off at reboot and only TLS may be used to remotely access the module securely. These options can be configured by the following procedure:

1. Select *Security Management -> Configuration* and open the **Additional Settings** tab (as depicted in figure 9).
2. Check the **Logoff all users at reboot** and **Use TLS instead of SSL for all Appliance SSL Communications** checkbox on the **Additional Settings** tab.
3. Click **OK**



Security Configuration

Misc

☑ Use TLS instead of SSL for all Appliance SSL Communications

☑ Logoff all users on reboot

☐ Generate Keys on Appliance instead of Client

Roam Secret Part A

Question 1
Question 2
Question 3

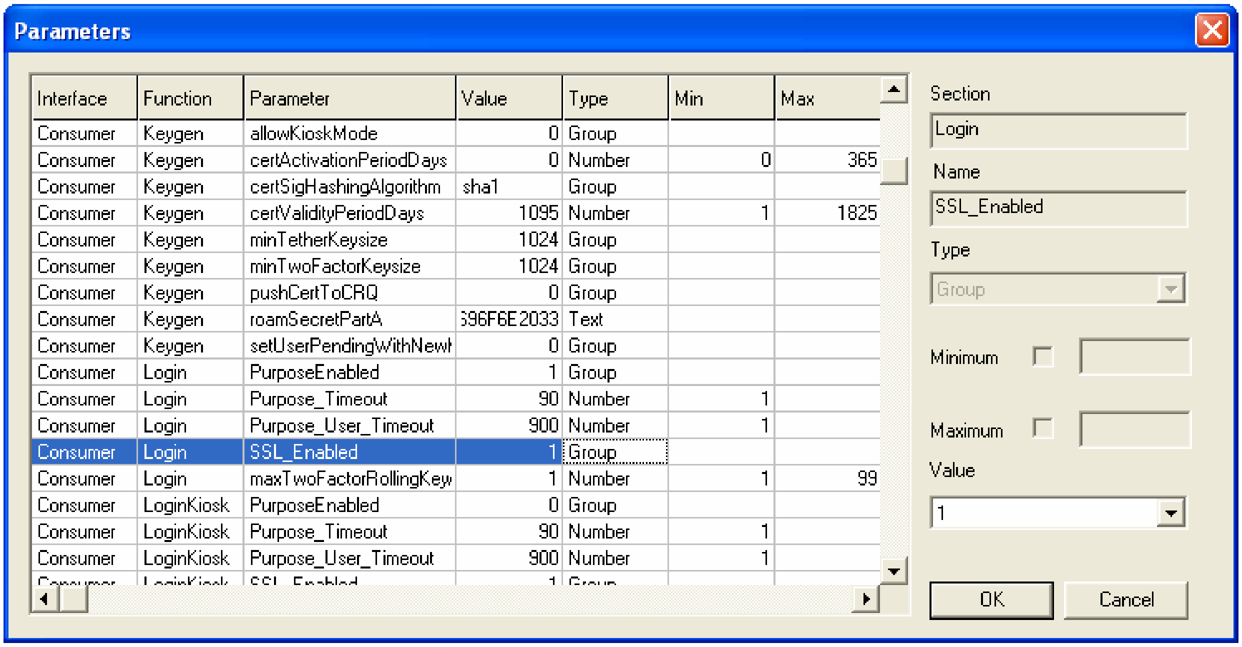
Figure 9 – Select to Use TLS and Logoff Users on Reboot

The Login, MirrorIn, OneShot, OneShotKiosk and Register protocols must use TLS to secure its communications. This can be configured by the following procedure:

1. Select *Security Management→ Parameters* to open the **Security Parameters** dialog (as depicted in Figure 10).
2. Scroll down to “Consumer Login SSL_Enabled”
3. Set **Value** to 1 in the drop down menu.
4. Repeat steps 2 and 3 for “Consumer LoginKiosk SSL_Enabled”, “Consumer Oneshot SSL_Enabled” “Consumer OneshotKiosk SSL_Enabled” “Consumer Register SSL_Enabled” “Manager Login SSL_Enabled” “Manager LoginKiosk SSL_Enabled”, “Manager

