Cisco Systems

Cisco Telepresence C40, C60, and C90 Codecs

(Firmware Version: TC5.0.2)
(Hardware Version: v1)

FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation

Document Version 1.0

Revision History

Version	Modification Date	Modified By	Description of Changes
1.0	2011-11-10	Espen Holmbakken	Initial version

Table of Contents

Table of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for Cisco TelePresence C40, C60, and C90 Codecs. This policy describes how the Cisco TelePresence C40, C60, and C90 codecs meet the requirements of FIPS 140-2. This document also includes instructions for configuring the security appliances in FIPS 140-2 mode.

This policy was prepared as part of the Level 2 FIPS 140-2 validation for the Cisco TelePresence C40, C60, and C90 Codecs.

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 NIST website at http://csrc.nist.gov/groups/STM/cmvp/.

In this document, the Cisco C series 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 Cisco website (http://www.cisco.com) contains information on the full line of products from Cisco.
- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

2 Cisco Telepresence C40, C60, and C90 codecs

The Cisco TelePresence portfolio creates an immersive, face-to-face experience over the network—empowering you to collaborate with others like never before. Through a powerful combination of technologies and design that allows you and remote participants to feel as if you are all in the same room, the Cisco TelePresence portfolio has the potential to provide great productivity benefits and transform your business. Many organizations are already using it to control costs, make decisions faster, improve customer intimacy, scale scarce resources, and speed products to market.

The Cisco TelePresence C series Codec is one of the most powerful, flexible TelePresence and collaboration engine available delivering crisp, clear 1080p end-to-end HD video, HD collaboration, and HD embedded Cisco TelePresence MultiSite (MultiSite). With more inputs and outputs than ever before, the integration possibilities are endless.

Cisco Telepresence provides full standard protocol H.323 (for Ethernet) and SIP (for Ethernet). Using these protocols, secure video conferencing is offered using Advanced Encryption Standard (AES) encryption for point-to-point calls and multipoint calls on Ethernet with the speed of up to 6000 kbps on the full Cisco Telepresence product line.

2.1 Module Overview

The Cisco C series Codec (version TC5.0.2) is the firmware installed in the Cisco C series endpoint product line. The firmware supports the following Cisco Telepresence codec servers: C40, C60, and C90.

The Cisco Telepresence C40, C60, and C90 codecs support a FIPS-Approved mode of operation and a non-FIPS-Approved mode of operation. The Cisco Telepresence C40, C60, and C90 codecs are 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	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

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

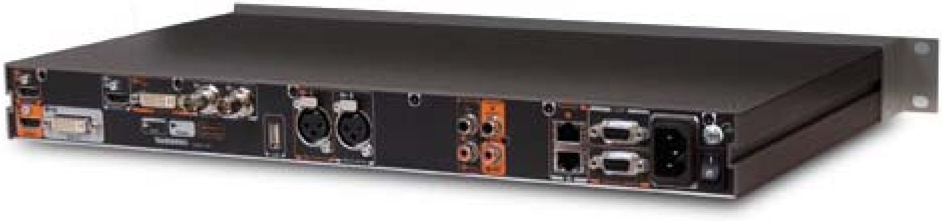

Figure 1 - Cisco Telepresence C40 Codec

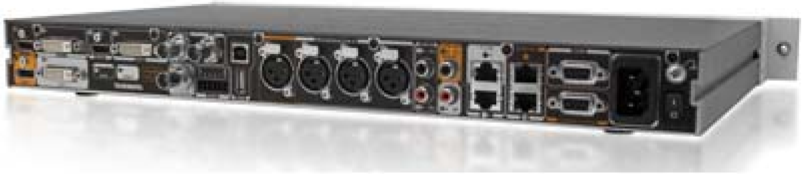

Figure 2 – Cisco Telepresence C60 Codec

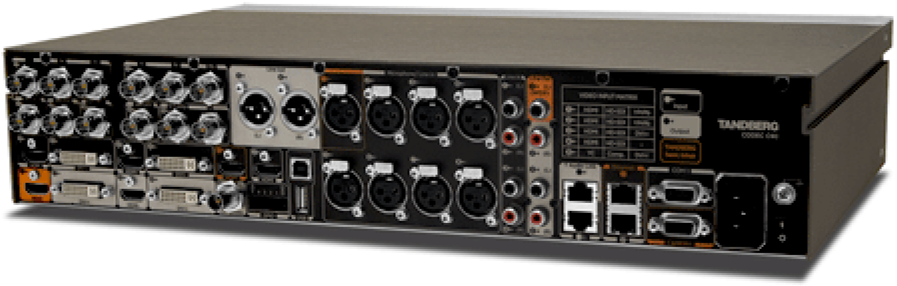

Figure 3 - Cisco Telepresence C90 Codec

2.2 Module Ports and Interfaces

Each 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 Table 2. 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.

Table 2 - Mapping of FIPS 140-2 Logical Interfaces to C series codec Server Interfaces

FIPS 140-2 Logical Interface	Cisco C series Codec Server Port/Interface
Data Input	Microphone input 1-8, Audio Line input 1-4, DVI input 3 and 5, Ethernet 1 and 2, HDMI input 1-4,, HD-SDI 1-4, Component input 1 and 2 , Composite/Svideo input 5,
Data Output	Audio Line output 1-4, DVI output 2 and 4, Ethernet 1 and 2, DCE Port Data 1, DCE Port Data 2, HDMI outputs 1 and 3, Audio XLR output 5 and 6, Composite output 5
Control Input	Infrared remote, Ethernet 1 and 2, DCE Port Data 1
Status Output	Audio Line output 1 and 2, DVI output 2 and 4, Ethernet 1 and 2, DCE Port Data 1, LEDs, HDMI output 1 and 3, Audio XLR output 5 and 6, GPIO
Power	Power socket

2.3 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.

Both roles can access the module through one of the following interfaces:

- infrared remote
- HTTPS
- SSHv2
- RS232

The infrared remote provides the operator with a menu-driven interface. The HTTP/HTTPS protocol provides a web-based interface. The SSHv2 and serial interfaces are command-line based.

Authentication is identity-based. Each user is authenticated upon initial access to the module. As required by FIPS 140-2, there are two main roles in the security appliances that operators may assume: a Crypto Officer role and User role. The administrator of the module assumes the Crypto Officer role in order to configure and maintain the module using Crypto Officer services, while the Users exercise only the basic User services.

The User and Crypto Officer passwords and PINs must each be at least eight (8) characters long, and the minimum number of character groups to three (numerical special characters, upper case and lower case characters), and maximum number of consecutive characters in password to be 2.

