VTC001

COS

Video

Teleconferencing

Profile

Sept. 9, 1994

Foreword

The Corporation for Open Systems International (COS) Video Teleconferencing Profile (hereafter referred to as the Profile) was created through the cooperative efforts of the members of the Video Teleconferencing Executive Interest Group (VTC EIG) of COS. The purpose of a video teleconferencing profile is to provide a standards-based reference document for users as an aid in defining their procurement specifications for video teleconferencing equipment, and for vendors as a guide to understand what features and functionality users may request. It is not possible, nor is it practical, to make assumptions regarding the environments (networking technologies and services provided) in which video teleconferences will occur (i.e., who will participate, where they are located, timing of the conferences, equipment used, etc.). Therefore, this Profile was developed to allow video teleconferences to take place regardless of which system is in use at either location.

This Profile is based on the international standards from the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) for video teleconferencing, specifically the H.320 series of Recommendations. There are also video teleconferencing standards from the American National Standards Institute (ANSI) that will be referenced by the Profile upon their ratification.

The Profile also defines Protocol Implementation Conformance Statements (PICS) that may be found in Annex A. The vendors will generally be required to complete these PICS prior to conformance or interoperability testing of their products. On the basis of the completed PICS, the products will be tested to determine whether the features are implemented. Users should feel free to request completed PICS as part of their procurement requirements to determine if the features and functionality they require have been implemented.

In an effort to make this Profile applicable to the widest user audience, additional Department of Defense (DOD) information and optional specifications are included in Annex B. There are certain situations of national security that government systems face that are not a concern for the average user and such concerns are addressed in Annex B. The DOD has indicated that adherence to Annex B is required for all departments and agencies of the DOD but is optional for all other user communities.

Table of Contents

* * * * * * * * * * *

We welcome comments and suggestions on this document, which may be forwarded to:

Nancy K. Pierce
Corporation for Open sysyems International
8260 Willow Oaks Corporate Drive, Suite 700
Fairfax VA 22031
Telephone: (703) 205-2750
Facsimile: (703) 846-8590
E-mail: nkp@cos.com

Comments specific to Annex B should be directed as noted in Section B.1.4

COS Video Teleconferencing Profile - VTC001

1. Scope

The COS Video Teleconferencing Profile (Profile) is applicable to end systems concerned with operating in the Video Teleconferencing environment. It specifies a combination of standards which cover national and international agreements for providing interoperable video teleconferencing services.

The Profile is applicable to video teleconferencing systems based upon the ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) H.320 Recommendation, regardless of the type of underlying network service. This Profile is restricted to point-to-point operation at this time.

As defined in the standards, a Video Teleconferencing Unit (VTU, or video CODEC) performs the following functions: coding/decoding of audio and video, and multiplexing of video, audio, data, and control signals, system control, and end-to-end signaling. It does not include I/O devices, embedded and non-embedded cryptographic devices, network interface equipment, end-to-network signaling, the network connections, or the network itself. NOTE: The scope of this Profile is broader than the scope of the VTU because the Profile includes items which are not a part of the VTU.

It is the intention of this Profile to provide enough specificity, which, if followed, should insure baseline interoperability between VTUs. As ANSI and ITU-T standards mature this document will be amended to include those changes. Interoperability tests based on this Profile have been developed and are available to vendors and users for product testing[1]. A register of interoperable systems that have successfully passed the interoperability tests will be maintained by COS for the user community. Proprietary features or algorithms are not precluded by this Profile, however, such features or algorithms are not supported by this Profile.

Certain functions and features of the ITU-T H.320 suite of Recommendations are described in Section 5 to give users a high level overview of the standards included in this Profile. Section 5 is not intended to be all-encompassing. The Protocol Information Conformance Statements (PICS) given in Annex A are the definitive list of functions and features provided by the ITU-T H.320 suite of protocols. Vendors seeking interoperability testing should complete such PICS. Users planning the acquisition of video teleconferencing systems are directed to such completed PICS to determine which features and functions are supported by commercial video teleconferencing systems.

This Profile is a living document that is based upon ratified standards and will evolve as the video standards and audiographic recommendations are completed. It will in the future point to ANSI standards and to standards or recommendations for multipoint operation.

---

[1]Contact COS for information.

1.1. Schematic

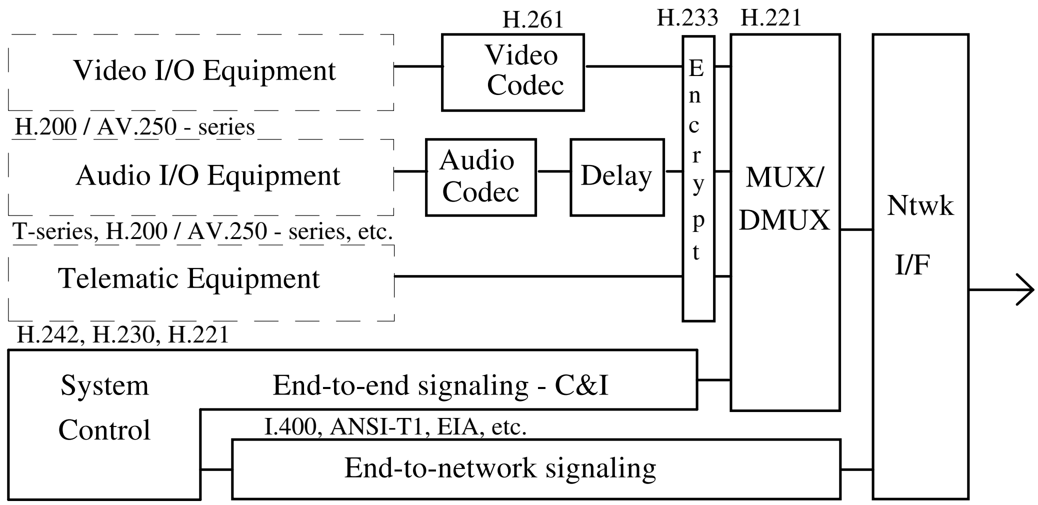


Figure 1.1. Video teleconferencing equipment schematic (dashed boxes are not included)

2. Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of this Profile. At the time of publication, the editions indicated were valid. All documents are subject to revision. Parties to agreements based on this Profile are warned against automatically applying any more recent editions of the documents listed below since the nature of references made by the Profile to such documents may be specific to a particular edition. Members of the cited standards organizations maintain registers of currently valid national and international standards and the ITU maintains published editions of its current Recommendations.

ITU-T H.221 — *Frame Structure for a 64 to 1,920 kbit/s Channel in Audiovisual teleservices, March 1993.*

ITU-T H.230 — *Frame-Synchronous Control and Indication Signals for Audiovisual Systems, March 1993.*

ITU-T H.233 — *Confidentiality System for Audiovisual Services, March 1993.*

ITU-T H.242 — *System for Establishing Communication Between Audiovisual Terminals Using Digital Channels up to 2 Mbit/s, March 1993.*

ITU-T H.261 — *Video CODEC for Audiovisual Services at px64 kbit/s, March 1993.*

ITU-T H.320	*Narrowband Visual Telephone Systems and Terminal Equipment, March 1993.*
ITU-T G.711	*Pulse Code Modulation (PCM) of Voice Frequencies, November 1988.*
ITU-T G.722	*7 kHz Audio-coding within 64 kbit/s, November 1988.*
ITU-T G.728	*Speech coding at 16 kilobits per second. Sept. 1992.*
FIPS PUB 46-1	*Data Encryption Standard.*
FIPS PUB 81	*Data Encryption Standard Modes of Operation.*
FIPS PUB 140-1	*Security Requirement for Equipment Using Data Encryption Standard.*
FIPS PUB 178	*Video Teleconferencing Services at 56 to 1920 Kb/s. December 1992*
EIA-366-A	*Interface Between Data terminal Equipment and Automatic Calling Equipment for Data Communications.*
NIUF Profile 940007	*NIUF Video Conferencing Application Profile.*
NIUF	*A Catalog of National ISDN Solutions for Selected NIUF Applications.*

[Editor's note: When all of the recent ANSI video series standards are balloted, approved, and numbered they will replace the ITU-T Recommendations.]

3. Definitions

All of the terms used in this part of the Profile are defined either in the referenced base standards (see Section 2), in the standards listed in annexes, or listed below.

Bit-rate Allocation Signal (BAS): An eight-bit word within the frame structure of ITU-T Recommendation H.221 which is used to transmit commands, control and indication signals, and capabilities.

CIF: see *Full Common Intermediate Format*

CODEC: Acronym for COder/DECoder. In video teleconferencing, an electronic device that converts analog signals, typically video, voice, and/or data, into digital form and compresses them into a fraction of their original size to save frequency bandwidth on a transmission path. It also performs the inverse operation, decompressing received signals and converting them back to analog.

Conferencing: Programs and meetings which may be for the purpose of presenting and exchanging information, comparing views, learning, planning, and decision-making. Conferences can be held in one location or conducted simultaneously at multiple locations and linked together by telecommunications systems.

Encoder: A device that encodes.

Encryption: The process of encrypting.

Frame: 1. When referring to an image, the set of all the picture elements in an image. 2. When referring to ITU-T H.221, a frame consists of 80 octets (bytes) of multiplexed signals.

Frame alignment: In the COS Profile, frame alignment refers to the ITU-T H.221 frame, not the image frame.

Frame Alignment Signal (FAS): In ITU-T H.221, this signal also contains additional bits for status, control and error detection.

Freeze-Frame Video: A frame of visual information selected from a video signal and processed through the video CODEC for transmission to remote sites. Not to be confused with still image. See *Still Image*.

Full Common Intermediate Format (FCIF): A video format defined in ITU-T H.261 that is characterized by 352 luminance pels on each of 288 lines, with half as many chrominance pels in each direction.

ITU-T: International Telecommunications Union - Telecommunications Standardization Sector, formerly the CCITT.

Minimum Picture Interval: The minimum time between pictures selected for encoding. Allowable values are 1/29.97, 2/29.97, 3/29.97, and 4/29.97 seconds per picture.

Motion Compensation: A type of interframe coding used by CODECs in the compression of motion video images. The process relies upon an algorithm that examines a sequence of image frames to measure the motion that occurs between frames.

μ-law: The PCM coding and companding standard used in Japan and North America.

***p*x64**: Family of 5 ITU-T Recommendations. These include H.261, H.221, H.242, H.230, and H.320. These standards form the basis for Video Teleconferencing (VTC) interoperability.

QCIF: Quarter Common Intermediate Format. A video format defined in ITU-T H.261 that is characterized by 176 luminance pels on each of 144 lines, with half as many chrominance pels in each direction. QCIF has 1/4 as many pels as FCIF.

Restricted Channel: A digital communications channel for which each increment of *p* gives a useful capacity of only 56000 bits per second, instead of 64000 bits per second. This is currently common in North America, and was originally due to a ones density limitation in T1 circuits.

Service Definition: A standards document which defines the scope of the standardization effort of commercial standards. Service definitions for video teleconferencing have been written by the ANSI T1A1.5 committee, and by ITU-T Study Group 1.

Still Image: Non-moving visual information such as graphs, drawings, pictures, or video frames not processed by the video CODEC portion of the VTU. This differs from freeze-frame images which are processed by the video CODEC portion of the VTU.

Teleconferencing System: A collection of equipment and integral components (customer premises equipment and facilities) required to process teleconferencing programs and control data, less network interface devices.

Terminal Equipment: A device or devices connected to a network or other communications system used to receive or transmit data. It usually includes some type of I/O device.

Unrestricted Channel: A digital communications channel, in which for each increment of *p*, all 64000 bits per second (bit/s) are available for information transfer. ISDN is an example of a network that uses 64000 bit/s communication channels.

Video: That portion of a signal that is related to moving images.

Videoconferencing: See *Video Teleconferencing*.

Video CODEC: See *CODEC*.

Video Teleconferencing (VTC): Two-way electronic form of communications that permits two or more people in different locations to engage in face-to-face audio and visual communication. Meetings, seminars, and conferences are conducted as if all of the participants are in the same room.

Video Telephony: Relating to video phones and video teleconferencing.

Wideband: In the case of wideband audio, G.722 specifies a bandwidth of 7 kHz.

Windowing: Capability to divide the video display into two or more separate regions with displays from different sources in each region. For example, four separate windows on the same display could simultaneously show a) data, b) motion video of the remote site, c) a still image, and d) motion video of the home site.

4. Abbreviations and acronyms

All of the abbreviations and acronyms used in this part of the Profile are defined either in the referenced base standards (see Section 2), in the standards listed in the annexes, or listed below. Those that are common with the terms in FED-STD-1037B have been included for the convenience of the reader.

ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
BAS	bit rate allocation signal
bit/s	bits per second
BNC	bayonet Neill-Concelman
BRI	Basic Rate Interface
CD-ROM	compact disk - read only memory
CIF	common intermediate format
CODEC	coder-decoder
COS	Corporation for Open Systems, International
CSU	Channel Service Unit
dBm	decibel(s) referenced to 1 milliwatt
DCE	Data Circuit-Terminating Equipment
DES	data encryption standard
DSU	Data Service Unit
DTE	Data Terminal Equipment
ECS	Encryption Control Signal
EPROM	erasable programmable read only memory

FAS	Frame Alignment Signal
FCIF	full common intermediate format
FEC	forward error correction
fps	frames per second
Hz	hertz
HSD	High speed data
ISDN	Integrated Services Digital Network
I/O	input/output
IMUX	inverse multiplexer
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Sector (formerly CCITT)
kbit/s	kilobits per second
kHz	kilohertz
LSD	Low speed data
Mbit/s	megabits per second
MLP	Multilayer Protocol
MPI	Minimum Picture Interval
ms	milliseconds
NTSC	National Television Standards Committee
PCM	pulse code modulation
QCIF	quarter common intermediate format
SB-ADPCM	sub-band adaptive differential pulse-code modulation
VTC	video teleconferencing
VTU	video teleconferencing unit

5. Subnetwork-type independent requirements

These requirements shall apply to all ITU-T H.320 based video teleconferencing (VTC) systems. For a list of the features or functions required from each recommendation or standard, as well as optional features, see Annex A. Note that certain options, e.g., *p*xn, are negotiable at connection time assuming the capability is implemented, while other options are non-negotiable, e.g., use of multipoint.

