DCMWG

Digital Content Management Working Group
of the World Airline Entertainment Association

WORLD AIRLINE ENTERTAINMENT ASSOCIATION

WAEA SPECIFICATION 0403
"DIGITAL CONTENT DELIVERY METHODOLOGY FOR AIRLINE IN-FLIGHT ENTERTAINMENT SYSTEMS"
VERSION 1.0

Adopted January 22, 2007, by the WAEA DCMWG

Adopted January 23, 2007, by the WAEA Technology Committee

Adopted January XX, 2007, by the WAEA Board of Directors

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 that 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 in-flight 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.

For background information on the work of the WAEA Digital Content Management Working Group (DCMWG), visit the web site <http://www.waea.org/tech/DCM_working_group.htm>, where official documents of the DCMWG are posted.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

FOREWORD

The Digital Content Management Working Group (DCMWG) is a working group established by the World Airline Entertainment Association (WAEA) Technology Committee to develop and publish technical specifications for delivery of digital content to in-flight entertainment systems (IFES). The DCMWG membership includes representatives of in-flight entertainment (IFE) equipment manufacturers, content providers, post-production laboratories, service providers, airlines and experts in the fields of digital video and audio compression, security, metadata and Internet technologies.

The work of the DCMWG was expanded to the development of this specification in 2003, following nearly three years during which the DCMWG functioned as an educational entity for the WAEA. A call for contributions from technology companies was widely distributed in January and February 2004. There were regular DCMWG meetings and discussions on the resulting contributions, leading to the development of this specification.

The key concerns, purposes and objectives of the DCMWG in establishing this specification are:

- The development and publication of an open, voluntary technical specification that encourages a common digital content delivery methodology for IFES
- The interoperability of content across multiple IFES implementations
- The utilization of efficient encoding methods for high quality image and sound, helping to ensure a quality airline passenger experience
- Non-proprietary and interoperable system components
- A secure IFE system infrastructure with secure content preparation and delivery
- Low complexity and high efficiency and effectiveness

The scope of work for this specification includes the interfaces, delivery processes, security and key management between content point of origin and delivery to onboard IFES. Content storage archives and onboard playback systems are outside the scope of this specification. It is intended that a future version of this specification will address onboard playback systems.

1 INTRODUCTION

The DCMWG recognizes that the commercial and consumer industries have created broad standards for creating, formatting and delivering digital content. This specification draws from those standards and applies them to IFES content. Other specifications generally allow a wide range of options to be utilized. However, there are certain requirements that are unique to IFES, e.g., IFES are generally constrained with respect to processing, bandwidth and screen resolution as a result of requirements for very low power, size and weight. By agreeing in this specification to constrain the use of digital content to a subset of these broader standards, greater interoperability will be achieved for digital content destined for IFES.

As a result of wide-ranging emerging compression technologies for the commercial and consumer industries that require decoding compatibility with MPEG-2, MPEG-4 and VC-1, integrated circuit (IC) manufacturers are designing decoders that support at least these formats. Many decoders are implemented with a digital signal processor where code can be downloaded for support of additional types of audio/video (A/V) codecs.

The DCMWG acknowledges that the short-term future includes MPEG-1 and MPEG-2, already in use in IFES, but that the mid-term to long-term outlook is trending towards adoption of MPEG-4 and VC-1 codecs. Consequently, the DCMWG, in recognition of these trends, sets forth parameters in the following areas in this specification:

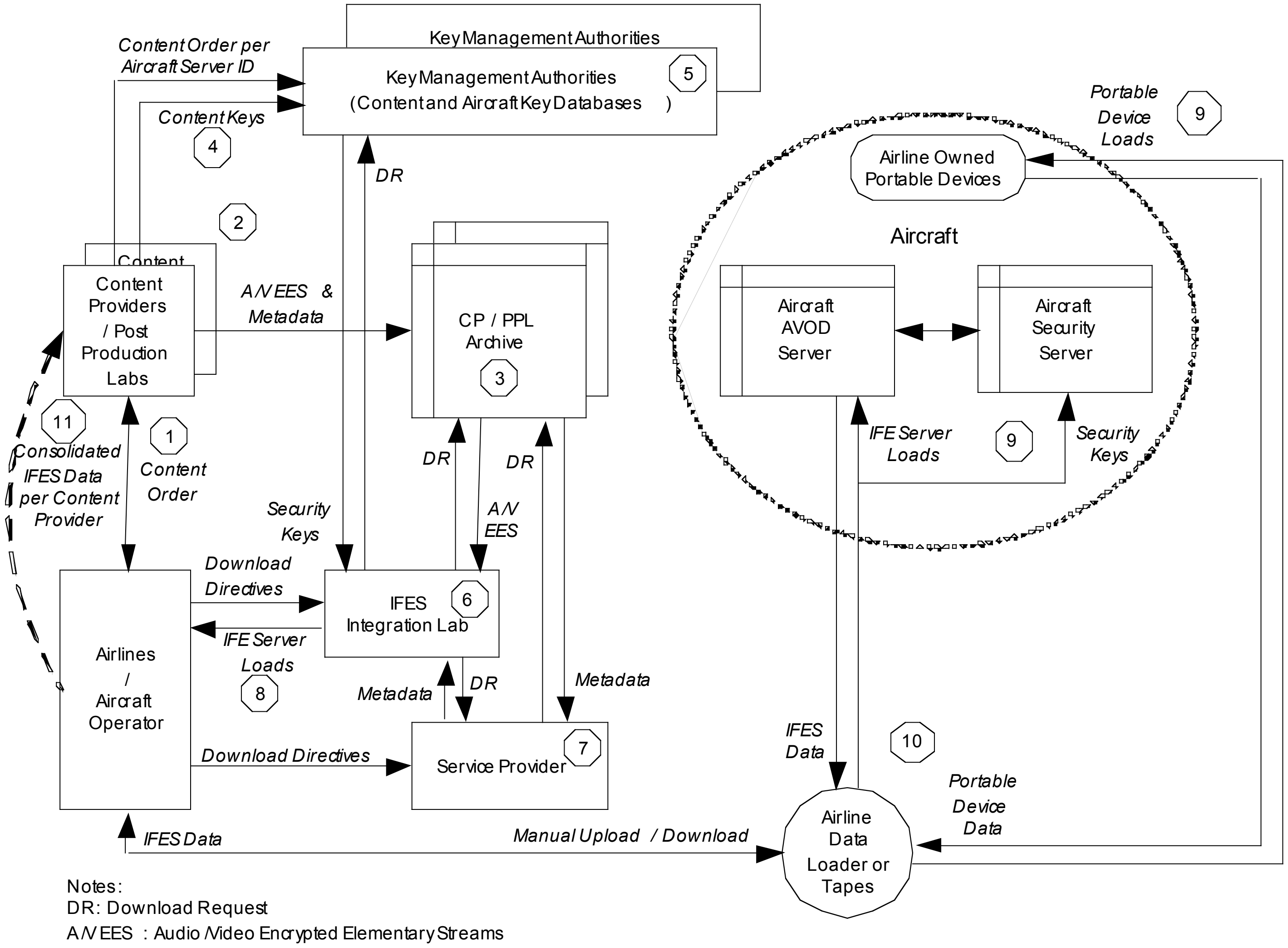
- Implementations of MPEG-4 Part 2, MPEG-4 Part 10 and VC-1.
- A security system for these new codecs that encourages the provisioning of early-window release content to aircraft IFES.

