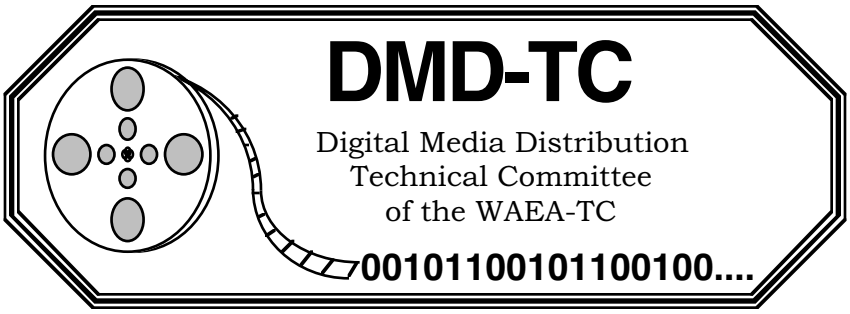

WAEA SPECIFICATION 0395

Content Delivery for In-Flight Entertainment

November 6, 2001

Version 2.0

As Amended and Approved by the
World Airline Entertainment Association
Technology Committee, November 6, 2001.
(Original Version 1.1 Approved June 7, 1996.)

IMPORTANT NOTICES

This document is a specification adopted by the World Airline Entertainment Association (WAEA). This document may be revised by the WAEA. It is intended solely as a guide for companies interested in developing products which can be compatible with other products developed using this document. WAEA makes no representation or warranty regarding this document, and any company using this document shall do so at its sole risk, including specifically the risks that a product developed will not be compatible with any other product or that any particular performance will not be achieved. WAEA shall not be liable for any exemplary, incidental, proximate or consequential damages or expenses arising from the use of this document. This document defines only one approach to compatibility, and other approaches may be available to the industry.

This document is an authorized and approved publication of WAEA. Only WAEA has the right and authority to revise or change the material contained in this document, and any revisions by any party other than WAEA are unauthorized and prohibited.

Compliance with this document may require use of one or more features covered by proprietary rights (such as features which are the subject of a patent, patent application, copyright, mask work right or trade secret right). By publication of this document, no position is taken by WAEA with respect to the validity or infringement of any patent or other proprietary right. WAEA hereby expressly disclaims any liability for infringement of intellectual property rights of others by virtue of the use of this document. WAEA has not and does not investigate any notices or allegations of infringement prompted by publication of any WAEA document, nor does WAEA undertake a duty to advise users or potential users of WAEA documents of such notices or allegations. WAEA hereby expressly advises all users or potential users of this document to investigate and analyze any potential infringement situation, seek the advice of intellectual property counsel, and, if indicated, obtain a license under any applicable intellectual property right or take the necessary steps to avoid infringement of any intellectual property right. WAEA expressly disclaims any intent to promote infringement of any intellectual property right by virtue of the evolution, adoption, or publication of this document.

Foreword

The Digital Media Distribution Technical Committee (DMD-TC) was formed on December 9, 1994, as a sub-committee of the World Airline Entertainment Association (WAEA) Technical Committee. The DMD-TC membership includes representatives from a broad range of organizations associated with the In-Flight Entertainment (IFE) industry as well as invited experts from outside the industry. The membership includes representatives of airlines, IFE equipment providers, movie studios and post-production houses, and experts in the fields of digital video, video compression, and security. The charter of the DMD-TC is to identify and standardize specifications for the distribution of digital entertainment media to In-Flight Entertainment systems.

Specification WAEA 0395 is the result of the committee's first project (DMD-95-1: Content Delivery for In-Flight Entertainment). This specification identifies and standardizes several aspects of source media, digitization, compression and encoding, encryption, duplication and distribution media. Much of this specification comprises references to other international and industry specifications with parameterizations for the specific needs of the IFE industry. By utilizing other standards, the DMD-TC and WAEA have aligned this specification with the broader trends in the digital multimedia industries.

The DMD-TC adopted version 1.1 of this specification in April 1996, which was subsequently approved by the WAEA Technical Committee in June 1996. This version 2.0 incorporates amendments and errata considered and adopted by the Digital Content Management Working Group of the WAEA during the fall of 2001 and approved by the WAEA Technology Committee in November 2001.

Specification WAEA 0395 is organized as follows: Sections 1 and 2 provide a brief introduction describing the purpose and scope of this specification. Sections 3 and 4 list references to other specifications and documents found in the normative and informative sections respectively. Sections 5, 6 and 7 provide definitions of terms, acronyms, and a description of conventions used in this document. Section 8 defines the general reference model for systems and processes that are the subject of this specification. This section identifies the interfaces and processes that are specified in this document. The normative requirements mandated by this specification are found in sections 9, 10, and 11. Section 9 deals with interface requirements. Section 10 describes security requirements. Section 11 covers quality assurance. Sections 12 and 13 provide normative and informative annexes respectively.

1. Introduction

1.1 Purpose

The purpose of this specification is to define methods of creating, formatting, and delivering digital media to IFE systems. The DMD-TC recognizes that the commercial industry has created broad standards in this general area, including Moving Picture Experts Group (MPEG) and Digital Video Broadcast (DVB). Wherever possible, this specification draws from those standards and applies them to this application. However, it is believed that this specification is needed for the following reasons:

The first is that other specifications generally allow some range of options to be chosen by the user. By agreeing in this specification to constrain the use of digital media to some subset of these broader standards, greater inter-operability will be achieved between movie studios or post-production houses (the providers of digital media), and the various IFE platforms.

The second reason for a unique specification is that there are certain requirements that are somewhat unique to IFE applications. For example, IFE systems are required to provide robust support for multiple languages, either as subtitles or supplementary audio programs, associated with a single video program. Also, IFE systems are generally constrained with respect to processing, storage capacity, communication bandwidth, and screen resolution as a result of requirements imposed on airborne systems for very low power, size and weight.

1.2 Overview of Applications

There are many IFE applications that might use digital media. In the interest of generating this specification in a timely manner, the DMD-TC has decided to first address a set of core applications. Future versions of this specification may be created which address other applications. The core applications addressed in this version are as follows:

a) Feature Entertainment

b) Short Subjects (including advertising)
c) News Features
d) Sports Features
e) Specialty Videos (Safety, Destination, Passenger Messages)
f) Television Series
g) Music and Audio Programs
h) Program Specific Information

1.3 Reference Model

This specification defines an overall system reference model, which provides an abstract description of the overall process of creating digital media and delivering it to IFE systems. The reference model identifies functions and interfaces between those functions. A detailed description of the system reference model is found in Section 8.

1.4 Interfaces

This specification specifies requirements for key interfaces in the reference model in order to ensure interchangeability of data across those interfaces.

2. Scope

This specification describes the specifications for content delivery to IFE systems. This comprises detailed specifications for source media, digitization, compression and encoding, security, and distribution media. The scope of these specifications provides for the ability to deliver digital audio-visual content from its origin to digital file servers aboard aircraft. This specification is limited to applications where source media are encoded prior to being delivered to the aircraft.

3. Normative References

The following international and industry standards contain provisions that, through reference in this text, constitute provisions of this specification. At the time of publication, the editions indicated were valid. All of these referenced standards are subject to revision, and parties to agreements based on this specification are encouraged to investigate the possibility of applying the most recent editions of the referenced standards indicated below. Members of the International Electrotechnical Commission (IEC) and the International Standards Organization (ISO) maintain registers of currently valid International Standards.

ARINC 485	Cabin Management and Entertainment System Protocols.
ARINC 628	Cabin Equipment Interfaces.
DMD-TC/CFC1/005	“English Language Caption Contribution Format”.
FIPS 46-3	Data Encryption Standard. National Institute of Standards and Technology. October 25, 1999. Available from <http://www.itl.nist.gov/fipspubs>.
ICAO Document 8585	“Designators for Aircraft Operating Agencies, Aeronautical Authorities and Services”, International Civil Aviation Organization.
IEC Publ. 908:1987	“CD Digital Audio System”.
IGMP RFC 1112	“Host Extensions for IP Multicasting”.
ISO 639	“Terminology - Codes for the Representation of Names of Languages”.
ISO 3166	“Codes for the Representation of Names of Countries”.
ISO 8859:1987	“Information processing - 8-bit single-byte coded graphic character sets, Latin alphabets”.
ISO/IEC 11172-1:1993	“Information Technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbps, Part 1: Systems” (a.k.a., MPEG-1 Systems).

ISO/IEC 11172-2:1993	“Information Technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbps, Part 2: Video” (a.k.a., MPEG-1 Video).
ISO/IEC 11172-3:1993	“Information Technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbps, Part 3: Audio” (a.k.a., MPEG-1 Audio).
ISO/IEC 13818-1:1996	"Information Technology - Generic coding of moving pictures and associated audio information, Part 1: Systems" (a.k.a., MPEG-2 Systems).
ISO/IEC 13818-2:1996	"Information Technology - Generic coding of moving pictures and associated audio information, Part 2: Video" (a.k.a., MPEG-2 Video).
ISO/IEC 13818-3:1995	"Information Technology - Generic coding of moving pictures and associated audio information, Part 3: Audio" (a.k.a., MPEG-2 Audio).
ISO/IEC CD 13522-5	“Information Technology - Coding of Multimedia and Hypermedia Information. Part 5: MHEG Subset for Base Level Implementation”.
Rec. ITU-R BT.601.4	“Encoding parameters of digital television for studios” (equivalent to CCIR 601).
Rec. ITU-R BR.648	“Digital recording of audio signals”.
SMPTE RP-186-1995	“Video Index Information Coding for 525 and 625 Line Television Systems”, Society of Motion Picture and Television Engineers.
WAEA 1289-2, Rev. 1	“Specifications for Mastertape Recording and Tape Duplicating of Airborne Audio Entertainment Systems”, World Airline Entertainment Association, January 1993.

4. Informative References

The following references contain information that relates to this specification, but are not provisions of this specification. At the time of publication, the editions indicated were valid.

EBTU Tech 3264-E, Specification of EBU Subtitling Data Exchange Format, European Broadcasting Union, Geneva, Switzerland, February 1991.

ECMA-169 Standard: 8 mm Wide Magnetic Tape Cartridge Dual Azimuth Recording - Helical Scan Recording.

ECMA-171 Standard: 3.81 mm Wide Magnetic Tape Cartridge for Information Interchange - Helical Scan Recording - DDS-2 Format Using 120 m Length Tapes.

ECMA-182 Standard: Data Interchange on 12.7 mm 48-Track Magnetic Tape Cartridges - DLT 1 Format.