5.1. Video, communications and control

5.1.1. General

Except as noted, the VTU shall conform with the requirements set forth in the five ITU-T px64 Recommendations, H.221, H.230, H.242, H.261, and H.320. Note that FIPS PUB 178 specifies details of use of the above Recommendations, however, it references the 1990 versions which have been superseded by the 1993 versions.

5.1.2. Operating mode

The VTU shall provide point-to-point bi-directional operation. Operation in multi-point topologies will be considered in future versions of this Profile.

5.1.3. Data transmission rates

The Recommendations relate to VTUs that operate at nominal bit rates of *p*x64000 bits per second (bit/s), where *p* is an integer that can range from 1 to 30. For unrestricted channels, such as provided by ISDN, each increment of data rate may actually be 64000 bit/s, but in restricted channels, each increment may be only 56000 bit/s. VTUs shall be able to operate with other VTUs on unrestricted and restricted channels. VTUs shall provide operation at least for *p*=1 and *p*=2. Proprietary algorithms for video coding are allowed by FIPS PUB 178. If a certain value of *p* is required by the procurement, the VTU must operate at that value according to ITU-T H.261 (see also FIPS PUB 178), and not just the proprietary video algorithm.

5.1.4. Video coding and decoding

The video CODEC subsystem used to provide VTC services within the scope of this Profile shall conform to the specifications set forth in ITU-T H.261.

5.1.5. Picture format (resolution)

The video CODEC shall provide full-color operation using at least the QCIF format in accordance with ITU-T H.261. If the procurement requires at least FCIF resolution or equivalent for motion video, then the standard algorithm of ITU-T H.261 shall be available at FCIF resolution.

5.1.6. Motion rendition

The decoder shall decode at least 7.5 pictures per second. This is equivalent to a Minimum Picture Interval (MPI) of 4/29.97 seconds per picture as described in ITU-T H.221, Annex 1, and ITU-T H.261, section 3.1.

5.1.7. Forward error correction (FEC)

The use of the FEC code in the decoder, as specified in ITU-T H.261 section 5.4, to correct transmission errors is optional.

5.1.8. Motion compensation

The requirement for Motion Compensation in the encoder is optional.

5.1.9. Freeze-frame video

All VTUs may optionally support a freeze-frame video transmission capability. Freeze-frame video is a frame selected from a video signal, and processed through the video CODEC for transmission to remote sites. Freeze-frame video is not the same as still image graphics. Motion video transmission is suspended until freeze-frame transmission is complete.

The VTU may optionally have the capability to output video signals representing both motion video and freeze-frame video simultaneously, or provide a single video output which can be switched by the user between motion video and freeze-frame video. If the capability of coding of freeze-frame images is provided it shall be performed by means of the technique described in ITU-T H.261 Annex D. This technique provides an image up to twice the resolution in each direction of the format currently being used for motion video, i.e. 352 x 288 pels for VTUs using QCIF motion video, and 704 x 576 pels for VTUs using FCIF motion video. VTUs capable of QCIF motion video shall optionally provide QCIF freeze-frame video (176 x 144 pels) capability. Four times QCIF (FCIF) freeze-frame video (352 x 288) shall be optional. VTUs capable of FCIF motion video shall optionally provide FCIF freeze-frame video (352 x 288) capability. Four times FCIF freeze-frame video (704 x 576) shall be another option. Freeze-frame video having two times horizontal and/or two times vertical resolutions are also allowable, but are not specifically listed as options under this Profile.

5.1.10. Emerging ITU-T T.120 audiographics Recommendations

At this time, the ITU-T Study Group VIII is completing a new suite of international Recommendations for audiographics conferencing known collectively as ITU-T T.120. They will include optional applications such as still image transfer, annotation, pointing and binary file transfer. These Recommendations are designed to operate over low and high speed MLP channels, which are part of the ITU-T H.320 Recommendation, so it is anticipated that T.120 applications will appear as capabilities in the next generation VTUs.

5.1.10.1. Still image and binary file transfer

Users of VTUs that have immediate requirements for sending data or image files should use existing data communication methods, whether in-band or out-of-band. As ITU-T T.120 applications which perform these and other functions are ratified, it is expected that this document will be modified to include them. For example, it is anticipated that T.127 will be used for binary data file transfer and T.126 for still image transfer.

5.1.11. Concurrent operation

As described in ITU-T Recommendation H.221 (FIPS PUB 178), concurrent operation can be provided by dynamically subdividing an overall transmission channel of 56 to 1920 kbit/s into lower rates suitable for audio and video.

5.1.11.1. Concurrent operation at *p*=1

Concurrent operation at *p*=1 is outside the scope of this Profile.

5.1.11.2. Concurrent operation at *p*=2

The VTC terminal equipment, including the video (motion or freeze-frame) and audio as stated in this Profile shall be capable of functioning concurrently at *p*=2.

With an unrestricted network (128 kbit/s), the VTU shall be capable of operating at (sending to the network and receiving from the network) the following minimum concurrent data rates for the given components. Actual operation at other data rates is allowed:

Video:	68.8 kbit/s
Audio:	56 kbit/s
Control signals:	3.2 kbit/s
Freeze-frame video:	Motion video can be frozen while freeze-frame video is being transmitted on the video channel.

With a restricted network (112 kbit/s), the VTU shall be capable of operating at (sending to the network and receiving from the network) the following minimum concurrent data rates for the given components. Actual operation at other data rates is allowed:

Video:	60.8 kbit/s
Audio:	48 kbit/s
Control signals:	3.2 kbit/s
Freeze-frame video:	Motion video can be frozen while freeze-frame video is being transmitted on the video channel.

If the optional Encryption Control Signal (ECS) is used, the video rate will be reduced by 0.8 kbit/s.

5.1.11.3. Concurrent operation at $p>2$

If the VTU is capable of operating at $p>2$, then the following features shall also be capable of operating concurrently at all the data rates of video operation above $p=2$:

Video (motion or freeze-frame)
Audio

5.2. Control and indication signals

The VTUs shall provide additional information which is needed for the proper functioning of the system. This additional information will contain ITU-T H.221 frame-synchronous control signals and indication signals such as freeze picture, video loopback, simple multipoint controls, etc., as specified in ITU-T H.230.

5.2.1. Call control (handshaking)

The VTUs shall interoperate with each other and the existing telecommunications system as specified in ITU-T H.242 and H.320.

5.2.2. Frame structure

The VTUs shall comply with the ITU-T H.221 frame structure for audiovisual teleservices in single or multiple channels as specified in ITU-T H.221. This requirement allows for the synchronization of multiple connections and the control of multiplexing audio, video, data, and other signals. Use of the unframed mode as per ITU-T H.221 is outside the scope of this Profile.

5.2.3. Camera interface

All systems shall support the capture of motion video and freeze frame video images using television cameras. For VTC equipment intended for use in North America that has external cameras, the electrical interfaces between the cameras and the VTU shall optionally meet the NTSC (EIA-170) standard. The mechanical interface shall optionally be BNC, F-type, or RCA connectors.

The interfaces between the VTU and the video display devices are outside the scope of this Profile.

5.2.4. Monitor interface

For VTC equipment intended for use in North America that has external video display monitors, the electrical interface between the monitors and the VTU shall optionally meet the EIA-170A (NTSC) or RGB standard. The mechanical interface shall optionally be BNC, F-type, or RCA connectors.

5.3. Audio

5.3.1. General

The audio coder/decoder (codec) subsystem shall be an integrated subsystem of the VTU equipment used for the purpose of video teleconferencing. This means the audio signal shall be transmitted in-band as per ITU-T H.221, and not out-of-band.

5.3.2. Speech quality modes

The audio subsystem shall be capable of operating in the speech modes as specified in section 5.3.2.1, and may optionally support the speech modes in sections 5.3.2.2 and 5.3.2.3.

5.3.2.1. Narrowband speech mode

Capability to operate in this mode is mandatory. This narrowband (3 kHz analog bandwidth) speech mode shall conform to the specifications set forth in ITU-T G.711, H.221, H.230, H.242, and H.320 (See also FIPS PUB 178).

This audio mode is known as Mode 0 in ITU-T H.221. Mode 0 is further broken out into four submodes, as specified in Annex 1 of ITU-T H.221: Mode 0U(A-law), Mode 0F(A-law), Mode 0U(μ-law), and Mode 0F(μ-law).

The audio subsystem shall be capable of operating in Mode 0F(μ-law). Mode 0F(A-law) is optional. The use of the unframed modes (0U) is outside the scope of the Profile and is not recommended.

5.3.2.2. Wideband speech at 48-56 Kbit/s

Wideband speech is optional and if provided shall conform to the specifications set forth in ITU-T G.722, H.221, H.230, H.242 (See also FIPS PUB 178).

The audio subsystem shall be capable of operating in the following two modes as specified in ITU-T G.722 and H.221:

Mode 2: 56 Kbit/s audio (unrestricted network)
Mode 3: 48 Kbit/s audio. (restricted or unrestricted network)

The indication signals for identifying the mode of operation shall conform to the specifications set forth in ITU-T G.722, H.242, and H.221 (Table H.221/A1).

The audio subsystem shall have the capability of automatically switching over from Mode 0 (see 5.3.2.1) to one of the higher quality Modes 2 or 3 if the other VTU to which it is connected has the capability for Modes 2 or 3.

5.3.2.3. Narrowband speech at 16 Kbit/s

ITU-T G.728 is optional but if provided shall be available at all the data rates at which the VTU is capable of operating.

5.3.2.4. Electrical and mechanical interfaces

The requirements in 5.3.2.5. and 5.3.2.6. are optional if the audio system is completely integrated into the VTU (i.e., videophone, PC-based desktop system, integrated rollabout system).

5.3.2.5. Electrical specification

Input and output line level room audio interfaces shall be provided that meet the following specifications. They shall have a 600 ohm balanced impedance, with a nominal signal level of -3 dBm ±1 dB. The digital overload point shall be +7 dBm ±1 dB. The audio gain from input to output, measured using digital loop-back, shall be 0 dB ±0.5 dB. All level measurements are made using pink noise. See Section B.7.1.7 in Annex B for further information on the audio subsystem.

5.3.2.6. Mechanical specification.

The VTU shall provide mechanical connections for the room audio system. The room audio system connection shall provide either

a.) one XLR male/female pair, or
b.) one pair RCA Phono jacks, one for input and one for output.

For the XLR pair, the female connector shall be the input to the VTU from the room audio system. The male connector shall be the output of the VTU to the room audio system.

5.3.3. Encoding and decoding

For Mode 0 narrowband speech, using the mandatory Mode 0F (μ-law), the characteristics of the Pulse Code Modulation (PCM) converter shall conform to the specifications set forth in G.711. The optional mode 0F (A-law) shall conform to G.711.

For wideband speech (G.722), the analog speech signal shall be encoded into and decoded from a digital bit stream using sub-band adaptive differential pulse code modulation (SB-ADPCM) for Modes 2 and 3. The characteristics of the SB-ADPCM converter shall conform to the specifications set forth in ITU-T G.722.

5.3.4. Lip synchronization

In order to conform to this Profile, synchronization between the video and audio signals shall be addressed in both the encoding and decoding processes of the audio subsystem. While delay compensation is not required, if it is used, the compensation for delay between the video signal and audio signal introduced during the encoding process shall be compensated for at the encoding process. Likewise, compensation for delay introduced at the decoding process shall be compensated for during the decoding process. The time delay between audio and video signal shall be measured as specified in Annex C of H.261.

5.4. Confidentiality and secure operation

As an option VTUs may provide confidentiality or secure operation. When provided this feature shall follow the specifications of ITU-T H.233 and this section, or it may use external cryptographic devices. For Type 1 (Classified) encryption using external devices, e.g., KG-194, the requirements of Section B.5.4 in Annex B shall apply.

5.4.1. Technical requirements.

If the confidentiality option is chosen the VTU shall conform with the specifications set forth in ITU-T H.233. ITU-T H.233 offers a choice of encryption methods, including the Data Encryption Standard (DES). The VTU shall be capable of encrypting video, audio, still images and data using DES.

[Editor's note: The 1993 version H.233 has been revised and is considered stable text although not yet approved. It should be considered in this area, especially for the use of the DES algorithm and the 64-bit Output Feedback Mode.]

5.4.2. Data encryption standard

If the confidentiality option is chosen, DOD users shall have the capability to operate using DES. The need for DES encryption in industry applications is up to the user. Operation using the DES algorithm is defined in FIPS PUB 46-1, *Data Encryption Standard*. The ITU-T H.233 algorithm identifier for DES, Mode 1 shall be used. The algorithm identifier is:

0 0 0 0 0 0 1 0
msb lsb

A VTU may also be capable of operation in any of the non-DES modes specified in ITU-T H.233. One possible implementation is shown in Figure 5.1.

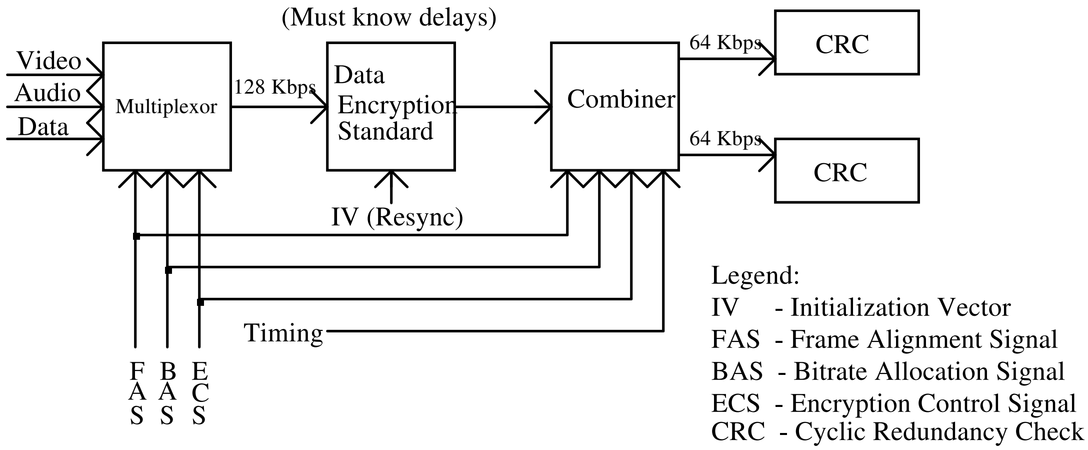


Figure 5.1. Block diagram of a sample Type 3 encryption implementation

5.4.3. Output feedback mode

If the confidentiality option is chosen, DOD users shall have the capability to operate using the DES algorithm and shall use the 64 bit Output Feedback Mode (OFB-64) as defined in FIPS PUB 81, *Data Encryption Standard Modes of Operation*. The ITU-T H.233 parameter identifier for OFB-64 shall be used. The parameter identifier is:

0 0 0 0 0 0 0 1
msb lsb

The initialization vector shall be 64 bits long.