-For access on the over RS232, HTTPS or SSH, the operator needs to type in a username and password. A password must, at the very minimum, satisfy all password criteria listed in section 3.1. That is, the password must be at least 8 characters, contain at least one alphabet letter (uppercase or lowercase), one special character, maximum two consecutive characters, and an integer. Therefore, the minimum password contains six (6) integers, one (1) special character and one (1) alphabet. The probability of randomly guessing the correct sequence is one (1) in 1,091,750,400. In FIPS mode, the module limits entering a password on the serial port and SSH by enforcing a four second delay between each password entry. Therefore, an attacker will be able to input 15 passwords in one minute with this four second delay. The probability that a random success or false acceptance is 15 out of 1,091,750,400, which is much less than 1 in 100,000. The web interface restriction is different, as an attacker is limited to 1500 attempts per minute. Therefore the probability of a random success is 1500 in 1,091,750,400 which is less than one in 100,000. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

Likewise, when logging into the module using the *infrared remote control*, the operator needs to enter a PIN. Since the PIN consists of 8 (eight) integers with a maximum 2 consecutive digits, the probability of randomly guessing the correct sequence is one (1) in *53,144,100. The maximum number of characters the infrared interface can handle is 50 characters per second. At a minimum, 8 movements are needed to enter in an 8 digit PIN on the remote, also adding three extra inputs to submit the PIN to the IR interface from the remote. This totals to 11 characters per second, meaning 4.54 PIN attempts can be made in one second, which also equals 272.73 PIN attempts per minute. T*he probability of a random *success within one minute is 272.73* in 53,144,100. Increasing the number of digits in the PIN further lowers the probability.

2.3.1 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”).

Table 3 – Crypto Officer Services

Service	Description	Input	Output	Keys/CSPs and Type of Access
User and password management	Create users, assign roles and change passwords of users.	Web interface	Users with Crypto Officer (admin) or User role. Status, success or failure	Write SHA-256 password hashes
Enable FIPS mode	Enter FIPS operational mode	Command	System reboot, system boots up in FIPS mode	None
Reset to factory default	Reset the codec server system	Command	Uninstalled module, this exits FIPS mode of operation	None
Login through infrared remote	Crypto Officer logs in the codec through infrared remote	Physical access, username and PIN	Status, success or failure	Verifies PIN Hash
Login through HTTPS	Crypto Officer logs in the codec through HTTPS	Codec’s IP address, username/password or certificate	Status, success or failure	RSA keys – Read DSA keys – Read AES key – Read, Write, and Delete TDES keys – Read, Write, and Delete Verifies Password Hash

Service	Description	Input	Output	Keys/CSPs and Type of Access
Login through SSH	Crypto Officer logs in the codec through SSH	Codec's IP address, username/password or certificate	Status, success or failure	DSA keys – Read, Write, and Delete AES key – Read, Write, and Delete TDES keys – Read, Write, and Delete Verifies Password Hash
Login through RS232	Crypto Officer logs in the codec through RS232	Physical access, username/password	Status, success or failure	Verifies Password Hash
Configure system settings	Configure network parameters that are necessary for placing/answering calls and system parameters Configuring module video, audio camera settings	Command, network parameters such as IP addresses,	Status, success or failure	None
Configure security settings	Enable/disable HTTPS/SSH/Serial port	Command, options	Status, success or failure	None
Install certificates	Install certificates for TLS sessions for HTTPS connections and certificates for IEEE 802.1.x	Command, certificates, private keys	Status, success or failure	RSA or DSA key pair- Write
Get logfiles	Access the logs stored on the codec	Command, options	Event log,	None
Get Status	Get status of the module	Command	Status	None
Zeroize	Zeroize the keys used by the module during a call or connection	Command, Hard Reset (power button)	Status	AES keys – Read, Write, and Delete TDES keys – Read, Write, and Delete HMAC keys – Read, Write, and Delete Diffie-Hellman keys – Read, Write, and Delete RSA keys – Read, Write, and Delete DSA keys – Read, Write, and Delete

2.3.2 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	Physical access, username and PIN	Status, success or failure	Verifies PIN Hash
Login through HTTPS	User logs in the codec through HTTPS	Codec's IP address	Status, success or failure	RSA keys – Read DSA keys – Read AES key – Read, Write, and Delete TDES keys – Read, Write, and Delete Verifies Password Hash
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 Verifies Password Hash
Login through RS232	User logs in the codec through RS232	None	Status, success or failure	Verifies Password Hash
Videoconferencing Calls	Place outgoing calls or answer incoming calls	Command, number of the receiver (when placing an outgoing call)	Status, success or failure	AES keys – Read, Write, and Delete
Configure user settings	Configure user settings like volume, background picture, layout, video input.	Command	Status, success or failure	None
Get Status	Get status of the module	Command	Status	None
Zeroize	Zeroize the keys used by the module during a call or connection	Command, Hard Reset (power button)	Status	AES keys – Read, Write, and Delete TDES keys – Read, Write, and Delete HMAC keys – Read, Write, and Delete Diffie-Hellman keys – Read, Write, and Delete

2.4 Cryptographic Key Management

The Codecs use a variety of keys and Critical Security Parameters (CSP's)

Table 5 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/ Key Component	Type	Generation	Storage	Zeroization	Use

Key/ Key Component	Type	Generation	Storage	Zeroization	Use
SSH host private key	DSA-1024	Generated based on random data	On Flash	At factory reset	SSH session handshake
SSH Session authentication key	HMAC-SHA1 key	Agreed upon server and client as part of ssh session setup	Stored in volatile memory	When session is terminated	Data authentication for SSH sessions
SSH Session encryption key	Triple-DES CBC key AES CBC 128bit key	Derived via the SSH protocol	Stored in volatile memory	When session is terminated	Data encryption/decryption for SSH sessions
Diffie-Hellman private exponent	Diffie-Hellman 1024	Generated by calling the Approved DRBG	Stored in volatile memory	When session is terminated	Used to derive the shared secret in the Diffie-Hellman key exchange
Diffie-Hellman shared secret	Diffie-Hellman 1024	Negotiated in the Q.931 phase of the H323 call setup according to H.235	Stored in volatile memory	When session is terminated	Used to derive the H323 call setup master key
H323 call setup master key	1024 bit shared secret	Derived from Diffie-Hellman key exchange	Stored in volatile memory	When session is terminated	Used to derive subsequent H323 keys
H323 Session key wrapping key	AES-128	Derived from the H323 call setup master key	Stored in volatile memory	When session is terminated	Used to AES encrypt the H323 Session key
H323 Session key	AES-128	Generated by calling the Approved DRBG	Stored in volatile memory	When session is terminated	Used to encrypt the H323 session traffic.
User PIN	Operator PIN	Provided by crypto officer or User upon login.	Stored hashed using SHA-1 on flash	At factory reset	This is used for H323 RAS authentication
sRTP master key	Shared Secret	Derived from TLS handshake	Stored in volatile memory	When session is terminated	Master key used for session key derivation
sRTP session authentication key (HMAC)	HMAC SHA-1	Derived from the sRTP master key using pseudo random function	Stored in volatile memory	When session is terminated	Keys used to authenticate sRTP packets
sRTP session encryption key	AES128 CTR	Derivedfrom the sRTP master key using pseudo random function	Stored in volatile memory	When session is terminated	Key used to encrypt/decrypt sRTP packets

