TANDBERG Telecom AS

TANDBERG MXP Codec

(Firmware Version: F6.0)

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation

Document Version 1.3

Prepared for:

TANDBERG
A Global Leader in Visual Communication

TANDBERG Telecom AS
Philip Pedersens vei 20
1366 Lysaker
Norway
Phone: (47) 67-125-125
Fax: (47) 67-125-234
http://www.tandberg.com

Prepared by:

Corsec

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
U.S.A.
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2007-01-09	Xiaoyu Ruan	Initial draft
0.2	2007-03-30	Xiaoyu Ruan	Removed TELNET from FIPS mode
0.3	2007-05-08	Xiaoyu Ruan	Submitted to CMVP
1.0	2007-11-22	Xiaoyu Ruan	Addressed CMVP comments
1.0.1	2008-01-09	Xiaoyu Ruan	Addressed CMVP comments
1.1	2008-01-14	Xiaoyu Ruan	Addressed CMVP comments
1.2	2008-02-01	Xiaoyu Ruan	Addressed CMVP comments
1.3	2008-05-14	Xiaoyu Ruan	Addressed CMVP comments

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

This document is a non-proprietary Cryptographic Module Security Policy for the TANDBERG MXP Codec from TANDBERG AS. This Security Policy describes how the TANDBERG MXP Codec meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. and Canadian 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/groups/STM/index.html.

In this document, the TANDBERG MXP Codec is referred to as the codec or the module.

1.2 References

This document deals only with the operations and capabilities of the module 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 TANDBERG website (http://www.tandberg.com) contains information on the full line of products from TANDBERG.
- The CMVP website (http://csrc.nist.gov/groups/STM/index.html) 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
- Finite state machine
- Other supporting documentation as additional references

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

2 TANDBERG MXP Codec

2.1 TANDBERG Video Conferencing System Overview

TANDBERG AS produces a full line of videoconferencing systems designed for medium-to-large groups, as well as individual desktops. TANDBERG products include video endpoints, video cameras, conferencing servers (Multipoint Control Units (MCUs) and Media Processing System (MPS) series), management software, protocol and translation gateways (Integrated Services Digital Network (ISDN) Gateway, 3G Gateway, Border Controller), and recording devices (content servers).

Figure 1 demonstrates the deployment architecture of TANDBERG video conferencing systems. Typically, a video conference consists of several endpoint attendees at different locations. Hardware components involved in a video conferencing system include endpoint servers, video endpoints, cameras, microphones, speakers, conferencing servers, protocol translation gateways, gatekeepers, and border controllers. The MCUs and MPS are necessary when the attendees of a conference exceed a certain number. The border controller, together with the TANDBERG Expressway technology, seamlessly and securely allows video communications by using default behavior of firewalls. The gatekeeper, on the other hand, provides critical functionality to enable Internet Protocol (IP) video communication. Video endpoints can be deployed throughout an enterprise Local Area Network (LAN). Security features are offered along with the full support for networking protocols. Notice that the MCUs, MPS, border controllers, and gatekeepers are other hardware devices and have nothing to do with the FIPS 140-2 validation for the TANDBERG MXP Codec. For detailed information on a specific device, please refer to its administrative and user manuals.

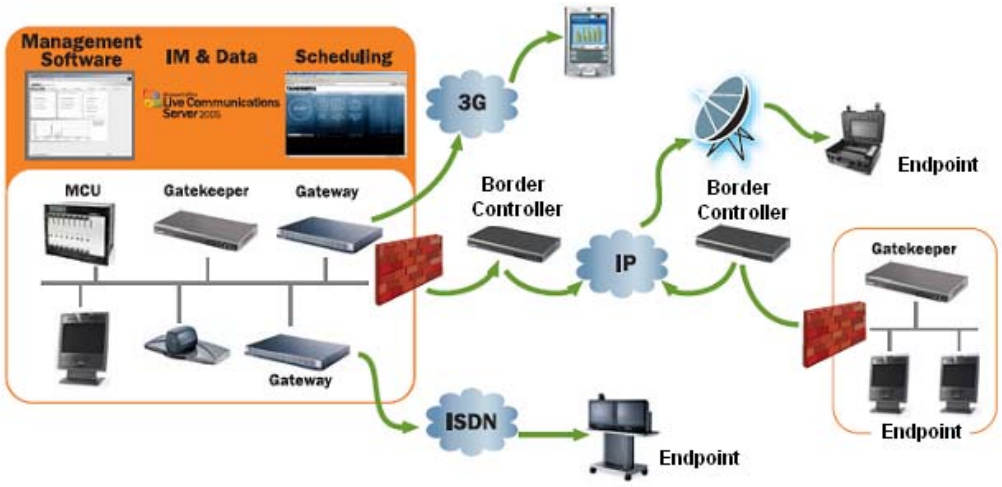

Figure 1 - Deployment of TANDBERG Video Conferencing Systems

TANDBERG provides full standard protocol support for H.320[1] (for ISDN networks) and H.323[2] (for Ethernet). Using these protocols, secure video conferencing is offered using Advanced Encryption Standard (AES) encryption

[1] H.320 is an umbrella recommendation by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) for running Multimedia (Audio/Video/Data) over ISDN based networks.

[2] H.323 is an umbrella recommendation by the ITU-T that defines the protocols to provide audio-visual communication sessions on any packet network.

for point-to-point calls and multipoint calls on ISDN and Ethernet with the speed of up to 768 kbps on the full TANDBERG product line.

