FIPS 140-2 Non-Proprietary Security Policy

Concepteers Teleconsole E

Firmware Version 2.0

Document Version 1.2

September 1, 2011

Prepared For:

Concepteers, LLC

121 Newark Ave, Suite 204

Jersey City, NJ 07302

www.concepteers.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the Teleconsole E.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment of Canada (CSEC) Cryptographic Module Validation Program (CMVP) runs the FIPS 140 program. The CMVP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for products meeting FIPS 140 validation. *Validated* is the term given to a product that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at
http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Teleconsole E from Concepteers provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The Concepteers Teleconsole E may also be referred to as the "module" in this document.

1.3 External Resources

The Concepteers website (http://www.concepteers.com) contains information on the full line of products from Concepteers, including a detailed overview of the Teleconsole E solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm) contains links to the FIPS 140-2 certificate and Concepteers contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPOS	General Purpose Operating System
HMAC	Hashed Message Authentication Code
IPSec	Internet Protocol Security
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
LCD	Liquid Crystal Display
NIST	National Institute of Standards and Technology
POST	Power On Self Test
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir Adelman
SHA	Secure Hashing Algorithm
TDES	Tripe Data Encryption Standard
TLS	Transport Layer Security
USB	Universal Serial Bus
WAN	Wide Area Network

Table 1 – Acronyms and Terms

2 Concepteers Teleconsole E

2.1 Product Overview

The Concepteers Teleconsole E provides secure remote access to internal equipment and network resources.

The module acts as a secure application-layer gateway that intermediates all requests between remote computers and internal resources. All requests from remote computers to a Teleconsole appliance and from an appliance to remote computers are encrypted using TLSv1.0/HTTPS encryption. Users gain authenticated access to authorized resources via an extranet session hosted by the appliance. Each request is subject to administratively defined access control and authorization policies before the request is forwarded to an internal resource.

2.2 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference / Electromagnetic Compatibility	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 – Validation Level by DTR Section

2.3 Algorithm Implementations

2.3.1 FIPS-Approved Algorithms

The cryptographic algorithm implementations of each module have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Asymmetric Key	RSA	ANSI X9.31 PKCS #1 v1.5 RSASSA-PSS	752	Sign / verify operations

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
	DSA	FIPS 186-2	479	Sign / verify operations
Hashing	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	FIPS 180-2	1374	Hashing
Keyed Hash	HMAC-SHA1 HMAC-SHA224 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	FIPS 198	903	Message verification Message digest
Symmetric Key	Triple-DES (CBC, CFB8, CFB128, ECB, OFB modes)	FIPS 46-3	1017	Data encryption / decryption
	AES (CBC, CFB8, CFB128, ECB, OFB with 128, 192 or 256 bit keys)	FIPS 197	1547	Data encryption / decryption
Random Number Generation	X9.31	X9.31 (AES)	836	Random Number Generation

Table 3 – Algorithm Certificates for FIPS-Approved Algorithms

2.3.2 Non-Approved Algorithms

The module implements the following non-approved algorithms:

- Diffie-Hellman (allowed for use in FIPS 140 mode of operation)
  - Used for key agreement/key establishment and supports 80-bits to 112-bits of encryption strength
- RSA (key wrapping; key establishment)
  - Provides between 80-bits and 112-bits of encryption strength.

The following algorithms are deprecated and will be disallowed according to timelines specified in NIST SP 800-131A:

- RSA (1024-bit)
- DSA (1024-bit)
- SHA-1
- HMAC-SHA1
- RNG

- Diffie-Hellman

Two-Key Triple DES is actually restricted; a key should only be used to encrypt more than 2^20 blocks of data.

2.4 Cryptographic Module Specification

The module is the Concepteers Teleconsole E running firmware version 2.0 on hardware rev A1. The module is classified as a multi-chip standalone cryptographic module. The physical cryptographic boundary is defined as the module case and all components within the case. No software or firmware is excluded from validation.