ECMA-197 Standard: Data Interchange on 12.7 mm 112-Track Magnetic Tape Cartridges - DLT 2 Format.

ECMA-209 Standard: Data Interchange on 12.7 mm 128-Track Magnetic Tape Cartridges - DLT 3 Format.

ECMA-231 Standard: Data Interchange on 12.7 mm 128-Track Magnetic Tape Cartridges - DLT 4 Format.

ECMA-246 Standard: 8 mm Wide Magnetic Tape Cartridge for Information Interchange - Helical Scan Recording - AIT-1 Format, 2nd ed.

ECMA-258 Standard: Data Interchange on 12.7 mm 128-Track Magnetic Tape Cartridges - DLT 3-XT Format.

ECMA-259 Standard: Data Interchange on 12.7 mm 128-Track Magnetic Tape Cartridges - DLT 5 Format.

ECMA-278 Standard: Data Interchange on 12.7 mm 128-Track Magnetic Tape Cartridges – Parallel Serpentine Format, 2nd ed.

ECMA-286 Standard: Data Interchange on 12.7 mm 128-Track Magnetic Tape Cartridges - DLT 6 Format, 2nd ed.

ECMA-291 Standard: 8 mm Wide Magnetic Tape Cartridge for Information Interchange - Helical Scan Recording AIT-1 with MIC Format

ECMA-292 Standard: 8 mm Wide Magnetic Tape Cartridge for Information Interchange - Helical Scan Recording AIT-2 with MIC Format

"The Protection of Computer Software - Its Technology and Application", edited by Derrick Grover, British Imformatics Society, 1992.

R.L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM*, 21(2): 120-126, February 1978.

RSA Laboratories. *Frequently Asked Questions About Today's Cryptography, version 4.1, May 2000*. Available from <http://www.rsasecurity.com/rsalabs/faq/>.

Schneier, Bruce. *Applied Cryptography*, Second Edition (fifth printing or greater). John Wiley & Sons, 1996.

5. Definitions

bit rate The rate at which the compressed bit stream is delivered from the channel to the input of a decoder.

byte aligned A bit in a coded bit stream is byte-aligned if its position is a multiple of 8-bits from the first bit in the stream.

compression Reduction in the number of bits used to represent an item of data.

constant bit rate; CBR Operation where the bit rate is effectively constant from start to finish of the bit stream.

control word An encrypted data item. Its clear form is used to encrypt/decrypt audio, video or coded data.

D-pictures A D-picture, or dc coded picture, is coded using information only from itself. Of the DCT coefficients, only the dc ones are present.

data element An item of data as represented before encoding and after decoding.

decoded stream The decoded reconstruction of a compressed bit stream.

decoder An embodiment of a decoding process.

decoding (process) The process that reads an input coded bit stream and outputs decoded pictures or audio samples.

digital storage media A digital storage or transmission device or system.

encryption The alteration of the characteristics of a data element using strong cryptographic algorithms to prevent unauthorized use.

entitlement control message; ECM
Entitlement Control Messages are private conditional access information which specify control words and possibly other, typically stream-specific, scrambling and/or control parameters.

entitlement management message; EMM
Entitlement Management Messages are private conditional access information which specify the authorization levels or the services of specific decoders. They may be addressed to single decoders or groups of decoders.

elementary stream A generic term for one of the coded video, coded audio or other coded bit streams in PES packets.

encoder An embodiment of an encoding process.

encoding (process) A process that reads a stream of input pictures or audio samples and produces a coded bit stream.

I-frame An I-frame, or intra-coded picture, is coded using information only from itself (without motion compensation prediction).

key A data item used with a cryptographic algorithm for encryption/decryption.

packetized elementary stream; PES
The data structure used to carry elementary stream data in MPEG-2 Systems. A PES packet consists of a PES packet header followed by a number of contiguous bytes from an elementary data stream.

pel Picture element, a single addressable point in a raster display. Also sometimes referred to as a pixel.

presentation time-stamp; PTS
A field that may be present in a PES packet header that indicates the time that a presentation unit is to be presented by the system target decoder.

program A program is a collection of program elements. Program elements may be elementary streams. Program elements need not have any defined time base; those that do, have a common time base and are intended for synchronized presentation.

Program Clock Reference; PCR
A time stamp in the Transport Stream from which decoder timing is derived.

Program Specific Information; PSI
PSI consists of normative data that is necessary for the demultiplexing of Transport Streams and the successful regeneration of programs.

reserved The term reserved, when used in the clauses defining the coded bit stream, indicates that the value may be used in the future for WAEA defined extensions. Unless otherwise specified within this specification, all reserved bits shall be set to 1.

transport stream A transport stream combines one or more elementary program streams with one or more independent time bases into a single bit stream.

trick modes Stream flow control mechanisms to allow functions such as rewind, fast-forward, pause, etc. during playback of an MPEG stream.

unicode A 16-bit fixed-width character encoding that encompasses virtually all characters widely used in computers.

video buffer verifier; VBV
A hypothetical decoder that is conceptually connected to the output of the encoder. Its purpose is to provide a constraint on the variability of the data rate that an encoder or editing process may produce.

variable bit rate; VBR An attribute of bit streams wherein the rate of arrival of bits at the input to a decoder varies with time.

6. Abbreviations and Symbols

AC3	Audio Compression – 3
ACM	Association for Computing Machinery
AES	Audio Engineering Society
AIT	Advanced Intelligent Tape
ASCII	American Standard Code for Information Interchange (a coding scheme which represents characters numerically).
asctxt	ASCII Text
ATM	Asynchronous Transfer Mode
bslbf	Bit string, left bit first
CBR	Constant Bit Rate
CCIR	Consultative Committee for International Radio

CRC	Cyclical Redundancy Check
DAT	Digital Archive Tape
dB	Decibel
DCT	Digital Component Technology (a digital videotape format). Also, Discrete Cosine Transform (as used in the MPEG compression algorithms).
DDS-2	Digital Data Storage – 2
DES	Data Encryption Standard
DLT	Digital Linear Tape (a digital videotape format)
DMD-TC	Digital Media Distribution Technical Committee
DTS	Digital Theater Sound
DVB	Digital Video Broadcast (a standardization organization)
DVC	Digital Video Cassette
DVD	An acronym for Digital Video Disc and/or Digital Versatile Disc, an audio, video and data optical storage disc.video and data optical storage disc.
DVS	Descriptive Video Services
EBU	European Broadcasting Union
ECM	Entitlement Control Message
ECMA	European Computer Manufacturer Association
EDL	Edit Decision List
EMM	Entitlement Management Message
FAQ	Frequently Asked Questions
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FIR	Finite Impulse Response
FTP	File Transfer Protocol
GB	Gigabytes
GOP	Group of Pictures
HMI	Human Machine Interface
ICAO	International Civil Aviation Organization
IDCT	Inverse Discrete Cosine Transform
IEC	International Electrotechnical Commission
IFE	In-Flight Entertainment
IGMP	Internet Group Management Protocol
IP	Intellectual Property. Also Internet Protocol.
ISO	International Standardization Organization
ITU	International Telecommunications Union
JPEG	Joint Photographic Experts Group
kbps	Kilobits Per Second
MB	Megabytes
Mbps	Megabits Per Second
MHEG	Multimedia and Hypermedia Information Coding Experts Group
mm	millimeter
MPA	Motion Picture Association
MPAA	Motion Picture Association of America
MPEG	Moving Picture Experts Group
NIST	National Institute of Standards and Technology

OC3c	Optical Carrier Level 3 - Concatenated
OMF	Open Media Format
PAX	Passenger
PCR	Program Clock Reference
PEL	Picture Element
PES	Packetized Elementary Stream
PSI	Program Specific Information
PTS	Presentation Time Stamp
RFC	Request For Comments
RSA	Last name initials of the three inventors of the RSA public-key cryptosystem, Drs. R.L. Rivest, A. Shamir, and L. Adleman.
SCSI	Small Computer Systems Interface
SDDS	Sony Dynamic Digital Sound
SIF	Source Input Format (*not* Common Interface Format (CIF))
SMPTE	Society of Motion Picture and Television Engineers
S-VHS	Super VHS (an analog videotape format)
TAR	Tape Archive
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
uimsbf	Unsigned integer, most significant bit first
unitxt	Unicode text file
unistr	Unicode text string
VBV	Video Buffer Verifier
VBR	Variable Bit Rate
VHS	Video Home System (an analog videotape format)
WAEA	World Airline Entertainment Association

7. Conventions

The mathematical operators used to describe this specification are similar to those used in the C programming language. The bitwise operators are defined assuming two's-complement representation of integers. Numbering and counting loops generally begin from 0.

7.1 Operators

7.1.1 Arithmetic Operators

+ Addition.

7.1.2 Relational Operators

< Less than.

: Ratio of two numbers

7.1.3 Bitwise Operators

>> Shift right with sign extension

<< Shift left with 0 fill.

7.1.4 Assignment

= Assignment operator.

7.1.5 Mnemonics

The following mnemonics are defined to describe the different data types used in this specification. The byte order of multi-byte words is most significant byte first.

asctxt file — File containing only seven-bit ASCII character codes. Each line within the file is concluded with a single carriage return, decimal 13. Numbers are represented as integers using either decimal or hexadecimal notation. Numbers are always formatted with the most significant digit left, least significant digit right. All spaces are ignored. An asctxt file has the following features:

Readable and changeable using standard editor.
Easily parsed by software.
Machine independent. Avoids word length and big/little endian issues.

binary file — File with no specific format. All byte values from 0 to 255 may be present.

bslbf — Bit string, left bit first, where "left" is the order in which bit strings are written in this specification. Bit strings are written as a string of 1s and 0s within single quote marks, e.g., '1000 0001'. Blanks within a bit string are for ease of reading and have no significance.

printf arg — Character string interpreted as the arguments to the C standard I/O procedure *printf***.** The \r escape sequence inserts a carriage return. The following conversion characters are used in this specification:

%s Print as ASCII text
%d Print as a decimal number
%x Print as a hexadecimal number

As an example, if *min* equals 125, then the printf arg of

("[running_time] %d\r", min)

yields the string

[running_time] 125

This string is 19 characters long, including the invisible carriage return.

uimsbf — Unsigned integer, most significant bit first.

unistr — String of standard UNICODE character codes (16 bits). Each string is formatted using the C standard, including the end-of-string marker of '0000'.

unitxt file — File solely comprised of packed *unistr*.