2.2 TANDBERG MXP Codec Overview

The TANDBERG MXP Codec (version F6.0) is the firmware installed in the TANDBERG endpoint product line. The firmware supports the following nineteen TANDBERG codec servers: TANDBERG 8000 MXP, TANDBERG 7000 MXP, TANDBERG 6000 MXP, TANDBERG 3000 MXP, TANDBERG 2000 MXP, TANDBERG 1500 MXP, TANDBERG 1700 MXP, TANDBERG 1000 MXP, TANDBERG 990 MXP, TANDBERG 880 MXP, TANDBERG 770 MXP, TANDBERG 550 MXP, TANDBERG Tactical MXP, TANDBERG Maestro MXP, TANDBERG Compass MXP, TANDBERG Utility MXP, TANDBERG Edge 75 MXP, TANDBERG Edge 85 MXP, and TANDBERG Edge 95 MXP.

For example, the TANDBERG 6000 and 3000 MXP Codec servers are large- and mid-sized endpoint products, respectively. Their front and rear panels are shown in Figure 2 and Figure 3.

Figure 2 - Front and Rear Panels of TANDBERG 6000 MXP Codec Server

Figure 3 - Front and Rear Panels of TANDBERG 3000 MXP Codec Server

The TANDBERG 6000 and 3000 MXP codec servers handle video and audio input and output and connect sites with other parties in a conference via Ethernet or ISDN. Optionally with MCU, MPS, or embedded multi-site functionality, the TANDBERG 6000 MXP Codec server is capable of handling up to six video and five audio sites, and the TANDBERG 3000 MXP Codec server is able to handle up to four video and three audio sites.

The cryptographic boundary is depicted in Figure 4 with the block diagram of TANDBERG 6000 MXP codec server. Logically, the cryptographic boundary contains a single firmware image that runs on the Central Processing Unit (CPU), video processors, and audio processors in the area defined by the red line. Notice that the module is the **firmware**, rather than the hardware. The firmware is stored in the flash memory shown in Figure 4. Although Figure 4 is the block diagram of the TANDBERG 6000 MXP codec server, it represents a typical structure of other codec server models that use the same firmware.

Notice that FIPS 140-2 testing was performed on the TANDBERG 6000 MXP codec server only. However, the TANDBERG MXP Codec firmware requires no code change or recompilation when it is installed on the other eighteen codec servers. According to Section G.5 of the *Implementation Guidance for FIPS PUB 140-2 and the*

Cryptographic Module Validation Program[3], the FIPS 140-2 validation for the TANDBERG MXP Codec firmware remains valid when the firmware is installed on other codec servers.