Key/ Key Component	Type	Generation	Storage	Zeroization	Use
sRTP salting key	Salting key	Generated using the module's Approved DRBG	Stored in volatile memory	When session is termintated	Used to generate the Initialization vector of the SRTP encryption stream
SIP TLS session keys	HMAC-SHA1 AES128	Derived according to the TLS protocol	Stored in volatile memory	When session is terminated	Used for user authentication/encryption over TLS connection on SIP
SIP TLS certificate private key	RSA/DSA	Provided by Crypto Officer	Stored on flash in plaintext	On factory reset	With SIP TLS client certificate
HTTPS TLS session key	HMAC-SHA1	Derived according to the TLS protocol	Stored in volatile memory	When session is terminated	Data authentication/encryption for TLS sessions (HTTPS client, HTTPS server, Syslog)
HTTPS TLS certificate and private key	RSA/DSA	Provided by Crypto Officer	Stored on flash in plaintext	On factory reset	With HTTPS TLS handshake
HTTPS TLS session encryption key	Triple-DES AES CBC 128 bit	Derived according to the TLS protocol	Stored in volatile memory	When session is terminated	Data encryption for TLS sessions
RNG seed key	Seed key	Using non-Approved RNG	Stored on flash	On factory reset	Used for RNG operations
Passwords	Operator password	Generated each time a user changes his/her password	Hashed using SHA-256 and stored on flash	On factory reset	Password hashes for users are stored on flash. Passwords are not stored in cleartext
File storage cryptographic key	AES-128	Generated from random data on module initialization	Stored on NOR-Flash	On factory reset	Used for encrypting the file storage on NAN-Flash
Firmware Integrity Key	DSA public key	Exists within the firmware binary	Stored on flash	Public key – not required to be zeroizable	Used for checking integrity of the firmware on every power-up

2.4.1 Key Generation

The module uses SP800-90 DRBG RNG to generate cryptographic keys. This RNG is FIPS-Approved as indicated by FIPS PUB 140-2.

The seed for the SP800-90 DRBG RNG is provided by a non-Approved RNG, which collects entropy from the Ethernet receiver.

2.4.2 Key Input/Output

RSA/DSA key pairs used for TLS are generated externally and input to the modules in plaintext. RSA, DSA, and DH private keys never exit the module, while the public keys are output in plaintext. In H.323 symmetric keys that are input into and output from the module are encrypted by 128-bit AES. For SIP master key is sent over TLS, which is used to generate the session keys. 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.

2.4.3 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.

2.4.4 Key Zeroization

For the SIP and H.323 protocol, 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 public 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 keys are stored on an AES-128 encrypted file storage, and zeroisation is done by overwriting the key with zeros.

2.5 Self-Tests

Implementation	Tests Performed
Codec Software	-DSA Firmware Integrity Test
OpenSSL	-AES KAT -Triple-DES KAT -SHA-1 KAT -DSA Sign/Verify -ECDSA Sign/Verify -RSA Sign/Verify

	-SP800-90 DRBG KAT -HMAC-SHA-1 KAT -HMAC-SHA-224 KAT (covers self-test for SHA-224) -HMAC-SHA-256 KAT (covers self-test for SHA-256) -HMAC-SHA-384 KAT (covers self-test for SHA-384) -HMAC-SHA-512 KAT (covers self-test for SHA-512)

The codecs perform all power-on self-tests automatically at boot when FIPS mode is enabled. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the codecs from passing any data during a power-on self-test failure. In the unlikely event that a power-on self-test fails, an error message is written to /var/log/fipslog followed by a security appliance reboot.

Implementation	**Conditional Tests Performed**
OpenSSL	-DSA, ECDSA, and RSA Pairwise Consistency Tests -SP800-90 DRBG and non-Approved RNG Continuous Random Number Generator Tests

If conditional self-tests fail, an error message will be written to /var/log/fipslog. Failure of a pair-wise consistency test for asymmetric keys or a continuous RNG test leads to reboot of the codec server.

If the integrity test for the running software fails, the system will reboot and an error message will be written to /var/log/fipslog.

2.6 Mitigation of Other Attacks

The codecs do not claim to mitigate any attacks in a FIPS approved mode of operation above and beyond the protection inherently provided by the codecs.

3 Secure Operation

The Cisco C series Codec meets Level 2 requirements for FIPS 140-2.

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

(1) Infrared remote

(2) HTTPS

(3) SSH

(4) RS232

The infrared remote provides the operator with a menu interface and the HTTPS protocol provides a web-based interface. The other three interfaces are command-line based.

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 Cisco C series codec server work in the FIPS-Approved mode, a Crypto Officer should perform the following operations:

1. The tamper-evident labels shall be installed for the module to operate in a FIPS Approved mode of operation. Refer to Section 'Physical Security' of this document for directions to apply the tamper-evident labels.

2. Log in to SSH or RS232. If the unit has not been previously used, the codec should be on a closed network. The username is "admin" and the password is blank.

3. Switch from non-FIPS mode to FIPS mode, by inputting the command *"xCommand Security FIPSmode Activate Confirm: Yes"* and hit the *"enter"* key on your keyboard. The connection will be terminated because the codec is being rebooted.

4. Log into SSH again, and enforce password policy by entering "*systemtools securitysettings ask"*, and change the following settings when prompted and set them to the values displayed in the square brackets (all other prompts can be left unaltered by pressing enter):

   Max consecutive equal digits in PINs [2]?

   Minimum number of digits in PINs [6]?

   Minimum number of characters in passwords [8]?

   Max consecutive identical characters in passwords [2]?

   Minimum number of character groups in passwords [3]?

5. Change the password of the Crypto Officer by using the command "*systemtools passwd"* and typing in the old password and new password twice.

6. Require that users and crypto officers log in to the GUI interface by setting the command

"xconfiguration Video OSD LoginRequired: on"

7. Log into the web interface as the Crypto Officer. Here you can go to "Maintenance" then "User Administration" to create users with USER role, or other Crypto Officers with ADMIN role.

8. The first time the crypto officer and all new users log onto GUI they must change their PIN (from blank if not specified when created). They might also be required to change their password the first time they log into web/ssh if this was a condition when creating the user.

In FIPS mode, encryption services for video calls between two modules are always required. This means that a call will only be accepted if both endpoints (modules) support encryption.

3.2 Approved Algorithms

The appliances support many different cryptographic algorithms; however, only the following FIPS approved algorithms may be used while in the FIPS mode of operation:

- AES encryption/decryption
- Triple DES encryption/decryption
- SHA (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512)
- HMAC-SHA-1 for hashed message authentication
- RSA sign and verify
- DSA sign and verify
- ECDSA sign and verify
- DRBG

The Tandberg C40, C60 and C90 have earned the CAVP algorithm certifications listed below

Algorithm	***Certificate number***
AES	1928
Triple-DES	1255
DSA	612
SHS	1693
RSA	994

HMAC	1162
ECDSA	276
DRBG	168

Caveat:

The following Non-Approved algorithms are allowed for use for key establishment purposes in the FIPS-Approved mode of the module:

- Diffie-Hellman (key agreement; key establishment provides 80-bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 80, 112, or 150 bits of encryption strength)
- AES (Cert. #1928, key wrapping; key establishment methodology provides 128 bits of encryption strength)

3.3 Non-Approved Algorithms

The modules implement the following non-FIPS-approved cryptographic algorithms:

- DES
- RC4
- RC2
- MD5
- HMAC-MD5
- Blowfish
- Camellia

Note: Non-FIPS approved algorithms cannot be used in FIPS mode of operation.