7.2 Method of Describing Bit Stream Syntax

The following constructs are used to express the conditions when data elements are present, and are in normal type. Note this syntax uses the "C"-code convention that a variable or expression evaluating to a non-zero value is equivalent to a condition that is true.

while (condition) {
data_element
. . .
}
	If the condition is true, then the group of data elements occurs next in the data stream. This repeats until the condition is not true.

do {
data_element
. . . }
while (condition)
	The data element always occurs at least once. The data element is repeated until the condition is not true.

if (condition) {
data_element
. . .
}
	If the condition is true, then the first group of data elements occurs next in the data stream.

else {
data_element
. . .
}
	If the condition is not true, then the second group of data elements occurs next in the data stream.

for (i = 0;i<n;i++) {
data_element
. . .
}
	The group of data elements occurs n times. Conditional constructs within the group of data elements may depend on the value of the loop control variable i, which is set to zero for the first occurrence, incremented to 1 for the second occurrence, and so forth.

data_element [ ]	data_element [ ] is an array of data. The number of data elements is indicated by the context.
data_element [n]	data_element [n] is the n+1th element of an array of data.
data_element [m][n]	data_element [m][n] is the m+1,n+1th element of a two-dimensional array of data.
data_element [l][m][n]	data_element [l][m][n] is the l+1,m+1,n+1th element of a three-dimensional array of data.
data_element [m..n]	is the inclusive range of bits between bit m and bit n in the data_element.

8. System Reference Model

8.1 Purpose

The system reference model identifies all of the pertinent interfaces between the source media and the IFE system. These interfaces are identified to form a common basis for understanding the overall system requirements. Some, but not all, of these interfaces are specified in this specification.

8.2 Overall System Description

The overall system is shown in the Top Level Reference Model of Figure 1.

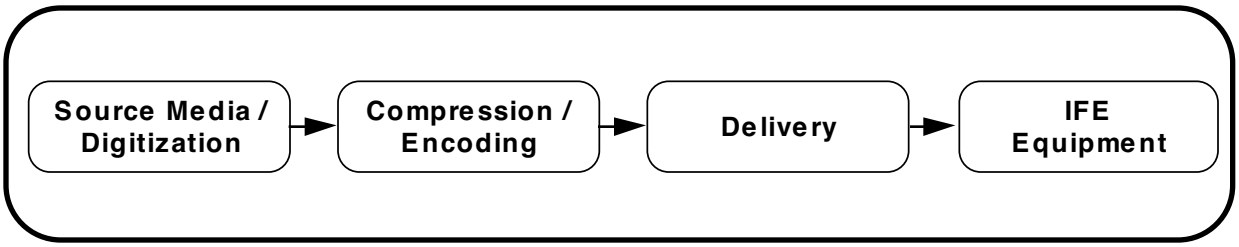

Figure 1 - Top-Level Reference Model

This specification places restrictions on the processes that can take place in the three left-most functions of the reference model in Figure 1 and implies requirements for the right-most function. Additionally, requirements for the syntax and semantics of interfaces between the top-level processes shown in Figure 1 are imposed. Specification of these interfaces further constrains industry standards for video compression.

This overall system deals with getting content from the providers (e.g., film studios), through the laboratories (post-production, compression houses), and through the distribution process for secure delivery to servers that are part of the IFE equipment. From an onboard server, through the distribution infrastructure, to the passenger seat, various service capabilities are provided by the IFE equipment manufacturers. For the purposes of this specification the IFE system is considered to be either equipment on board an aircraft or a secure IFE processing facility for the purpose of supporting on-board IFE equipment. A means of assuring acceptance of an IFE processing facility is compliance with the recommendations of an MPA security review.

8.3 Detailed System Description

8.3.1 Source Media/Digitization

The Source Media/Digitization block of the top-level reference model can be further broken into more detail as shown in Figure 2. This process results in CCIR 601 video and other elements as defined in Section 8.3.2.1.

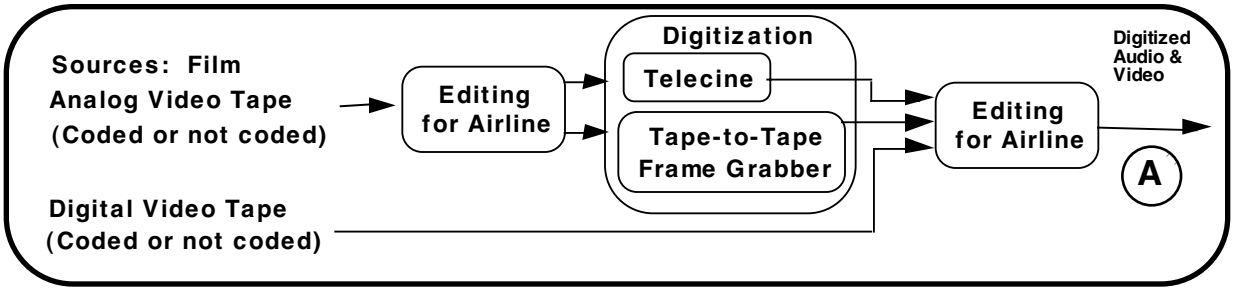

Figure 2 - Source Media/Digitization

8.3.1.1 Source Media

The possible source media may include:

a) **Film:**

- 35 mm, 16 mm, 65/70 mm

b) **Analog Video Tape:**

- Betacam SP & M-II - Analog component
- 1” Type C & Type B - Analog composite
- 3/4” U-matic - Color under analog composite
- VHS, S-VHS, Hi-8, 8 mm Video, Miscellaneous video

c) **Digital Video Tape:**

- SMPTE 240M - High-Definition component digital
- D-1 / DCT / Digital Betacam / D-5 - CCIR-601 component digital
- D-2 / D-3 - composite digital
- DVC - 4:2:0 digital

d) **Program Information Sources:**

- Edit Decision Lists (EDL’s)
- Open Media Format data (OMF)
- Video Indexes
- Security data
- Subtitling and captioning information
- Program Metadata

8.3.1.2 Editing for Airline (analog domain)

In the analog domain, editing includes film editorial processes and video editorial processes.

8.3.1.3 Digitization

This is an analog to digital conversion process. The majority of film digitization is performed by telecine systems. Tape-to-tape processes convert analog video to digital component video.

8.3.1.4 Editing for Airline (digital domain)

In the digital domain, editing includes video editorial processes, program information authoring, and possible further tape-to-tape manipulation. Time compression is not recommended.

8.3.2 Compression/Encoding

The Compression/Encoding block of the top level reference model can be further broken into more detail as shown in Figure 3 and Figure 4. Two possible processes are described based on different data encryption methods. These processes result in compressed, encrypted, digital files.

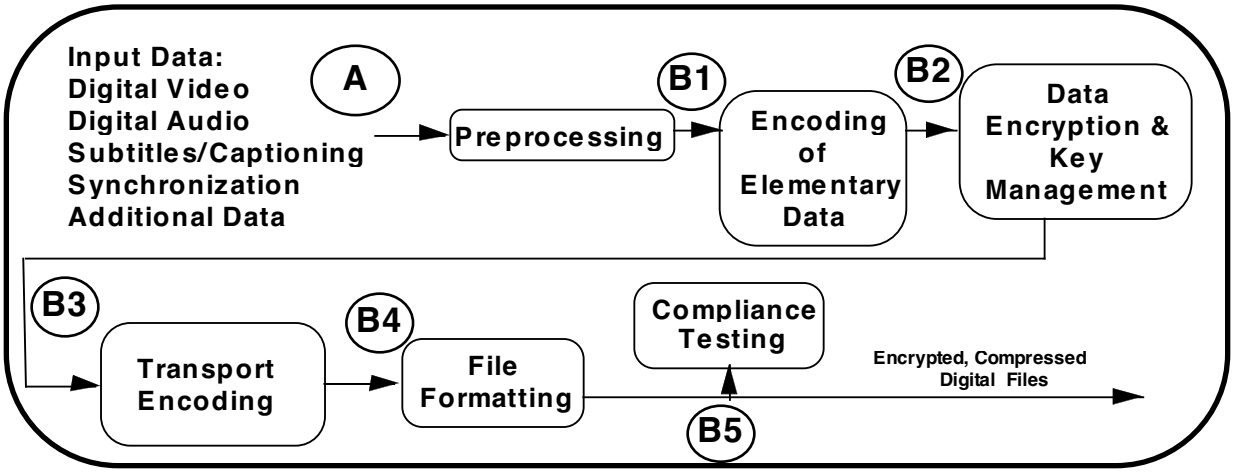

Figure 3 - Compression/Encoding With MPEG Level Encryption

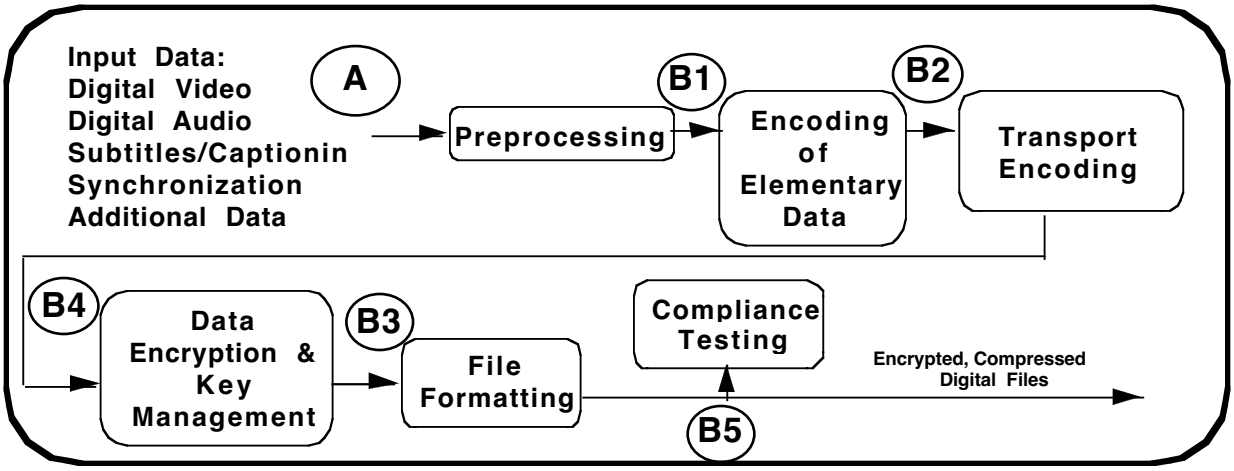

Figure 4 - Compression/Encoding With File Level Encryption

8.3.2.1 Input Data Types

The input data for Compression/Encoding include:

a) **Digital Video:**

- CCIR 601 Program Material

b) **Digital Audio:**

- AES/EBU digital audio bitstream (ch. 1-4 audio from digital video or other media)
- Content may include additional languages, commentary, Descriptive Video Service (DVS), etc.
- Monaural or stereo (A single digital audio stream may convey a monaural or a stereo program.)

c) **Subtitles and Captioning:**

- Data file (with composition and geometry information)

d) **Synchronization:**

- Time code
- Index file (corresponding to presentation time stamp)

e) **Additional Data:**

- Chapter stops
- 3:2 pulldown instructions
- Content aspect ratio information
- Source pel aspect ratio information
- Field dominance information
- Time code lists
- Audio dynamic range type
- Program information sources (EDL, OMF, video index, etc.)
- Program Metadata

8.3.2.2 Preprocessing

Optional preprocessing includes:

a) **Spatial/Temporal filtering:**

- Noise and grain reduction, electronic aperture correction, etc.

b) **Dirt & scratch removal processes**

c) **Facility information, user defined data creation**

8.3.2.3 Encoding of Elementary Data

This function includes encoding of elementary data:

a) **Data streams created:**

- Elementary video
- Elementary audio
- I-frame index
- Presentation Time Stamp (PTS)

8.3.2.4 Security

The security function optionally includes:

a) Encryption of data streams

b) Key generation and management.