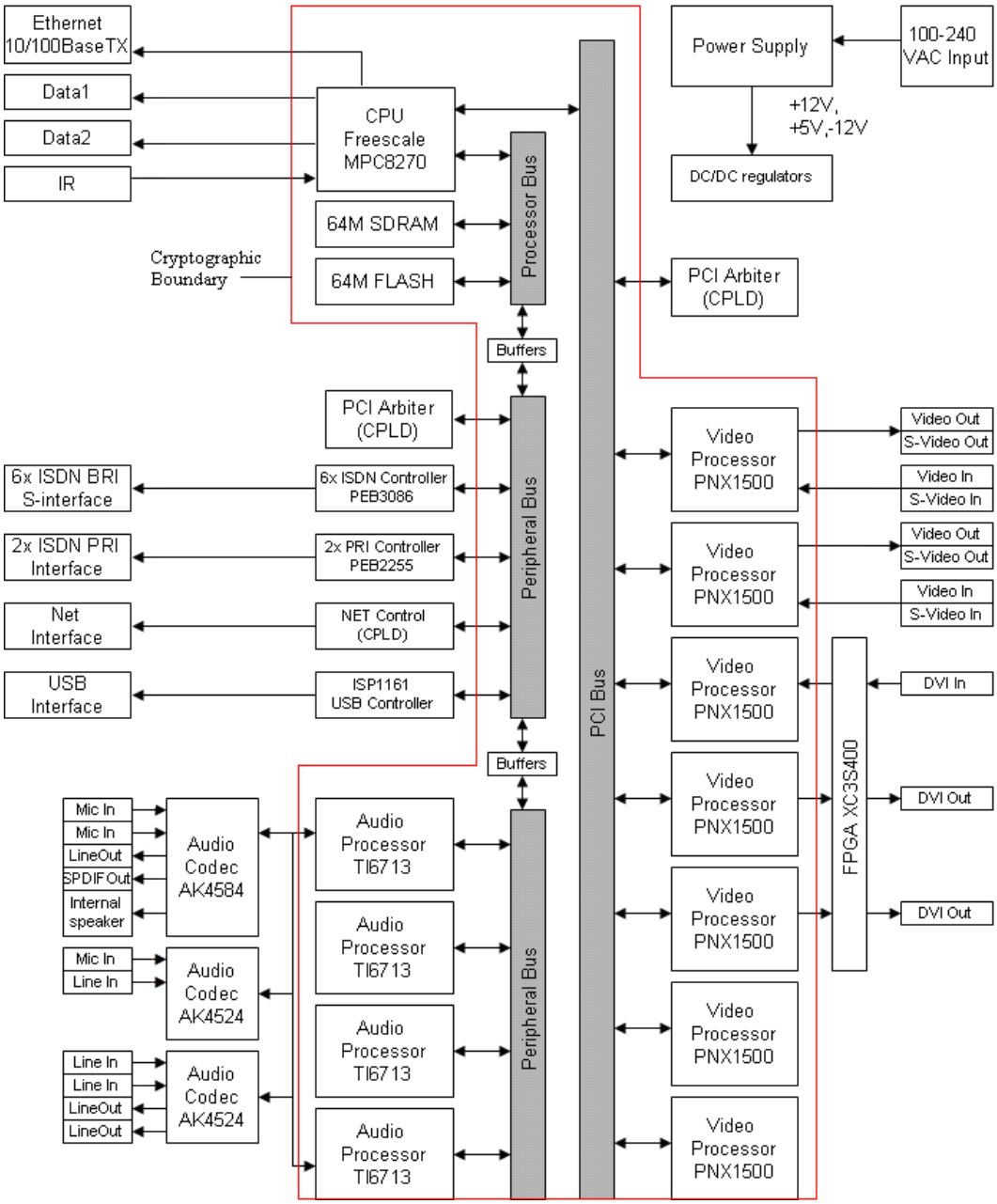

Figure 4 - Module Cryptographic Boundary

[3] Available at http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

The TANDBERG MXP Codec supports a FIPS-Approved mode of operation and a non-FIPS-Approved mode of operation. The TANDBERG MXP Codec is validated at the following FIPS 140-2 Section levels (when operated in the FIPS-Approved mode).

Table 1 - Security Level Per FIPS 140-2 Section

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

In Table 1, N/A indicates "Not Applicable". EMI and EMC refer to Electromagnetic Compatibility and Electromagnetic Interference, respectively.

2.3 Module Interfaces

The module is a firmware image installed on TANDBERG MXP codec servers. The firmware's interfaces are mapped to the ports on the server.

A firmware module does not have any physical ports. The firmware module interfaces, shown on Table 2, are provided to show a mapping between the firmware and the hardware that the firmware is installed on. The hardware ports are listed for clarification.

The following is the list of ports of the TANDBERG 6000 MXP codec server. The other eighteen models supported by the module implement the same types of ports. However, the numbers of ports may be different. Figure 5 shows the ports on the TANDBERG 6000 MXP codec server's rear panel.

- Three microphone input ports (audio input)
- Three audio input ports (RCA[4] audio ports)
- Three audio output ports (RCA audio ports), one of which serves as S/PDIF[5] output when the system is configured with stereo and S/PDIF active.
- Four video input ports (two S-Video ports and two RCA video ports)

[4] An RCA port is a type of electrical connector that is commonly used in the audio/video market. The name "RCA" derives from the Radio Corporation of America, which introduced the design by the early 1940s to allow phonograph players to be connected to amplifiers.

[5] S/PDIF stands for Sony/Philips Digital Interface Format. S/PDIF is a collection of hardware and low-level protocol specifications for carrying digital audio signals between devices and stereo components.

- Four video output ports (two S-Video ports and two RCA video ports)
- Two Digital Visual Interface (DVI) output ports
- One DVI input port
- One V.35 network port
- Two ISDN Primary Rate Interface (PRI) ports
- Six ISDN Basic Rate Interface (BRI) ports
- One Ethernet port
- One Universal Serial Bus (USB) port (for future use, currently not software-enabled)
- Two Data Communications Equipment (DCE) ports, Data 1 and Data 2. Data 1 is usually used for RS232 connection and Data 2 is usually a THSI (TANDBERG High Speed Interface) used for connecting the TANDBERG Precision HD Camera[6]. When Precision HD Camera is connected, video input 1 will be disabled.
- LEDs indicating system status
- Power socket

The following is a list of the logical interfaces implemented in the module:

- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

Table 2 maps the codec server interfaces with the FIPS 140-2 logical interfaces.