- Simplification of the process of content distribution, including enhanced automation of the supply chain between content providers, postproduction laboratories, service providers, security entities, IFES content integrators, IFES providers and airlines.

The DCMWG intends, as a separate initiative, to examine the evolving high-speed Internet access technologies. This includes automated content delivery through the entire supply chain. The passage from manual delivery to automated delivery will facilitate migration from monthly delivery to on demand delivery of content and data. Also, when aircraft have high-speed Internet access on the ground, it is contemplated that content, keys, metadata and other required elements can be delivered directly to the aircraft, potentially bypassing the need for physical media delivery.

2 SYSTEM REFERENCE MODEL

This specification is primarily intended for third and future generations of cabin networks that are compliant with ARINC Specifications 808, 809 and 820. Present IFE systems compliant with ARINC Specification 628 may not be able to accommodate this specification.



Notes:
DR: Download Request
A/V EES : Audio /Video Encrypted Elementary Streams

Figure 1: System Reference Model with Manual Content Loading to Aircraft

The system reference model addressed by this specification is illustrated in Figure 1. With respect to Figure 1, the following workflow descriptions and key components apply, with the numbers in the figure corresponding to the numbered items below:

1. A content provider accepts an order from an airline or from an airline's authorized agent.
2. Content is delivered to a postproduction laboratory (PPL). The content provider elects to encrypt the content or to provide it in the clear.
3. The PPL provides the A/V encrypted elementary streams and, with metadata (as required), stores the A/V encrypted elementary streams in an Internet accessible archive.
4. Content providers and/or PPLs generate security keys that are provided to a Key Management Authority (KMA) with the content orders (and aircraft specific identification in the future).
5. The content provider and/or PPL authorize a KMA to distribute keys.
6. Based on airline requests, encrypted content and keys are accessed or delivered accordingly by or to an IFE integration laboratory.
7. Metadata is accessed by the service provider, which customizes the metadata to airline graphical user interface (GUI) style.
8. The IFE integration laboratory produces IFE server loads that contain encrypted content, security keys and electronic program guide (seat GUIs) on a transport media.
9. These IFE server loads are sent encrypted to the airline, which loads them onto onboard servers with portable or embedded data loaders. The onboard servers play out the content for use by passengers. Alternatively, similar encrypted IFE server loads are transferred onto airline owned portable devices for use by passengers. Passenger-owned notebook computers, personal digital assistants and personal electronic devices are outside the scope of this specification.
10. IFES data and portable device data, consisting of passenger usage and maintenance information, are downloaded to the airline data loader for further processing by the airline. As agreed between the necessary parties, passenger content usage data may be shared to enable better content customization.

3 REFERENCES

3.1 Normative References

The following international and industry standards contain provisions that, through reference in this specification's 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.

Cable Television Laboratories, Inc., (CableLabs) Asset Distribution Interface Specification, Version 1.1, 2006. Available from <www.cablelabs.com>.

Cable Television Laboratories, Inc., (CableLabs) Video-On-Demand Content Specification, Version 1.1, 2006. Available from <www.cablelabs.com>.

ISO/IEC 11172-3:1993, "Information Technology – Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to About 1,5 Mbit/s – Part 3: Audio", 1993. Available from <www.iso.ch>.

ISO/IEC 13818-1:2000, "Information technology – Generic Coding of Moving Pictures and Associated Audio Information: Systems", 2000. Available from <www.iso.ch>.

ISO/IEC 14496-1:2004, "Information Technology – Coding of Audio-Visual Objects – Part 1: Systems", 2004. Available from <www.iso.ch>.

ISO/IEC 14496-2:2004, "Information Technology – Coding of Audio-Visual Objects – Part 2: Visual", 2004. Available from <www.iso.ch>.

ISO/IEC 14496-3:2005, “Information Technology – Coding of Audio-Visual Objects – Part 3: Audio”, 2005. Available from <www.iso.ch>.

ISO/IEC 14496-8:2004, “Information Technology – Coding of Audio-Visual Objects – Part 8: Carriage of ISO/IEC 14496 Contents Over IP Networks”, 2004. Available from <www.iso.ch>.

ISO/IEC 14496-10:2005, “Information Technology – Coding of Audio-Visual Objects – Part 10: Advanced Video Coding”, 2005. Available from <www.iso.ch>.

ISO/IEC 14496-14:2003, “Information Technology – Coding of Audio-Visual Objects – Part 14: MP4 File Format”, 2003. Available from <www.iso.ch>.