8.3.2.5 Transport Encoding

The transport encoding function includes:

a) Packetizing elementary streams

b) Synchronize and multiplex elementary data streams

8.3.2.6 File Formatting

The file formatting function includes formatting the stream and metadata for distribution.

8.3.2.7 Support for Compliance Testing

The formatted file may be subjected to compliance testing. Testing of compliance at points other than interface B5 may be reasonable.

8.3.3 Delivery

The Delivery block of the top-level reference model can be further broken into more detail as shown in Figure 5. This is a process to deliver the compressed, potentially encrypted, digital files to the IFE equipment onboard the aircraft.

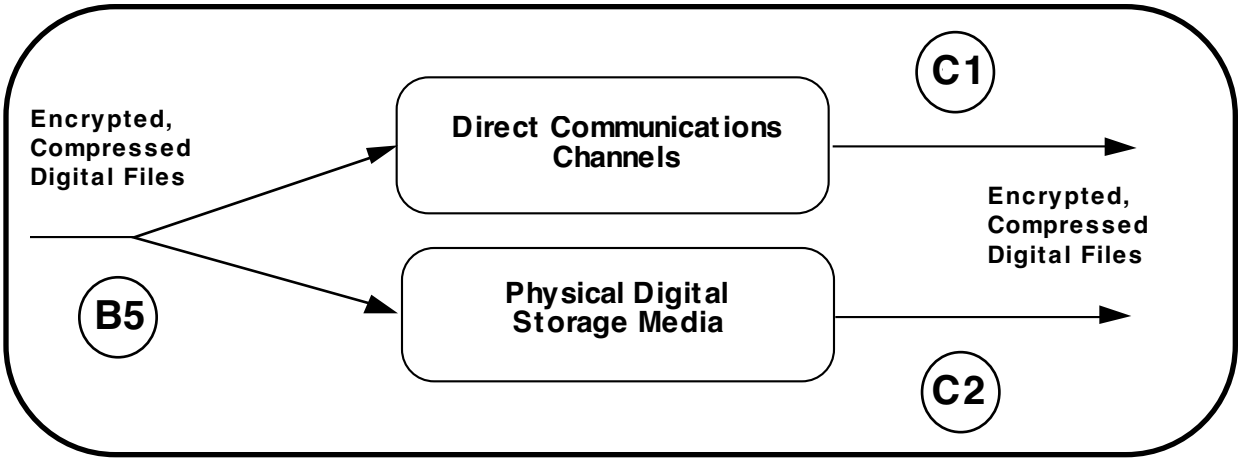

Figure 5 - Delivery

8.3.3.1 Delivery via Direct Communications Channels

The interface provides a method of loading digital media to IFE equipment via a direct communication channel using a standard electronic signaling interface.

8.3.3.2 Delivery via Digital Storage Media

This interface provides a method of loading media onto IFE equipment using physical media such as tapes or disks.

8.3.4 In-Flight Entertainment (IFE) Equipment

The IFE Equipment block of the top-level reference diagram can be further broken into more detail as shown in Figure 6. This is the actual place where the In-Flight Entertainment services are provided. From a server to the passenger seat, various service capabilities are provided by the IFE equipment manufacturers. Common to all is the concept of the digital server. This common point is the target destination for data provided according to this specification.

The remainder of the IFE equipment can be modeled, as shown, with an on-board distribution capability to distribute entertainment to the passengers, a capability to provide services to each passenger, and the display, sound, and other aspects of the human machine interface (HMI) that eventually allows the passenger to enjoy the programming.

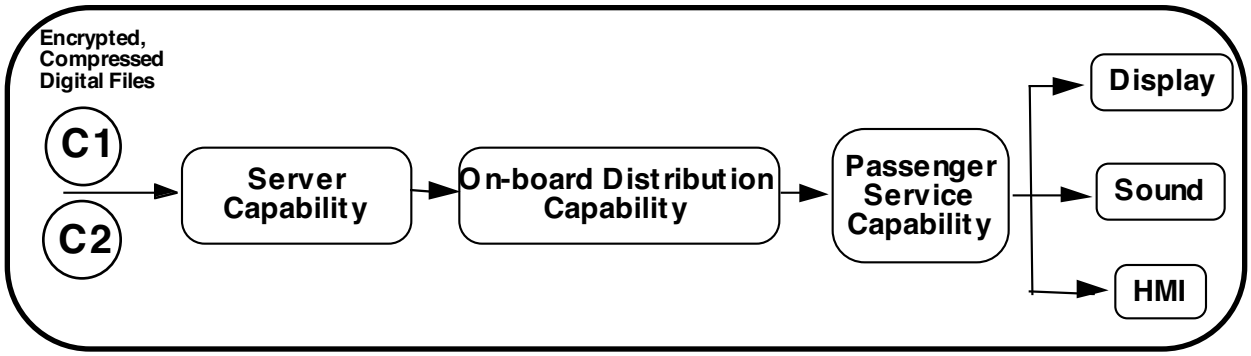

Figure 6 - In-Flight Entertainment Equipment

9. Specification of Interfaces

9.1 Interface A - Source Media/Digitization Output

Interface A provides the interface between the input data defined in Section 8.3.2.1 and possible preprocessing functions. This interface includes all digitized or coded content data with logical and temporal relationships to the compression encoding function. All video and audio elements described in Section 8.3.2.1 will be able to be conveyed across this interface. While captioning, subtitles, synchronization and additional data may be conveyed across this interface, data may also be delivered in file form directly to the Delivery process interface.

9.1.1 Audio and Video

Video shall be digitized according to ITU Recommendation ITU-R BT.601.4, *Encoding Parameters of Digital Television for Studios*. Content aspect ratio information shall be fixed to a single aspect ratio, either 4:3 or 16:9. Source pel aspect ratio information shall be fixed to a single aspect ratio.

A mechanism shall be provided to allow audio and video information for a given program to be synchronized.

Audio that is part of audio-visual programming shall be conveyed according to ITU Recommendation REC ITU-R BR.648, *Recording of Audio Signals*. Discrete six track surround sound formats, such as AC3, SDDS, and DTS, are not supported. Monaural compatible stereo surround sound formats, such as Dolby Headphone, are allowed.

Audio that is part of audio-only programming shall be conveyed according to ITU Recommendation REC ITU-R BR.648, *Recording of Audio Signals* or according to IEC Publication 908:1987 *CD Digital Audio System*.

Since the quality of the resulting compressed digital output of the processes addressed in this specification will depend largely on the quality of the initial input, the input shall be created from the highest quality source material available. See Section 13.4 Input Sources for informative guidelines regarding source material.

9.1.2 Scene Changes

If available, information regarding scene changes and 3:2 pulldown should be provided with the digitized audio-visual material. This information shall be provided in accordance with SMPTE RP-186 - 1995.

9.1.3 Media Content Description

Some of the information required to populate the media content description file (e.g. category type, content owner, etc.) shall be provided by the content provider and shall be passed across this interface. The information shall be provided according to the syntax defined in Section 12.1, Media Content Description File. Some information is not known at this time (e.g. encoded bit rate). This information shall be added at the appropriate interface as it becomes available.

9.2 Interface B1 - Preprocessing Output

Interface B1 provides the interface from the preprocessing function to the elementary data encoding function. All preprocessing (such as filtering, dirt and scratch removal processes, and noise reduction) is optional.

9.3 Interface B2 - Encoding Output

Interface B2 provides the interface from elementary data encoding function to the encryption and key management function.

9.3.1 Encoding of Elementary Data

The Elementary data encoding function includes the generation of MPEG-1 or MPEG-2 elementary video streams, MPEG-1 elementary audio streams, and optionally an I-frame index. Trick modes will be supported by the IFE equipment by using a list of I-frame locations within the main stream referenced to presentation time stamps. As an alternative to standards conversions at the A1 interface, 625 line, 25 Hz input material may be transformed directly in the encoding process to a bit stream as specified in 9.3.1.1.1.

9.3.1.1 Video Encoding

Video will be encoded using either MPEG-1 (ISO/IEC 11172-2) or MPEG-2 (ISO/IEC 13818-2).

9.3.1.1.1 Resolution

Three video encoding specifications are allowed to provide for different display sizes. The three specifications are as follows:

a) Displays up to and including 15 inches measured diagonally:

- 352 x 240 (SIF) MPEG-1

b) Any display size:

- 352 x 480 (Half D-1) MPEG-2

  OR

- 720 x 480 (Full D-1) MPEG-2

9.3.1.1.2 Bit Rate

The video bit rate for MPEG-1 encoding shall be 1.5 Mbps. The video bit rate for MPEG-2 encoding shall be 3.5 Mbps. This bit rate refers to the video elementary stream only without audio. Video shall be encoded using the Constant Bit Rate (CBR) mode.

Variable Bit Rate (VBR) MPEG is beyond the scope of this specification. Provisions for VBR encoding may be included in a future release of this specification based on availability of technology to support VBR and demand from the IFE industry. Note that systems implemented in the near term which include the capability to process VBR streams shall also provide the capability to process CBR streams in order to be considered compliant with this specification.

9.3.1.1.3 Aspect Ratio

Content may be encoded at either 4:3 or 16:9 aspect ratios. Single source mastering shall not be used to derive 4:3 aspect ratio from material encoded at 16:9. The pel aspect ratio shall be according to ITU Recommendation ITU REC-R BT.601.4 (1:1.095).