Oneshot SSL_Enabled" "Manager OneshotKiosk SSL_Enabled" "Manager Register SSL_Enabled" and "Manager MirrorIn SSL_Enable"

5. Click **OK**



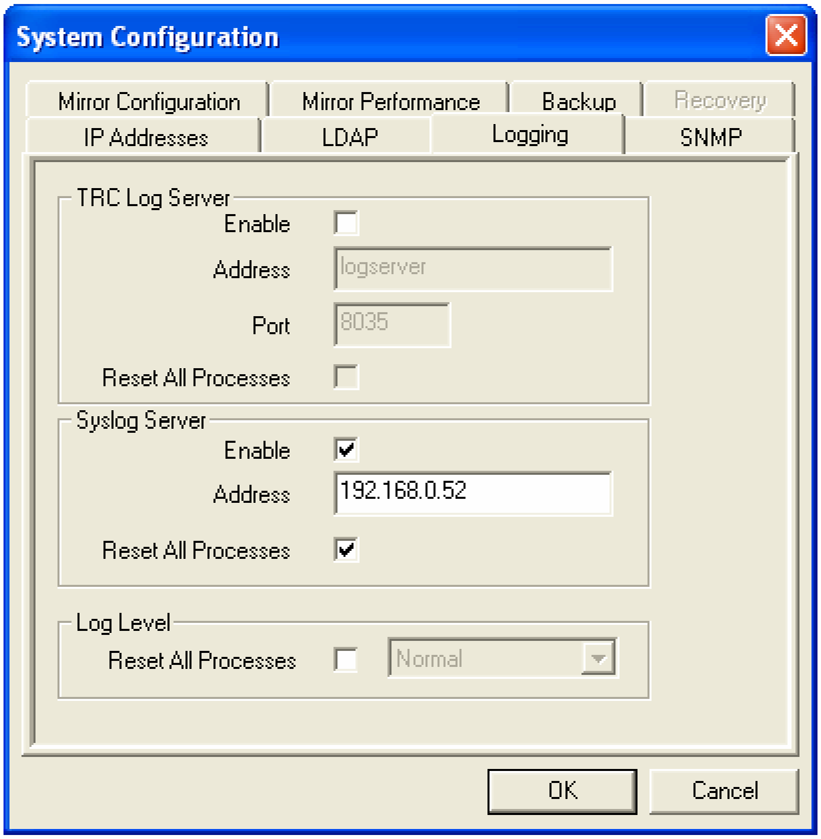
Interface	Function	Parameter	Value	Type	Min	Max
Consumer	Keygen	allowKioskMode	0	Group		
Consumer	Keygen	certActivationPeriodDays	0	Number	0	365
Consumer	Keygen	certSigHashingAlgorithm	sha1	Group		
Consumer	Keygen	certValidityPeriodDays	1095	Number	1	1825
Consumer	Keygen	minTetherKeysize	1024	Group		
Consumer	Keygen	minTwoFactorKeysize	1024	Group		
Consumer	Keygen	pushCertToCRQ	0	Group		
Consumer	Keygen	roamSecretPartA	396F6E2033	Text		
Consumer	Keygen	setUserPendingWithNewl	0	Group		
Consumer	Login	PurposeEnabled	1	Group		
Consumer	Login	Purpose_Timeout	90	Number	1	
Consumer	Login	Purpose_User_Timeout	900	Number	1	
Consumer	Login	SSL_Enabled	1	Group		
Consumer	Login	maxTwoFactorRollingKey	1	Number	1	99
Consumer	LoginKiosk	PurposeEnabled	0	Group		
Consumer	LoginKiosk	Purpose_Timeout	90	Number	1	
Consumer	LoginKiosk	Purpose_User_Timeout	900	Number	1	
Consumer	LoginKiosk	SSL_Enabled	1	Group		

Section: Login
Name: SSL_Enabled
Type: Group
Minimum ☐
Maximum ☐
Value: 1

Figure 10 – Use TLS with Protocols

Enable logging to a syslog server or TriCipher log server. This option can be configured by the following procedure:

1. Select *System Management -> Configuration* and open the **Logging** tab (as depicted in figure 11)
2. Check the **Enable** log server to be used and provide its IP address
3. Check **Reset All Processes**
4. Click **OK**



TRC Log Server

Enable ☐

Address logserver

Port 8035

Reset All Processes ☐

Syslog Server

Enable ☑

Address 192.168.0.52

Reset All Processes ☑

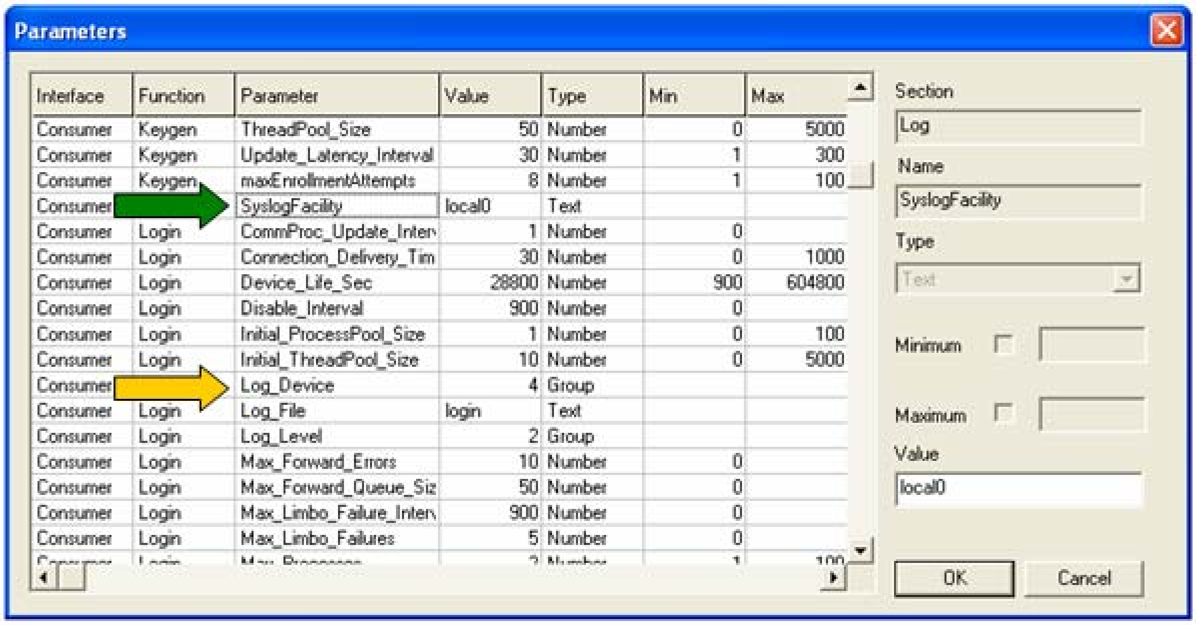
Log Level

Reset All Processes ☐ Normal

Figure 11 – Logging Configuration

The following additional configuration sets syslog logging:

1. Select *System Management→ Parameters* to open the **Security Parameters** dialog (as depicted in Figure 12)
2. Click on **OK** at the warning
3. Scroll through the list and ensure that all process that are supposed to use syslog have their “Log Device” parameter set to four (4), yellow arrow)
4. Set the “syslog facility” to be used for both appliance interfaces (Consumer/User and Manager/CO) a value of local0, (green arrow).