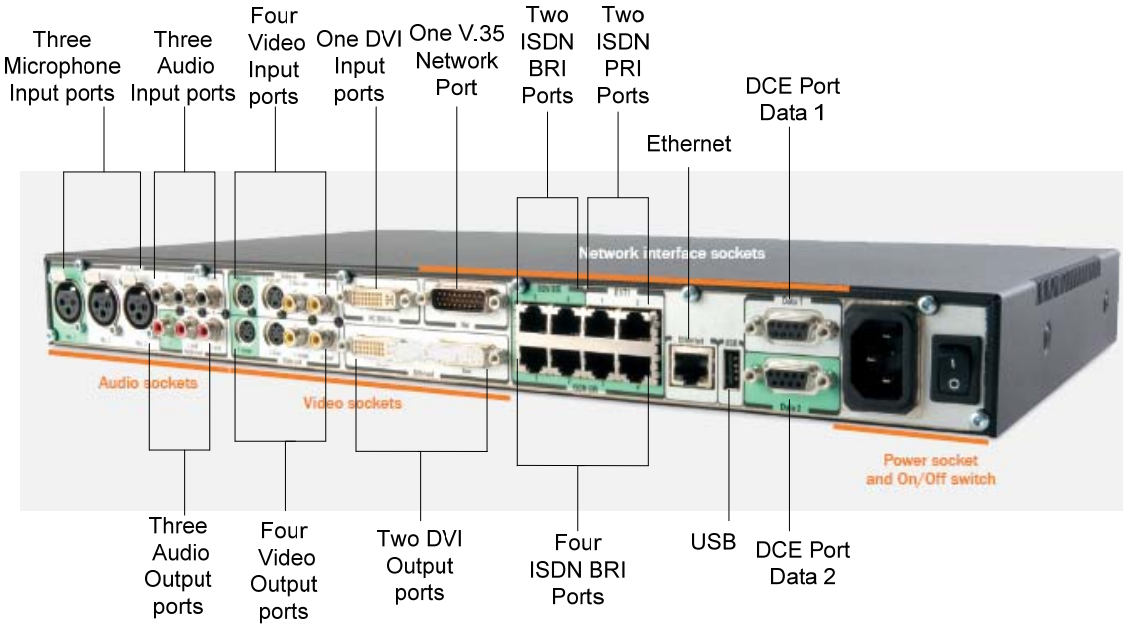

Figure 5 - Rear Panel of TANDBERG 6000 MXP Codec Server

[6] TANDBERG Precision HD camera is a high definition video capture device that provides superior video quality at any bandwidth. Designed specifically for videoconferencing, it provides crystal-clear, true-to-life quality for rich interaction and collaboration.

Table 2 - Mapping of FIPS 140-2 Logical Interfaces to TANDBERG MXP Codec Server Interfaces

FIPS 140-2 Logical Interface	TANDBERG MXP Codec Server Port/Interface
Data Input	Infrared remote, microphone input, audio input, DVI input, V.35 network, ISDN BRI, ISDN PRI, Ethernet, DCE Port Data 1, DCE Port Data 2
Data Output	Audio output, video output, DVI output, V.35 network, ISDN BRI, ISDN PRI, Ethernet, DCE Port Data 1, DCE Port Data 1
Control Input	Infrared remote, V.35 network, ISDN BRI, ISDN PRI, Ethernet, DCE Port Data 1
Status Output	Audio output, video output, DVI output, V.35 network, ISDN BRI, ISDN PRI, Ethernet, DCE Port Data 1, Light-Emitting Diode (LEDs)
Power	Power socket

2.4 Roles and Services

The modules support two authorized roles: Crypto Officer and User. The services of a Crypto Officer include module management, settings, and firmware upgrades. The User role places and answers videoconferencing calls with or without security features as specified by the security configurations of itself and other parties to the call.

Under the FIPS mode of operation, both roles can access the module through one of the following interfaces:

(1) infrared remote
(2) Hypertext Transfer Protocol (HTTP) / HTTPS (Hypertext Transfer Protocol over Transport Layer Security or TLS)
(3) Secure Shell (SSH) version 2
(4) RS232

The infrared remote provides the operator with a menu-driven interface. The HTTP/HTTPS protocol provides a web-based interface. The SSH and RS232 interfaces are command-line based.

Additionally, the Crypto Officer can access the codec via Simple Network Management Protocol (SNMP) version 1 and File Transfer Protocol (FTP) to perform certain limited operations. These two interfaces do not provide any security-related services or configurations.

2.4.1 Crypto Officer Role

Table 3 shows the services for the Crypto Officer role in the FIPS mode of operation. The purpose of each service is shown in the first column (“Service”), and the corresponding function is described in the second column (“Description”).

Notice that IP stands for Internet Protocol. RSA is a well-known asymmetric cryptographic algorithm named after its inventors Rivest, Shamir, and Adleman. DSA is short for Digital Signature Algorithm. CSP refers to Critical Security Parameter. TDES refers to Triple Data Encryption Standard.

Table 3 - Crypto Officer Services

Service	Description	Input	Output	Keys/CSPs and Type of Access
Install	Assemble the systems and setup network configurations.	Command	Result of installation	None
Uninstall	Disassemble the codec server system.	Command	Uninstalled module	None

Service	Description	Input	Output	Keys/CSPs and Type of Access
Login through infrared remote	Crypto Officer logs in the codec through infrared remote.	None	Status, success or failure	None
Login through HTTP/HTTPS	Crypto Officer logs in the codec through HTTP/HTTPS.	Codec's IP address	Status, success or failure	Diffie-Hellman keys – Read RSA keys – Read DSA keys – Read AES key – Read, Write, and Delete TDES keys – Read, Write, and Delete
Login through SSH	Crypto Officer logs in the codec through SSH.	Codec's IP address	Status, success or failure	Diffie-Hellman keys – Read, Write, and Delete DSA keys – Read, Write, and Delete AES key – Read, Write, and Delete TDES keys – Read, Write, and Delete
Login through RS232	Crypto Officer logs in the codec through RS232.	None	Status, success or failure	None
Login through SNMP	Crypto Officer logs in the codec through SNMP.	Codec's IP address, community name	Status, success or failure	None
Login through FTP	Crypto Officer logs in the codec through FTP.	Codec's IP address	Status, success or failure	None
Generate keys	Generate keys using ANSI X9.31 Appendix A.2.4 RNG for HTTPS, SSH, H.320, and H.323 protocols	Command	Keys	Entries generated by ANSI X9.31 Appendix A.2.4 RNG in Tables 5, 6, 7, and 8. Type of access – Read and Write
Power-up self-tests	Run power-up self-tests.	Turn on or reboot the codec	Status, success or failure	None
Configure network settings	Configure network parameters that are necessary for placing/answering calls.	Command, network parameters such as IP addresses	Status, success or failure	None
Configure security settings	Choose from "Auto Encryption" (i.e., alternating bypass), "Encryption Off" (i.e., bypass), and "Encryption On". For "Encryption On" and "Auto Encryption", further choose from "AES" and "Auto".	Command, options	Status, success or failure	None
Configure system settings	Configure other system parameters.	Command, options	Status, success or failure	None
Install certificates	Install certificates for TLS sessions for HTTPS connections.	Command, certificates, private keys	Status, success or failure	RSA or DSA private key - Write
Upgrade firmware	Install a new firmware.	Command, options	Status, success or failure	DSA public key for upgrade integrity test - Read
Get status	Check the status of the codec.	Command, options	Event log	None

2.4.2 User Role

Table 4 shows the services for the User role under the FIPS mode of operation. Similar to Table 3, the purpose of each service is shown in the first column ("Service"), and the corresponding function is described in the second column ("Description"). Notice that, depending on what services the operator will be requesting after login, the login procedures for the infrared remote, HTTP/HTTPS, SSH, and RS232 can be grouped as either Crypto Officer or User services.