9.3.1.1.4 Frame Rate

The frame rate shall be 29.97 Hz for video sources or 23.976 Hz for film sources.

9.3.1.1.5 Encoding Parameters

a) The encoder shall use the full range of bits 0-255 for encoding. Note that the value of black (0 ire) shall be 16, and the value of white shall be 235.

b) The chroma format shall be 4:2:0 only.

c) The first line of video to be encoded shall be Line 22, Field 1.

d) Horizontal Line Extraction: 720 to 352 - Start 8 pels from left, 2:1 conversion

e) Frame rate changes shall be allowed during the program.

f) Down-filtering from CCIR-601 to SIF shall be at least equivalent in quality to that of the 7-tap Finite Impulse Response (FIR) and 4-tap FIR filters described in ISO/IEC 11172-2:1993 on subclause D.3.1.

g) Maximum Group of Pictures (GOP) size shall be 60.

h) The maximum Video Buffer Verifier (VBV) buffer size used in encoding shall be 1835008 bits.

i) No D-pictures.

j) Every effort should be made to ensure the accuracy of various MPEG-2 display parameters. These parameters include the progressive_frame flag as defined in ISO/IEC 13818-2.

9.3.1.2 Audio Encoding

Audio shall be encoded per MPEG-1, Layer II using the following parameters:

a) No emphasis shall be used.

b) No Cyclical Redundancy Check (CRC) shall be used.

c) Program reference level for source shall be set to –12 dB below full scale (digital clip).

d) 44.1 kHz sampling rates shall be supported:

- 44.1 kHz Audio for Video: Joint Stereo @ 128 kbps data rate
Dual Channel or Independent Stereo @ 256 kbps data rate
Single Channel @ 128 kbps data rate
- 44.1 kHz Audio Only: Joint Stereo @ 128 kbps data rate
Dual Channel or Independent Stereo @ 256 kbps data rate
Single Channel @ 128 kbps data rate

All the above-referenced audio sampling rates need to be supported in a manufacturer's implementation. One or more of these audio rates will be used in a program.

e) Audio shall be tailored for the aircraft environment per WAEA 1289-2, Rev. 1. The private bit in the audio header shall be set to 0.

9.3.2 Subtitles

This specification does not specify an input format for subtitle and caption information. See the separate document DMD-TC/CFC/005 published with this specification entitled "Recommended File Format for English Language Subtitles" for a discussion of possible subtitle file formats. Either symbolic unicode representation or bitmap syntax shall be used to represent subtitles or captions. When using bitmap syntax, subtitles should not be embedded in video since this impacts the compression performance and the subtitles cannot be turned off. This is only allowed in cases where non-subtitled source material is not available.

9.4 Interface B3 - Data Encryption Output

Interface B3 provides the interface from the encryption and key management function to the system and transport encoding function. The data passed across this interface consists of encrypted data, and encrypted keys that will be used to decrypt the data. Two methods of encryption are allowed: MPEG level encryption and file level encryption. This interface is specified in detail in Section 10, Security.

9.5 Interface B4 - Transport Encoding Output

Interface B4 provides the interface from the system and transport encoding to the file formatting function. The data shall be formatted in 188 byte transport stream packets with no intervening data as defined by the MPEG2 transport specification (ISO/IEC 13818-1:1995). All Program Specific Information (PSI) tables that are included must appear as the first packets in the encoded stream so that they may be extracted, modified and transmitted in a multi-program multiplexed stream. There shall be no PSI tables embedded within the rest of the elementary streams of the program. The first non-zero and non-one valued packet identifier shall signify the Program Map Table as defined in MPEG-2. The second non-zero and non-one valued packet identifier shall signify the first packet of the multiplexed elementary streams of the program. At a minimum, the following descriptors shall be included in the Program Map Table: video stream descriptor, audio stream descriptor, target background grid descriptor and maximum bit rate descriptor. A maximum bit rate descriptor shall be present which is applicable to the entire transport stream of the program following the PSI tables.

9.6 Interface B5 - File Format Output

Interface B5 provides the interface from the file formatting function to the delivery function. This interface provides a convenient point to perform compliance testing. Interface B5 defines the file format for the MPEG transport stream data from interface B4. In addition, the contents of several auxiliary files are defined. These files are placed into one file archive, called a ***tarfile***, stored on the magnetic media. See Section 12.1 for a detailed description of the file format.

9.7 Interface C1 - Direct Communications Interface

The C1 interface requirements define a robust, standards based communications network interface to the IFE server equipment that is network topology and media independent.

9.7.1 Point-to-Point File Transfer

As shown in Figure 7, Internet FTP protocol on top of TCP/IP shall be used for point-to-point transfer of file(s). The implementation of data link and physical layers are not specified in this specification.

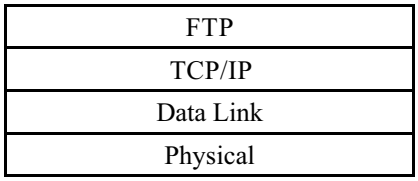

Figure 7 - C1 Interface Point-to-Point File Transfer Protocol

9.7.2 Point-to-Multipoint File Transfer

The protocol stack shown in Figure 8 shall be used for applications where multicast file transfer capability is required. Internet Group Management Protocol (IGMP RFC 1112) shall be used for this method. The implementation of data link and physical layers are not specified in this specification.

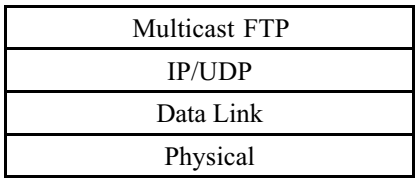

Figure 8 - C1 Interface Point-to-Multipoint File Transfer Protocol

9.8 Interface C2 - Digital Storage Media Output

The C2 interface specifies physical digital storage media for transferring information to the IFE server for video and audio content updates. Airlines are particularly desirous that file transfers at this interface occur as quickly as possible. The rapid rate of technological change in storage capacity and data transfer rates precludes specifying a fixed media type for this interface. Hard drives, DVD discs, DLT tapes, AIT tapes, DAT tapes and DDS-2 tapes are all formats currently in use. Informative references for DLT, AIT, DAT and DDS-2 formats are given in Section 4.

It is expected that IFE manufacturers will migrate to faster performing technologies as they become available. However, to efficiently support IFE content delivery during aircraft gate turnarounds the following minimum performance characteristics for the C1 and C2 Interface are specified:

a) IFE equipment requires modular growth potential for a high speed network communications interface (e.g., ATM OC3c, FDDI, etc.) to support the C1 Interface at the physical and data link layers of the OSI model (layers 1 and 2 respectively).

b) Minimum file transfer performance at the C1 or C2 interface shall transfer a 4 GB file in 20 minutes or less. This corresponds to a sustained 28 Mbps information transfer rate, excluding overhead. It should be noted that many airlines have requested media load performance capabilities in excess of this rate.

10. Security

The content delivery system must be capable of protecting intellectual property of any value from unauthorized access. It is desirable that the security system have minimum impact on the operations of the airlines for handling protected content.

There are a number of mechanisms that can be used to protect intellectual property delivered using this specification. The intellectual property owner shall determine if a particular item or class of intellectual property must be protected, and if a particular security system offered by an IFE vendor is acceptable. This section specifies requirements for two methods based on encryption. Both of these methods are known to meet the requirements of content providers. Compliance with one of these methods will assure approval. If an alternate method is adopted, it must be individually approved by the intellectual property owners.

10.1 Secure Facilities.

Secure facilities include the following:

a) Facilities that have adopted the recommendations resulting from an MPA security review.

b) Those portions of airport premises which are within the airport security perimeter.

c) IFE equipment installed on an aircraft.

10.2 Encryption-Based Security

Two methods of encryption-based security are defined in this specification: MPEG level encryption and file level encryption.

a) **MPEG Level Encryption:** The use of a key to encrypt all or parts of the MPEG elementary bitstreams. Keys will in turn be encrypted using a public key encryption system, and the resulting Control Words are distributed within the MPEG stream to the airlines who are entitled (have been granted a license) to a program.

b) **File Level Encryption:** The use of a key to encrypt an entire content file. The keys will in turn be encrypted, using a public key encryption system, and the resulting Control Words will be distributed to the airlines who are entitled (have been granted a license) to a program.

This section defines a set of basic security services that may be utilized by the content provider/laboratory, delivery system provider, and airline. The security services are supported by security mechanisms or tools.

There are three parties that may be involved with the implementation of the security requirements of this specification: the laboratory where the media is encoded, the operator of the IFE system, and the provider of the IFE system. Note that the operator of the IFE system may or may not be an airline.

10.2.1 Terminology

In this specification the following terminology is used:

a) **Encryption:** The alteration of the characteristics of the data using strong cryptographic algorithms in order to protect the data from unauthorized use.

b) **Control Word:** An encrypted data item. Its clear form is used to encrypt/decrypt audio, video or coded data.

c) **Key:** A data item used with a cryptographic algorithm for encryption/decryption.

The following generic security services are identified which, in combination, meet the security requirements of this specification:

a) **Data Encryption** - Data encryption is used to protect content from being accessed without authorization and to keep confidential the control/signaling information that is exchanged between the participants. Such control/signaling information would include the exchange of cryptographic keys.

b) **Key Management** - The main focus of key management is the secure distribution of suitable keys to decryption parties.

10.2.2 Requirements

The security requirements for systems using encryption are:

a) Intellectual property of any value shall be protected from unauthorized access.

b) Content shall be encrypted whenever it is being transferred between secure processing facilities or storage facilities.

c) There shall be no provisions to electrically off-load the decrypted content stored on IFE equipment on-board aircraft other than for the delivery of content within the IFE system.

d) Encrypted elementary streams or files for a particular program shall all be identical.

e) There shall be at least one cryptographic key per program.

f) Each airline shall have at least one public/private key to decrypt the control word, and no single public/private key shall be shared between or among airlines.

g) The entitlement key expiration is highly desirable.

h) The content may only be decrypted after (or as) it is loaded onto the IFE equipment and then may be stored there as clear data. Although not desirable, delivered media can fly with the airplane and does not need to be erased if encrypted. If it is chosen to store encrypted data within the IFE equipment, the management of encrypted data and keying materials within the IFE equipment is beyond the scope of this specification.

i) Keys and decryption engines should be implemented in a physically secure device that prevents unauthorized access.