Interface	Function	Parameter	Value	Type	Min	Max
Consumer	Keygen	ThreadPool_Size	50	Number	0	5000
Consumer	Keygen	Update_Latency_Interval	30	Number	1	300
Consumer	Keygen	maxEnrollmentAttempts	8	Number	1	100
Consumer		SyslogFacility	local0	Text		
Consumer	Login	CommProc_Update_Inter	1	Number	0	
Consumer	Login	Connection_Delivery_Tim	30	Number	0	1000
Consumer	Login	Device_Life_Sec	28800	Number	900	604800
Consumer	Login	Disable_Interval	900	Number	0	
Consumer	Login	Initial_ProcessPool_Size	1	Number	0	100
Consumer	Login	Initial_ThreadPool_Size	10	Number	0	5000
Consumer		Log_Device	4	Group		
Consumer	Login	Log_File	login	Text		
Consumer	Login	Log_Level	2	Group		
Consumer	Login	Max_Forward_Errors	10	Number	0	
Consumer	Login	Max_Forward_Queue_Siz	50	Number	0	
Consumer	Login	Max_Limbo_Failure_Inter	900	Number	0	
Consumer	Login	Max_Limbo_Failures	5	Number	0	
Consumer	Login	Max_Processes	2	Number	1	100

Section
Log

Name
SyslogFacility

Type
Text

Minimum ☐

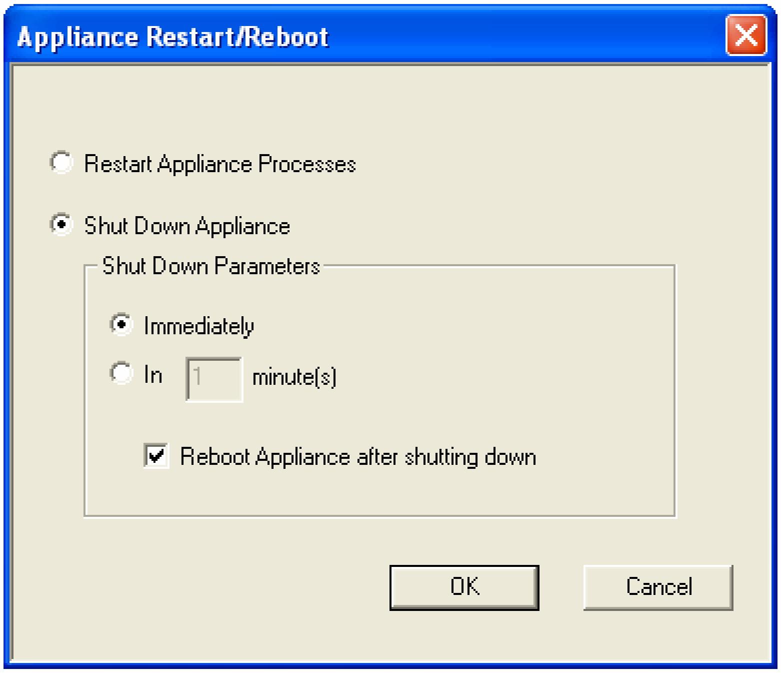
Maximum ☐

Value
local0

Figure 12 – Syslog parameter configuration

At this point, the module must be rebooted to enable all of the changes. Upon reboot, initialization of the module for FIPS is complete and the module is now configured securely. This can be accomplished by the following steps:

1. Select *System Management*→ *Restart/Reboot* to open the Appliance **Restart/Reboot** dialog (as depicted in Figure 13).
2. Select **Shut Down Appliance**
3. Click **OK**



○ Restart Appliance Processes

● Shut Down Appliance

Shut Down Parameters

● Immediately

○ In 1 minute(s)

☑ Reboot Appliance after shutting down

Figure 13 – Reboot Appliance

3.1.3 Management

The Crypto Officer must make sure that the configuration for the TACS is always maintained as detailed in the Initialization section above. RSA key pairs must be a minimum of 1024 bits in length. SHA-1 must be used as the hashing algorithm. All passwords and Activation Codes must be at least alphanumeric and at least 8 characters long (or more). Digital certificates generated with FIPS-approved algorithms may be utilized.

The Crypto-Officer should periodically backup the configuration of the module.