The physical boundary is pictured below:

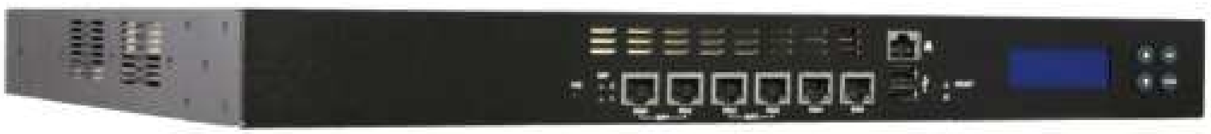

Figure 1 – Physical Boundary

2.5 Module Interfaces

The table below describes the main physical interfaces of the module:

Physical Interface	Description / Use
LEDs	For power indication: • Unlit—system is powered off • Green—system powered on and running. Hard Drive Activity • Blinking red – hard drive activity
RJ45 Serial Port	Console Connection for appliance
GbE Ports	Provides wired connectivity to up to 6 different networks.
USB Ports	For USB connections to devices
Power Receptacles	Provides power to the appliance
LCD	Reports real-time status, alarms, and general system information
Power Jacks	Provides power to the appliance
LCD buttons	Provides navigation for the LCD menu. Not enabled in FIPS mode.

Table 4 – Teleconsole E Interface Descriptions

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input	RJ45 Serial Port USB Ports GbE Ports
Data Output	RJ45 Serial Port USB Ports GbE Ports
Control Input	GbE Ports On/Off Switch
Status Output	GbE Ports LCD LEDs
Power	Power Jacks

Table 5 – Logical Interface / Physical Interface Mapping

2.6 Roles, Services, and Authentication

There are two roles (a Crypto Officer role and User role) in the module that operators may assume, and the respective services for each role are described in the following sections. The module supports identity-based authentication.

2.6.1 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service	Description	CSP	Roles
Configure	Initializes the module for FIPS mode of operation	Operator Passwords	Crypto Officer
Decrypt	Decrypts a block of data using AES or TDES	TLS Session Keys	Crypto Officer User
Encrypt	Encrypts a block of data using AES or TDES	TLS Session Keys	Crypto Officer User

Service	Description	CSP	Roles
Generate Keys	Generates keys for TLS operations	TLS Session Keys Session Certificate Diffie Hellman Public Key Diffie Hellman Private Key RSA Public Key RSA Private Key DSA Public Key DSA Private Key HMAC key for message verification Premaster Secret Master Secret RNG XKEY RNG XSEED	Crypto Officer User
Self-Test	Perform Self Tests	HMAC key (for module integrity) Diffie Hellman Public Key Diffie Hellman Private Key RSA Public Key RSA Private Key DSA Public Key DSA Private Key	Crypto Officer User
Sign	Signs a block of data	Diffie Hellman Private Key RSA Private Key DSA Private Key	Crypto Officer User
Verify	Verifies the signature of a signed block of data	Diffie Hellman Public Key RSA Public Key DSA Public Key	Crypto Officer User

Service	Description	CSP	Roles
Zeroize CSPs	Clears CSPs and certificates from memory. Note that the "Delete Certificate" option in the GUI is part of the service.	TLS Session Keys Session Certificate Diffie Hellman Public Key Diffie Hellman Private Key RSA Public Key RSA Private Key DSA Public Key DSA Private Key HMAC key for message verification Operator Passwords Premaster Secret Master Secret RNG XKEY RNG XSEED	Crypto Officer User
Show Status	Shows status of the module. FIPS mode is indicated via check box in the GUI.	None	Crypto Officer User
User Management	Manage user permissions	Operator Passwords	Crypto Officer

Table 6 – Operator Services and Descriptions

2.6.2 Operator Authentication

2.6.2.1 Password-Based Authentication

In FIPS-approved mode of operation, the module is accessed via Graphical User Interface from a remote workstation. Other than status functions available by viewing LEDs or the LCD, the services described in Table 6 – Operator Services and Descriptions are available only to authenticated operators.