Table 4 - User Services

Service	Description	Input	Output	Keys/CSP and Type of Access
Login through infrared remote	User logs in the codec through infrared remote.	None	Status, success or failure	None
Login through HTTP/HTTPS	User logs in the codec through HTTP/HTTPS.	Codec's IP address	Status, success or failure	Diffie-Hellman keys – Read RSA keys – Read DSA keys – Read AES key – Read, Write, and Delete TDES keys – Read, Write, and Delete
Login through SSH	User logs in the codec through SSH.	Codec's IP address	Status, success or failure	DSA keys – Read, Write, and Delete AES key – Read, Write, and Delete TDES keys – Read, Write, and Delete
Login through RS232	User logs in the codec through RS232.	None	Status, success or failure	None
Videoconferencing Calls	Place outgoing calls or answer incoming calls. Calls can be configured with encryption and decryption options.	Command, number of the receiver (when placing an outgoing call)	Status, success or failure	Diffie-Hellman keys – Read, Write, and Delete AES keys – Read, Write, and Delete

2.5 Physical Security

The module itself is a firmware. The TANDBERG MXP codec servers supported by the module are production-grade embodiments that include metal cases which completely surround the module and are removable using screws or hand screws. There are no locks or permanent closures.

2.6 Operational Environment

The module is the firmware running three Operating Systems (OS) simultaneously, including Nucleus Plus RTOS[7] version 1.13.5 (PowerPC Freescale MPC8270), Trimedia pSOS version 254 (video processors Phillips PNX1500),

[7] Nucleus Plus RTOS is a Real-Time Operating System (RTOS) and full-featured toolset created by the Embedded Systems Division of Mentor Graphics for various platforms.

and DSP/BIOS[8] version 5.20.05 (audio processors TI6713). All of them are limited operational environments according to FIPS 140-2 the definitions.

According to FIPS 140-2 Section 4.6: "If the operational environment is a limited operational environment, the OS requirements in Section 4.6.1 do not apply.", and the FIPS 140-2 requirements for operational environment are not applicable to the TANDBERG MXP Codec firmware.

2.7 Cryptographic Key Management

The module implements the following Approved cryptographic algorithms:

- AES – Electronic Codebook (ECB) mode with a 128-bit key, counter mode with a 128-bit key, Output Feedback (OFB) mode with a 128-bit key, Cipher Block Chaining (CBC) mode with a 128-, 192-, or 256-bit key (Certificate # 504)
- TDES – ECB mode with three 64-bit independent keys, CBC mode with three 64-bit independent keys (Certificate # 514)
- RSA following Public Key Cryptography Standards (PKCS) #1 for signature generation and verification – 1024-, 2048-, or 4096-bit keys (Certificate # 218)
- DSA – 1024-, 2048-, or 4096-bit keys (Certificate # 208)
- Secure Hash Algorithm (SHA)-1 (Certificate # 574)
- Keyed-Hash Message Authentication Code (HMAC)-SHA-1 with 160-bit key (Certificate # 257)
- American National Standards Institute (ANSI) X9.31 Appendix A.2.4 Random Number Generator (RNG) with 128-bit AES (Certificate # 282)

The module implements the following non-Approved cryptographic algorithms:

- A non-Approved RNG for entropy gathering for the ANSI X9.31 Appendix A.2.4 RNG
- 1024-bit Diffie-Hellman key agreement scheme providing 80 bits of security.
- 1024-, 2048, or 4096-bit RSA PKCS#1 key wrapping providing 80 bits, 112 bits, or 150 bits of security.

Four protocols implemented in the codec, H.320, H.323, SSH, and HTTPS, are security-related. Table 5, Table 6, Table 7, and Table 8 introduce cryptographic keys, key components, and CSPs involved in these four protocols, respectively. CSPs for firmware upgrade are tabulated in Table 9. Notice that, the variables with the same name in different tables have nothing to do with each other. For example, Kx in Table 5 and Table 6 represent two separate variables. Also notice that XOR indicates the exclusive-or operation, and CA is short for "certification authority".

Another important remark follows. The module supports both a FIPS mode and a non-FIPS mode of operation. The two modes do not share keys, key components, or CSPs. i.e., a key, key component, or CSP that is established or used in FIPS mode is not used in non-FIPS mode and vice versa.

Table 5 - List of CSPs for H.320

Key/ Key Component	Type	Generation / Input	Output	Storage	Zeroization	Use
a, b, g, p	1024-bit Diffie-Hellman keys	Generated by ANSI X9.31 Appendix A.2.4 RNG	No	Plaintext in volatile memory	Upon generation of Kx	Negotiate Kx

[8] DSP/BIOS kernel is a scalable real-time multi-tasking kernel by the Texas Instruments.