10.2.3 Encryption Methods

10.2.3.1 Data Encryption

The program content shall be encrypted using an encryption methodology of sufficient strength to prevent unauthorized recovery of the content. For MPEG-1 encoded content, the Data Encryption Standard (DES) with a 56-bit key provides acceptable strength. For MPEG-2 encoded content, three key Triple-DES with 56-bit keys provides acceptable strength.

Other encryption algorithms may be used if it can be shown that they are at least as strong as the above-referenced minimum requirements. The selected encryption algorithm should be approveable for international use.

10.2.3.2 Key Encryption

Control Words shall be generated by encrypting the keys used to encrypt/decrypt the data using a public key encryption algorithm of sufficient strength to prevent unauthorized recovery. The RSA algorithm with 1024-bit keys meets this requirement. Other public key encryption algorithms may be used if it can be shown that they are at least as strong as RSA with a 1024-bit key. This method requires that two keys be generated. The airlines shall be responsible for generating both keys. Each airline shall generate a unique public/private key pair, so that each airline in turn will have a unique control word. The public keys shall be provided to the content provider where encryption is to be performed. The airline or their agent shall be responsible for maintaining the secrecy of the private keys.

10.2.3.3 Packet Header and Adaptation Fields

For MPEG level encryption, the ISO 13818-1 specification specifically prohibits the encryption of transport packet headers and adaptation fields. This allows transport control and de-multiplexing/re-multiplexing without requiring decryption. This allows the Program Clock Reference (PCR), for example, to be carried and modified by multiplexers without encryption.

For file level encryption these requirements do not apply.

10.2.4 Key Management

Access control through the use of keys will be managed jointly by the content provider/laboratory, the delivery system provider, and the airline.

10.2.4.1 MPEG Level Encryption

The MPEG-2 transport layer provides for the distribution of conditional access information in the form of Entitlement Control Messages (ECM), Entitlement Management Messages (EMM), and a field that identifies whether or not a data packet is encrypted. Programs encoded per this specification shall use this MPEG-2 transport layer information as follows:

The ECM packets shall carry Control Words embedded in the transport layer data stream. These ECM packets shall be used as frequently as required to strengthen the encryption method.

EMM's define the association between control words in the ECM and the airline that uses that control word. The EMM's shall be distributed by embedding them in the transport bitstream in accordance with the MPEG-2 (ISO/IEC 13818-1) requirements.

The MPEG-2 Transport Packet header contains the transport encryption control field to indicate the status and the parity (even or odd) of the CW used to encrypt the packet payload. This field must be used to indicate whether the data is encrypted. MPEG-2 has defined only that the '00' state means clear.

10.2.4.2 File Level Encryption

The Product_File_Set on the distribution media includes an encryption_keys_file that contains control words and entitlement information. The syntax of the encryption_keys_file is described in Section 12.1.7. The control words shall be changed as frequently as required to strengthen the encryption method.

11. Quality Assurance

Compliance with this specification does not guarantee acceptable quality of the encoded media, and does not replace the need for skill and judgment in the art and science of motion picture and video laboratory practices. Nothing in this specification is intended to replace normal content provider quality assurance processes.

12. Normative Annexes

12.1 Media Content Description File

Interface B5 defines the file format for the MPEG transport stream data from interface B4. In addition, the contents of several auxiliary files are defined. A graphical view of the file hierarchy is shown below as an introduction to the details of the files and their content.

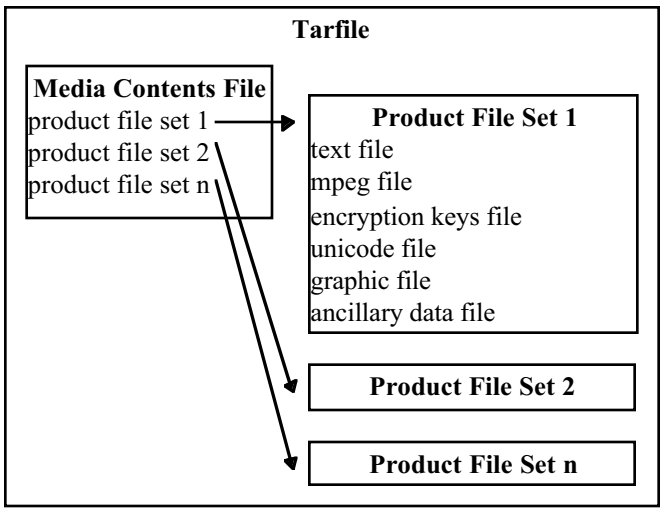

Figure 9 - Media Content File Hierarchy

These files are placed into one file archive, called a ***tarfile***, stored on the magnetic media. No file path shall be included in the tarfile. The order of the files within the tarfile are as shown in Section 12.1.1.

12.1.1 Tarfile

tarfile{	No. of Bytes	Mnemonic
media_contents_file,	length of file	asctxt file
for(i=0;i<number_of_products;i++){		
product_file_set[i]	length of files	
}		
}		

12.1.1.1 Semantic Definition of the Fields in Tarfile.

a) **media_contents_file -** This file shall be the first file in the tarfile. The media_contents_file is a asctxt file that lists and describes all of the products on the tape or disk media. The media_contents_file shall contain sufficient data to differentiate any two different releases of tapes or disks. The name of this file shall be "CONTENTS.TXT". The contents of this file are described in detail in paragraph 12.1.2.

b) **product_file_set -** There shall be one product_file_set for each product on the magnetic media. Each file within a product file set shall have the same name with different extensions. The contents of this file set is described in detail in paragraph 12.1.3.

12.1.2 Media_Contents_File

media_contents_file{	Mnemonic
(“[post_production_house] %s\r”, post_production_house)	printfarg
(“[sequence_number] %s\r”, sequence_number)	printfarg
(“[media_contents] %s\r”, media_contents)	printfarg
(“[file_date] %d/%d/%d\r”,day, month, year)	printfarg
(“[number_of_products] %d\r”, number_of_products)	printfarg
for (i=0;i<number_of_products;i++){	
(“[product] %d \r” , i)	printfarg
(“[file_name] %s \r” , product_file_name[i])	printfarg
}	
}	

12.1.2.1 Semantic Definition of the Fields in the Media_Contents_File.

The media_contents_file shall have the name “CONTENTS.TXT”. The media_contents_file is an asctxt file that contains a set of value fields preceded by a key word (e.g. [post_production_house]) and followed by a carriage return (\r). The keywords are reserved and shall not be contained in any of the value fields. The keywords and data in this file shall be formatted exactly as shown, as the data will be used in computer computations. All fields shall be included in the order shown.

a) **post_production_house -** Name of post-production house that created this file.

b) **sequence_number -** Number generated by the production house that when combined with post_product_house uniquely identifies the contents of this magnetic media.

c) **media_contents -** User defined text string to aid in the identification of the contents of the magnetic media. (e.g., “Tape with Feature Film X, Trailer Y and TV Spot Z”).

d) **file_date -** Date that this file was last altered.

e) **number_of_products -** Number of product_file_sets (feature films, news segments, television episodes, etc.) on this media.

f) **product_file_name -** Name of a product_file_set, less extension. No two products on the same media shall have the same name, although the same name may be on two different media. The name shall be eight characters or less. The name shall only contain the uppercase letters A through Z, the numbers 0 through 9, and the following special characters: underscore(_), caret(^), dollar sign ($), tilde(~), exclamation point(!), number sign(#), percent sign(%), apostrophe(’), and the grave accent(`). No other special characters shall be used.

12.1.3 Product_File_Set

product_file_set{	No. of Bytes	Mnemonic
text_file	Length of file	asctxt file
mpeg_file	Length of file	binary file
encryption_keys_file	Length of file	asctxt file
unicode_file	Length of file	unitxt file
graphics_file	Length of file	binary file
ancillary_data_file	Length of file	not applicable
}		

12.1.3.1 Semantic Definition of the Fields in the Product_File_Set.

a) **text_file -** There shall be one text_file for each product. The text_file is a asctxt file that contains product specific data required for the content provider and the IFE equipment to manage the other files in the product_file_set. The file extension for this file shall be ".TXT". The contents of this file are described in detail in paragraph 12.1.4.

b) **mpeg_file -** There shall be one mpeg_file for each product. The mpeg_file is a binary file that contains the MPEG system and transport encoded output from interface B4. The file extension for this file shall be ".MPG". This file contains sufficient information from which a vendor-specific I-frame index can be derived.

c) **encryption_keys_file -** There shall be one encryption_keys_file for each product that uses file level encryption. The encryption_keys_file is a asctxt file that contains keys used to encrypt the mpeg_file. The file extension for this file shall be ".KEY". The contents of this file are described in detail in paragraph 12.1.7.

d) **unicode_file -** The unicode_file is optional. If unicode data is provided, there shall be one unicode_file for each product_file_set. The unicode_file is a unitxt file that contains product information included solely for passenger and flight attendant consumption. The file extension for this file shall be ".UNI". The contents of this file are described in detail in paragraph 12.1.5.

e) **graphics_file** - The graphics_file is optional. It contains a single JPEG image associated with the product. The file extension for this file shall be ".JPG".

f) **ancillary_data_file** - The ancillary data file is optional. It may contain any data, in any format desired by the user. The file extension shall be ".USR".