ISO/IEC 14496-15:2004, “Information Technology – Coding of Audio-Visual Objects – Part 15: Advanced Video Coding File Format”, 2004. Available from <www.iso.ch>.

ISO/IEC 15938, Parts 1-11, “Information Technology – Multimedia Content Description Interface”, 2002-2005. Available from <www.iso.ch>.

ISO/IEC 21000, Parts 1-17, “Information Technology – Multimedia Framework (MPEG-21)”, 2003-2006. Available from <www.iso.ch>.

ITU-R Recommendation BT.601-5, “Studio Encoding Parameters of Digital Television for Standard 4:3 and Wide-screen 16:9 Aspect Ratios”, October 1995. Available from <www.itu.int>.

SMPTE 421M-2006, “Television – VC-1 Compressed Video Bitstream Format and Decoding Process”, 2006. Available from <www.smpte.org>.

WAEA Specification 1289-2, Revision 3, “Specification for Mastertape Recording, Tape Duplication, Compact Disc Replication, and Digital Encoding for Airborne Audio Entertainment Systems”, 20 January 2005. Available from <www.waea.org>.

Worldwide Web Consortium Recommendation: Extensible Markup Language (XML) 1.0, Fourth Edition, 16 August 2006. Available from <www.w3c.org>.

3.2 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.

ARINC Project Paper 809, Draft 9, “3rd Generation Cabin Network, Seat Distribution System”, November 2006. Available from <www.arinc.com>.

ARINC Project Paper 820, Draft 2, “3rd Generation Cabin Network, Wireless In-Flight Entertainment System”, November 2006. Available from <www.arinc.com>.

ARINC Specification 628, “Cabin Equipment Interfaces”, Parts 0-9, 1999-2006. Available from <www.arinc.com>.

ARINC Specification 808, “3rd Generation Cabin Network, Cabin Distribution System”, November 2006. Available from <www.arinc.com>.

Consumer Electronics Association (CEA) Standard 608-D, “Line 21 Data Services”, 2006. Available from <www.global.ihs.com>.

CEA Standard 708-C, “Digital Television Closed Captioning”, 2006. Available from <www.global.ihs.com>.

Federal Information Processing Standards (FIPS) Publication 46-3, “Data Encryption Standard”, 25 October 1999. Available from <www.csrc.nist.gov>.

FIPS Publication 180-2, “Secure Hash Signature Standard”, 1 August 2002. Available from <www.csrc.nist.gov>.

FIPS Publication 197, “Specification for the Advanced Encryption Standard (AES)”, 26 November 2001. Available from <www.csrc.nist.gov>.

IETF Request For Contributions 4122, “A Universally Unique IDentifier (UUID) URN Namespace”, July 2005. Available from <www.ietf.org>.

ISO 15706:2002, “Information and Documentation – International Standard Audiovisual Number (ISAN)”, November 2002. Available from <www.iso.ch>.

SMPTE Standard 430.2-2006, “D-Cinema Operations – Digital Certificate”, 2006. Available from <www.smpte.org>.

WAEA Specification 0395, Version 2.0, “Content Delivery for In-Flight Entertainment”, 6 November 2001. Available from <www.waea.org>.

4 VIDEO COMPRESSION

To ensure visual quality on a wide array of screen sizes and the interoperability of content, the following video codecs meet the requirements of this specification:

- MPEG-4 Part 2 (ISO/IEC 14496-2:2004)
- MPEG-4 Part 10 (ISO/IEC 14496-10:2005)
- SMPTE VC-1 (SMPTE 421M-2006)

Image data parameters shall be as specified in Table 1.

Coded Picture Format	Video Encoding Resolution
Full-frame (4:3) SDTV	720 x 480 (“Full D-1”, ITU-R Recommendation BT.601-5)
Widescreen (16:9) SDTV	720 x 480 (“Full D-1”, ITU-R Recommendation BT.601-5)

Table 1: Coded Picture Format and Video Encoding Resolution

Video shall be encoded at a minimum of 1.0 Mbps for MPEG-4 Part 2, MPEG-4 Part 10 or SMPTE VC-1. It is desirable that a fixed encode rate of 1.0 Mbps be utilized. This bit rate refers to the video elementary stream only without audio. Video shall be encoded using constant bit rate (CBR) mode.

Support for 4:3 content to be displayed in 16:9 screens without distortion is required and support for 16:9 content to be displayed in 4:3 screens without distortion is required. While systems may be technologically capable of automatically converting 4:3 content into 16:9 displays, or 16:9 content into 4:3 displays, the execution of this capability may be bound by private agreements. Implementers are cautioned to read and understand all applicable agreements. IFES manufacturer and content provider migration to 16:9 content and 16:9 displays is encouraged.

High definition content (as opposed to standard definition content) is outside the scope of this specification. It is anticipated that high definition content will be addressed in a future version of this specification. Video editing may be performed prior to encoding; these processes are outside the scope of this specification.

5 AUDIO COMPRESSION

To ensure aural quality and interoperability of content, the following audio codecs meet the requirements of this specification:

- MPEG-4, Part 3 – High Efficiency Advanced Audio Coding (HE-AAC) (ISO/IEC 14496-3:2005)
- MPEG-4, Part 3 – Low Complexity Advanced Audio Coding (LC-AAC) (ISO/IEC 14496-3:2005)
- MPEG-1 Audio, Layer 3 (MP3) (ISO/IEC 11172-3:1993)

Audio content shall be encoded at the data rates specified in Table 2.

Audio Formats	HE-AAC CBR in Kb/s	LC-AAC & MP3 CBR in Kb/s
Joint Stereo	64	128
Dual Channel or Independent Stereo	128	256
Single Channel Monaural	64	128

Table 2: Audio Formats and Data Rates

Audio quality shall comply with WAEA Specification 1289-2, Revision 3, “Specification for Mastertape Recording, Tape Duplication, Compact Disc Replication, and Digital Encoding for Airborne Audio Entertainment Systems”.

Frequency response shall be 20 Hz to 20 kHz at ± 3 dB (“Hi-Fi”). Sampling frequency shall be 44.1 kHz for all audio content.