Key/ Key Component	Type	Generation / Input	Output	Storage	Zeroization	Use
Kx	AES symmetric key (128-bit)	Generated by 1024-bit Diffie-Hellman key agreement. The key strength of Kx is 80 bits	No	Plaintext in volatile memory	Upon generation of Koa, Kia, Kob, Kib	Encrypt and decrypt Na1, Na2, Na3, Na4, Nb1, Nb2, Nb3, Nb4
Na1, Na2, Na3, Na4, Nb1, Nb2, Nb3, Nb4	Random string used as key component (128-bit each)	Generated by ANSI X9.31 Appendix A.2.4 RNG	AES encrypted using key Kx	Plaintext in volatile memory	Upon generation of Koa, Kia, Kob, Kib	Derive Koa, Kia, Kob, Kib
Koa	AES symmetric key (128-bit)	Na1 XOR Nb3	No	Plaintext in volatile memory	Upon session termination	Encrypt outgoing video and audio data
Kia	AES symmetric key (128-bit)	Nb1 XOR Na3	No	Plaintext in volatile memory	Upon session termination	Decrypt incoming video and audio data
Kob	AES symmetric key (128-bit)	Nb1 XOR Na3	No	Plaintext in volatile memory	Upon session termination	Encrypt outgoing video and audio data
Kib	AES symmetric key (128-bit)	Na1 XOR Nb3	No	Plaintext in volatile memory	Upon session termination	Decrypt incoming video and audio data
RNG seed and seed key	RNG seed and AES key	Generated by non-Approved RNG	Never output	Plaintext in volatile memory only	When new seed and seed key values are fed	Generate keys and key components

Table 6 - List of CSPs for H.323

Key/ Key Component	Key Type	Generation / Input	Output	Storage	Zeroization	Use
a, b, g, p	1024-bit Diffie-Hellman keys	Generated by ANSI X9.31 Appendix A.2.4 RNG	Endpoint's public key is output with AES encrypted with P.[9] Private keys are not output.	Plaintext in volatile memory	Upon session termination	Negotiate Kx
Kx	AES symmetric key (128-bit)	Generated by 1024-bit Diffie-Hellman key agreement. The key strength of Kx is 80 bits	No	Plaintext in volatile memory	Upon session termination	Encrypt and decrypt Km

[9] For FIPS 140-2 purposes, the keys are output in plaintext.

Key/ Key Component	Key Type	Generation / Input	Output	Storage	Zeroization	Use
P	AES cipher key (128-bit)	High-order 128 bits of the 160-bit SHA-1 hash of the common security pin code	No	Plaintext in volatile memory	Upon session termination	Generate round keys
key_clen	HMAC key	Generated by a pseudo-random function	No	Plaintext in volatile memory	Upon session termination	Verity integrity of packets
Km	AES symmetric key (128-bit)	Generated by ANSI X9.31 Appendix A.2.4 RNG	AES encrypted using key Kx	Plaintext in volatile memory	Upon session termination	Encrypt and decrypt video and audio data
RNG seed and seed key	RNG seed and AES key	Generated by non-Approved RNG	Never output	Plaintext in volatile memory only	When new seed and seed key values are fed	Generate keys and key components

Table 7 - List of CSPs for SSH

Key/ Key Component	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Kh	1024-bit Diffie-Hellman keys	Generated by ANSI X9.31 Appendix A.2.4 RNG	Public keys are output in plaintext. Private keys are not output.	Plaintext in volatile memory	Upon session termination	Negotiate Ks
Kdsa	1024-bit DSA keys	Generated by ANSI X9.31 Appendix A.2.4 RNG	Public keys are output in plaintext. Private keys are not output.	Plaintext in flash memory	Upon exiting FIPS mode	Private key is used to sign the server's part of the transaction. Public key is used to verify the signature.
Ks	AES or TDES Symmetric key(s)	1024-bit Diffie-Hellman key agreement	No	Plaintext in volatile memory	Upon session termination or when a new Ks is generated (after a certain timeout)	Encrypt and decrypt data
RNG seed and seed key	RNG seed and AES key	Generated by non-Approved RNG	Never output	Plaintext in volatile memory only	When new seed and seed key values are fed	Generate keys and key components

Table 8 - List of CSPs for HTTPS

Key/ Key Component	Key Type	Generation / Input	Output	Storage	Zeroization	Use

Key/ Key Component	Key Type	Generation / Input	Output	Storage	Zeroization	Use
MS	TLS master secret	1. Input in encrypted form from client 2. Negotiated via Diffie-Hellman scheme	No	Plaintext in volatile memory only	Upon session termination	Derive Ks
KRsaPub	RSA public key	Loaded in a .PEM formatted file in plaintext from a non-networked general purpose computer	In plaintext as part of certificate	Plaintext in flash memory	When the certificate becomes invalid	Client encrypts MS, client verifies signatures
KRsaPriv	RSA private key	Loaded in a .PEM formatted file in plaintext from a non-networked general purpose computer	No	Plaintext in flash memory	When the certificate becomes invalid	Server decrypts MS, server generates signatures
KDsaPub	DSA public key	Input in plaintext as part of certificate	In plaintext as part of certificate	Plaintext in flash memory	When the certificate becomes invalid	Client verifies signatures
KDsaPriv	DSA private key	Input in plaintext form	No	Plaintext in flash memory	When the certificate becomes invalid	Server generates signatures
Kh	1024-bit Diffie-Hellman keys	Generated by ANSI X9.31 Appendix A.2.4 RNG	Public keys are output in plaintext. Private keys are not output	Plaintext in volatile memory	Upon session termination	Negotiate Ks
Ks	AES or TDES symmetric key(s)	Derived from MS	No	Plaintext in volatile memory	Upon session termination	Encrypt and decrypt data
RNG seed and seed key	RNG seed and AES key	Generated by non-Approved RNG	Never output	Plaintext in volatile memory only	When new seed and seed key values are fed	Generate keys and key components