The module supports identity-based authentication. Passwords must be a minimum of 6 characters (see Guidance and Secure Operation section of this document). The password can consist of alphanumeric values and special characters, {a-z},{A-Z},{0-9},{`~!@#$%^&*()_+={}[]\|;:’”,./<>?], yielding 93 choices per character. The probability of a successful random attempt is $1/93^6$, which is less than 1/1,000,000.

The module will lock an account after 3 failed authentication attempts; thus, the maximum number of attempts in one minute is 3. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $3/93^6$ which is less than 1/100,000.

2.6.2.2 Certificate-Based Authentication

The module also supports authentication via digital certificates. The module supports identity-based authentication via a public key with 1024-bit, and 2048-bit RSA keys. A 1024-bit RSA key has at least 80-bits of equivalent strength. The probability of a successful random attempt is $1/2^{80}$, which is less than 1/1,000,000. Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one-minute period is $60/2^{80}$ which is less than 1/100,000.

A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is $1/2^{112}$, which is less than 1/1,000,000. Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one-minute period is $60/2^{112}$ which is less than 1/100,000.

2.7 Physical Security

The module is a multiple-chip standalone module and conforms to Level 2 requirements for physical security. For details on tamper evidence, please see Section 3.1.2.

2.8 Operational Environment

The module operates in a limited operational model and do not implement a General Purpose Operating System.

The module meets Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) Class A requirements as defined by 47 Code of Federal Regulations, Part15, Subpart B.

2.9 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

Keys and CSPs	Storage Locations	Storage Method	Input	Input Method	Output	Output Method	Generated	Zeroized	Access
TLS Session Keys (TDES, AES)	RAM	Plaintext	No	NA	Yes	Encrypted with Premaster Secret	Yes (FIPS Approved RNG)	Yes (Reset[1])	CO RWD User RWD
Session Certificate (X.509v3)	On disk	Plaintext	No	NA	Yes	Plaintext during TLS negotiation	Generated by the module during the installation / initialization process	Yes (Reset)	CO D User RWD
Diffie Hellman Public Key	RAM	Plaintext	No	NA	Yes	Plaintext during TLS negotiation	Yes (FIPS Approved RNG)	Yes (Reset or generate new value)	CO RWD
Diffie Hellman Private Key	RAM	Plaintext	No	NA	No	NA	Yes (FIPS Approved RNG)	Yes (Reset or generate new value)	CO RWD
RSA Public Key	RAM	Plaintext	No	NA	Yes	Plaintext during TLS negotiation	Yes (FIPS Approved RNG)	Yes (Delete Certificate)	CO RWD

[1] References to “reset” in this table indicate reimaging the module to reload the firmware and initiate FIPS mode

Keys and CSPs	Storage Locations	Storage Method	Input	Input Method	Output	Output Method	Generated	Zeroized	Access
RSA Private Key	RAM	Plaintext	No	NA	No	NA	Yes (Generated according to the X9.31 standard)	Yes (Delete Certificate)	CO RWD
DSA Public Key	RAM	Plaintext	No	NA	Yes	Plaintext during TLS negotiation	Yes (FIPS Approved RNG)	Yes (Delete Certificate)	CO RWD
DSA Private Key	RAM	Plaintext	No	NA	No	NA	Yes (FIPS Approved RNG)	Yes (Delete Certificate)	CO RWD
HMAC key (160-bit HMAC-SHA1 for message verification)	RAM	Plaintext	No	NA	Yes	Wrapped with RSA/DSA Public Key	Yes (FIPS Approved RNG)	Yes (Reset or generate new value)	CO RWD
Operator Passwords	On disk	Plaintext	Yes	Electronic	No	NA	No	Yes (Reset or generate new value)	CO RWD User RWD
Premaster Secret (48 Bytes)	RAM	Plaintext	No	NA	Yes	Encrypted with Public Key	Yes (FIPS Approved RNG)	Yes (Reset or generate new value)	CO D User D
Master Secret (48 Bytes)	RAM	Plaintext	No	NA	No	NA	Yes (FIPS Approved RNG)	Yes (Reset or generate new value)	CO D User D