Audio editing may be performed prior to encoding; these processes are outside the scope of this specification.

6 MPEG SYSTEM

MPEG system multiplexing is required for the delivery of elementary encoded video and audio, data and metadata. PPLs provide the required encrypted elementary streams and each IFES manufacturer or their agent multiplexes them pursuant to their unique IFES MPEG systems requirements. This allows for cross-utilization of the same encoded content with different IFES architectures.

The following systems multiplexing meet the requirements of this specification:

- MPEG-4, Part 15 (ISO/IEC 14496-15:2004)
- MPEG-4 over MPEG-2 as specified in MPEG-2 Systems (ISO/IEC 13818-1:2000)
- MPEG-4 over IP networks (ISO/IEC 14496-8:2004)
- MPEG-4 over http as specified in MPEG-4 Systems (ISO/IEC 14496-1:2004)

Precise synchronization of multiplexed elementary video and audio streams is required to prevent noticeable and objectionable lip-sync problems. It is a synchronization requirement of this specification that video shall lag audio no more than 20 ms and video shall lead audio no more than 40 ms.

7 SECURITY

7.1 Security Introduction

IFES must be capable of protecting intellectual property from unauthorized access. It is desirable that security systems have minimum impact on the operations of airlines for handling protected content. Both plain text and secure content shall be accommodated throughout the content delivery process. Not all content need be made secure. The content provider shall determine if a particular item or class of intellectual property must be protected, and if a particular security implementation offered by an IFE vendor is acceptable.

This security section provides guidelines and recommended practices for an interoperable security system for IFE content management. A more complete specification would be required in order to provide sufficient guidance to actually implement such a system. This security guideline is divided into two phases as follows:

In Phase 1:

- The goal of Phase 1 is to supplement WAEA Specification 0395 in order to obtain a consistently secure path for IFE content to the point it is loaded on the aircraft.
- Phase 1 includes the conversion of content to secure content and back, and the management of keys and access authorizations from the time the secure content file is created, through all phases of content management and integration, and loading on the aircraft. Once the secure content is loaded on the aircraft,

the IFE system will either decrypt the content to store it as plain text, or leave it encrypted in a form supporting decryption at playback.

- Implementation of Phase 1 guidelines will improve security through greater protection of keys while maintaining flexibility for manufacturers. It should also reduce content management complexity by using a common key management methodology and by enabling more efficient methods for moving secure content through the delivery process.

In Phase 2:

- The goal of Phase 2 will be to extend the security to onboard IFES so that A/V content will remain encrypted on the aircraft at all times except for the decrypted stream used only during playback.
- Discussion of Phase 2 in this document is only for the purpose of providing background to the working group that develops the detailed Phase 2 guideline.

The following assumptions apply to both Phase 1 and Phase 2:

- Key management should not necessarily depend on the path that secure content takes to get to the aircraft.
- Key management should be agnostic as to the A/V codecs that are used.

This security section by itself is not sufficient to enable the development of interoperable KDMs. At a minimum, follow-up work to turn this guideline into a standard must address the following:

- Method for verification of secure content management and secure playback devices.
- Establishment of the trust domain and qualification of Registry services.
- Secure content packaging.
- KDM format, and, potentially, an IFE-specific KDM profile.
- Profiles for file-based and Essence encrypting of video, audio, subtitling, and captioning files.
- The means by which encrypted content will be securely processed and distributed without the need for decryption prior to its use by passengers.

7.1.1 Definitions for Section 7

Device Key: The private key of a secure content management device or a secure playback device. Confidentiality of the Device Key is essential to the secure operation of the device.

Essence: The raw encoded form of audio, video or contextual data, not including the metadata, that together make up the information content of the stream or any wrapper data that is added to aid access to or improve the robustness of the stream.

Key Delivery Message (KDM): A cryptographically secure file containing an encrypted content key, access rights information, and the ID of the secure content file to be decrypted. The content key in this message is encrypted using the public key to the device that the KDM was generated for.

Order: A data object containing instructions for the distribution of Secure Content and associated keys, authorized by the content provider.

Order Management System: The system that provides the security data, which is then used by the Key Management System (KMS) to associate Orders to secure devices in a Registry. An Order Management System may have other non-security related functions, but that is outside the scope of this guideline. In the absence of an external Order Management System, the KMS may perform this function internally.

Play Window: A period of time, defined as a "do not play before" and "do not play after" date and time pair. Play windows are always in reference to Coordinated Universal Time.

Registry: A repository that contains information about all secure devices that service the IFE market segment. In technical terms, this is the database containing the digital certificates associated with RSA public keys for secure content management devices and secure playback devices.

Secure Content: Content that has been encrypted in accordance with this guideline.

Secure Content Management Device: IFE equipment or general-purpose computer that can encrypt or decrypt content. A secure content management device may be installed in a PPL, a content integration facility, an airside content loading facility, or onboard the aircraft.

Secure Playback Device: IFE equipment that can independently decrypt and render some stored Secure Content, without creating a plain text content copy. A Secure Playback Device may be installed onboard the aircraft or it may be an IFE portable device.

Secure Virtual Content Library: A symbolic concept, this represents the entire collection of Secure Content files known to any of the IFE key management systems.

7.1.2 Security System Architecture

The security system architecture diagram in Figure 2 describes the interrelationships for security in Phase 1 and Phase 2. The dashed lines represent the exchange of Order information – the essential data elements for the original Order and its fulfillment. The dotted lines indicate the exchange of security information – KDMs and other messages. The solid lines represent the flow of secure content. Airline 1 is an example of a legacy content path, from the content integrator to the airline, with the security managed by the integrator. In the example of Airline 2, the onboard system can receive a KDM directly from the KMS.