3.4 Physical Security

All Critical Security Parameters are stored and protected within each appliance's enclosure which is protected using tamper-evident labels (TELs). The Crypto Officer is responsible for properly placing all tamper evident labels. The tamper-evident labels required for FIPS 140-2 compliance are provided in the FIPS Kit (Part Number CISCO-FIPS-KIT=). The FIPS kit includes the TELs, as well as a document detailing the number of seals required per platform and placement information. These security labels are very fragile and cannot be removed without leaving signs of tampering.

Each of the C40, C60 and C90 modules require six (6) tamper-evident labels. The Crypto-Officer must first take note of where the labels are to be placed on the module. Then, the Crypto-Officer must ensure that the surfaces of the module (where the TELs are to be placed) are cleaned with rubbing alcohol. The Crypto-Officer can use a small paper towel with a dab of rubbing alcohol or an alcoholic swab to clean the surfaces. After the rubbing alcohol dries, the Crypto-Officer must apply these TELs in the positions shown in the photos of the modules below before making the module available for use in the FIPS-Approved mode.The Crypto-Officer shall inspect the module enclosure and the TELs periodically for signs of tampering.

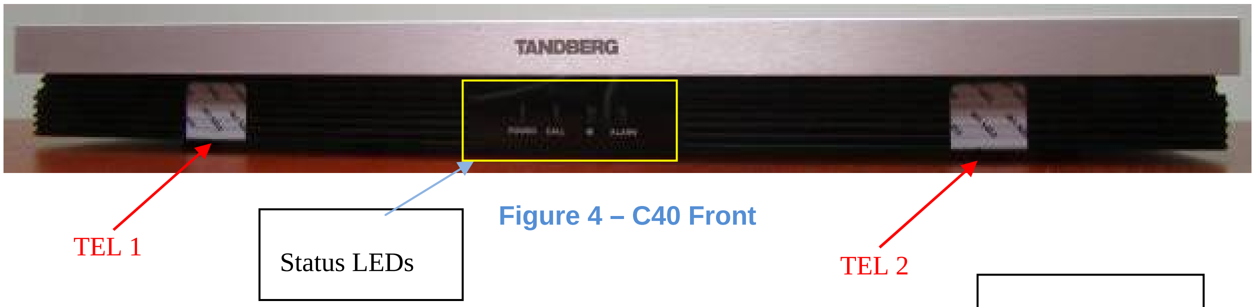

Figure 4 – C40 Front

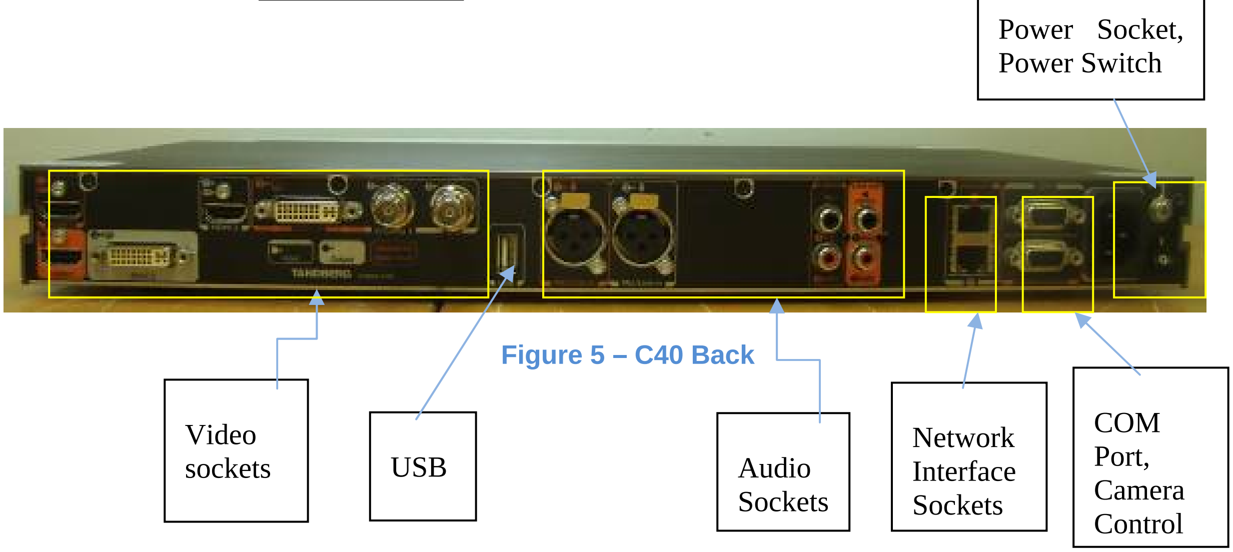

Figure 5 – C40 Back

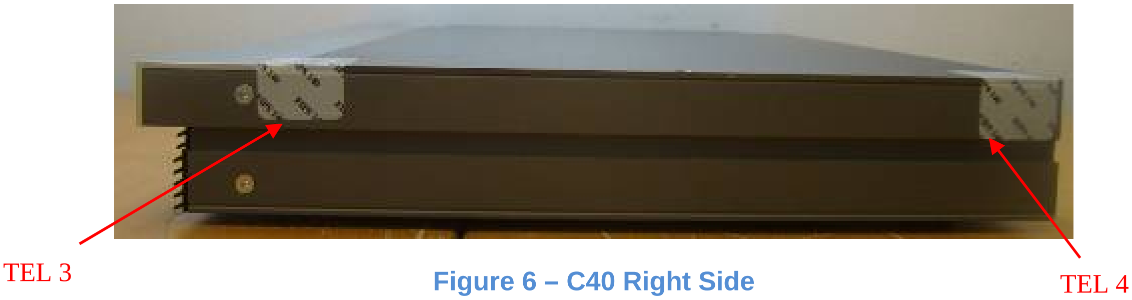

Figure 6 – C40 Right Side

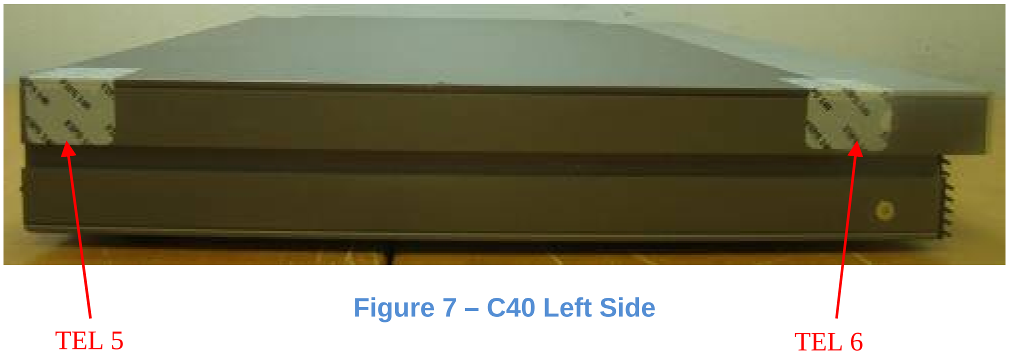

Figure 7 – C40 Left Side

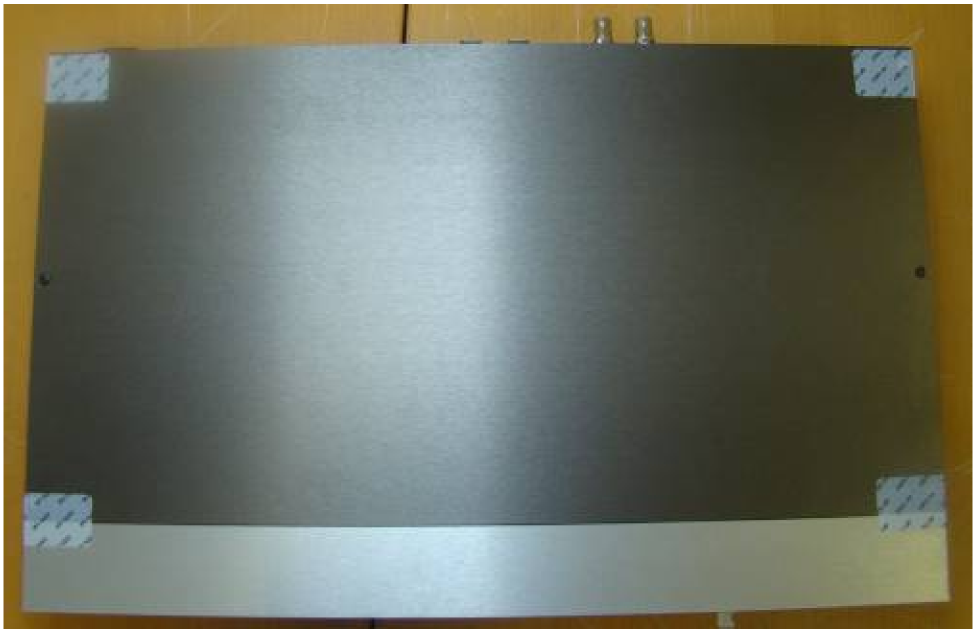

Figure 8 - C40 Top

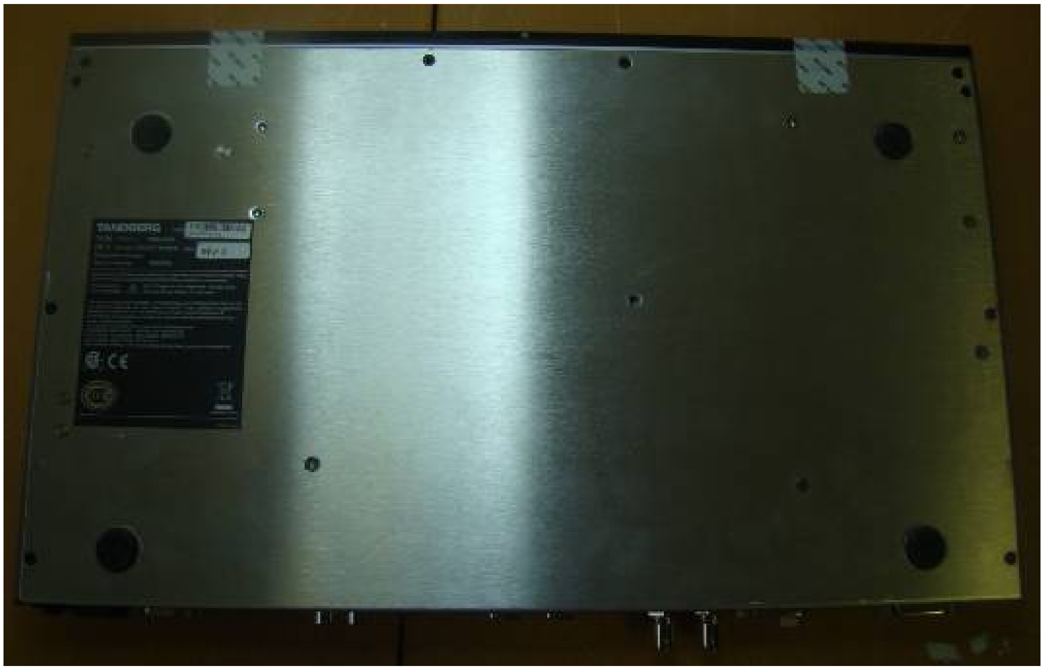

Figure 9 - C40 Bottom

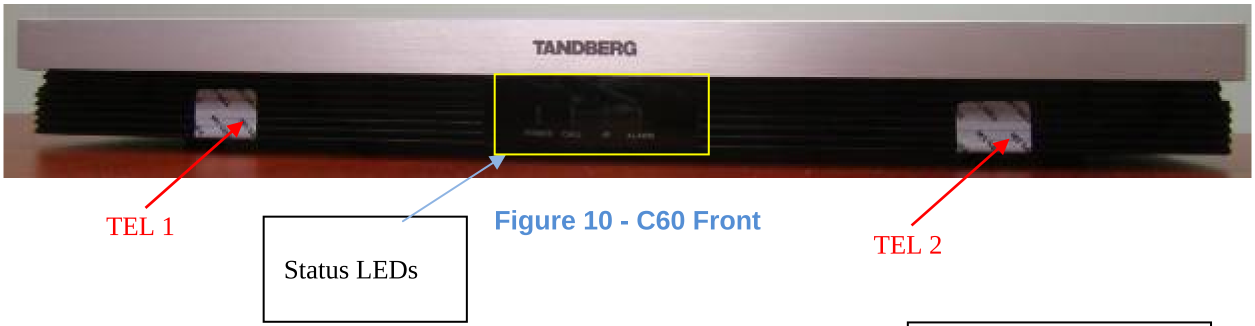

Figure 10 - C60 Front

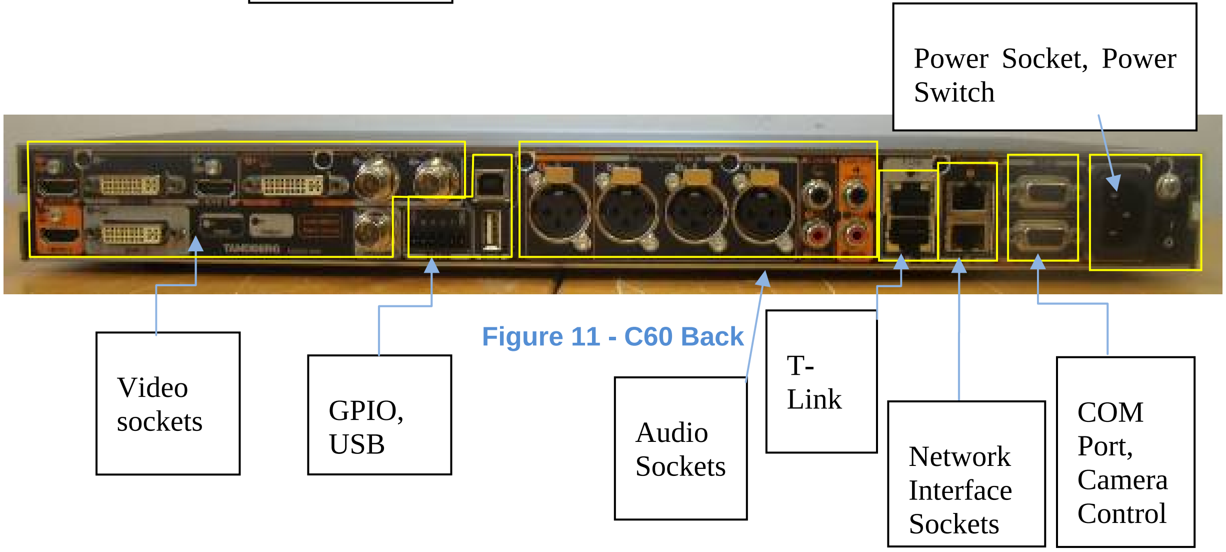

Figure 11 - C60 Back

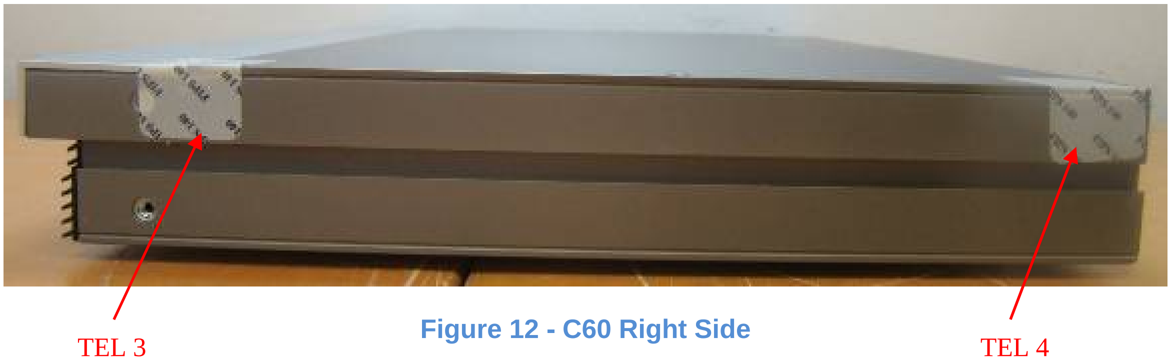

Figure 12 - C60 Right Side

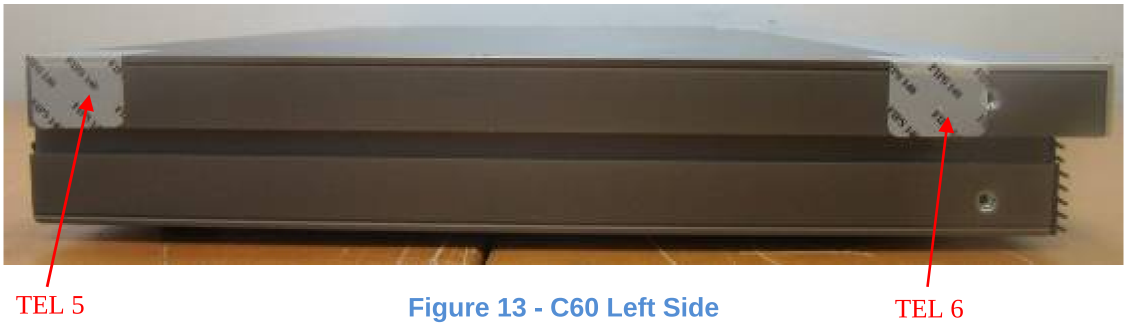

Figure 13 - C60 Left Side