Keys and CSPs	Storage Locations	Storage Method	Input	Input Method	Output	Output Method	Generated	Zeroized	Access
RNG XKEY	RAM	Plaintext	No	NA	No	NA	Yes (system entropy)	Yes (Reset or generate new value)	CO D User D
RNG XSEED	RAM	Plaintext	No	NA	No	NA	Yes (system entropy)	Yes (Reset or generate new value)	CO D User D

R = Read W = Write D = Delete

Table 7 – Key/CSP Management Details

Private, secret, or public keys are protected from unauthorized modification and substitution. The module ensures only authenticated operators have access to keys and functions that can generate keys. Unauthenticated operators do not have write access to modify, change, or delete private, secret, or public keys.

2.10 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module will output an error dialog and will enter an error state. When the module is in an error state, no keys or CSPs will be output and the module will not perform cryptographic functions.

The module does not support a bypass function.

The following sections discuss the module's self-tests in more detail.

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

- Module integrity check via CRC32
- RSA pairwise consistency key (signing and signature verification)
- RSA KAT
- DSA pairwise consistency key (signing and signature verification)
- TDES KAT (encryption and decryption on all modes and implementations)
- AES KAT (encryption and decryption on all modes, key sizes, and implementations)
- SHA-1, SHA-256, and SHA-512 KAT (on all implementations)
- HMAC-SHA1, HMAC-SHA256 and HMAC-SHA512 (on all implementations)
- PRNG KAT

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation.

2.10.1.1 Status Output

An operator can discern that all power-on self-tests have passed via normal operation of the module and the following log message.

```
FIPS mode initialized and running
```

In the event the integrity check fails, the module will output the following message:

```
        Integrity check failed.  Can not start
```

In the event a POST fails, the module will output the following log message:

```
        FIPS mode failed; reverting to non-FIPS mode
```

Note that data output will be inhibited while the module is in an error state (i.e., when a POST fails). No keys or CSPs will be output when the module is in an error state.

2.10.2 Conditional Self-Tests

Conditional self-tests are test that run continuously during operation of the module. If any of these tests fail, the module will enter an error state. The module can be restarted to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. The module performs the following conditional self-tests:

- Pairwise consistency test for RSA implementations
- Pairwise consistency test for DSA implementations
- Continuous RNG test run on output of ANSI X9.31 PRNG
- Continuous test on output of ANSI X9.31 PRNG seed mechanism
- Continuous test to ensure seed and seed key are not the same values

The module does not perform a software load test because no additional software/firmware can be loaded in the module while operating in FIPS-approved mode.

2.10.2.1 Status Output

In the event a conditional self test fails, the module will output the following log message:

```
        FIPS Conditional Test Failed
```

Note that data output will be inhibited while the module is in this error state. No keys or CSPs will be output when the module is in an error state.

2.11 Mitigation of Other Attacks

The module does not mitigate attacks.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Enabling FIPS Mode and General Guidance

FIPS Mode is enabled by checking the "FIPS Mode" box in Teleconsole Administration / Configuration / Server Setup. Enabling FIPS mode will open/lock down features where appropriate (e.g., enabling self tests).

Additionally, the Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

- Verify that the firmware version of the module is Version 2.0. No other version can be loaded or used in FIPS mode of operation.
- Ensure the labels are placed in the proper position as shown in Figure 2 – Tamper Evidence Label Placement (Sides).
- Inspect the tamper evident labels periodically to verify they are intact.
- All operator passwords must be a minimum of 6 characters in length. The maximum password length is set by the Crypto Officer. The default maximum length is 16 characters. The largest possible maximum password length is 99 characters.
- Do not disclose passwords and store passwords in a safe location and according to his/her organization's systems security policies for password storage.
- Keys and CSPs shall be zeroized when transitioning to a FIPS mode from non-FIPS mode.
- Using the backup feature is not allowed in FIPS mode of operation. The Crypto Officer shall not use the Backup function.
- Importing RSA/DSA private keys is not allowed in FIPS mode of operation. The Crypto Officer shall not import private keys.