5.4.4. Validation

All DES implementations must be validated by NIST. Software implementations (other than firmware) are not in compliance with this Profile. The following firmware implementations are acceptable: Read-Only Memory (ROM), microcode, Erasable Programmable Read-Only Memory (EPROM), Compact Disk Read-Only Memory (CD-ROM), and Chip implementations.

5.4.5. Levels of security protection

All VTUs using DES shall follow the security requirements for cryptographic modules as defined in FIPS PUB 140-1, *Security Requirements for Equipment Using Data Encryption Standard*. FIPS PUB 140-1 describes 4 levels of protection for various aspects including the basic design, module interfaces, authorized roles and services, and physical security. The selection of the appropriate level of protection is beyond the scope of this Profile and is left to the discretion of the user. FIPS PUB 140-1 compliance shall be validated by NIST (assuming NIST has an active validation program at the time of procurement).

5.4.6. Visual indication

VTUs using this clause shall optionally provide an external electrical or visual security status signal which can be used by a display device to give a real time visual indication of whether information (audio, video, still image, and all data) transmitted across the network is Type 3 protected, or in the clear.

6. Subnetwork-type dependent requirements.

6.1. General

The network interface requirements are predicated upon the end user and the type of network to be used.

6.2. VTU network interface

The VTU to network interface is entirely dependent upon the type of underlying sub-network used. Examples of point-to-point VTU interconnection include leased digital circuits, switched digital circuits, or Integrated Services Digital Network (ISDN).

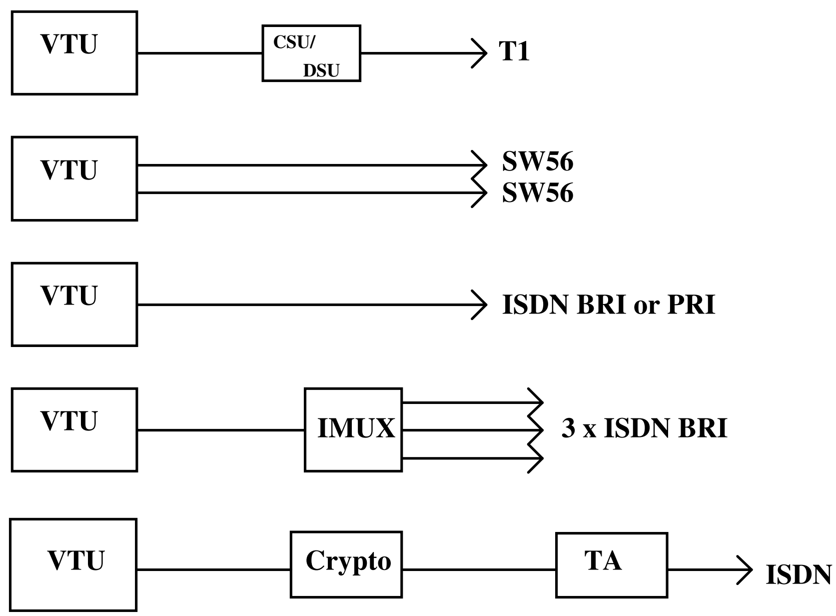


Figure 6.1 Examples of some network connections

6.3. Integrated Services Digital Network

ISDN is seen as a potentially popular network service for video teleconferencing, however, given the range of services and network interface possibilities, this Profile does not specify any single approach.

6.3.1. ISDN Basic rate interface (BRI)

ISDN interfaces are optional. Two optional BRI ISDN interface configurations are provided for information. See 6.3.1.1 and 6.3.1.2. Included in the scope of this Profile are ISDN BRI interfaces between the VTU and the terminal adapter (TA).

All of the configurations in 6.3.1 are in accordance with the North American ISDN Users Forum (NIUF) profile, *NIUF Video Conferencing Application Profile 940007*, and the

NIUF catalog, *A Catalog of National ISDN Solutions for Selected NIUF Applications*. Any of these configurations may be chosen, depending on the needs of the user. The use of D-channel signaling is permitted for unclassified and unclassified sensitive operation. The use of D-channel signaling originating from the VTU is not permitted with classified operation. See Section B.6.1 of Annex B for ISDN BRI configurations.

6.3.1.1. Option 1, external terminal adapter

Option 1 is for unclassified and Type 3 unclassified sensitive operation. The VTU shall have one or two ports. These shall be used to connect to an external ISDN Terminal Adapter (TA). See Figure 6.2. The TA is outside the scope of this Profile. Note that if the VTU user specifies the one port version, and two B channels are used, the necessary inverse multiplexing (IMUX) function to go from a single port to two B channels must be performed by the TA. In the dual port version, the IMUX function is performed within the VTU. See Section B.7.5.2 of Annex B for other possible configurations.

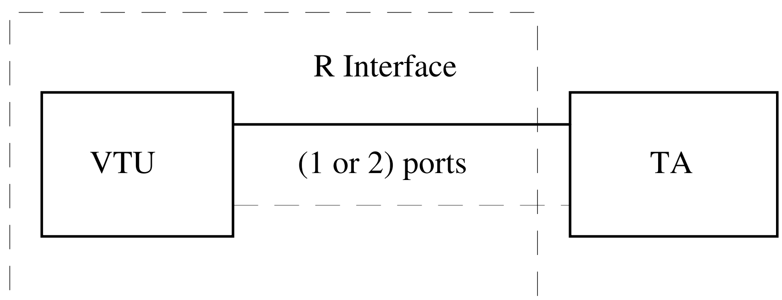


Figure 6.2. Option 1, external TA (Interior of dashed box indicates scope of the Profile)

6.3.1.2. Option 2, external terminal adapter with dialing interface

Option 2 is for unclassified and Type 3 unclassified sensitive operation. In addition to requirements of option 1, the VTU shall have two dialing interfaces (EIA-366-A), one for each B channel, for convenient dialing through the VTU.

Existing VTUs, or VTUs that require the use of specific non-ISDN interface connectors, will require the use of Terminal Adapters.

Other VTUs may be designed to attach at the user side of the Network Termination (S/T reference point on NT1).

Still other VTUs may incorporate the NT1 function. Such design decisions are as much a financial as an engineering choice and are beyond the scope of this Profile.

6.4. VTU network interface

As an option, a two-channel network interface to the VTU is recommended. This is needed for interoperability at p=2 unless an inverse multiplexer is used to interface to the network.

Annex A (normative)

COS Video Teleconferencing Profile Implementation Conformance Statements

A.1. Introduction

Since the Protocol Implementation Conformance Statements (PICS) for the H-series have not yet been developed, proposed drafts of these PICS are included as this Annex. This Annex is to be used in conjunction with Section 5. If there is any disagreement between this Annex and Section 5, Section 5 takes precedence.

The PICS specify requirements for implementations of this Profile. They are used to determine areas where interoperability testing may be carried out and as a screening device to determine if a vendor meets all mandatory requirements. The PICS may also be used by purchasers of video teleconferencing systems to determine which features have been implemented.

The columns of the PICS are as follows: *Index* is used in international standards and is only included for conformance. *Protocol Feature* refers to the features of the protocol in question. *Std. Clause* indicates the clause of the standard where the feature is described. *Std. Status* indicates whether the feature is mandatory, optional, etc. *Predicate* is another international standard convention included for completeness. *Implemented* has two ballot boxes where the vendor may indicate support or non-support.

A.1.1. Symbols and conventions

M	=	Mandatory.
O	=	Optional.
O.<n>	=	Optional, but support of at least one of the group of options labeled by the same numeral <n> is required.
C	=	Conditional.
X	=	Prohibited use.
Yes	=	Supported.
No	=	Not supported.
cp<n>	=	Completion predicate - this item is not to be completed (i.e., Status is N/A) if the condition in the predicate list at the end of each table is true.
sp<n>	=	Status predicate - the status of this item is conditional based on the expression in the predicate list at the end of each table.

A.2. Identification

A.2.1. Vendor information

Vendor Company:

Contact Name:

Street:

City/State:

Voice telephone:

FAX telephone:

e-mail address:

A.2.2. Device identification

Product name:

Product number:

Revision number:

Other:

A.3. H.261 PICS

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	Source format - CIF	3.1	O		Y[ ] N[ ]
	Source format - QCIF	3.1	M		Y[ ] N[ ]
	Prediction	3.2.1	O		Y[ ] N[ ]
	Motion compensation - encoder	3.2.2	O		Y[ ] N[ ]
	Motion compensation - decoder	3.2.2	M		Y[ ] N[ ]
	Loop filter	3.2.3	O		Y[ ] N[ ]
	Transformer	3.2.4	M		Y[ ] N[ ]
	Quantization	3.2.5	M		Y[ ] N[ ]
	Clipping	3.2.6	M		Y[ ] N[ ]
	Forced updating	3.4	M		Y[ ] N[ ]
	Data structure	4.1	M		Y[ ] N[ ]
	Video multiplex arrangement	4.2	M		Y[ ] N[ ]
	Multipoint considerations	4.3	O		Y[ ] N[ ]
	Transmission coder	5	M		Y[ ] N[ ]
	Inverse transform accuracy spec.	Annex A	M		Y[ ] N[ ]
	Hypothetical Reference Decoder	Annex B	M		Y[ ] N[ ]
	Codec delay measurement method	Annex C	-		-
	Still Image Transmission	Annex D	O		Y[ ] N[ ]

A.4. H.221 PICS

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	Frame Alignment Signal	1.1	M		Y[ ] N[ ]
	Bit-rate Allocation Signal	1.2	M		Y[ ] N[ ]
	Encryption Control Signal	1.3	O		Y[ ] N[ ]
	Remaining capacity	1.4	M		Y[ ] N[ ]
	Frame Alignment - General	2.1	M		Y[ ] N[ ]
	Multiframe structure	2.2	M		Y[ ] N[ ]
	Loss & recovery of frame alignment.	2.3	M		Y[ ] N[ ]
	Loss & recovery of multiframe align	2.4	M		Y[ ] N[ ]
	Timing recovery	2.5	M		Y[ ] N[ ]
	Description of the CRC-4 procedure	2.6	O		Y[ ] N[ ]
	Computation of the CRC-4 bits	2.6.1	O		Y[ ] N[ ]
	Frame alignment monitoring	2.6.2.2	O		Y[ ] N[ ]
	Error rate monitoring	5.6.2.3	O		Y[ ] N[ ]
	Multiple B-connections	2.7.1	O		Y[ ] N[ ]
	Multiple H0-connections	2.7.2	O		Y[ ] N[ ]
	Encoding of the BAS	3.1	M		Y[ ] N[ ]
	Values of the BAS	3.2	M		Y[ ] N[ ]
	Procedures for use of the BAS	3.3	M		Y[ ] N[ ]
	Trans. of generic SBE characters	3.4	O		Y[ ] N[ ]
	Audio command - neutral	Annex A.1	O		Y[ ] N[ ]
	Audio command - Au-off, U	Annex A.1	O		Y[ ] N[ ]
	Audio command - Au off, F	Annex A.1	O		Y[ ] N[ ]
	Audio command - A-law, OU	Annex A.1	O		Y[ ] N[ ]
	Audio command - A-law, OF	Annex A.1	O		Y[ ] N[ ]
	Audio command - μ-law, OU	Annex A.1	X		
	Audio command - μ-law, OF	Annex A.1	M		Y[ ] N[ ]
	Audio command - G.722, m1	Annex A.1	O		Y[ ] N[ ]
	Audio command - G.722, m2	Annex A.1	O		Y[ ] N[ ]
	Audio command - G.722, m3	Annex A.1	O		Y[ ] N[ ]
	Audio command - Au-40k	Annex A.1	O		Y[ ] N[ ]
	Audio command - Au-32k	Annex A.1	O		Y[ ] N[ ]
	Audio command - Au-24k	Annex A.1	O		Y[ ] N[ ]
	Audio command - G.728	Annex A.1	O		Y[ ] N[ ]
	Audio command - Au -<16k	Annex A.1	O		Y[ ] N[ ]
	Audio command - Au-ISO-64 to 256	Annex A.1	O		Y[ ] N[ ]
	Audio command - Au-ISO-384	Annex A.1	O		Y[ ] N[ ]
	Xfer rate command - 64	Annex A.2	M		Y[ ] N[ ]
	Xfer rate command - 2 x 64	Annex A.2	M		Y[ ] N[ ]
	Xfer rate command - 3 to 6 x 64	Annex A.2	O		Y[ ] N[ ]
	Xfer rate command - 384	Annex A.2	O		Y[ ] N[ ]
	Xfer rate command - 2 x 384	Annex A.2	O		Y[ ] N[ ]

A.4. H.221 PICS cont.

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	Xfer rate command - 3 to 5 x 384	Annex A.2	O		Y[ ] N[ ]
	Xfer rate command - 1536	Annex A.2	O		Y[ ] N[ ]
	Xfer rate command - 1920	Annex A.2	O		Y[ ] N[ ]
	Xfer rate command - 128 to 320	Annex A.2	O		Y[ ] N[ ]
	Xfer rate command - 512 to 1472	Annex A.2	O		Y[ ] N[ ]
	Xfer rate command - Loss-i.c.	Annex A.2	O		Y[ ] N[ ]
	Channel No. 2-6	Annex A.2	O		Y[ ] N[ ]
	Video, etc. cmd - Video-off	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - H.261	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Vid-imp.(R)	Annex A.3	X		
	Video, etc. cmd - Video-ISO	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - AV-ISO	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Freeze-pic.	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Fast-update	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Encryp-on	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Encryp-off	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Au-loop	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Vid-loop	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Dig-loop	Annex A.3	M		Y[ ] N[ ]
	Video, etc. cmd - Loop-off	Annex A.3	M		Y[ ] N[ ]
	Video, etc. cmd - SM-comp	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Cancel SM-comp	Annex A.3	O		Y[ ] N[ ]
	video, etc. cmd - 6B-H0-comp	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Not-6B-H0-comp	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Restrict	Annex A.3	O		Y[ ] N[ ]
	Video, etc. cmd - Derestrict	Annex A.3	O		Y[ ] N[ ]
	LSD/MLP cmd - LSD off	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 300	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 1200	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 4800	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 6400	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 8000	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 9600	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 14400	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 16k	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 24k	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 32k	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 40k	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 48k	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 56k	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 62.4k	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - 64k	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - Var-LSD	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - DTI(r)	Annex A.4	X		
	LSD/MLP cmd - MLP-off	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - MLP-4k	Annex A.4	O		Y[ ] N[ ]
	LSD/MLP cmd - MLP-6.4k	Annex A.4	O		Y[ ] N[ ]

A.4. H.221 PICS cont.