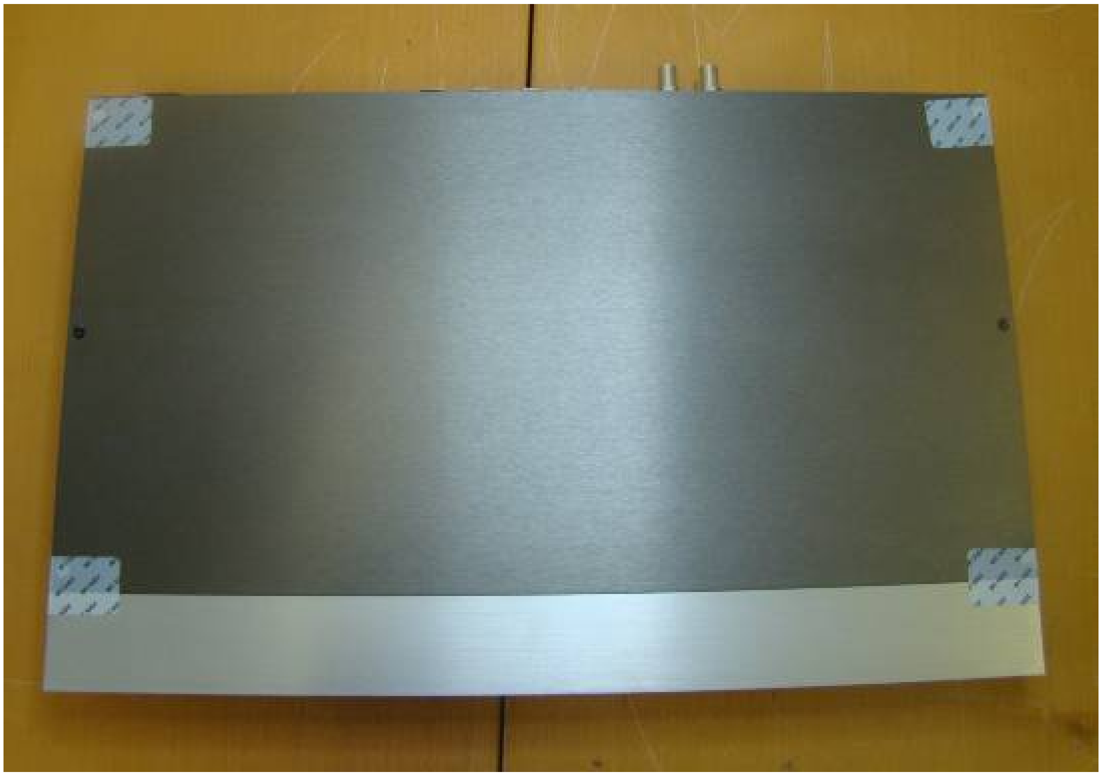

Figure 14 - C600 Top

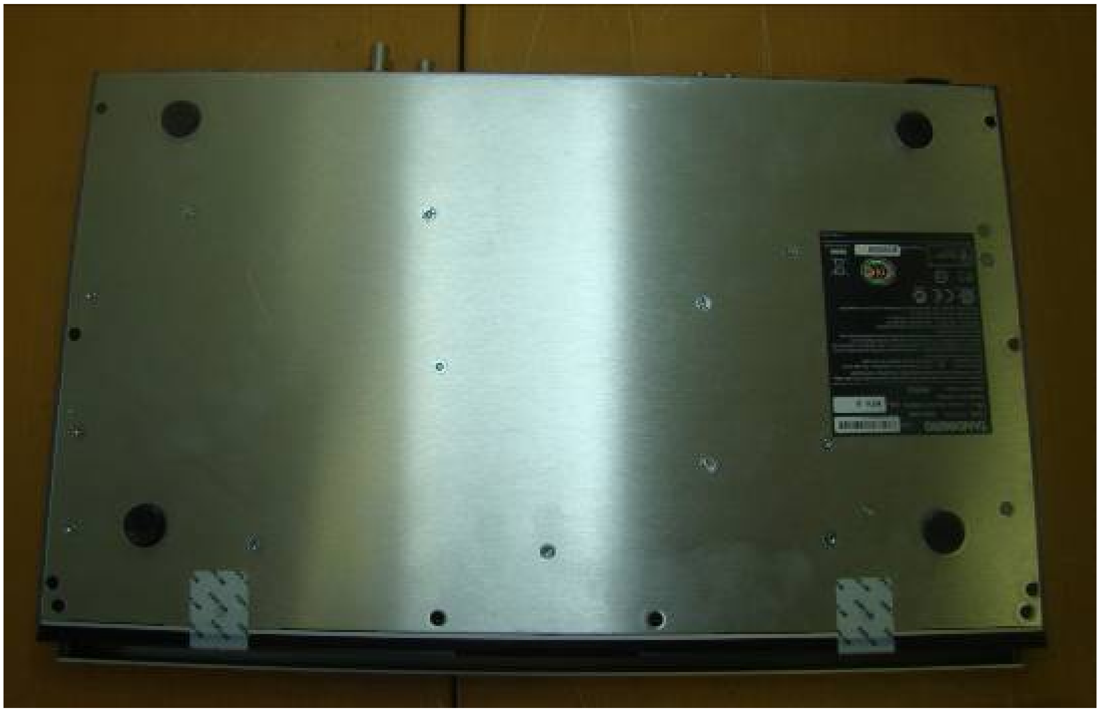

Figure 15 - C60 Bottom

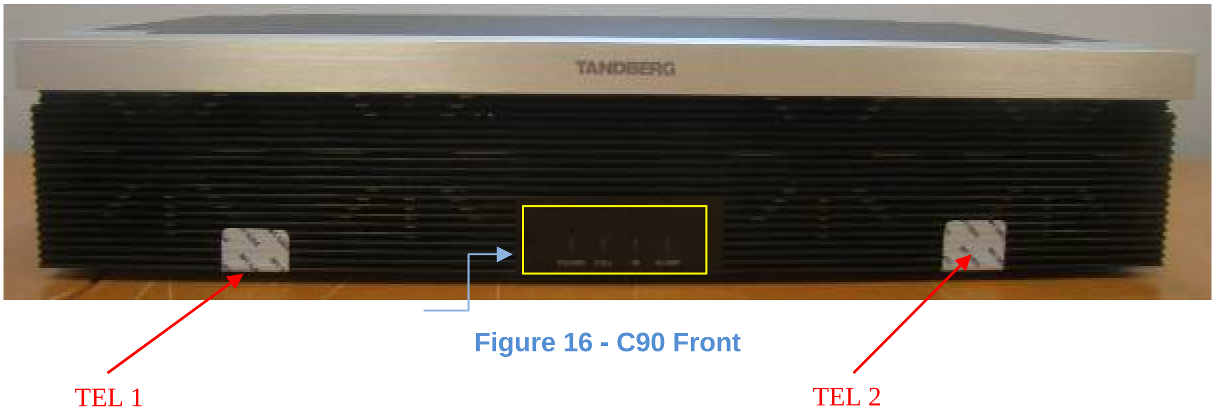

Figure 16 - C90 Front

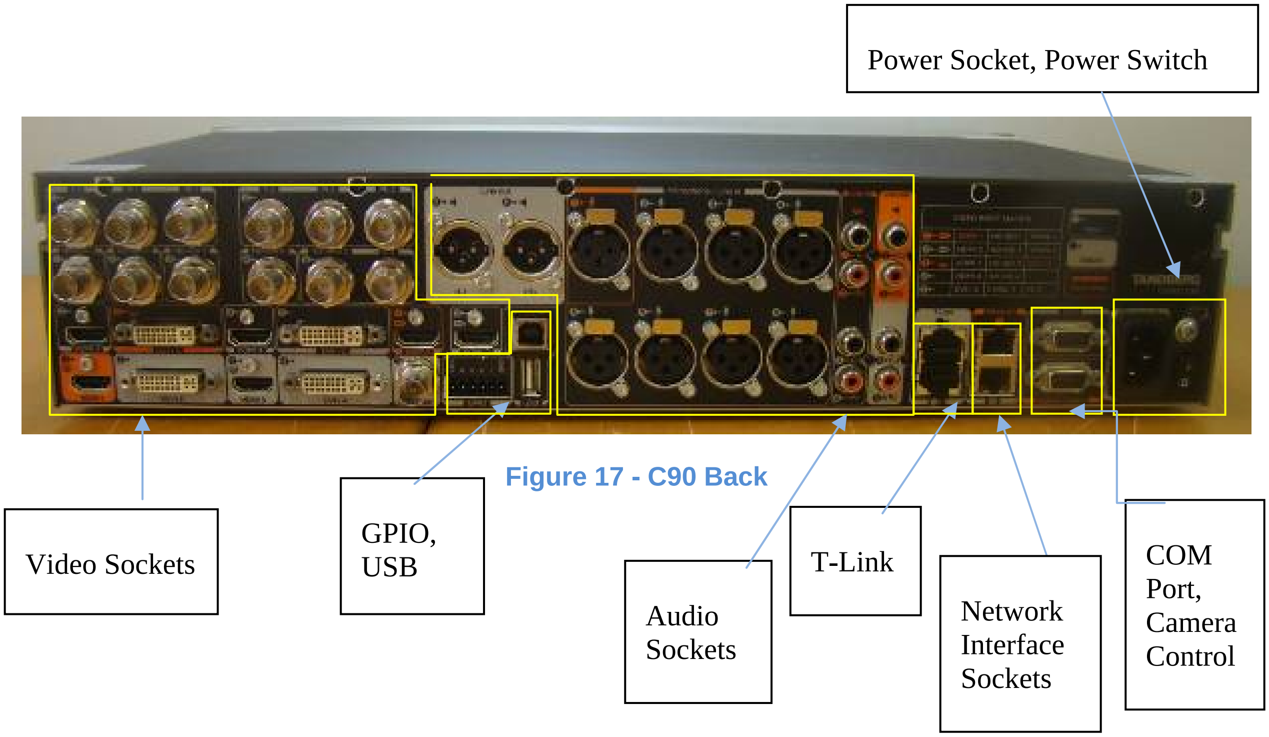

Figure 17 - C90 Back

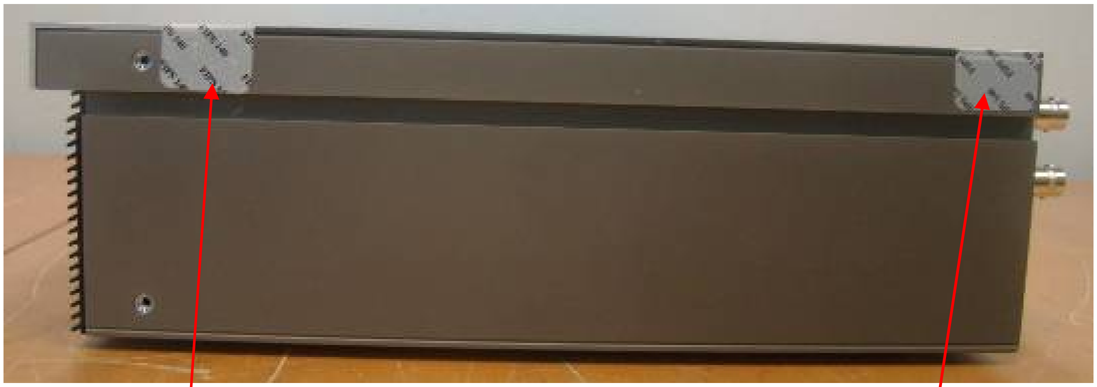

Figure 18 - C90 Right Side

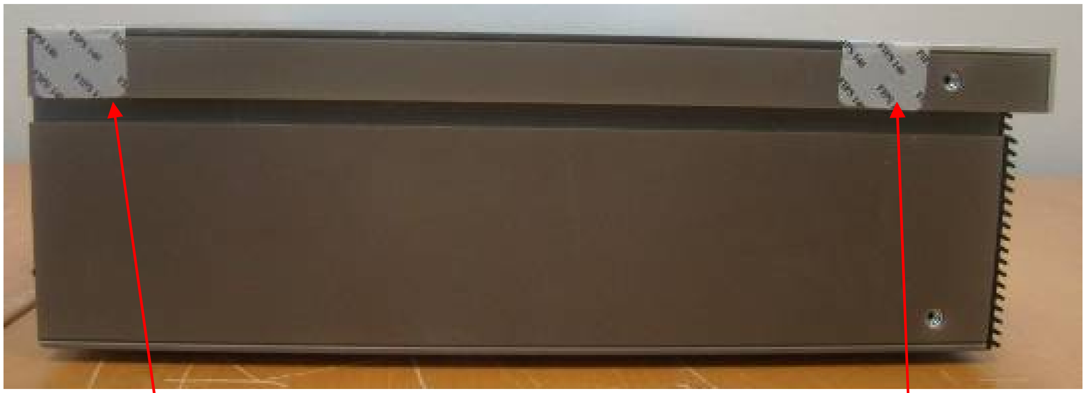

Figure 19 - C90 Left Side

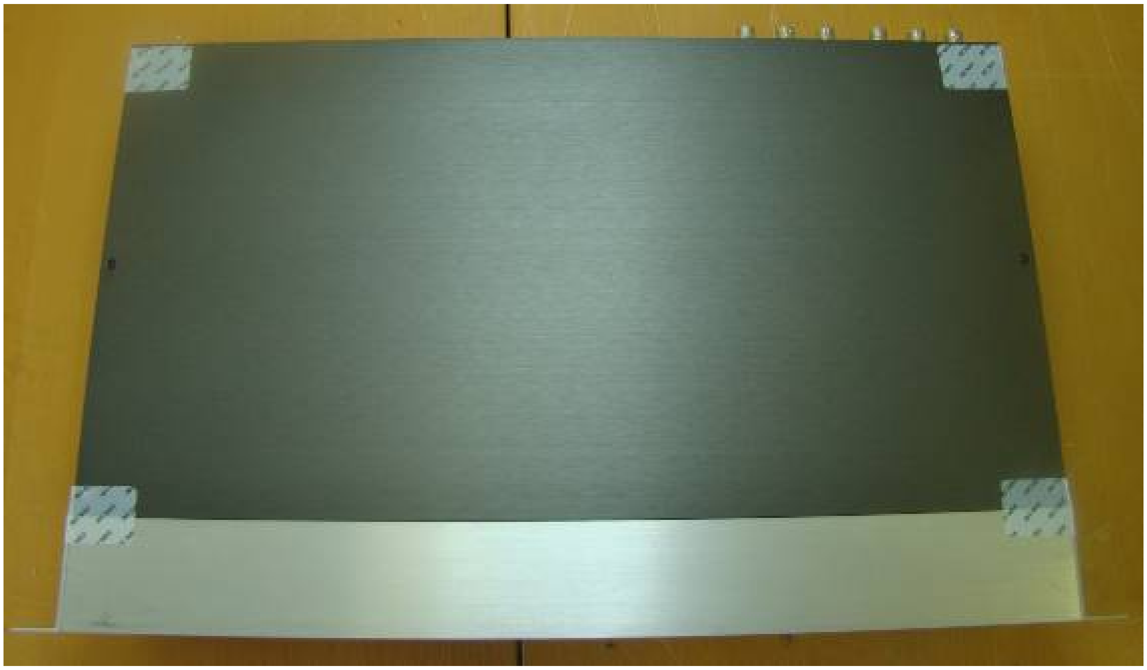

Figure 20 - C90 Top

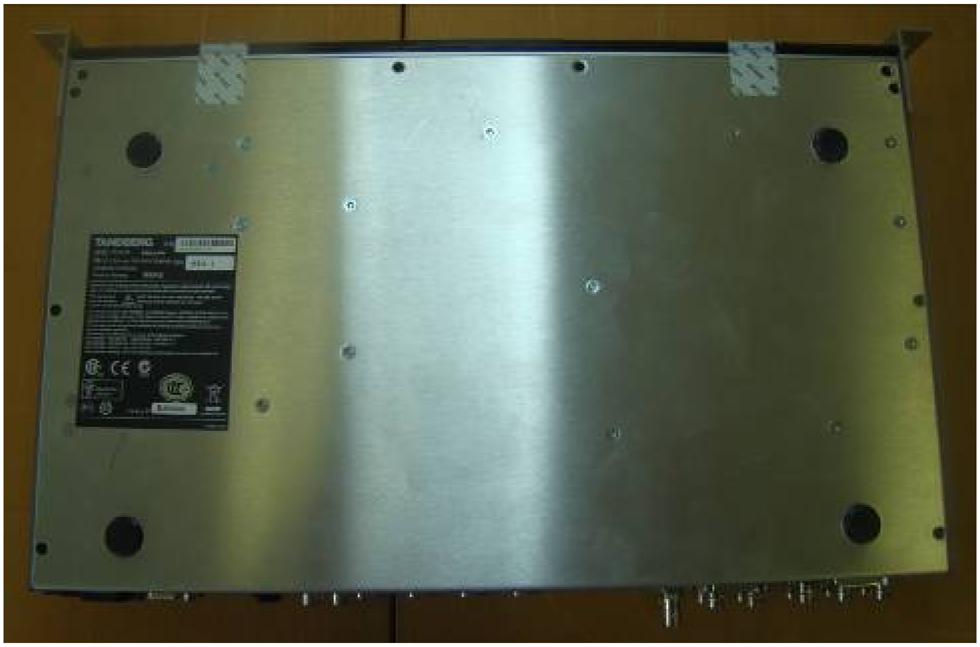

Figure 21 - C90 Bottom

3.5 Acronyms

Table 6 - 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
CSP	Critical Security Parameter
CVS	Concurrent Versions System
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
GPIO	General Purpose Input/Output
HD	High-Definition
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Transport Layer Security
IP	Internet Protocol
KAT	Known Answer Test
LAN	Local Area Network
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
PKCS	Public Key Cryptography Standards
PRI	Primary Rate Interface

Acronym	Definition
RCA	Radio Corporation of America
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
RTOS	Real-Time Operating System
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TDES	Triple Data Encryption Standard
TEL	Tamper-Evident Label
TLS	Transport Layer Security
USB	Universal Serial Bus
XOR	Exclusive-or