Table 9 - List of CSPs for Firmware Upgrade

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
KdsaCA	DSA public key	Hard-coded in flash memory	No	Plaintext in flash memory	Never	Verify CA's signature
KdsaUpgrade	DSA public key	Input along with the upgrade package in plaintext as part of the certificate signed by CA	No	Plaintext in flash memory	When the certificate becomes invalid	Verify DSA signature on the upgrade package

2.7.1 Key Generation

The module uses ANSI X9.31 Appendix A.2.4 RNG to generate cryptographic keys. This RNG is FIPS-Approved as indicated by Annex C to FIPS PUB 140-2. The seed for the ANSI X9.31 Appendix A.2.4 RNG is provided by a non-Approved RNG, which collects entropy from the infrared remote receiver, Ethernet receiver, and ISDN driver routines.

2.7.2 Key Input/Output

RSA key pairs are generated externally and input to the modules in plaintext. RSA, DSA, and Diffie-Hellman private keys never exit the module, while the public keys are output in plaintext. In H.323 and H.320, symmetric keys that are input into and output from the module are encrypted by 128-bit AES. In HTTPS, session keys exit the module in encrypted form during TLS handshakes (protected within RSA key transport). Other CSPs and keys, such as the DSA keys for integrity tests never output from the module.

WARNING: KRsaPub and KRsaPriv for HTTPS (see Table 8) must be imported via HTTP in a *secure environment*. To realize a secure environment, the general purpose computer running the HTTP client (e.g., Firefox, Internet Explorer) must be *standalone* and *not-networked*. In essence, the general purpose computer serves as a key loader as defined in FIPS 140-2. See the "Certificate Management" section of the Administrator Manual for details.

2.7.3 Key Storage

The DSA and RSA public and private key pairs and the DSA public keys for integrity tests are stored in the module's flash memory in plaintext. Session key and Diffie-Hellman public and private key pairs are held in volatile memory (SDRAM) in plaintext.

2.7.4 Key Zeroization

For H.320 and H.323 protocols, all Diffie-Hellman keys, symmetric keys, HMAC keys, and key components are zeroized when they are no longer needed, usually at the end of the session, or when encryption is disabled during a call. For the SSH protocol, a session key is zeroized at the end of the session, or when a new session key is generated after a certain timeout. A DSA key pair is zeroized when the codec exits FIPS mode. For the HTTPS protocol, the TLS session key is zeroized at the end of the session. The RSA and DSA key pairs are not automatically zeroized. The DSA key for the firmware integrity test and keys for other power-up self-tests are hard-coded. This is allowed by FIPS 140-2 according to Section 7.4 of the Implementation Guidance.

The zeroization of the keys is carried out by overwriting the storage area or memory location with zeros.

2.8 Self-Tests

The TANDBERG MXP Codec performs the following self-tests at power-up:

- A firmware integrity test using DSA to ensure that the module has not been modified
- Known Answer Test (KAT) on TDES with 3 independent keys (64 bits each) in ECB mode
- KAT on AES with a 128-bit key in ECB mode
- KAT on HMAC-SHA-1
- KAT on RSA with 1024-bit keys for signature generation/verification and encryption/decryption
- KAT on ANSI X9.31 Appendix A.2.4 RNG
- Pair-wise consistency test for DSA keys

If the power-up self-tests fail, the codec server will be automatically rebooted. An error message "FIPS Algorithm self-test failed. Fatal Error!" will be written to the system event log before the reboot.

The conditional self-tests performed by the module include the following four tests.

- Pair-wise consistency test for new DSA keys
- Bypass test
- Continuous RNG test on the ANSI X9.31 Appendix A.2.4 RNG
- Continuous RNG test on the non-Approved RNG
- Software/firmware load test using DSA to ensure that the upgrade has not been modified

If conditional self-tests fail, an error message will be written to the system event log. Failure of a pair-wise consistency test for new DSA keys or a continuous RNG test leads to reboot of the codec server. Failure of a bypass test forbids the operator to change the security settings ("No Encryption", "Auto Encryption", or "Encryption On"). If an integrity test for the upgrade package fails, the upgrade will not be installed.

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 level 1 requirements for this validation.

3 Secure Operation

The TANDBERG MXP Codec meets Level 1 requirements for FIPS 140-2. The module does not require any initial authentication by an operator during the first time the module is accessed. During the first time the module is accessed, it is assumed that the operator is the owner of the system. It is the Crypto Officer's responsibility to configure the module. See Table 3 for details.

As stated in Session 2.4, an operator can access the module through one of the following interfaces:

(1) infrared remote
(2) HTTP/HTTPS
(3) SSH
(4) RS232

The infrared remote provides the operator with a menu interface and the HTTP/HTTPS protocol provides a web-based interface. The SSH and RS232 interfaces are command-line based. Additionally, an operator can access the codec via SNMP and FTP to perform certain limited operations. SNMP and FTP services are not security-relevant.

The client application (web browser) used for HTTPS connections must support TLS version 1 or later. For SSH connections, the client application must support SSH version 2 or later.

The sections below describe how to place and keep the module in the FIPS-Approved mode of operation and how to make secure calls.