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	LSD/MLP cmd - Var-MLP	Annex A.4	O		Y[ ] N[ ]
	Audio cap - Neutral	Annex A.5	O		Y[ ] N[ ]
	Audio cap - A-law	Annex A.5	O		Y[ ] N[ ]
	Audio cap - µ-law	Annex A.5	M		Y[ ] N[ ]
	Audio cap - G.722-64	Annex A.5	O		Y[ ] N[ ]
	Audio cap - G.722-48	Annex A.5	O		Y[ ] N[ ]
	Audio cap - G.728	Annex A.5	O		Y[ ] N[ ]
	Audio cap - Au-ISO	Annex A.5	O		Y[ ] N[ ]
	Video etc. cap - QCIF	Annex A.6	M		Y[ ] N[ ]
	Video etc. cap - CIF	Annex A.6	O		Y[ ] N[ ]
	Video etc. cap - 1/29.97	Annex A.6	O		Y[ ] N[ ]
	Video etc. cap - 2/29.97	Annex A.6	O		Y[ ] N[ ]
	Video etc. cap - 3/29.97	Annex A.6	O		Y[ ] N[ ]
	Video etc. cap - 4/29.97	Annex A.6	M		Y[ ] N[ ]
	Video etc. cap - Vid-imp(R)	Annex A.6	X		
	Video etc. cap - Video-ISO	Annex A.6	O		Y[ ] N[ ]
	Video etc. cap - AV-ISO	Annex A.6	O		Y[ ] N[ ]
	Video etc. cap - MBE-cap	Annex A.6	O		Y[ ] N[ ]
	Video etc. cap - Esc-CF(R)	Annex A.6	X		
	Video etc. cap - Encryp	Annex A.6	O		Y[ ] N[ ]
	Trans rate cap - B, H0	Annex A.7	O (Note 1)		Y[ ] N[ ]
	Trans rate cap - 2B	Annex A.7	M		Y[ ] N[ ]
	Trans rate cap - 6B	Annex A.7	O		Y[ ] N[ ]
	Trans rate cap - 2 x H0	Annex A.7	O		Y[ ] N[ ]
	Trans rate cap - 5 x H0	Annex A.7	O		Y[ ] N[ ]
	Trans rate cap - H11/H12	Annex A.7	O		Y[ ] N[ ]
	Trans rate cap - Restrict	Annex A.7	M		Y[ ] N[ ]
	Trans rate cap - 6B-H0-comp	Annex A.7	O		Y[ ] N[ ]
	Trans rate cap - 128/192/256/320	Annex A.7	O		Y[ ] N[ ]
	Trans rate cap - 512/768/1152/1472	Annex A.7	O		Y[ ] N[ ]
	LSD/MLP cap - 300(to 64k)	Annex A.8	O		Y[ ] N[ ]
	LSD/MLP cap - Var-LSD	Annex A.8	O		Y[ ] N[ ]
	LSD/MLP cap - MLP-4k	Annex A.8	O		Y[ ] N[ ]
	LSD/MLP cap - MLP-6.4k	Annex A.8	O		Y[ ] N[ ]
	LSD/MLP cap - Var-MLP	Annex A.8	O		Y[ ] N[ ]
	Escape table values - HSD	Annex A.9	O		Y[ ] N[ ]
	Escape table values - H.230	Annex A.9	O		Y[ ] N[ ]
	Escape table values - Start-MBE	Annex A.9	O		Y[ ] N[ ]
	Escape table values - NS-cap	Annex A.9	O		Y[ ] N[ ]
	Escape table values - NS-comm.	Annex A.9	O		Y[ ] N[ ]
	Escape table values - Cap-mark	Annex A.9	O		Y[ ] N[ ]
	Escape table values - Data-apps	Annex A.9	O		Y[ ] N[ ]
	HSD/H-MLP values - 64k to 1536k	Annex A.10	O		Y[ ] N[ ]
	HSD/H-MLP values - HSD-other	Annex A.10	O		Y[ ] N[ ]
	HSD/H-MLP values - Var-HSD	Annex A.10	O		Y[ ] N[ ]
	HSD/H-MLP values - H-MLP-62.4k	Annex A.10	O		Y[ ] N[ ]

A.4. H.221 PICS concl.

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	HSD/H-MLP values - H-MLP-r	Annex A.10	O		Y[ ] N[ ]
	HSD/H-MLP values - Var-H-MLP	Annex A.10	O		Y[ ] N[ ]
	HSD/H-MLP cmds - 64k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - 128/192/256k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - 320k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - 384k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - HSD-other	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - H-MLP-off	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - H-MLP-62.4k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - H-MLP-64k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - H-MLP-128k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - H-MLP-192k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - H-MLP-256k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - H-MLP-320k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - H-MLP-384k	Annex A.11	O		Y[ ] N[ ]
	HSD/H-MLP cmds - Var-H-MLP	Annex A.11	O		Y[ ] N[ ]
	LSD/HSD appl. - Still image H.261	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - V.120 LSD	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - V.120 HSD	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - ISO-SP on LSD	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - ISO-SP on HSD	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - ISO-SP spatial	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - ISO-SP progressiv	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - ISO-SP arithmetic	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - Graphics cursor	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - Group 3 fax	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - Group 4 fax	Annex A.12	O		Y[ ] N[ ]
	LSD/HSD appl. - ISO-SP on in LSD	Annex A.13	O		Y[ ] N[ ]
	LSD/HSD appl. - ISO-SP on in HSD	Annex A.13	O		Y[ ] N[ ]
	LSD/HSD appl. - Cursor data LSD	Annex A.13	O		Y[ ] N[ ]
	LSD/HSD appl. - Fax on in LSD	Annex A.13	O		Y[ ] N[ ]
	LSD/HSD appl. - Fax on in HSD	Annex A.13	O		Y[ ] N[ ]
	LSD/HSD appl. - V.120 LSD	Annex A.13	O		Y[ ] N[ ]
	LSD/HSD appl. - V.120 HSD	Annex A.13	O		Y[ ] N[ ]

Note 1: The transmission rate capability for one B-channel is mandatory, the capability for 384 kbit/s H0 is optional.

A.5. H.242 PICS

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	Audio capabilities	2.1	M		Y[ ] N[ ]
	Video capabilities	2.2	M		Y[ ] N[ ]
	Transfer rate capabilities	2.3	M		Y[ ] N[ ]
	Data capabilities	2.4	O		Y[ ] N[ ]
	Terminals on restricted ntwks capab.	2.5	M		Y[ ] N[ ]
	Capability exchange - Sequence A	5.1	M		Y[ ] N[ ]
	Mode switching - Sequence B	5.2	M		Y[ ] N[ ]
	Frame reinstatement Sequence C	5.3	M		Y[ ] N[ ]
	Mode initialization - $p = 1$	6.1.1	M		Y[ ] N[ ]
	Mode initialization - $p > 1$	6.1.2	M		Y[ ] N[ ]
	Dynamic switching - F to F	6.2.1	M		Y[ ] N[ ]
	Dynamic switching - F to U	6.2.2	O		Y[ ] N[ ]
	Dynamic switching - U to F/U	6.2.3	O		Y[ ] N[ ]
	Mode 0 forcing - single channel	6.3.1	M		Y[ ] N[ ]
	Mode 0 forcing - two or more chans.	6.3.2	M		Y[ ] N[ ]
	Mode mismatch recovery	6.4	M		Y[ ] N[ ]
	Frame alignment loss	7.1.1	M		Y[ ] N[ ]
	Frame synchronization loss	7.1.2	M		Y[ ] N[ ]
	Channel renum. - loss of 1 channel	7.2.1	O		Y[ ] N[ ]
	Channel renum - loss of add'l chan.	7.2.2	O		Y[ ] N[ ]
	Channel renum - loss of initial chan	7.2.3	O		Y[ ] N[ ]
	Initial channel	8.1.1	M		Y[ ] N[ ]
	Additional channels	8.1.2	M		Y[ ] N[ ]
	Terminal disconnection	8.2	M		Y[ ] N[ ]
	Call transfer	8.3	O		Y[ ] N[ ]
	Conferencing	8.4	O		Y[ ] N[ ]
	PCM Format conversion	8.5	O		Y[ ] N[ ]
	Act/deact data channels	9.1	O		Y[ ] N[ ]
	MLP	9.2	O		Y[ ] N[ ]
	Simultaneous LSD and HSD	9.3	O		Y[ ] N[ ]
	Simultaneous HSD and MLP	9.4	O		Y[ ] N[ ]
	Restricted networks	10	M		Y[ ] N[ ]
	56 to 64 kbit/s interworking	10.2.6	O		Y[ ] N[ ]
	Framing signal (56 kbit/s)	10.3.1	M		Y[ ] N[ ]
	Transmission formats (56 kbit/s)	10.3.2	M		Y[ ] N[ ]
	n x 56 kbit/s operation	10.3.3	O		Y[ ] N[ ]
	n x H0 operation	10.3.4	O		Y[ ] N[ ]
	Procedures for use of BAS codes	11	M		Y[ ] N[ ]
	Bit occupancy and BAS codes	12	M		Y[ ] N[ ]
	SM-comp and 6B-H0 interconnect	13	X		
	Encryption control signal channel	14	O		Y[ ] N[ ]

A.6. H.233 PICS

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	Ctl & Ind within the H.221 frame	3.1.1	O		Y[ ] N[ ]
	Message formats	3.1.2	M		Y[ ] N[ ]
	Identifier	3.1.2.1	M		Y[ ] N[ ]
	Length	3.1.2.2	M		Y[ ] N[ ]
	Bit string	3.1.2.3	M		Y[ ] N[ ]
	Unenciphered ECS channel	3.1.3	M		Y[ ] N[ ]
	Session exchange blocks	3.1.3.1	M		Y[ ] N[ ]
	Initialization vectors	3.1.3.2	M		Y[ ] N[ ]
	Error protection	3.1.3.3	M		Y[ ] N[ ]
	Transmission encryption method	3.2	M		Y[ ] N[ ]
	Procedure for use of the system	3.3	O		Y[ ] N[ ]
	Multilayer protocol encryption	4	X		

Note: This PICS is an instance where there should be predicate information supplied, i.e., the mandatory items in the above table are only mandatory if encryption is selected.

A.7. VTC Systems - G.711 PICS

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	Can the implementation work at 64kbit/s - A-law?	3.1	O		Y[ ] N[ ]
	Can the implementation work at 64kbit/s - µ-law?	3.1	O		Y[ ] N[ ]
	Can the implementation work at 56kbit/s - A-law?	H.221 Annex A.1	O		Y[ ] N[ ]
	Can the implementation work at 56kbit/s - µ-law?	H.221 Annex A.1	M		Y[ ] N[ ]

A.8. VTC Systems - G.722 PICS

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	Can the implementation work at 64kbit/s?	1.3	O		Y[ ] N[ ]
	Can the implementation work at 56kbit/s	1.3	O		Y[ ] N[ ]
	Can the implementation work at 48kbit/s?	1.3	O		Y[ ] N[ ]

A.9. VTC Systems - G.728 PICS

Index	Protocol Feature	Std. Clause	Std. Status	Predicate	Imple-mented?
	Can the implementation work at 16kbit/s?	All	O		Y[ ] N[ ]

A.10. VTC Systems - Annex B PICS

Index	Protocol Feature	Std. Section	Std. Status	Predicate	Imple-mented?
	FIPS PUB 178	B.5.1.1	M		Y[ ] N[ ]
	Transmission data rates - *p*=1, *p*=2	B.5.1.2	M		Y[ ] N[ ]
	Proprietary codec	B.5.1.3	O		Y[ ] N[ ]
	Motion rendition	B.5.1.4	M		Y[ ] N[ ]
	VTU Network interface	B.5.1.5	O		Y[ ] N[ ]
	High Resolution Graphics	B.5.2	O(Note 1)		
	Security - interoperate with KG-194	B.5.4	O		Y[ ] N[ ]
	Security - resyncronization capability	B.5.4.3.2	O		Y[ ] N[ ]
	ISDN BRI	B.6.1.1	O		Y[ ] N[ ]
	Secure ISDN BRI	B.6.1.2	O		Y[ ] N[ ]

Note 1: Requires no change to the VTU hardware or software; the software may be implemented on PCs connected to the VTU data ports.

Annex B (normative for Department of Defense)

B.1. Scope.

B.1.1. Purpose.

The purpose of this Annex is to provide the DOD with interoperability and performance requirements and options that are not covered in the main body of the profile. Annex B presents more detail than the Profile in several areas incorporating specific information on the use of external encryption devices for classified conferences, and on the transfer of still images. These requirements and options are based on the work done in developing MIL-STD-188-331 which was approved March 29, 1994. Note that a PICS for the features of Annex B is included in Section A.10 of Annex A.

The technical parameters of this Annex may be exceeded to satisfy certain specific requirements, provided that the minimum mandatory requirements are met and that interoperability is maintained. The Annex will be revised in the future to include other VTC-related requirements such as secure multipoint.