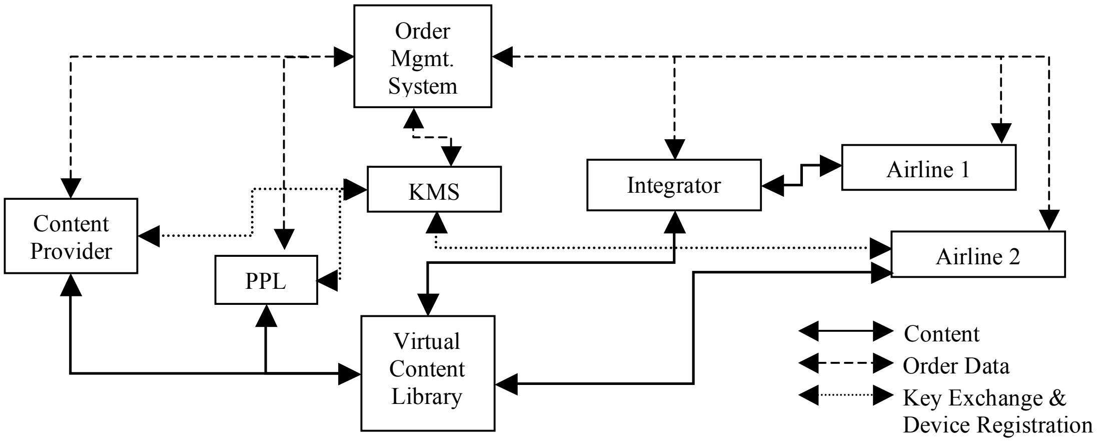


Figure 2: Security System Architecture Diagram

The process starts when a content Order is created to fulfill a transaction between a content provider and an airline (or a content aggregator acting as an agent of one or more airlines). The Order is recorded in some type of Order Management System that the KMS can reference for process flow and Order information. In the absence of an external Order Management System, each KMS would need to manage an Order Management System internally.

The content provider instructs a PPL to provide the content files necessary to fulfill the order. To do this, the PPL may:

- *Case 1*: Starting with a digital source master, encode and encrypt the content to create a new secure content file for the virtual content library.
- *Case 2*: Call out an encrypted content file already in the virtual content library.
- *Case 3*: Decrypt an existing encrypted content file it has rights to access, modify it as needed to fulfill the order, and then re-encrypt and repackage the file, thus also creating a new secure content file in the virtual content library.

Once the PPL associates a secure content file to fulfill the order, the KMS makes the keys available to the content integrator and/or airline specified in the order. The KMS does this by generating KDMs for each device that is specified by the digital rights information in the order. Each KDM is specific to the secure devices associated with the digital certificate used to generate it.

Since a KDM is cryptographically protected, any convenient method, including a non-secure method, can be used to deliver the KDM. Likewise, since the secure content is cryptographically protected, any convenient method may be employed for delivery of the secure content.

7.2 Key Management Systems

The primary function of a Key Management System (KMS) is to provide assurance that Secure Content is enabled only for authorized Secure Playback Devices and that all Device Keys used in the security system remain confidential. To this end, a KMS:

- Maintains a Registry of digital certificates and their association to trusted devices and the location of those devices.
- Generates Key Delivery Messages (KDMs).
- Cooperates with other KMSs.

This security guideline assumes there may be multiple independent KMSs and therefore one or more Registries representing the entire population of secure devices. For example, a content provider may contract with a PPL to perform key management, while an airline may contract with a content integrator. Each of these KMSs will need to cooperate in order to ensure that Secure Content may be used on all compliant Secure Playback Devices and Secure Content Management Devices. At a minimum, the following high-level functions must be supported between KMSs:

- Exchange of an intermediary KDM for further distribution of a content key.
- Exchange of order fulfillment information, either directly between KMSs, or through an Order Management System or exchange.

7.2.1 Registry, Certificates, and RSA Key Pairs

Each KMS will maintain a Registry that associates the digital certificates of Secure Content Management Devices and Secure Playback Devices to their owner and location, e.g., a content provider, PPL, content integrator, airline or specific aircraft. A Registry operates as follows:

- Each secure device is associated with a 2048 bit RSA public-private key pair. (A detailed description of the RSA algorithm can be found in “A method for obtaining digital signatures and public-key cryptosystems”, by R. Rivest, A. Shamir, and L. Adleman in *Communications of the ACM*, 21(2):120-126, February 1978.)
- Each public key is contained in an X.509 compliant digital certificate as specified in SMPTE Standard 430.2-2006, “D-Cinema Operations – Digital Certificate”.
- The KMS accepts these digital certificates from trusted sources and imports them into its Registry.
- The KMS provides a trusted means for the digital certificates to be associated to the appropriate operator (content provider, PPL, content integrator or airline) and location.

The level of granularity (i.e., how many devices are associated with an individual certificate) varies by implementation in existing IFE systems. However, good cryptographic practice requires that a certificate is associated with only one secure device, and that the private key is generated in hardware and never exposed outside that secure device. Therefore, unique private keys are highly recommended for all Secure Content Management Devices at PPLs and content integrators. For loading content on aircraft, legacy systems that currently use a shared private keying system may participate in Phase 1. For new Phase 1 content loaders and for Phase 2 Secure Playback Devices, a unique Device Key is highly recommended.

Note that a device with a “shared secret” Device Key represents a substantial potential liability. If such a device is compromised, it may be necessary to revoke and renew all such devices in order to reestablish security. In analogous situations, such a security compromise has sometimes led to a permanent breakdown of security due to the high cost of renewal.

7.2.2 Key Delivery Messages

The KMS will generate KDMs for Secure Content in the Secure Virtual Content Library, on an order-by-order basis, and deliver them to the appropriate operators of secure devices to fulfill each order. Each KDM will comply with the relevant SMPTE digital cinema standards and contain at a minimum, the KDM ID, the Play Window, and the AES content key. A KDM may be referenced by more than one content file. In addition, a KDM may be used to pass a content key from one KMS to another.