12.1.4 Text_File

text_file{	Mnemonic
("[post_production_house] %s\r", post_production_house_name)	printfarg
("[sequence_number] %s\r", sequence_number)	printfarg
("[title] %s\r", product_title)	printfarg
("[episode] %s\r", episode)	printfarg
("[content_owner] %s\r", content_owner_name)	printfarg
("[distributor] %s\r", distributor_name	printfarg
("[release_date] %d/%d/%d\r", day, month, year)	printfarg
("[event_date] %d/%d/%d\r", day, month, year)	printfarg
("[event_time] %s\r", event_time)	printfarg
("[file_date] %d/%d/%d\r", day, month, year)	printfarg
("[encoding_date] %d/%d/%d\r", day, month, year)	printfarg
("[transport_bit_rate] %d\r, transport_bit_rate)	printfarg
("[running_time] %d\r, running_time)	printfarg
if(encoded with 4:3 aspect ratio){	
("[aspect_ratio] 4:3\r")	printfarg
}	
else{	
("[aspect_ratio] 16:9\r")	printfarg
}	
if(audio contouring on){	
("[audio_contouring] on\r")	printfarg

}	
else{	
(“[audio_contouring] off\r”)	printfarg
}	
for (i=0;i<number_audio_channels;i++){	
if(audio_mode== “joint_stereo” or “single_channel”){	printfarg
(“[audio_pid] %d\r”, pid[ ])	printfarg
(“[mode] %s\r”, audio_mode)	printfarg
(“[language] %s\r”, language[ ])	printfarg
}	
else if(audio_mode==“dual_channel”){	
(“[audio_pid] %d\r”, pid[ ])	printfarg
(“[mode] %s\r”, “dual_channel”)	printfarg
(“[right_language] %s\r”, language[ ])	printfarg
(“[left_language] %s\r”, language[ ])	printfarg
}	
}	
(“[number_subtitle_channels] %d\r”, number_subtitle_channels)	printfarg
for (i=0;i<number_subtitle_channels;i++){	
(“[channel] %d\r”, i)	printfarg
(“[subtitle_pid] %d\r”, pid[ ])	printfarg
(“[language] %s\r”, language[ ])	printfarg
if(bitmap encoded subtitles){	
(“[subtitle_encoding] bitmap\r”)	printfarg
}	
else{	
(“[subtitle_encoding] unicode\r”)	printfarg
}	
}	
}	

12.1.4.1 Semantic Definition of the Fields in the Text_File.

The text_file shall have the name “*product_file_name*.TXT”. The text_file is a asctxt file that contains a set of value fields preceded by a key word (e.g., [post_production_house]) and followed by a carriage return (\r). The keywords are reserved and shall not be contained in any of the value fields. The keywords and data in this file shall be formatted exactly as shown, as some of the data will be used in computer computations. Some of the fields are required for the presentation of the product and cannot be found in interface B4. Other fields are provided solely for informational purposes and will be indicated as such below. Data provided in interface B4 shall take precedence over informational data provided here. All fields shall be included in the order shown.

a) **post_production_house -** Name of post-production house that created this file. (Informational.)

b) **sequence_number -** Number generated by the production house that when combined with post_production_house uniquely identifies this product_file_set. (Informational.)

c) **title -** User defined text string to aid in the identification of the contents of the product (e.g., “Feature Film XYZ”). (Informational.)

d) **episode** - Number indicating the episode for episodic titles. A value of 0 indicates non-episodic.

e) **content_owner** - Name of the content owner.

f) **distributor** - Name of the distributor.

g) **release_date -** Date program released by content owner. (Informational.)

h) **event_date -** Date event occurred (for news events). (Informational.)

i) **event_time -** Time event occurred (for news events). (Informational.)

j) **file_date -** Date that this file was last altered.

k) **encoding_date -** Date that this file was encoded.

l) **transport_bit_rate -** Bit rate per second of MPEG 2 transport stream. (Informational, provided in interface B4.)

m) **running_time -** Run time of product in minutes. (Informational.)

n) **aspect_ratio** - One of two values, either “4:3” or “16:9”. (Informational, provided in interface B4.)

o) **audio_contouring -** One of two values, either “on” or “off”. This field is required by the decoder to determine if additional contouring is required.

p) **number_audio_channels -** Number of MPEG encoded audio streams (up to 16). The number of audio channels and the following audio channel information is required because it is not completely defined in interface B4.

q) **audio_pid -** MPEG packet identifier associated with this audio stream.

r) **mode -** Mode of encoding on MPEG audio channel. One of three values, either “joint_stereo”, “dual_channel” or “single_channel”.

s) **language -** Three letter code for the language assigned to this audio channel. Dual_channel encoded audio streams may have a different language on each channel. The language code is specified by ISO 639 Part 2.

t) **number_subtitle_channels -** number of subtitle channels encoded into auxiliary MPEG streams. The number of subtitle channels and the following subtitle channel information is required if subtitles are to be displayed, because it is not defined in interface B4.

u) **subtitle_pid -** MPEG packet identifier associated with this subtitle stream.

v) **language -** Three letter code for the language assigned to this subtitle. The language code is specified by ISO 639 Part 2.

w) **subtitle_encoding -** One of two values, either “bitmap” or “unicode”.

12.1.5 Unicode_File

unicode_file{	Mnemonic
(“[number_unicode_languages] %d\r”, number_unicode_languages)	printfarg
for (i=0;i<number_unicode_languages;i++){	
“[language]” language[i] “[end]”	unistr
product_unicode_description	
}	
}	

12.1.5.1 Semantic Definition of the Fields in the Unicode_File.

The unicode_file shall have the name "*product_file_name*.UNI". The unicode_file is a unitxt file that contains one or more character strings preceded by a starting key word (e.g., [language]) and followed by the keyword [end]. Both the character strings and the keywords are C UNICODE strings. The keywords are reserved and shall not be contained in any of the character strings. The key words in this file must be formatted exactly as shown, as they may be used in computer computations. All fields shall be included in the order shown

a) **number_unicode_languages -** Number of languages included in the unicode_file. The number of unicode languages is informational for the purpose of processing the unicode file.

b) **language -** Three letter code for the language used in the product_unicode_description. The language code is specified by ISO 639 Part 2.

c) **product_unicode_description -** Set of key words and descriptive text in character strings. It is intended that the descriptive text bracketed by the keywords in this section will be formatted and displayed on a passenger or CFS monitor. Therefore, except for the preceding *language* code, the descriptive text may be free form. The values shown are suggestions and may be amended as desired. The contents of this record are described in detail in paragraph 12.1.6.

12.1.6 Product_Unicode_Description

product_unicode_description{	Mnemonic
"[category]" category "[end]"	unistr
"[genre]" genre "[end]"	unistr
"[intended_audience]" intended_audience "[end]"	unistr
"[original_edited]" original_edited "[end]"	unistr
"[editing_statement]" editing_statement "[end]"	unistr
"[running_time]" running_time "[end]"	unistr
"[color_bw]" color_bw "[end]"	unistr
"[animated_live-action]" animated_live-action "[end]"	unistr
"[mpaa_rating] mpaa_rating "[end]"	unistr
"[credits]" credits "[end]"	unistr
"[awards]" awards "[end]"	unistr
"[reviews]" reviews "[end]"	unistr
"[synopsis1]" synopsis1 "[end]"	unistr
"[synopsis2]" synopsis2 "[end]"	unistr
"[synopsis3]" synopsis3 "[end]"	unistr
"[synopsis4]" synopsis4 "[end]"	unistr
"[identification_numbers]" identification_numbers "[end]"	unistr
"[music_descriptors]" music_descriptors "[end]"	unistr
"[user_defined]" user_defined "[end]"	unistr
}	

12.1.6.1 Semantic Definition of the Fields in the Product_Unicode_Description

a) **The following Category values are allowed:**

Feature Films
News/Current Affairs/Documentaries
Television Programs

Trailers
Advertisements and Promotions
Short Subjects
Cartoons
Sports
Shopping/Licensing & Merchandising
Music Videos/Ballet/Dance
Airline-Related Programs
Children's/Youth Programs
Games/Gambling
Audio Programs
Destination Information
Customs Information
Safety Information
Duty-Free Information
Airline Instructional Information
Point of Interest/Geographical Information
Airport Information

b) **Some category values have additional information in the form of genre values. Genre values are defined as follows:**

- **Feature Films:**

  Feature Films-General
  - Thriller/Detective
  - Action/Adventure
  - Western
  - War
  - Science Fiction/Fantasy/Horror
  - Comedy
  - Musical
  - Soap/Melodrama/Folkloric
  - Romance
  - Classical/Religious/Historical Drama
  - Adult
  - Other (future use, user defined)

- **News/Current Affairs/Documentaries:**

  News/Current Affairs/Documentaries-General
  - Weather Report
  - News Magazine
  - Documentary
  - Discussion/Interview/Debate
  - Other (future use, user defined)

- **Television Programs:**

  Television Program-General
  - Episodic
  - Game Show/Quiz/Contest
  - Variety Show
  - Talk Show
  - Arts/Culture
  - Social/Political/Economics
  - Education/Science
  - Leisure/Hobbies
  - Other (future use, user defined)

- **Sports:**

Sports-General
Special Events (Olympic Games, World Cup, etc.)
Sports Magazines
Football/Soccer
Tennis/Squash/Racquetball
Team Sports (excluding football)
Golf
Athletics
Motor Sports
Water Sports
Winter Sports
Equestrian Events
Martial Sports
Other (future use, user defined)

- **Children's/Youth Programs:**

Children's/Youth Programs-General
Pre-School Children's Programs
Programs for Ages 6 to 12
Programs for Ages 13 to 17
Informational/Educational/School Programs
Puppet Shows
Other (future use, user defined)

- **Music Videos/Ballet/Dance:**

Music Videos/Ballet/Dance-General
Rock/Pop
Classical Music
Folk/Traditional Music
Jazz
Opera
Ballet
Other (future use, user defined)

c) **intended_audience -** child, youth, young adult, or adult program orientation

d) **original_edited** - flag indicating if this is an original or airline edited version.

e) **editing_statement -** disclaimer statement such as “This film has been edited for content and time”, etc.

f) **running_time -** program duration

g) **color_bw -** flag indicating if this is a color or black-&-white program

h) **animated_live-action -** flag indicating if this is an animated or live-action program

i) **mpaa_rating -** G, PG, PG-13, R, NC-17, Unrated

j) **credits -**

- Star 1, 2, 3, etc. (Last Name, First Name)
- Producer (Last Name, First Name)
- Director (Last Name, First Name)
- Screenwriter (Last Name, First Name)
- etc.

k) **awards -** major awards and year received

l) **reviews** - text of critical reviews, if permitted by content owner

m) **synopsis1** - first synopsis (e.g., general synopsis)

n) **synopsis2 -** second synopsis (e.g., youth-oriented synopsis)

o) **synopsis3 -** third synopsis (e.g., male or female-oriented synopsis)

p) **synopsis4 -** fourth synopsis (e.g., international synopsis)

q) **identification_numbers -** designations of episode numbers, television spot codes, etc.

r) **music_descriptors -**

- Performers (Last Name, First Name)
- Composer (Last Name, First Name)
- Musical Genre

s) **user_defined -** reserved for future user, user defined data

12.1.7 Encryption_Keys_File

encryption_keys_file{	Mnemonic
(“[product_byte_size] %d\r”, product_byte_size)	printfarg
(“[encryption_block_size] %d\r”, encryption_block_size)	printfarg
(“[encryption_method] %s\r”, encryption_method)	printfarg
(“[number_of_entitlees] %d\r”, number_of_entitlees)	printfarg
for (i=0;i<number_of_entitlees;i++){	
(“[entitlee_id] %s\r”, entitlee_id[i])	printfarg
for (j=0;j<number_of_encryption_blocks;j++){	
(“%x\r”, encryption_key[i][j])	printfarg
}	
}	
}	

12.1.7.1 Semantic Definition of the Fields in the Encryption_Keys_File

The encryption_keys_file shall have the name “*product_file_name*.KEY”. The encryption_keys_file is a asctxt file that contains a set of value fields preceded by a key word and followed by a carriage return (\r), with one exception. The encryption keys are not preceded by a keyword. The keywords are reserved and shall not be contained in any of the value fields. The keywords and data in this file shall be formatted exactly as shown, as the data will be used in computer computations. All fields shall be included in the order shown.

a) **product_byte_size -** Size of product in memory, excludes file system overhead.

b) **encryption_block_size -** Size of block, in bytes, to which the encryption key was applied.

c) **encryption_method -** ‘DES’ or others as requested.

d) **number_of_entitlees -** Number of entitlees public keys that were used to make this file.

e) **entitlee_id[ ] -** ID of entitlee that submitted public key. (e.g., ICAO airline designator code)

f) **encryption_key[ ][ ] -** Array of keys, one per encryption block per entitlee.