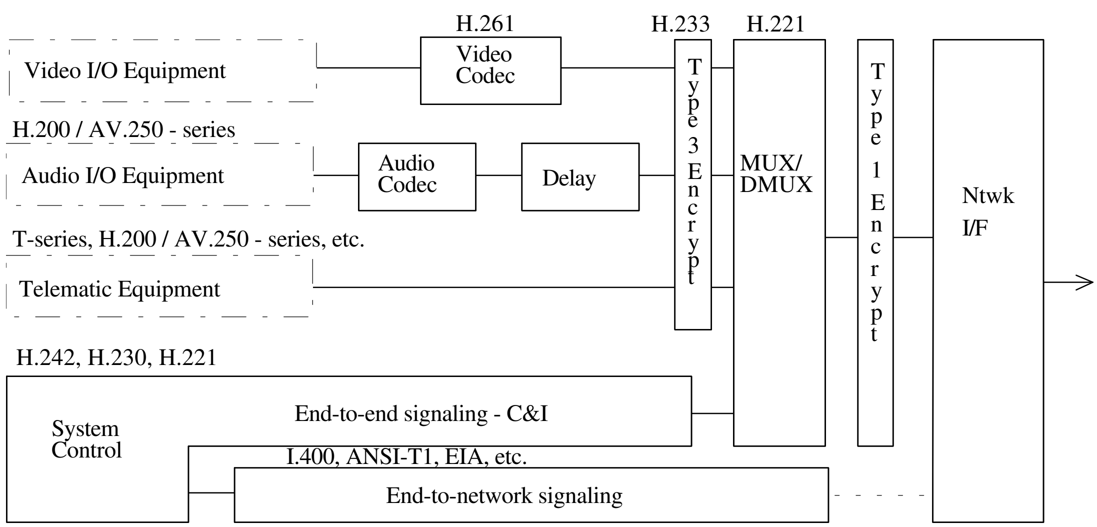


Figure B.1. Video teleconferencing equipment schematic (dashed boxes are not included)

B.1.2. Demarcation.

The scope of this Annex is the same as the scope of the Profile except that it includes an optional encryption device for classified operation which is placed between the multiplexer/demultiplexer and the network interface. See Figure B.1.

B.1.3. Application.

This Annex applies to all procurements initiated for DOD VTC and videophone equipment operating between 56 and 1920 kbit/s after the effective date of the Profile. Examples include, but are not limited to, roll-about units as well as portable, modular, and desktop systems, studios, and cards integrated into personal computers. This Annex does not preclude the procurement of proprietary features as long as the corresponding standard features are also procured. See the definitions of *mandatory* and *optional* features for further explanation. This Annex is also recommended for DOD contractors and anyone else who needs to communicate with DOD by way of VTC. This Profile, together with the Annex can be used in the design and installation of new VTC equipment and subsystems, and in authorized upgrading of existing VTC subsystems and equipment.

B.1.4. Comments.

Beneficial comments (recommendations, additions, and deletions) and any pertinent data that may be of use in improving this Profile should be addressed to the Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Organization (JIEO), TBBC (ATTN: Mr. Rittenbach), Fort Monmouth, NJ 07703-5613.

B.2. Normative references.

B.2.1. Government documents.

B.2.1.1. Specifications, standards, and handbooks.

The following specifications, standards, and handbooks form a part of this Profile to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the issue of the Department of Defense Index of Specifications and Standards (DODISS) and supplements thereto, cited in the solicitation.

B.2.1.1.1. Federal standards.

FED-STD-1037B	*Glossary of Telecommunication Terms*

B.2.1.1.2. Military standards.

MIL-STD-188-114A	*Electrical Characteristics of Digital Interface Circuits*
MIL-STD-188-198	*Joint Photographic Experts Group (JPEG) Image Compression for the National Imagery Transmission Format Standard (Approved for U.S. release only)*
MIL-STD-2500	*National Imagery Transmission Format (Version 2.0) for the National Imagery Transmission Format Standard (Approved for U.S. release only)*

Copies of MIL-STD-188-198 (NITFS JPEG) and MIL-STD-2500 (NITFS) compliant software are available from: Ms. Kathleen Bastien, The Analytic Sciences Corporation, Reading, MA, (617) 942-2000.

Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from

Defense Printing Service Detachment Office
Standardization Documents Order Desk
700 Robbins Ave.
Building 4, Section D
Philadelphia, PA 19111-5094

Federal standards are also available from

General Services Administration
GSA Specification Unit (WFSIS)
Room 6039
7th & D Streets SW
Washington, DC 20407 USA
Telephone: 202-472-2205

B.2.1.2. Other government documents, drawings, and publications.

The following Government documents, drawings, and publications also form a part of this Profile to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

B.2.1.2.1. DOD directives.

4640.14	*Base and Long-Haul Telecommunications Equipment and Services*

B.2.1.2.2. Other government documents.

DODISS	*Department of Defense Index of Specifications and Standards*
MIL-HDBK-1300	*National Imagery Transmission Format Standard Handbook (Approved for U.S. release only)*
DISA/JIEO Circular 9008	*NITFS Certification Test and Evaluation Program Plan*
NSTISS 4009	*National INFOSEC Glossary, National Security Telecommunications and Information Systems Security*
Warner Amendment	*Public Law 97-86, 1 December 1981*

B.2.2. Non-government publications.

The following documents form a part of this Profile to the extent specified herein. Unless otherwise specified, the issues of the documents that are DOD adopted are those listed in the issue of the DODISS cited in the solicitation. Unless otherwise specified, the issues of documents not listed in the DODISS are the issues of the documents cited in the solicitation. If not in the DODISS and not in the solicitation, then use the latest approved version of the standard.

B.2.2.1. Electronic Industries Association (EIA) publications.

EIA-422-A	*Electrical Characteristics of Balanced Voltage Digital Interface Circuits*
EIA-449	*General-Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*

Copies of EIA standards can be purchased from

Electronic Industries Association
Standards Sales
2001 Pennsylvania Avenue NW
Washington, DC 20006
Telephone: 202-457-4966
Fax: 202-457-4985

B.2.2.2. ANSI publications.

ANSI T1.601	*American National Standard for Telecommunications - ISDN Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT*
ANSI T1.605	*American National Standard for Telecommunications - ISDN Basic Access Interface for S and T Reference Points*
ANSI T1A-EIA-619	*Aggregation of Multiple Independent 56 Kbit/s or 64 Kbit/s Channels onto a Synchronized Wideband Connection (formerly known as the BONDING standard)*

B.2.2.3. ITU-T publications.

ITU-T P.30	*Subscribers' Lines and Sets*
ITU-T P.34	*Transmission Characteristics of Hands-Free Telephones*
ITU-T P.50	*Artificial Voices*
ITU-T P.51	*Artificial Ear and Artificial Mouth*
ITU-T P.64	*Determination of Sensitivity Frequency Characteristics of Local Telephone Systems to Permit Calculation of their Loudness Ratings*

ITU-T V.35	*Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits*
ITU-T X.21	*Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Synchronous Operation on Public Data Networks*

Copies of ANSI, FIPS, FED-STD, EIA, and ITU-T standards are included in *Open Systems Standards*, Volumes 1-6, edited by Harold C. Folts, McGraw Hill, Publisher.

Non-Government standards and other publications are normally available from the organizations that prepare or distribute them. These documents also may be available in or through libraries or other informational services.

B.2.3. Order of precedence.

In the event of a conflict between the main body of the COS Profile, Annex A, Annex B, FIPS PUB 178, and the references cited in each of these documents, the following order of precedence shall apply for DOD:

1) FIPS PUB 178
2) Annex B
3) Main body of the Profile
4) Annex A
5) References cited in these documents.

Nothing in this Annex, however, supersedes applicable laws and regulations, unless a specific exemption has been obtained.

B.3. Definitions

Definitions of terms used in this Annex shall be as specified in FED-STD-1037B. Those definitions unique to this Annex and not defined in FED-STD-1037B, are provided in this paragraph.

Audio: The voice or sound portion of a teleconference.

Camera: In television, an electronic device using an optical system and a light-sensitive pickup tube or chip to convert visual signals into electrical impulses.

Classified: Any information that has been determined to require protection against unauthorized disclosure to avoid harm to U.S. national security. The classifications TOP SECRET, SECRET, and CONFIDENTIAL are used to designate such information, referred to as "classified information".

Compression: See *data compression*, FED-STD-1037B, definition 1.

Cryptographic resynchronization: The VTU having the capability to automatically send a signal for resynchronization to the cryptographic device whenever resynchronization is needed.

Data communications port: A port used to transfer information between functional units by means of data transmission, according to a protocol.

Data port: See *data communications port*.

Data rate: In digital data communications, the rate at which data (bits in this case) is transmitted, usually expressed in bits per second.

DB-25S: A standardized 25-pin connector used in EIA-232-D and EIA-530 data communications.

Desktop and individual workstation: An input/output display device with local computer power that allows an individual to perform some computational work and/or data-base access from a local or remote location. This device may also have videophone and/or VTC capabilities.

EIA-232-D (formerly RS-232-D): A serial interface standard for transmission of unbalanced signals between a variety of computer, media, and multimedia peripherals. EIA-232-D transmits at a maximum of 19.2 kbit/s for up to a distance of about 50 feet and uses a 25-pin connector.

B.3 Definitions, continued.

EIA-422 (formerly RS-422): A serial electrical interface standard for transmission of balanced and unbalanced signals between a variety of higher-end computer, media, and multimedia peripherals. EIA-422 allows a maximum data rate of 10 Mbit/s.

EIA-449 (formerly RS-449): A serial mechanical interface standard for transmission of balanced and unbalanced signals between a variety of higher-end computer, media, and multimedia peripherals. EIA-449 allows a maximum data rate of 10 Mbit/s and uses a 37- or 9-pin connector.

EIA-530: A replacement for EIA-449 that uses a DB-25 (EIA-232-D) connector instead of a 37-pin connector, while keeping the most important electrical signals intact. EIA-530 is to be used in conjunction with EIA-422-A.

Electric Industries Association: A U.S. commercial standards organization. The acronym EIA precedes a numerical designation, such as EIA-232-D, which replaces the now obsolete RS (Recommended Standard) designation, for example, RS-232-D.

Embedded encryption: Encryption integrated into the VTU box.

High-resolution graphics: Graphics captured and displayed at a higher resolution than the NTSC standard (EIA-170-A).

Huffman Coding: An entropy coding technique to compress data in which frequent events are represented by short codes, and rare events are represented by long codes. Used in Group 3 facsimile and JPEG.

Inverse multiplexer: A device used to create a single, higher-speed network data channel by combining, separating, and synchronizing multiple, independent 56- or 64-kbit/s network data channels. Also known as an *aggregator*.

ISDN: See FED-STD-1037B, *Integrated Services Digital Network*. Note: Access channels include a basic rate (two 64-kbit/s "B" channels + one 16-kbit/s "D" channel) and a primary rate (twenty-three 64-kbit/s "B" channels and one 64-kbit/s "D" channel).

Mandatory feature: If a given feature is mandatory in this Profile, then once the Profile is adopted, the feature must be included in all future military VTC procurements, unless a waiver is obtained.

Multipoint: A telecommunications system that permits three or more locations to intercommunicate in a conference call.

B.3 Definitions, continued.

Network: See FED-STD-1037B. In this Profile, *network* infers the system of cables, microwave links, and switching centers that allow the transmission of data, as opposed to the terminal equipment (such as CODECs and I/O devices) connected to the cables.

Network interface equipment: The equipment connected between the network and the VTU. Such examples of this equipment include (a) the channel service unit (CSU), (b) the data service unit (DSU), and the (c) terminal adapters.

NITF: National Imagery Transmission Format. The format for secondary imagery transmission defined in the NITFS.

NITFS: National Imagery Transmission Format Standard. A set of military standards described in MIL-HDBK-1300, for secondary imagery dissemination.

Nondevelopmental item (NDI). NDIs are items procured from immediately available stock, with no development costs.

Optional feature: If a feature is optional in this Profile, the user must decide to purchase the Profile feature or not. If purchased, this feature shall meet the specifications in the Profile. (Anyone wanting to be exempt from this rule shall first obtain a waiver.) The purpose is to improve interoperability, without forcing users to buy unnecessary features. The Profile does not prevent the user from buying a particular feature implemented in a nonstandard way. However, if both standard and nonstandard modes are purchased, the feature must be easily switched back to the standard mode.

For example, if a high-resolution, still imagery mode is an optional feature in this Profile, it would be the user's decision to purchase the Profile high-resolution, still-image-mode or not. If purchased, the version shall meet the Profile specifications for the high-resolution, still image mode. This will allow for interoperability of high-resolution, still images among those users purchasing this Profile feature. If the procuring agency desires, it can also buy a nonstandard version of the high-resolution, still image mode, as long as the equipment can be easily switched back to the standard high-resolution, still image mode. For "mandatory optional" see B.7.1.3.

***p*:** An integer that can range from 1 to 30. It relates to VTUs that operate at nominal bit rates of integer multiples of 64000 bits per second (bit/s), where the integer is *p*. For unrestricted channels, such as provided by ISDN, each increment of data rate may actually be 64000 bit/s, but in restricted channels, each increment may be only 56000 bit/s.

Recommended standard: A prefix to EIA standards, such as RS-232-D. This designation is now obsolete; it has been replaced by the prefix EIA, for example, EIA-232-D.

B.3 Definitions, continued.

Resolution: See FED-STD-1037B, definition 3. For video equipment, often measured in terms of pels.

Teleconferencing: The use of teleconferencing to conduct a seminar.

TEMPEST-approved: See FED-STD-1037B. A TEMPEST-approved device that meets stringent requirements. The electromagnetic waves it emits have been reduced through shielding or other techniques to a point where it would be extremely difficult for a hostile force to gather information from the electromagnetic waves and disclose the classified information being transmitted.

Type 1: A classified or controlled cryptographic equipment, assembly, component, or item endorsed by the National Security Agency (NSA) for securing telecommunications and automated information systems for the protection of classified or sensitive U.S. Government information exempted by the Warner Amendment for use by the U.S. Government and its contractors, and subject to restrictions in accordance with the International Traffic in Arms Regulation.

Type 2: An unclassified cryptographic equipment, assembly, component, or item endorsed by the National Security Agency for use in telecommunications and automated information systems for the protection of unclassified but sensitive information. Type 2 equipment is exempted by the Warner Amendment. Type 2 is available to U.S. Government departments, agencies, sponsored elements of state and local government, sponsored U.S. Government contractors, and sponsored private sector entities. It is subject to restrictions in accordance with the International Traffic in Arms Regulation.

Type 3: An unclassified cryptographic equipment, assembly, component, or item that implements an unclassified algorithm registered with the National Institute of Standards and Technology (NIST) as a FIPS for use in protecting unclassified sensitive, or commercial, information. This definition does not include Warner-Amendment-exempt equipment.

Unclassified: Information that is not classified.

Unclassified sensitive: A designation for information that is not classified, but needs to be protected from unauthorized disclosure. Examples of types of information that fall under this category are For Official Use Only (FOUO), proprietary, contractor sensitive, limited distribution, and personal in nature.