7.2.3 Content Integrators and Access to Secure Content

Once the PPL has entered a Secure Content file into the Secure Virtual Content Library, the content integrator must determine how that Secure Content file will be integrated into the IFE program update for the airline:

- *Case 1*: For some orders, the original secure content file associated with an order can be used by the onboard system without change. For such files, the content integrator would only need a KDM to perform quality control and testing.
- *Case 2*: In other cases, the original secure content file may need to be modified to achieve compatibility with the playback equipment. For those files, the content integrator would use a KDM to decrypt the file, make the appropriate modifications to the plain text content, and subsequently re-encrypt the modified content. This newly encrypted file would be assigned a new content ID, but may reference the previous KDM. Alternatively, the content integrator may assign a new content key and communicate that to the KMS, as it would need to generate a new KDM to deliver the key to the aircraft IFE system.
- *Case 2a*: Legacy systems using triple-DES encryption represent a special form of Case 2. The PPL would provide the content file encrypted with AES-128 in accordance with this guideline. The content integrator would decrypt the file and re-encrypt it using triple-DES, and then be responsible for distributing that triple-DES key to the aircraft equipment. This is represented in the security system architecture diagram as the example of Airline 1 (see Figure 2).

The KMS is agnostic as to whether or not the content integrator follows Case 1 or Case 2. However, in Case 2, the Secure Content Management Device should be designed such that plain text content files are never created in the content integrator's content management system. The entire operation of decrypting the file, modifying it, and re-encrypting the new file should be a seamless and secure process. Since the content integrator is modifying the content, there may also be quality control considerations; however, such quality control issues are outside the scope of this security section.

7.2.4 Updating KDMs for New or Replacement Secure Devices

In the event that a new Secure Content Management Device or Secure Playback Device is added to a facility or aircraft, or that such an existing device is replaced for service or maintenance, new KDMs may need to be delivered as follows in order to access Secure Content:

- For Phase 1 legacy systems where the original and replacement device share the same private key, the existing KDMs are still valid.
- For Phase 1 legacy systems where the original and replacement device do not share the same private key, the KDMs may be replaced through a connection to the KMS. Alternatively, this replacement can be accomplished using a key escrow scheme and the new KDMs are delivered using the same methodology as the original KDMs.

7.3 Secure Content

Each Secure Content file will be protected by encryption using the AES-128 cipher (FIPS Publication 197). The Secure Content file should contain a UUID content identifier (IETF Request For Contributions 4122) and/or an ISAN content identifier (ISO 15706:2002) sufficient to relate the Secure Content file to the KDMs issued for that file. In order to enable re-use of Secure Content files, no order-specific security information is contained in the Secure Content file itself.

With the AES-128 cipher, cipher-block chaining (CBC) mode shall be used. In order to support channel changes and data loss recovery, it is required that the CBC chain be allowed to restart on the order of 0.5 seconds to allow decryption entry points into a stream.

The RSA algorithm, modulus 2048, with SHA-256 hash generation is used for secure key distribution, for device authentication, for IFE object authentication, and for authentication of log message integrity.

The Secure Content Management Device will write a cryptographically protected log entry and communicate said entry to the KMS for the following actions:

- For each encryption of a content file.
- For each decryption of a secure content file, further indicating if a plain text content file is created as an output of the decryption operation.

In order to support real-time playback of Secure Content, a set of encryption profiles must be developed to include Essence encryption as well as file level encryption.

7.4 Digital Rights Delivery

The KMS obtains the digital rights information from the Order Management System. It is anticipated that digital rights are delivered in the KDM as defined in the relevant SMPTE digital cinema standards. Digital rights shall reference the content file using the content ID. Digital rights shall not be included in the metadata of the Secure Content file.

7.4.1 Device Security Manager

Each Secure Content Management Device or Secure Playback Device shall include a device security manager that is able to read the KDM. The device security manager is responsible for enforcing Play Windows, for writing any secure log entries, and for packaging those log entries for transmission to the KMS.

If the content playback environment operates in its own security sub-domain, the device security manager also acts as the local KMS for that security domain.

7.5 Security Robustness

Security robustness is the responsibility of the IFES equipment manufacturer. The following guidelines are provided as indicators of a highly robust system:

1. Secure devices are assumed to be operating in a hostile environment, always susceptible to being moved from their approved location to an unauthorized location.
2. Portable playback devices and data loaders are more easily tampered with or removed from a secure environment and therefore the security system should always protect keys in hardware on these devices.
3. Secure devices installed onboard aircraft provide a higher degree of physical security, which may provide more flexibility to the IFE manufacturer to protect keys in software.
4. Hardware protection of keys implies the following robustness rules:
    a. No physical access to components containing keys or plain text content shall be allowed. Security devices shall be tamper-evident such that any attempt to gain access to components containing keys or plain text content has a high probability of destroying the components and keys, leaving obvious evidence of the attempt.
    b. Critical security parameter protection for plain text RSA private Device Keys, content keys, and keys controlling those keys by storage and processing in a secure IC. Such secure IC shall be designed so that no command is available to export a critical security parameter either as plain text or under any cover knowable outside the IC.
5. Security devices that perform time-related functions shall support an internal real-time clock (RTC).

   a. RTC external adjustments are constrained to a maximum of 10 minutes per year; any drift outside of those limits is deemed to be a critical device malfunction.
   b. The RTC should be afforded the same protection against attack as the Device Keys.

6. If a forensic marking scheme is used, unmarked content shall be afforded protection such that the security device shall be inoperable if interfaces carrying unmarked content are exposed to monitoring and recording.

7.6 Phase 2 Guidelines

The following comments are provided as input to the working group that develops the Phase 2 security guidelines:

- Secure content is loaded on the aircraft and it remains encrypted except during actual playback. An unencrypted content copy is never created.
- A method or methods must be defined to provide access to the content keys and digital rights information in the event that a Secure Playback Device is replaced onboard an aircraft.
- Secure playback logs will be defined for data capture and compliance purposes.

8 OTHER CONSIDERATIONS

8.1 Metadata

To allow automated generation of passenger GUIs, A/V content attribute metadata should be provided for, at a minimum, title, credits, synopsis, ratings, promotional material, and key art. Audio only content attribute metadata should be provided for, at a minimum, title, credits, lyrics, ratings and key art.