13. Informative Annexes

13.1 Bit Rate

MPEG elementary streams created in accordance with the specified bit rates given in Sections 9.3.1.1.2 and 9.3.1.2 are intended to be compatible and interoperable with all IFE systems. Certain applications for content may dictate a variance from these specified bit rates. Such variance is outside the scope of this specification, though subject to content provider approval.

13.2 Patented technology

The intention of this specification is to only require the use of intellectual property that meets the ISO/IEC/ITU guidelines for inclusion of intellectual property in international standards. It is the responsibility of parties implementing this specification to ensure they obtain necessary licenses for use of intellectual property used in their implementation.

13.3 Copyright Marking

Copyright should be indicated using the provisions provided by the MPEG specification (ISO/IEC 13818) within the MPEG transport layer. This should be used when storing material from multiple copyright holders on a single media. MPEG-2 (ISO/IEC 13818) has a provision to mark copyright material at different levels such as at the system Packetized Elementary Stream (PES) level, at the video picture level, and at the audio multichannel level. It is recommended to indicate copyright at video picture level and audio multichannel level where copyright extensions are specified. The following pseudo code is specified in ISO/IEC 13818-2:

copyright_extension(){	No. of bits	Mnemonic
extension_start_code_identifier	4	uimsbf
copyright_flag	1	bslbf
copyright_identifier	8	uimsbf
original_or_copy	1	bslbf
reserved	7	uimsbf
marker_bit	1	bslbf
copyright_number_1	20	uimsbf
marker_bit	1	bslbf
copyright_number_2	22	uimsbf
marker_bit	1	bslbf
copyright_number_3	22	uimsbf
next_start_code()		
}		

extension_start_code_identifier -- This is a 4-bit integer which identifies the extension.

copyright_flag This is a one bit flag. When copyright_flag is set to '1', it indicates that the source video material encoded in all the coded pictures following the copyright extension, in coding order, up to the next copyright extension or end of sequence code, is copyrighted. The copyright_identifier and copyright_number identify the copyrighted work. When copyright_flag is set to '0', it does not indicate whether the source video material encoded in all the coded pictures following the copyright extension, in coding order, is copyrighted or not.

copyright_identifier This is a 8-bit integer which identifies a Registration Authority as designated by ISO/IEC JTC1/SC29. Value zero indicates that this information is not available. The value of copyright_number shall be zero when copyright_identifier is equal to zero.

When copyright_flag is set to '0', copyright_identifier has no meaning and shall have the value 0.

original_or_copy This is a one bit flag. It is set to '1' to indicate that the material is an original, and set to '0' to indicate that it is a copy.

reserved This is a 7-bit integer, reserved for future extension. It shall have the value zero.

copyright_number_1 This is a 20-bit integer, representing bits 44 to 63 of copyright_number.

copyright_number_2 This is a 22-bit integer, representing bits 22 to 43 of copyright_number.

copyright_number_3 This is a 22-bit integer. representing bits 0 to 21 of copyright_number.

copyright_number This is a 64-bit integer, derived from copyright_number_1, copyright_number_2, and copyright_number_3 as follows:

copyright_number **=** (copyright_number_1 << 44) + (copyright_number_2 << 22) + copyright_number_3.

The meaning of copyright_number is defined only when copyright_flag is set to '1'. In this case, the value of copyright_number identifies uniquely the copyrighted work marked by the copyrighted extension and is provided by the Registration Authority identified by copyright_identifier. The value 0 for copyright_number indicates that the identification number of the copyrighted work is not available.

When copyright_flag is set to '0', copyright_number has no meaning and shall have the value 0.

Similar to ISO/IEC 13818-2, ISO/IEC 11172-3 has specified the following copyright related field in multichannel (MC) header:

copyright_identification_start One bit to indicate that the copyright_identification_bit in this frame is the first of 72-bit copyright identification. If no copyright identification is transmitted, this bit should be kept '0'.

'0' no start of copyright identification in this frame

'1' start of copyright identification in this frame

copyright_identification_bit One bit which is part of a 72-bit copyright identification field. The start is indicated by the copyright_identification_start bit. The field consists on an 8-bit copyright_identifier, followed by a 64-bit copyright_number. The copyright identifier indicates a Registration Authority as designated by ISO/IEC JTC1/SC29. The copyright_number is a value obtained from this Registration Authority which identifies the copyright material.

13.4 Input Sources

The source media may include:

a) **Digital Video Tape:**

- Any digital video tape that can properly contain the information of CCIR-601 is acceptable for storage of digitized film and video material.

b) **Film:**

- Film usually originates as a 16 mm or 35 mm inter-positive element or low contrast print. This element is telecined to create a 4:2:2, 29.97 Hz, 2:1 interlaced, CCIR-601 video version of the film. Most film originates as 24 fps and is converted to 29.97 Hz using 3:2 pull-down. The material should be inverse telecined to remove the 3:2 pull-down before compression.

c) **Analog Video Tape:**

- Analog video tape sources are recommended only for material for which no suitable film or digital tape sources are available. Component analog tape sources are preferable to composite analog tape sources. The quality of the conversion process will impact the eventual quality and compression performance of the overall system.

d) **Audio Sources:**

- Audio may be pre-processed for dynamic range reduction for presentation in high noise environments such as aircraft. No audio signal processing can be assumed in the IFE systems to reduce dynamic

range. Some IFE systems will include noise cancellation headsets so care should be taken to allow acceptable playback for both playback systems using the same audio source. If this is not possible, then an auxiliary source for high dynamic range audio should be provided.

e) **Editing for Airline:**

- Common film and video editing in the analog and digital domain will likely be performed prior to digitization. These processes are outside the scope of this specification.

13.5 Recommended File Format for English Language Subtitles

See the supplemental document DMD-TC/CFC/005, "Recommended File Format for English Language Subtitles" for a complete description of the recommended format and syntax for subtitles and captions.

13.6 Group of Pictures (GOP) Size

Recommended GOP size: 12 frames for 23.976 Hz frame rate source material

15 frames for 29.97 Hz frame rate source material

m = 1, 2, or 3

13.7 Security

13.7.1 Principles of DES

For tutorial information on DES see "The Protection of Computer Software - It's Technology and Application", edited by Derrick Grover, British Imformatics Society, 1992. A complete specification of DES is found in National Institute of Standards and Technology (NIST), FIPS Publication 46-1: Data Encryption Standard, January 22, 1988.

13.7.2 Public Key Algorithm

DES is a very fast and efficient cipher. However, DES uses the same key for encryption and decryption of its data. The problem is how to get the key to the intended recipient without interception by unauthorized parties. A public key algorithm, such as RSA, can be used to encrypt the DES key.

Public key encryption works by using two keys, public/private pair, one to encrypt and one to decrypt data. This public/private key pair is generated using the RSA key algorithm. One is the private key, which should be kept as secret. The other is the public key, which can be revealed to anyone. Any data encrypted with one of the keys, either public or private key, can be decrypted only by the other of the pair. Knowing one key does not help deriving the other key. Once data is encrypted with one of the keys, it cannot be decrypted with the same key.

For encryption, first, a random DES key is generated and used to encrypt the data. Then, a public key encryption is used to encrypt the DES key. This encrypted DES key can now be included with the encrypted data for distribution. The intended receiver first decrypts the DES key using the other half of the public/private key pair, then uses the decrypted DES key to decrypt the data.

13.7.2.1 RSA Algorithm

For tutorial information on the RSA algorithm see RSA Laboratories' *Frequently Asked Questions About Today's Cryptography, version 4.1, May 2000,* available from <http://www.rsasecurity.com/rsalabs/faq/>. A detailed description of the RSA algorithm can be found in "A method for obtaining digital signatures and public-key cryptosystems", by R.L. Rivest, A. Shamir, and L. Adleman in Communications of the ACM, 21(2):120-126, February 1978. The RSA worldwide web server (http://www.rsasecurity.com/rsalabs) has extensive references on this subject as well.

13.8 Compliance Testing

There are two desired areas of compliance testing for a system utilizing this specification:

a) Bitstream compliance testing

b) IFE equipment compliance testing

Bitstream compliance testing is to certify the output of a content provider/laboratory. IFE equipment compliance testing is to certify the ability of IFE equipment to play a compliant bitstream. It is possible that a bitstream may be allowed to meet only a partial subset of all specifications and still be considered to be compliant as long as the bitstream obeys the range limits and syntax rules. Compliant IFE systems may support specific profiles of this specification, e.g., in the areas of: number of audio channels, subtitling format, encryption method, and file media type. This is analogous to the MPEG conformance situation.

For example, an MPEG compliant bitstream can consist of only I-frames which is syntactically compliant with the MPEG specification because the I-frame sequence is simply a subset of the full syntax. Decoders, however, cannot escape true conformance. For example, decoders that cannot decode P or B frames are not legal MPEG decoders. Likewise, full arithmetic precision must be obeyed before any decoder can be called MPEG compliant. The Inverse Discrete Cosine Transfer (IDCT), inverse quantizer, and motion compensated prediction must meet the specification requirements, which are fairly rigid (e.g., no more than 1 least significant bit of error between reference and test decoders). Real-time compliance is more complicated to measure than arithmetic precision, but it is reasonable to expect that decoders that skip frames on reasonable bitstreams are not likely to be considered compliant.

In order for compliance testing to be successful, testing tools need to be available from multiple third-party sources.

13.9 Delivery of Supplementary Elementary Streams

The DMD-TC recognizes that the ability to deliver supplementary elemental bitstreams (i.e., additional subtitle or audio tracks) to the IFE equipment independently from previously delivered streams would be very useful. While a complete solution to this problem was not identified prior to the time this specification was released, future versions may address this capability.