Videophone: A VTC terminal where most of the equipment is integrated into a single desktop unit.

B.3 Definitions, concluded.

Video CODEC: See CODEC (in paragraph 3 of main body of the Profile).

Video teleconferencing unit (VTU): VTC equipment that performs the following functions: coding/decoding of audio and video; and multiplexing of video, audio, data, and control signals, system control, and end-to-end signaling. It does not include I/O devices, embedded and non-embedded cryptographic devices, network interface equipment, end-to-network signaling, network connections, or the network itself. NOTE: The scope of this Profile is broader than the scope of the VTU because the scope of the Profile includes cryptographic devices and other items that the VTU does not include.

Warner Amendment: Title 10, United States Code, Section 2315, "Law inapplicable to the procurement of automatic data processing equipment and services for certain defense purposes." Enacted as Public Law 97-86, 1 December 1981. The Warner Amendment amends Section 111 of the Federal Property and Administrative Services Act of automatic data processing equipment (currently defined to include telecommunications services and equipment) if the function, operation, or use of the equipment or services:

(1) involves intelligence activities;
(2) involves cryptologic activities related to national security;
(3) involves the command and control (C2) of military forces;
(4) involves equipment that is an integral part of a weapon or weapons system; or
(5) subject to (6) is critical to the direct fulfillment of military or intelligence missions.
(6) subpart (5) does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications.

The Warner Amendment has the effect of exempting the above DOD applications from the mandatory-use provisions for FTS-2000. See DOD Directive 4640.14 for detailed instructions for Warner exemption determinations.

Warner-exempt: A telecommunications requirement that meets the stipulations as stated in the Warner Amendment, which thereby exempts that requirement from the mandatory-use provisions of FTS-2000.

B.4. Abbreviations and acronyms.

The abbreviations and acronyms used in Annex B and not already listed in the main body of the Profile are defined below. Those that are common with the terms in FED-STD-1037B have been included for the convenience of the reader.

AR	Army Regulation
bit/s	bit(s) per second
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
COMRAT	compression rate code
COMSEC	communications security
COTS	commercial off-the-shelf
DCT	discrete cosine transform
DCTN	Defense Commercial Telecommunications Network
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODISS	Department of Defense Index of Specifications and Standards
EIA	Electronic Industries Association
FED-STD	federal standard
FHDR	file header
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
FSCLAS	File Security Classification field
IC	Image Compression field
JIEO	Joint Interoperability and Engineering Organization
JPEG	Joint Photographic Experts Group
LOS	loss of synchronization
MILDEP	military department, such as the Air Force, Army, Navy
MIL-HDBK	military handbook
MIL-STD	military standard
NACSIM	National COMSEC Information Memorandum
NDI	nondevelopmental item
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NITFS	National Imagery Transmission Format Standard
NSA	National Security Agency
NSTISS	National Security Telecommunications and Information Systems Security
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory/Information Memorandum
NT1	Network Termination 1
NTISSI	National Telecommunications and Information Systems Security Instruction

NTISSP	National Telecommunications and Information Systems Security Policy
OPNAVINST	Chief of Naval Operations Instruction
OPNAVNOTE	Chief of Naval Operations Note
PUB	publication
RD	Receive Data
RS	recommended standard
RT	receive timing
SD	Send Data
ST	Send Timing
TA	Terminal Adapter
TEMPEST	compromising emanations
TT	terminal timing

B.5. Subnetwork-type independent requirements.

These requirements, in addition to those in main body of the Profile apply to all DOD VTC systems.

B.5.1. Video communications and control.

B.5.1.1. General.

Except as noted, the VTU shall conform to the requirements set forth in FIPS PUB 178. FIPS PUB 178 is based on the five ITU-T *p* x 64 standards: H.221, H.230, H.242, H.261, and H.320.

The FIPS PUB references the 1990 versions of the above standards. However, it is being updated to reference the 1993 versions. The 1993 versions shall be used.

B.5.1.2. Data transmission rates.

VTUs shall be able to operate at $p = 2$ with a single 128-kbit/s channel, and if a second network interface port is specified, with two 64-kbit/s channels. For other *p* values, operation only with a single channel is required.

Operation at $p > 2$ is optional. If the procurement requires a higher *p* value, then all *p* values in the set {1, 2, 4, 6, 12, 18, 23, 24} less than or equal to the requirement shall also be provided.

B.5.1.3. Video coding and decoding.

The video CODEC subsystem can also provide other proprietary solutions in addition to ITU-T H.261.

B.5.1.4. Motion rendition.

The encoder shall be capable of encoding at least an average of 6 pictures per second, excluding pictures with scene changes. This is to help ensure a minimum level of motion rendition.

B.5.1.5. VTU network interface.

As an option, a minimum of one synchronous EIA-449 attachment port is strongly recommended as specified in B.5.4.3.1 and B.5.4.3.2. This will allow interface to KG-194 cryptographic devices, should a classified conference be required. (There may be a need to do classified conferencing in an emergency even if the VTU is normally used for non-classified purposes.)

B.5.2. Still images.

B.5.2.1. General.

The ability to capture, exchange, and display still images is optional. In addition, the ability to output images digitally to personal computers and workstations may optionally be supported. Image-capture devices may include standard cameras and scanning devices. The actual graphic input devices such as cameras and digital scanners are outside the scope of this Profile; however, the interface to cameras is specified in 5.2.3.

This Profile makes a distinction between freeze-frame video and still images. Freeze-frame video is optional and is addressed in 5.1.9. It defines a frame selected from a video signal, and processed through the video CODEC for transmission to remote sites. Still images are optional and are addressed in 5.1.10.1 and B.5.2.2.

The still image mode specified in 5.1.10 of this Profile is not yet commercially available. As an interim solution, users may continue to use proprietary methods for still image transfer currently in use by the Defense Commercial Telecommunication Network (DCTN), or they may use an implementation of the Joint Photographic Experts Group Standard (JPEG) specified in the National Imagery Transmission Format Standard (NITFS) and paragraph B.5.2.2.

B.5.2.2. NITFS-JPEG mode.

The optional use of the NITFS-JPEG standard allows for images of various resolutions to be transferred between VTUs, from low to very high resolution. The resolution is limited only by the resolution of the hardware devices such as cameras, scanners, and monitors.

B.5.2.2.1. Implementation.

NITFS-JPEG may be implemented through the VTU data ports or out-of-band and requires no change to the VTU hardware and software. It is typically implemented on PCs or computer workstations connected to the VTU data ports. Alternatively it may be integrated into the VTU. Since the data interface specified in 5.1.10 is not yet commercially available, proprietary or out-of-band data communications may be used until standards-based solutions become commercially available. When the high or low speed MLP data ports using the T.120 protocol described in 5.1.10 become available, NITFS may be transferred through these channels using the T.127 file transfer protocol.

B.5.2.2.2. Availability.

NITFS-JPEG software is available free of charge to U.S. government and corporate organizations and can run on ordinary PC's. For copies, contact the source listed in B.2.1.1.2. Enhanced commercial implementations of software and hardware are available for purchase. For a list of vendors certified to be NITFS compliant, contact Mr. Stephen Kerr, DISA-JIEO-TCDC, Ft. Huachuca, AZ.

B.5.2.2.3. Software.

Version 2.0 (or later) of the software described by MIL-HDBK-1300 shall be used. Version 2.0 includes the JPEG Image Compression standard (MIL-STD-188-198). This will provide a full range of still-image capabilities ranging from low- to high-resolution for monochrome, gray-scale, and color images. Initiation and termination of NITFS file transfer is negotiable manually. No BAS codes are assigned to this file transfer.

B.5.2.2.4. JPEG compression.

This Profile tailors JPEG in a standard manner by fixing many optional parameters such as quantization tables and Huffman coding tables. NITFS also adds headers and other types of data such as computer-generated graphics, labels, and text to the resulting data file. Several items of each data type may be included in one message, yet any data types may be omitted. MIL-HDBK-1300 describes the NITFS and its components.

If NITFS is selected as an option, then the JPEG compression scheme specified in MIL-STD-188-198 is mandatory. If NITFS is selected as an option, operation Types 1 and 2 are mandatory. Type 1 is 8-bit sample precision gray-scale sequential DCT with Huffman coding. Type 2 is 24-bit color, 8-bit sample precision per component (3 components), sequential discrete cosine transform (DCT) with Huffman coding.

B.5.2.2.5. NITF header.

In the NITF File Header (Table 1, MIL-STD-2500) the File Type & Version (FHDR) field shall be set to the value "NITFnn.nn", where "nn.nn" is the software version number. In addition, the File Security Classification field (FSCLAS) shall either specify a valid classification value ("T," "S," "C," "R," or "U") or the value "N". "T" indicates Top Secret, "S" indicates Secret, "C" indicates Confidential, and "R" indicates Restricted (unclassified sensitive). "N" indicates the classification is not specified in the message. The other fields in the NITF header may be filled with zeros or user-selected values.

B.5.2.2.6. Image sub-header.

The image sub-header (Table III in MIL-STD-2500) shall specify value "C3" in the image compression (IC field). "C3" indicates the type of image compression, in this case, JPEG. The default compression rate code (COMRAT field) shall be "00.5". The first two digits to the left of the decimal point indicate the type of image. In this case, "00" indicates a general-purpose image. The single digit to the right of the decimal point indicates the desired transmission quality level from 1 to 5. In this case, "5" indicates the highest-quality level. The higher the quality level, the less compression will take place, and the longer the transmission time per image. The other fields in the image sub-header may be filled with zeros or user-selected values.

B.5.2.2.7. Additional specifications.

In addition, the mandatory set of NITFS capabilities shall be provided, as specified for CLEVEL 2 in DISA/JIEO Circular 9008, *NITFS Certification Test and Evaluation Program Plan*. This provides for an image size of 64 to 1024 vertical pixels by 64 to 1024 horizontal pixels. The minimum compliant set of capabilities includes JPEG compression and decompression, using sequential DCT, Huffman entropy encoding, and an 8-bit precision mode of operation. In addition, the NITFS terminals shall be able to pack and unpack 8-bit monochrome, 8-bit color, and 24-bit color images. Circular 9008 extends JPEG to include items such as quantization tables and color space definitions.

B.5.3. Data communications.

At this time, the ITU-T Study Group 8 is completing a new suite of international standards for audiographic and video conferencing, known collectively as ITU-T.120. They will include not only data communications protocols and procedures, but will also include optional applications such as still image transfer, annotation, pointing, and binary file transfer. These standards are designed to operate over low and high speed MLP data channels within the H.221 multiplexed data stream. They are not yet implemented in commercially available products. It is anticipated that commercial T.120 applications will appear in the next one to three years. Until these become available, proprietary or out-of-band data transfer techniques may be used.

B.5.4. Security.

B.5.4.1. General.

This paragraph specifies a standard means of securing the transmitted signals for classified information. The capability to interface and operate with cryptographic equipment for classified operation is optional. If the user requires the VTU for use in conducting classified conferences, the requirements of B.5.4.3 and its subparagraphs are mandatory.

The following area is briefly addressed in B.7.2, but only as a recommendation, not as a mandatory or optional feature: compromising emanations (TEMPEST). The following areas related to security are outside the scope of this Annex: physical security, including room security; user authorization; and key management and distribution

B.5.4.2. Levels of security.

This Annex identifies three levels of security for the protection of the information transmitted between VTUs. The three security levels are described in the B.5.4.2.1 through B.5.4.2.3.

B.5.4.2.1. Unencrypted.

Information that is unclassified and not sensitive requires no protection by cryptographic equipment and can be transmitted in an unencrypted (plain-text) mode. All VTUs shall be able to transmit and receive unencrypted information.

B.5.4.2.2. Unclassified but sensitive (Type 3).

Information that is unclassified but sensitive and not exempted by the Warner Amendment (as defined in Title 10, United States Code, Section 2315) shall be protected by Type 3 cryptographic equipment that is certified by the National Institute of Standards and Technology (NIST). In this Profile, this information will be referred to as "Type 3." The method of encrypting this information is specified in 5.4 of the main body of the Profile.

B.5.4.2.3. Classified (Type 1).

Information that is classified and information that is unclassified but sensitive Warner Amendment information shall be protected by Type 1 cryptographic equipment certified by the National Security Agency (NSA). In this Profile, this information will be referred to as "Type 1." As an option, it is strongly recommended that VTUs be able to interface with and operate with Type 1 cryptographic equipment. For the purposes of this Profile, Type 2 Warner-exempt information shall be protected by Type 1 cryptographic equipment.

The protection of classified VTC information shall be accomplished by encrypting the signal output from the VTU before it enters the network interface equipment to go out to the network, and by decrypting the signal coming from the network through the network interface equipment before it goes into the VTU. To minimize the number of encryption devices and simplify the key management required in a conference above 56/64 kbit/s, the VTUs shall operate in a single-channel mode (using a single EIA-449 network interface). A cryptographic device is placed between the network interface equipment and the VTU. See Figure B.2 for a simplified diagram of the connections between the network, network interface equipment, cryptographic device, and VTU. To operate over a network that contains a restricted channel at one end of the link and an unrestricted channel at another end of the link, special provisions must be made. See B.7.4 for more details.

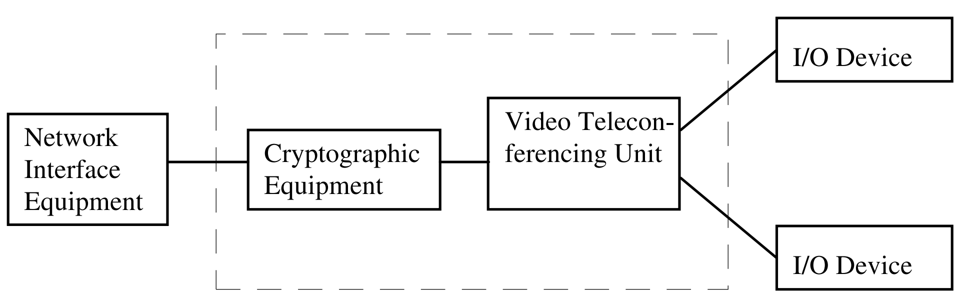


Figure B.2. Line of demarcation with external cryptographic device

ITU-T H.233 recommends that the VTU service channel (which contains the FAS, BAS, and ECS signals) remain unencrypted; however, the encryption scheme just described is a trunk encryption applied between VTUs that encrypts the entire signal, including the VTU service channel. The encrypted signal is decrypted prior to reaching the destination VTU.