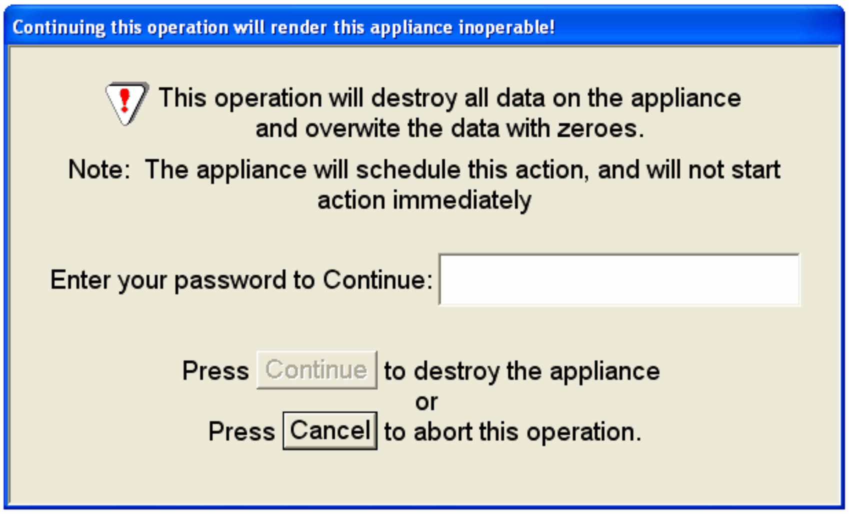
The Crypto-Officer must periodically check the module for signs of tampering, including unusual dents, scrapes, or damage to tamper-evident labels, and verify that the tamper-evident labels still have the proper serial numbers. Additionally, the Crypto-Officer should monitor the module's logs for strange activity. If indications of suspicious activity are found, the Crypto-Officer should immediately take the module offline and investigate.

The module permits updates by the Crypto Officer. After downloading the update, the module verifies a RSA digital signature over the update to ensure that it is an unmodified TriCipher firmware update. However, the Crypto-Officer must also ensure that the update is validated to FIPS 140-2 or by checking the version and build of the firmware and verifying this has been validated to FIPS 140-2 or before activating the update. Since upgrading the module with a release that has not been validated to FIPS 140-2 will take the module out of FIPS mode, the Crypto-Officer must either zeroize the module (see Zeroization below) before activating the update or not proceed with activating the update.

3.1.4 Zeroization

At the end of its life cycle or when taking the module out of FIPS mode, the module must be fully zeroized to protect CSPs. This can be accomplished through the following steps:

1. Select *Security Management* → *Zero-Out Appliance Data*. A warning message will open (as depicted in Figure 14).
2. Enter Super Manager Password
3. Click **Continue**


Continuing this operation will render this appliance inoperable!

This operation will destroy all data on the appliance and overwite the data with zeroes.

Note: The appliance will schedule this action, and will not start action immediately

Enter your password to Continue:

Press Continue to destroy the appliance
or
Press Cancel to abort this operation.

Figure 14 – Zero-Out Appliance Data

This operation destroys all data on the appliance. All data are erased, all files deleted, all configuration information is lost, and the Appliance can no longer be used. The destruction operation will begin immediately and be completed several seconds after the Continue button is clicked. Shutdown of the device will take several minutes to complete after the keys have been destroyed. It is the Crypto-Officer’s responsibility to ensure that zeroization has completed.

If the Appliance is operating in a mirrored pair or mirrored triad configuration, this feature destroys only the unit that the Crypto Officer is currently logged into. To destroy the second unit or the third unit, the

Crypto Officer must log into each unit separately and perform the zeroization process on each.

3.2 User Guidance

The User does not have the ability to configure sensitive information on the TACS, with the exception of his password and CSPs generated on the Client side. The User must be diligent to pick strong passwords (8 characters or greater, a minimum of alphanumeric), and must not reveal his password to anyone. The CSPs generated by the Client should be generated using FIPS Approved algorithms. Additionally, the User should be careful to protect any CSPs in their possession.

4. Acronyms

ANSI	American National Standards Institute
API	Application Programming Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CVS	Concurrent Versions System
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	(Keyed-) Hash MAC
KAT	Known Answer Test
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OS	Operating System
PC	Personal Computer
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SP	Secure Platform
SSH	Secure SHell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VSS	Visual Source Safe