The following metadata formats are applicable to content meet the requirements of this specification:

- MPEG-7 (ISO/IEC 15938, Parts 1-11), including XML (Worldwide Web Consortium Recommendation: XML 1.0, Fourth Edition)
- MPEG-21 (ISO/IEC 21000, Parts 1-17)
- Cable Television Laboratories, Inc., (CableLabs) Video-On-Demand Metadata Specifications, Version 1.1 (CableLabs Asset Distribution Interface Specification, Version 1.1, and CableLabs Video-On-Demand Content Specification, Version 1.1)

All files and metadata associated with particular content should include a corresponding UUID content identifier and/or an ISAN content identifier. ISAN has a dedicated field in MPEG-4.

8.2 Content Source Media

Recommended source media for the A/V content encoding process include:

- One content release, Full D-1 resolution, full-frame 4:3 SDTV format, language tracks with Hi-Fi audio,
- One content release, Full D-1 resolution, widescreen 16:9 SDTV format, language tracks with Hi-Fi audio,
- Promotional material, Full D-1 resolution, full-frame 4:3 SDTV format, language tracks with Hi-Fi audio,
- Promotional material, Full D-1 resolution, widescreen 16:9 SDTV format, language tracks with Hi-Fi audio,
- Key art files, JPEG format,
- A metadata file containing content description information (e.g., title, credits, synopsis, ratings and other metadata).

Recommended source media for the audio only content encoding process include:

- Audio programs with Hi-Fi audio,

- Key art files, JPEG format,
- A metadata file containing content description information (e.g., title, credits, lyrics, ratings and other metadata).

8.3 Quality

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 postproduction laboratory practices. Nothing in this specification is intended to replace normal content provider quality assurance processes.

8.4 Intellectual Property Disclaimer

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, which, paraphrased, requires licensing of intellectual property on a fair, reasonable and non-discriminatory basis. It is the responsibility of parties implementing this specification to ensure they obtain necessary licenses for use of intellectual property used in their implementation.

This specification is based on material submitted by various participants during the drafting process. The WAEA has not made any determination whether these materials could be subject to valid claims of patent, copyright or other proprietary rights by third parties, and no representation or warranty, expressed or implied, is made in this regard. Any use of or reliance on this document shall constitute an acceptance thereof "as is" and be subject to this disclaimer.

9 INFORMATIVE ANNEX: MEDIA ACCESSIBILITY OVERVIEW

9.1 Introduction

9.1.1 Captioning

There are millions of people worldwide that have a hearing loss so acute that they cannot fully understand the audio portion of A/V content. This is especially true of the elderly, the fastest growing category of individuals who are deaf and hard of hearing. Text captions enable viewers who are deaf and hard of hearing to understand the audio portion of A/V content. Captions can also benefit adults and children learning to read, as well as people learning second languages.

Like subtitles, captions display spoken dialogue as printed words on the screen. Unlike subtitles, captions are specifically designed for viewers who are deaf and hard of hearing. Captions are carefully placed to identify speakers, on-screen and off-screen sound effects, music, and laughter. Closed-captions are hidden as data within the A/V content's data package, and they must be decoded in order to be displayed. Open captions are imprinted as part of the A/V content's visual display and cannot be turned on or off.

9.1.2 Descriptive Narration

Descriptive narration is a service that makes A/V content accessible to people who are blind or who have low vision. Descriptive narration consists of a script written to highlight key visual elements that a viewer who is blind or who has low vision would ordinarily miss in the content (e.g., action, settings, costumes, gestures, and scene changes). The script is then voiced by a professional narrator, interspersing the descriptions between dialog so as not to interfere with the audio or dialog of the content. The descriptive narration track is then mixed with the original content audio track to create a new audio track that includes the descriptions. Such descriptive narration audio is delivered to users via a variety of technologies, depending on the platform: stereo television's secondary audio program for broadcast and cable distribution, selectable audio tracks for DVD distribution, and via infrared or frequency modulation systems in motion picture theaters.

9.1.3 Accessible Navigation

People who are blind or who have low vision have difficulty navigating on-screen menus, particularly those which employ touch screens. Solutions to overcome these difficulties are proposed in this annex that may help create a better passenger experience for those with visual impairments.

9.2 Captioning in IFE

There are several techniques that can be employed to provide captioning in IFES:

9.2.1 Parallel Content

For A/V content that is provided to IFE passengers, it is possible to provide a parallel content library with open captions imprinted in the A/V content, allowing the deaf and hard of hearing to select from the library of captioned material.

If open captions are offered, they should be readable at a distance of 4.25 times the diagonal size of the display. Given the limitations of most IFE screens (i.e., their limited size and close distance to the viewer), open captions should use the same process as subtitling, which provides readable characters while keeping most of the picture visible. This implementation also interferes less with the appearance of the A/V content.

9.2.2 Closed-Captioned Content

Alternatively, A/V content may be made available with closed-caption data. This data can take the form of line-21 data for analog content (CEA 608-D, “Line 21 Data Services”) or digital television closed-caption data for digital content (CEA 708-C, “Digital Television Closed Captioning”). Line 21 closed-caption decoder technology is widely available as integrated circuits or software. Decoding could happen at the seatback, or could be centralized at an onboard server and accomplished in software for each passenger.

9.2.3 Subpicture Stream Technology

Captions are commonly provided for DVD titles as subpicture streams specifically authored for the needs of deaf and hard-of-hearing viewers. Similarly, an IFES could utilize such captions as subpicture streams and provide a passenger interface to allow for the selection of a given subpicture stream. The MPEG-4 format also supports text data in the stream file.

9.3 Descriptive Narration in IFE

Care should be taken to provide descriptive narration audio that can contend with a noisy airborne environment by utilizing WAEA Specification 1289-2, Revision 3. Like captioning, several techniques can be employed to provide descriptive narration in IFES:

9.3.1 Parallel Content

For A/V content that is provided to IFES, it is possible to provide a parallel content library with descriptive narration, allowing the blind or low vision passenger to select from the library of described material.