B.5.4.3. Type 1 cryptographic equipment.

The KG-194/194A or compatible equipment shall be used to protect Type 1 information passing through the VTU. If KG-194-compatible equipment is used, it must be compatible in terms of both encryption and key-management schemes, except that existing KG-81 equipment may continue to be used until KG-194 or compatible equipment is available.

If a requirement exists for classified conferencing, each transmission channel used by the VTU shall be protected by Type 1 cryptographic equipment. This will require one cryptographic unit at each VTU. If more than one transmission channel is used, as in the case of operation at p = 2 using ISDN or switched 56 circuits, then an IMUX shall be used to multiplex and demultiplex the two transmission channels to the single cryptographic unit.

B.5.4.3.1. Electrical and mechanical interfaces.

The cryptographic equipment is compatible with MIL-STD-188-114A and EIA-422-A. The cryptographic equipment will appear to the VTU as a DCE (data circuit-terminating equipment). The cryptographic equipment will appear to the network interface equipment as a data terminal equipment (DTE). See Figure B.3.

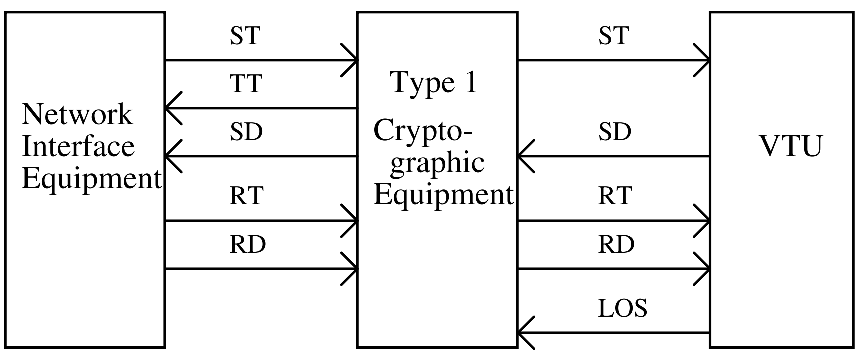


Figure B.3. EIA-449/EIA-422-A Electrical interface for VTU, cryptographic device, and network interface device.

All of the signal lines connecting the cryptographic equipment to the VTU and the network interface equipment shall have differential balanced connections.

The interface between the network interface equipment and the cable to the cryptographic equipment shall include the following signals: Send Timing (ST), Terminal Timing (TT), Send Data (SD), Receive Timing (RT), and Receive Data (RD). See Table B.1. This interface shall conform to the specifications of EIA-449 (mechanical) and EIA-422-A (electrical). The cryptographic equipment does not generate a clock signal to the network interface equipment. Rather, the TT signal is derived by the cryptographic equipment from the ST signal provided by the network interface equipment. A minimum of one synchronous EIA-449 attachment port shall be provided on the VTU to provide capability to connect to a cryptographic device. The electrical characteristics shall be as specified in EIA-422-A for balanced voltage digital-interface circuits.

The interface between the VTU and the cable to the cryptographic equipment shall include, in accordance with EIA-449 and EIA-422-A, the signals ST, SD, RT, and RD. The interface shall also use a nonstandard loss of synchronization (LOS) signal. This LOS signal shall be balanced, in accordance with EIA-422-A, with pin 3 designated as the "A" lead and pin 21 as the "B" lead.

SIGNAL	EIA-449 PINS		DESCRIPTION
	A LEAD	B LEAD	
LOS	3	21	Loss of Synchronization
RD	6	24	Receive Data
RT	8	26	Receive Timing
SD	4	22	Send Data
ST	5	23	Send Timing
TT	17	35	Terminal Timing

TABLE B.1. Type 1 Cryptographic equipment interface signals.

B.5.4.3.2. Resynchronization.

The VTU shall be able to provide a resynchronization signal to Type 1 cryptographic equipment. Detection of loss-of-sync and initiation of an automatic resynchronization by the VTU is required to support real-time VTC.

During normal operation, the VTU shall express a logic "1," in accordance with EIA-422-A, paragraph 4.1, on the LOS line to the cryptographic equipment. If the VTU loses frame alignment, as defined in ITU-T Recommendation H.221, paragraph 2.3, *Loss and Recovery of Frame Alignment*, the VTU shall express a logic "0" pulse with a duration not less than 2^{18} bits plus 3.0 milliseconds and less than 2^{19} bits plus 3.0 milliseconds on the LOS line.

The logic "0" pulse shall also be in accordance with EIA-422-A, paragraph 4.1. Type 1 cryptographic equipment will continue to provide the clock signal and hold the Receive Data (RD) signal line at a logic "0" while it resynchronizes. The VTU shall restart the Type 1 resynchronization process, as defined in this paragraph, within 30 seconds after both of the following conditions have been met:

a. the LOS line has returned to logic "1"; and
b. the VTU is unable to find the frame alignment, as defined in ITU-T Recommendation H.221.

This process shall continue until frame alignment is achieved.

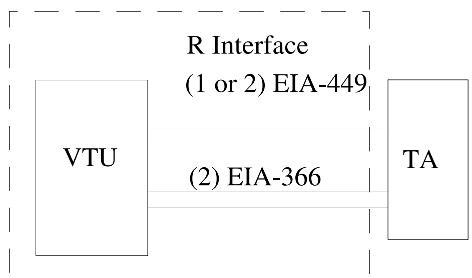
B.6. Subnetwork-type dependent requirements.

B.6.1. ISDN Basic Rate Interface (BRI).

ISDN interfaces are optional. Two optional interfaces are specified in 6.3.1.1 and 6.3.1.2 of the Profile. Further details regarding option 2 are specified in B.6.1.1 below. A third option for classified operation is also included in B.6.1.2.

B.6.1.1. Option 2, External terminal adapter with dialing interface.

This addresses additional requirements to 6.3.1.2 of this Profile.



(Interior of dashed-line polygon indicates scope of profile)

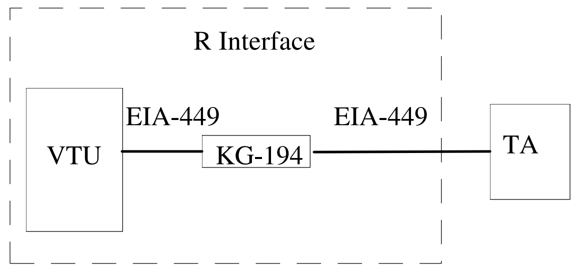
Figure B.4. Option 2, External TA with dialing interface.

The EIA-366-A dialing interface is not permitted to be physically or electrically connected during classified operation. (See Figure B.8 in B.7.5.1.2 for a typical configuration.) Note that if the VTU user specifies the one EIA-449 port version, and two B channels are used, the necessary IMUX function to go from a single channel to two B channels must be performed by the TA. See Figure B.4.

In the dual-port version, the IMUX function is performed within the VTU.

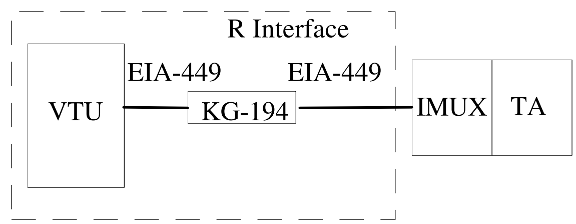
B.6.1.2. Option 3, Classified operation.

Option 3 is for Type 1 classified operation, in accordance with B.5.4.3. The VTU shall use only one EIA-449 port, as described in B.5.4.3.1, and B.5.4.3.2. See Figures B.5 and B.6.



(Interior of dashed-line polygon indicates scope of profile)

Figure B.5. Option 3, Classified operation with single channel.



(Interior of dashed-line polygon indicates scope of profile)

Figure B.6. Option 3, Classified operation with multiple channels.

Dialing must be performed on the network side of the cryptographic device. In this option, dialing is typically done through the TA. (See Figure B.9 in B.7.5.1.3 for a more detailed configuration.) No physical or electrical connection between the VTU and the network or network interface is permitted other than through the cryptographic device. Note that if two B channels are used, the necessary IMUX function to go from a single channel to two B channels must be performed by the IMUX/TA, as shown in Figure B.6.

B.7. Notes.

(This section contains information of a general or explanatory nature that may be helpful; however, the section is not mandatory.)

B.7.1. Acquisition guidance.

B.7.1.1. Nondevelopmental items.

The selected minimum essential (mandatory) requirements identified in this Profile should allow maximum flexibility by permitting nondevelopmental item (NDI) or commercial off-the-shelf (COTS) acquisition.

B.7.1.2. Tailoring.

To ensure proper application of this Profile, invitations for bids, requests for proposals, and contractual statements of work should tailor the requirements in paragraphs 5, 6, B.5, and B.6 of this Profile to exclude any unnecessary options. For procurement of new equipment, the mandatory portions must be included, but it is up to the individual to decide which options should be procured.

B.7.1.3. Mandatory optional.

The term *mandatory optional* for a given feature is not used in this Profile but is sometimes used in procurement contracts to indicate that a vendor must include pricing on features that the purchaser has the option of buying under the contract. Care must be taken to distinguish between the language of the Profile and the language of the procurement contract, since they serve different purposes. A feature that is optional in the Profile could be mandatory, mandatory optional, optional, or omitted entirely from the procurement contract, depending on the user's needs.

B.7.1.4. Software upgrades.

It is recommended that procurement officials add language to their contracts to mandate that upgrades or enhancements to the VTU be implemented in software as much as possible. Having upgrades in software instead of hardware will usually allow for more cost-effective changes.

B.7.1.5. Overseas conferences.

It is recommended that procurement officials require the A-law audio coding option, as specified in 5.3.2.1, if it is anticipated that overseas conferences with non-DOD sites will be held.

B.7.1.6. Electrical and mechanical interfaces.

For classified operation with KG-194 cryptographic devices, it is recommended that the procuring agency specify the electrical and mechanical interfaces of the cables connecting the KG-194 at both the network interface and the VTU. For ISDN TAs an EIA-449 to EIA-530 cable may be required since TAs typically do not have EIA-449 interfaces.

B.7.1.7. Audio.

B.7.1.7.1. Audio subsystem.

It is the responsibility of the room audio subsystem to provide the specified electrical input level to the VTU, and to amplify the specified output electrical level from the VTU to the proper acoustic level. In addition, it may cancel or suppress echoes, mix various microphones, and distribute signals to loudspeakers. These functions are room-dependent and are outside the scope of this Profile. For guidance in obtaining the proper audio levels, see ITU-T Recommendations P.30, P.34, P.50, P.51, and P.64.

B.7.1.7.2. Narrowband speech mode.

The 0F (framed) modes are for audio data rates of 56 kbit/s (unrestricted network) and 48 kbit/s (restricted network).

B.7.1.7.3. Audio at $p = 1$.

For operation at $p = 1$ use of G.711 or G.722 will result in an audio-only connection. To obtain audio and video at $p = 1$, use G.728 audio.

B.7.1.8. Video.

B.7.1.8.1. Video picture-quality definition.

Procurement officials should be aware that video picture-quality standards are not yet mature. Acquisition authorities should take measures to ensure levels of video picture-quality necessary for their applications, especially when acquiring a variety of products from different vendors. One method of doing this is by requesting demonstrations of picture quality while interoperating with different vendors.

B.7.1.8.2. Freeze-frame picture quality.

The limiting factors in freeze-frame video quality are often the cameras and monitors. Typically, the resolution of the cameras and monitors is designed for the motion video resolution and may not provide the desired freeze-frame picture quality. For example, the freeze-frame resolution of 4 x FCIF (704 x 576 pels) exceeds the specifications of NTSC cameras and monitors (maximum 480 horizontal lines). To make full use of the 4 x FCIF resolution, special cameras and monitors have to be procured.

B.7.1.8.3. Picture format (resolution).

If the user requires the VTU to operate at a rate equal to or greater than $p = 6$, then it is recommended that the VTU also have the capability for FCIF resolution at rates equal to and above $p = 2$.

B.7.2. TEMPEST recommendations.

B.7.2.1. General.

The following are recommendations only (not mandatory). TEMPEST requirements for secure VTC systems should be applied case by case, in accordance with MILDEP or DOD TEMPEST requirements. TEMPEST protection must be considered if the VTU is being used for the processing of classified information.

Any equipment certified under NACSIM 5100A is still acceptable for use under NSTISSAM TEMPEST/1-92 (see B.7.2.3). There are both facility and equipment TEMPEST zones. A facility TEMPEST zone is a defined area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated without emanating electromagnetic radiation beyond the controlled space boundary of the facility. NOTE: Facility TEMPEST zones are determined by measuring electromagnetic attenuation provided by a building's properties and the free space loss to the controlled space boundary. Equipment TEMPEST zone assignments are based on the level of compromising emanations produced by the equipment.

B.7.2.2. TEMPEST requirements.

TEMPEST requirements should be referred to the individual MILDEPs as follows:

- Air Force - Information Warfare Center
- Army - Intelligence Security Command
- Navy and Marine Corps - Naval Electronic Systems Security Command
- NSA - NSA TEMPEST Advisory Group

Below are the addresses of the commands:

Air Force: Commander
Air Force Information Warfare Center/EAC
San Antonio, TX 78243-5000

Army: Commander	
	TEMPEST Det 902 MI GP ATTN: IAGPA-A-VH Vint Hill Farms Station Warrenton, VA 22186-5126
Navy/ Marine Corps:	Naval Electronic Systems Security Engineering Center ATTN: INFOSEC Department 3801 Nebraska Avenue, NW Washington, DC 20393-5270
NSA:	Department of Defense National Security Agency TEMPEST Advisory Group ATTN: C9 Fort George G. Meade, MD 20755-6000

For DOD agencies not listed above, contact the NSA office for information.

B.7.2.3 TEMPEST documents.