3.1 Crypto Officer Guidance

In order to have the TANDBERG MXP codec server work in the FIPS-Approved mode, a Crypto Officer shall perform the following operations:

Infrared remote:

Go to the "Control Panel" menu, select "Security", and then choose "On" for the "FIPS Mode" option. Save this change. The codec will be rebooted.

Web browser (HTTP/HTTPS):

Go to the "Endpoint configuration" menu, select the "Security" tag, and then click on the "Enable FIPS Mode" button. The codec will be rebooted.

Command line interface (SSH, RS232):

To switch from non-FIPS mode to FIPS mode, input the command "fipsmode on" and hit the "enter" key on your keyboard. The connection will be terminated because the codec is being rebooted.

In order to have the TANDBERG MXP codec server work in the non-FIPS mode, a Crypto Officer shall perform the following operations:

Infrared remote:

Go to the "Control Panel" menu, select "Security", and then choose "Off" for the "FIPS Mode" option. Save this change.

Web browser (HTTP/HTTPS):

Go to the "Endpoint configuration" menu, select the "Security" tag, and then click on the "Disable FIPS Mode" button. Make sure that message "FIPS Mode is currently disable" is shown to the right of the "FIPS mode" entry.

Command line interface (SSH, RS232):

To switch from non-FIPS mode to FIPS mode, input the command "fipsmode off" and hit the "enter" key on your keyboard.

In FIPS mode, encryption services for video calls are configured with a menu option or a command. The Crypto Officer can set the encryption options to "Encryption Off", "Auto Encryption", or "Encryption On". This requires that there be (respectively) no encryption on any calls, encryption where the other side will support it, or that all calls be encrypted. The following instructions show how to configure the security setting:

Infrared remote:

Go to "Control Panel", select "Security", and then choose "On", "Auto", or "Off" for the "Encryption" option. When "Encryption" is configured to either "On" or "Auto", the Crypto Officer also needs to choose an "Encryption Mode" by selecting "AES" or "Auto". Finally save these changes.

Web browser (HTTP/HTTPS):

Go to "Endpoint configuration", select "Security", and then choose "On", "Auto", or "Off" for the "Encryption" option. When "Encryption" is configured to either "On" or "Auto", the Crypto Officer also needs to choose an "Encryption Mode" by selecting "AES-128" or "Auto". Finally save this page.

Command line interface (SSH, RS232):

Execute "encrypt on", "encrypt auto", or "encrypt off" to configure a proper encryption option. When "encrypt on" or "encrypt auto" is configured, the Crypto Officer also needs to set an "Encryption Mode". This can be done by executing an "encmode aes128" or "encmode auto" command.

During the process of a call, the television or monitor displays a padlock at the upper right corner showing the current encryption status. An AES-encrypted call is indicated by a double padlock. A TDES-encrypted call is indicated by a single padlock. A plaintext call is indicated by an open padlock.

3.2 User Guidance

Before placing or answering videoconferencing calls, the User should examine the security settings by performing the following operations:

Infrared remote:

Go to the "Control Panel" menu, select "Security". Make sure that the "FIPS mode" is set to "On".

Web browser (HTTP/HTTPS):

Go to the "Endpoint configuration" menu, select the "Security" tag. Make sure that message "FIPS Mode is currently enabled" is shown to the right of the "FIPS mode" entry.

Command line interface (SSH, RS232):

*Input the command "fipsmode" and hit the "enter" key on your keyboard. If the return value is "*P fipsmode on", then the codec is running in the FIPS mode. If the return value is "*P fipsmode off", then the codec is running in the non-FIPS mode.*

"Encryption Off" suggests no encryption on any calls; "Auto Encryption" indicates that encryption will be applied where the other side will support encryption; "Encryption On" requires that all calls be encrypted. "AES" means only AES symmetric cryptography is allowed for encryption. "Auto selection" will negotiate through AES and no encryption. The User should make sure the current setting satisfies his/her security requirements before placing and answering calls.

During the process of a call, the television or monitor displays a padlock symbol at the upper right corner showing the current encryption status. An AES-encrypted call is indicated by a double padlock. A TDES-encrypted call is indicated by a single padlock. A plaintext call is indicated by an open padlock. The User should terminate the call immediately and check the encryption setting if an unexpected encryption status is reported.

4 Acronyms

Table 10 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BIOS	Basic Input/Output System
BRI	Basic Rate Interface
CA	Certification Authority
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DC	Direct Current
DCE	Data Communications Equipment
DSA	Digital Signature Algorithm
DSP	Digital Signal Processor
DVI	Digital Visual Interface
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
HD	High-Definition
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Transport Layer Security
FTP	File Transfer Protocol
IM	Instant Messaging
IP	Internet Protocol
IR	Infrared Remote
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
KAT	Known Answer Test
LAN	Local Area Network

Acronym	Definition
LED	Light-Emitting Diode
MCU	Multiple Control Unit
MPS	Media Processing System
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
PCI	Peripheral Component Interconnect
PKCS	Public Key Cryptography Standards
PRI	Primary Rate Interface
RCA	Radio Corporation of America
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
RTOS	Real-Time Operating System
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
S/PDIF	Sony/Philips Digital Interface Format
SSH	Secure Shell
TDES	Triple Data Encryption Standard
THSI	TANDBERG High Speed Interface
TLS	Transport Layer Security
USB	Universal Serial Bus
VAC	Volts Alternating Current
XOR	Exclusive-or