9.3.2 Multiple Audio Tracks

A/V content may be made available for IFES with multiple audio tracks, such as alternate languages or a descriptive narration audio track. The IFES provides a user interface allowing for the selection of a given alternate audio track, including the descriptive narration.

9.4 Accessible Navigation in IFE

Most IFES rely on graphical user interfaces, which typically include hierarchies of onscreen menus not readily usable by people who are blind or who have low vision. Accommodation of these users can be accomplished in a number of ways, or more often, using a combination of the following methods:

9.4.1 Tactile Controls

User handsets have tactile indicators (“nibs”) on essential keys and differentiated key shapes (square, triangle, round) so that different functions are readily discernable.

9.4.2 Audible Feedback

The IFES user interface can be programmed to provide audible feedback. Key elements include descriptions of positioning within the menu structure, available choices, navigation instructions, audible prompts, and audible versions of other key information on the screen that is otherwise only available to sighted users. When this feature is enabled as an option by user choice, audio files that enunciate the name or function of a menu, button or key press are automatically triggered as the user navigates the GUI. Such techniques are commonly referred to as “talking menus”.

9.4.3 Speech Control

Where there are no tactile controls for IFES navigation, speech-to-text solutions, if practicable and available, may allow the passenger to speak commands to the system to accomplish such tasks as moving the cursor and selecting menu items.

10 INFORMATIVE ANNEX: ACRONYMS AND ABBREVIATIONS

A/V	Audio/Video
AES	Advanced Encryption Standard
ARINC	Aeronautical Radio, Inc.
AVOD	Audio/Video On-Demand
CBC	Cipher-Block Chaining
CBR	Constant bit rate
CEA	Consumer Electronics Association
CP	Content Provider
dB	Decibels
DCMWG	Digital Content Management Working Group
DES	Data Encryption Standard
DR	Download Request
DVD	Digital Versatile Disc
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HE-AAC	High Efficiency Advanced Audio Coding
Hi-Fi	High-Fidelity audio with a frequency response of 20 Hz to 20 kHz at ± 3 dB
http	Hypertext Transfer Protocol
Hz	Hertz (cycles per second)
IC	Integrated Circuit
ID	Identifier
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IFE	In-Flight Entertainment
IFES	In-Flight Entertainment Systems
IP	Internet Protocol

ISAN	International Standard Audiovisual Number
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-R	International Telecommunication Union - Radiocommunication
JPEG	Joint Photographic Experts Group
Kb	Kilobit
KDM	Key Delivery Message
kHz	Kilohertz (one thousand cycles per second)
KMA	Key Management Authority
KMS	Key Management System
LC-AAC	Low Complexity Advanced Audio Coding
Mbps	Megabit per second
MP3	MPEG-1 Audio, Layer 3
MPEG	Moving Picture Experts Group
PPL	Postproduction Laboratory
RSA	A cryptographic algorithm invented by R. Rivest, A. Shamir and L. Adleman
RTC	Real-Time Clock
SAMI	Synchronized Accessible Media Interchange
SHA	Secure Hashing Algorithm
SDTV	Standard Definition Television
SMPTE	Society of Motion Picture and Television Engineers
UUID	Universally Unique Identifier, type 4 (pseudo-random), as defined in IETF Request For Contributions 4122
VC	Video Codec
WAEA	World Airline Entertainment Association
XML	Extensible Mark-Up Language

11 INFORMATIVE ANNEX: LIST OF PARTICIPANTS

This specification could not have been produced without the dedicated involvement of many individuals and companies. The following persons participated in the creation of this document by attendance at one or more meetings of the WAEA DCMWG. Their company affiliation at the time of their participation is also given.

Ginette Aelony	PGA-Avionics
Atul Anandpura	e.Digital Corp. (Leader, Audio Compression)
John Arceneaux	U.S. Dept. of Homeland Security
Ken Brady	Thales Avionics Inc.
Wayne Brown	Oxford Media (Leader, Interactive Data)
Jay Cardon	Rockwell Collins
Michael Childers	Innovative Media Solutions (Co-Chair, DCMWG)
Ford Cirni	Rockwell Collins
Jim Condon	Videon Central
Fred Diether	Intersound Inc.

John Dolan	AD Aerospace
Rolf Goedecke	Airbus
Larry Goldberg	WGBH (Leader, Media Accessibility Overview)
Eric Grab	DivXNetworks, Inc. (Leader, Video Compression)
Mark Griffin	Videon Central
Kamran Guivian	Panasonic Avionics Corp.
Cliff Hall	Oxford Media Corp. (Leader, MPEG Systems)
Wade Hanniball	Universal Pictures
P.J. Harr	Twentieth Century Fox (Leader, Metadata)
Victor Hernandez	Thales Avionics Inc.
Larry Iboshi	Imagik Corp.
Jinha Kim	Warner Bros.
Brent Kovar	Sky Way Aircraft, Inc.
Julian Levin	Twentieth Century Fox (Co-Chair, DCMWG)
Al McGowan	TEAC Aerospace Technologies
Melinda Meyer	Buena Vista Non-Theatrical, Inc.
John Nelson	Cinea, Inc. (Leader, Security)
Earl Nicks	ARINC Inc.
Royal O’Brien	DiStream
John O'Connor	Cine Magnetics Video & Digital Laboratories
Denise Rodriguez	U.S. Airways
Bryan Rusenko	Crest Digital
John Salzman	Spafax
Rich Salter	Salter Group
Pierre Schuberth	Rockwell Collins (Co-Chair, DCMWG)
Donald Schultz	Boeing Commercial Airplanes
Randy Schwarz	Panasonic Avionics Corp.
Sudhakar Shetty	Boeing Commercial Airplanes
Eric Silverstein	Atlas Air Entertainment Concepts
Scott Terry	Spafax
Jason Songer	Spafax
Brian Vessa	Sony Pictures Entertainment
Lance Ware	SyncCast
Philip Watson	Panasonic Avionics Corp.
Jim Williams	Motion Picture Association of America