TEMPEST requirements are stated in the following documents or their latest revision:

NACSIM 5100A	*Compromising Emanations Laboratory Test Requirements, Electromagnetics. National Security Telecommunications and Information System Security (NSTISS)*
NTISSI 7000	*National Telecommunications and Information Systems Security Instruction, TEMPEST Countermeasures for Facilities, 7 October 1988*
NTISSP 300	*National Telecommunications and Information Systems Security Policy, National Policy on the Control of Compromising Emanations, 3 October 1988*
NSTISSAM TEMPEST/1-92	*Compromising Emanations Laboratory Test Requirements, Electromagnetics. National Security Telecommunications and Information System Security (NSTISS)*
	Commercial COMSEC Endorsement Program Procedures, 31 August 1987, National Security Agency
	INFOSEC System Security Products & Services Catalog, October 1990, National Security Agency

The above documents can be obtained from:

National Telecommunications & Information
Systems Security Committee
Director, NSA
Fort George G. Meade, MD 20755-6000

OPNAVINST C5510.93E	*Navy Implementation of National Policy on Control of Compromising Emanations, 22 February 1988, with OPNAVNOTE C 5510 of 13 October 1990*
AR 380-19-1	*Control of Compromising Emanations, September 1990 (Army)*

B.7.3. Type 3 Cryptographic equipment - export restrictions.

Type 3 is for transmission of unclassified sensitive information. Use of the DES algorithm outside the DOD community is beyond the scope of this Annex. DES is an export-controlled algorithm. Export of the DES algorithm is handled case by case. Commercial export is controlled by the State Department. FIPS PUB 46-1 and FIPS PUB 140-1 contain information concerning the export of DES.

B.7.4. Classified operation over restricted networks.

Type 1 data encryption from a VTU operating on an unrestricted network, in restricted mode, will result in encryption of the bit 8 sub-channel. A gateway between the unrestricted network and a restricted network will remove the bit 8 sub-channel. This results in corruption of the encrypted data, such that the far-end cryptographic equipment is not able to properly decrypt the data back into the original bit pattern.

For operation of VTUs using Type 1 security over an unrestricted network connected to a restricted network, the following procedure should be used: Each VTU is connected through a cryptographic device to a network interface device (that is, an inverse multiplexer (IMUX), or a terminal adapter). The network interface device at the unrestricted network must interface to the cryptographic device at multiples of 56 kbit/s and perform the bit 8 sub-channel stuffing/stripping for the unrestricted network. The cryptographic device and the VTU at both ends of the network receive network timing at 56 kbit/s. This approach puts the encrypted data in bits 1 to 7 only. These bits will not be affected by the gateway, and the encrypted data will not be corrupted.

B.7.5. Network access alternatives.

Network interfaces, except for those specified in 6.3.1, 6.4, and B.6.1 are outside the scope of this Profile. The following is for information only.

B.7.5.1. ISDN access alternatives.

Paragraphs 6.3.1, 6.4, and B.6.1 of the Profile specify several options for connecting to ISDN, but do not preclude the use of other alternatives. This paragraph and its subparagraphs describe various methods of basic rate interface (BRI) ISDN connectivity. VTU vendors may integrate some of this equipment into their profile-compliant designs. Paragraph B.7.5.1.3 addresses Type 1 classified operation. Paragraphs B.7.5.1.1, B.7.5.1.2, B.7.5.1.4, and B.7.5.1.5 address unclassified and unclassified sensitive operation. For unclassified sensitive operation, the VTU and the Type 3 cryptographic equipment are typically integrated into a single physical unit.

Three physical interfaces are associated with ISDN: the R interface, the S/T interface, and the U interface. It is recommended that if the S/T interface is provided, it be in accordance with ANSI T1.605, *ISDN Basic Access Interface for S and T Reference Points* (Layer 1 Specification). It is recommended that if the U interface is provided, it be in accordance with ANSI T1.601, *ISDN Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT* (Layer 1 Specification).

B.7.5.1.1. External terminal adapter.

Figure B.7 shows a typical configuration, including the interface between the VTU and the separate terminal adapter, which is the R interface.

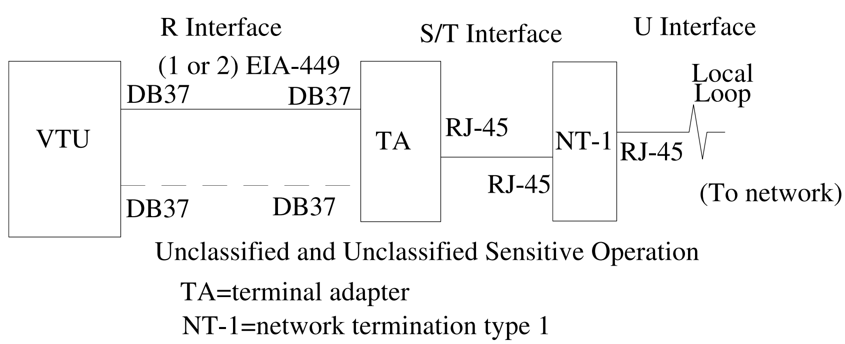


Figure B.7. Network configuration for external terminal adapter.

The R interface of the VTU consists of two 56/64 kbit/s EIA-449 ports, or one 112/128 kbit/s EIA-449 port. Paragraph 6.3.1.1 also makes use of this configuration. If the VTU has one port, the external terminal adapter will have to include an inverse multiplexing function to create the two B channels from the one VTU port and vice versa. This version is for unclassified or Type 3 unclassified, sensitive operation.

B.7.5.1.2. External terminal adapter with dialing interface.

Figure B.8 shows a typical configuration, including the interface between the VTU and the separate terminal adapter, which is the R interface.

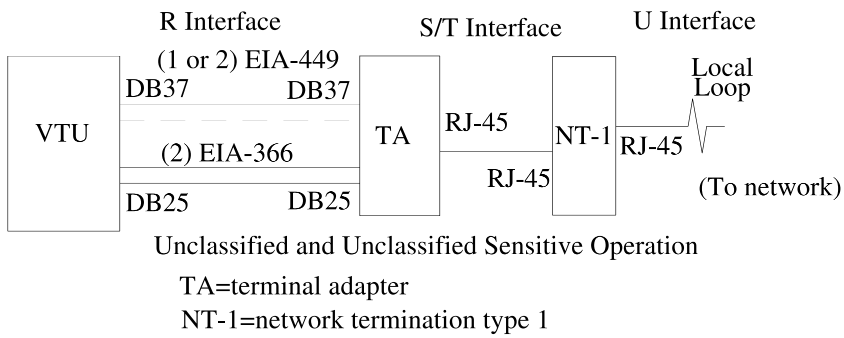


Figure B.8. Network configuration for external terminal adapter with EIA-366 dialing interface.

The R interface of the VTU consists of two 56/64 kbit/s EIA-449 ports, or one 112/128 kbit/s EIA-449 port. The R interface also includes two EIA-366-A dialing interfaces: one for each B channel. Paragraphs 6.3.1.2 and B.6.1.1 also make use of this configuration. If the VTU has one port, the external terminal adapter will have to include an inverse multiplexing function to create the two B channels from the one VTU port and vice versa. This configuration is for unclassified or Type 3 unclassified, sensitive operation. Type 1 classified operation is not permitted.

B.7.5.1.3. Classified operation.

For Type 1 classified operation, the cryptographic equipment is added at the R interface, as shown in Figure B.9.

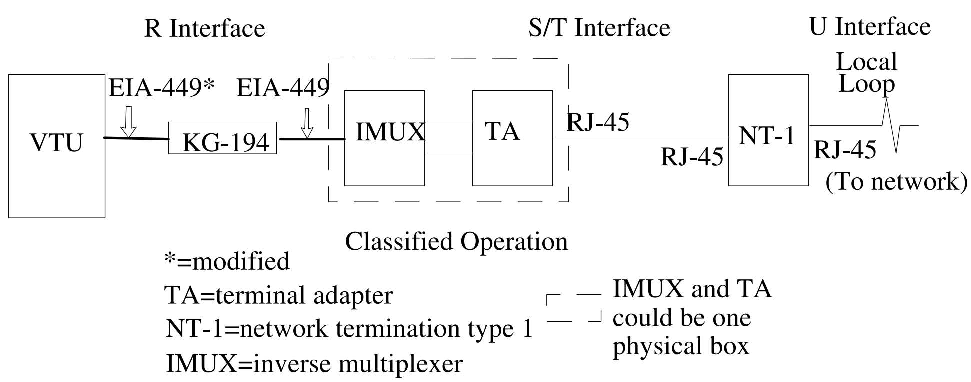


Figure B.9. Network configuration for classified operation.

If the VTU has the EIA-366 port, there can be nothing physically connected to it during a classified conference.

B.7.5.1.4. Integrated terminal adapter.

Figure B.10 shows a diagram of this configuration.

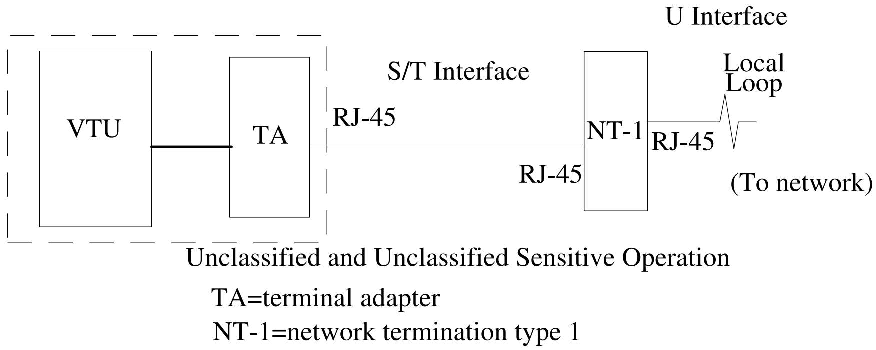


Figure B.10 Network configuration for integrated Terminal Adapter.

The terminal adapter is integrated with the VTU into a single physical unit. The NT-1 is physically separate. This is only for unclassified and unclassified, sensitive operation. In this case, the integrated unit will provide the S/T interface to the Type 1 network termination. The connector at the S/T interface is an RJ-45. Type 1 classified conferencing is not permitted with this configuration.

B.7.5.1.5. Integrated terminal adapter and network termination.

Figure B.11 shows a diagram of this configuration.

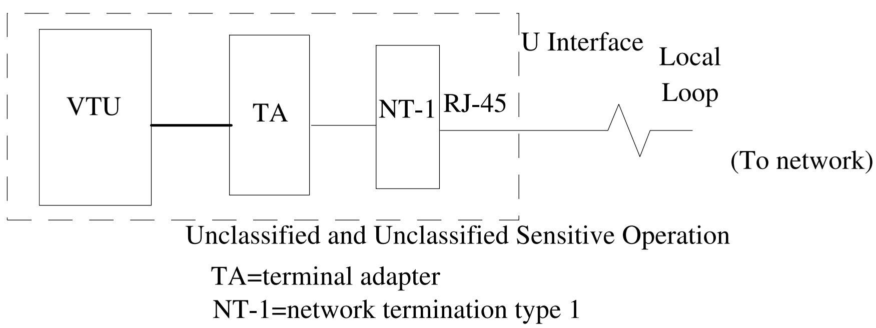


Figure B.11. Network configuration for integrated TA and NT1.

This is only for unclassified and unclassified, sensitive operation. The VTU, TA and NT! are integrated into a single physical unit. The integrated unit will now provide the U interface for the network. Type 1 classified conferencing is not permitted with this configuration.

B.7.5.2. Inverse multiplexers.

To provide interoperability between inverse multiplexers, the following is recommended.

B.7.5.2.1. Unclassified operation.

An inverse multiplexer (IMUX) is used to connect a single-channel VTU to a multiple-channel VTU through a multiple-channel network. The VTU is connected to an IMUX.

The IMUX-Network-IMUX connection provides a clear data channel at a specified data rate (that is, 128 kbit/s). At the other end, the IMUX is connected to the other VTU.

The IMUX operates in Mode 1, as defined in ANSI T1A-EIA-619 (formerly known as the BONDING standard). In this mode, the IMUX-Network-IMUX interface initially operates in a framed mode to achieve channel synchronization. When synchronization is achieved, the framing is dropped and the entire channel capacity is used for transmitting the data stream.

The IMUX-VTU interface is at the same data rate (that is, 128 kbit/s) as the total data rate (2 x 64 kbit/s) of the IMUX-Network interface. This is because the IMUX-Network data streams do not contain framing information.

Setup and control of the IMUX can be done manually or automatically. Loss of synchronization between the network channels must be detected and reset manually by initializing the IMUX to a framed mode, as described above.

B.7.5.2.2. Classified operation.

The VTU is connected to a cryptographic device (KG-194). The cryptographic device is then connected to an IMUX. The IMUX-Network-IMUX connection provides a clear data channel at a specified data rate (128 kbit/s). At the other end, the IMUX is connected to a cryptographic device (KG-194). The cryptographic device is connected to the far-end VTU.

The IMUX operates in Mode 1, as defined in ANSI T1A-EIA-619. In this mode, the IMUX-Network-IMUX interface initially operates in a framed mode to achieve channel synchronization. When synchronization is achieved, the framing is dropped and the entire channel capacity is used for transmitting the encrypted data stream. Since the framing information is encrypted, no capabilities can be communicated between the terminal and the IMUX.

The IMUX-KG interface is at the same data rate (128 kbit/s) as the total data rate (2 x 64 kbit/s) of the IMUX-Network interface. This is because the IMUX-Network data streams do not contain framing information.

Setup and control of the IMUX must be done manually to ensure RED-BLACK separation. No VTU-to-IMUX communication or electrical connection is allowed. Loss of synchronization between the network channels must be detected and reset manually by initializing the IMUX to a framed mode, as described above.

B.7.5.3. Other network interfaces.

The VTU may support additional interfaces to the TA, which are outside the scope of this Profile. Below are some examples of such interfaces:

- V.35
- Dual V.35
- V.35 with EIA-366-A
- Dual V.35 with dual EIA-366-A
- X.21
- Dual X.21

The VTU may also support direct network interfaces, which are outside the scope of this Profile. Below are some examples of direct network interfaces:

- Primary rate ISDN interface
- North America T1 interface
- 2-wire switched 56-kbit/s interface
- 4-wire switched 56-kbit/s interface.

B.7.6. Content.

This Profile including the annexes does not address the following areas:

- Analog videoconferencing
- Transmission data rates below 56 kbit/s
- Transmission data rates above 1920 kbit/s
- Network considerations
- Conference dialing and hookup
- Conference scheduling
- Multipoint
- Operational security procedures
- Simplex and broadcast modes of operation
- Key management

Some of these, including multipoint will be addressed in future versions of the Profile.