3.1.2 Placement of Tamper Evidence Labels

To meet Physical Security Requirements for Level 2, the module enclosure must be protected with tamper evidence labels. The tamper evident labels shall be installed for the module to operate in a FIPS

Approved mode of operation. Concepteers applies the labels at time of manufacture; the Crypto Officer is responsible for ensuring the labels are applied as shown below. Once applied, the Crypto Officer shall not remove or replace the labels unless the module has shown signs of tampering, in which case the Crypto Officer shall reimage the module[2] and follow all Guidance to place the module in FIPS mode.

The Crypto Officer is responsible for

- Verifying the labels are attached to the appliance as shown in the illustration below
- Maintaining the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

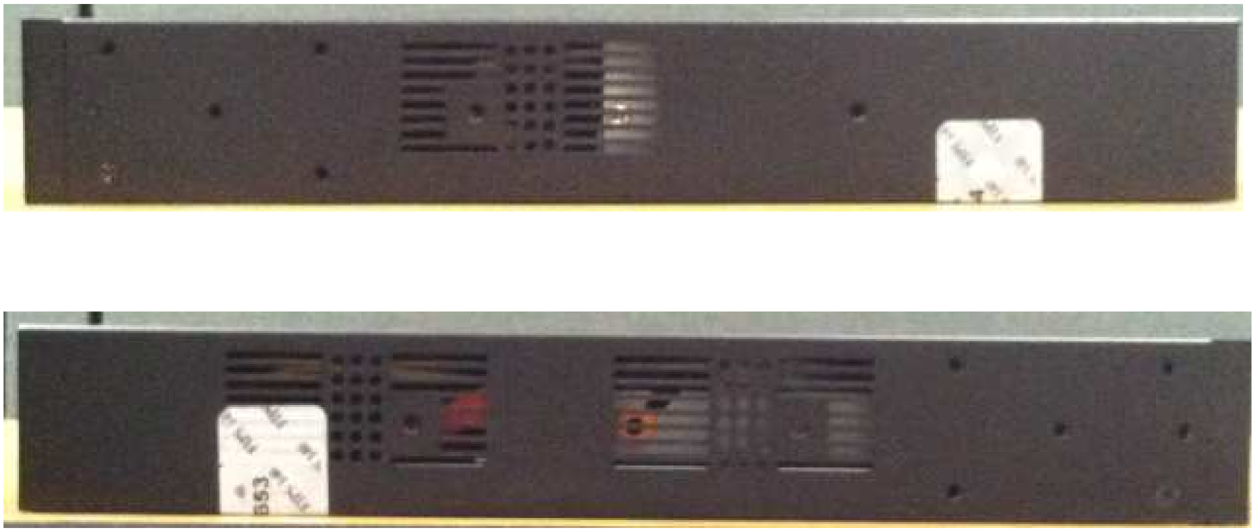

Figure 2 – Tamper Evidence Label Placement (Sides)

If one of the labels is tampered, the Crypto Officer shall reimage the module to reload the firmware, zeroize all keys and CSPs, and have the tamper labels reapplied. Note that Concepteers does not offer the purchase of additional labels. If labels need to be replaced, please contact Concepteers.

[2] Firmware is obtained from Concepteers and is loaded via Teleconsole Administration / Firmware Upgrade as specified in the Teleconsole administration guide.

3.2 User Guidance

3.2.1 General Guidance

The User must not disclose passwords and must store passwords in a safe location and according to his/her organization’s systems security policies for password storage.

End of Document