INTERNATIONAL STANDARD

ISO 26430-5

First edition
2009-12-15

Digital cinema (D-cinema) operations —

Part 5: Security log event class and constraints

Opérations du cinéma numérique (cinéma D) —

Partie 5: Classe et contraintes d'événement du journal de sécurité

Reference number
ISO 26430-5:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 26430-5 was prepared by the Society of Motion Picture and Television Engineers (as SMPTE 430-5-2008) and was adopted, under a special "fast-track procedure", by Technical Committee ISO/TC 36, *Cinematography*, in parallel with its approval by the ISO member bodies.

ISO 26430 consists of the following parts, under the general title *Digital cinema (D-cinema) operations*:

- *Part 1: Key delivery message* [equivalent to SMPTE 430-1]
- *Part 2: Digital certificate* [equivalent to SMPTE 430-2]
- *Part 3: Generic extra-theater message format* [equivalent to SMPTE 430-3]
- *Part 4: Log record format specification* [equivalent to SMPTE 430-4]
- *Part 5: Security log event class and constraints* [equivalent to SMPTE 430-5]
- *Part 6: Auditorium security messages for intra-theater communications* [equivalent to SMPTE 430-6]
- *Part 9: Key delivery bundle* [equivalent to SMPTE 430-9]

SMPTE 430-5-2008

SMPTE STANDARD

D-Cinema Packaging — Security Log Event Class and Constraints

Page 1 of 25 pages

Table of Contents

Page

Foreword 2
Introduction 2
1 Scope 3
2 Conformance Notation 3
3 Normative References 3
4 Overview (Informative) 4
5 Definitions 5
5.1 Definition of Terms 5
5.2 Definition of Processes and Validation 6
5.2.1 Composition Playlist Validity 6
5.2.2 Frame Playback Process 6
5.2.3 Complete CPL Playback 6
5.3 Security Event Class 6
5.4 Security Class Namespace 6
5.5 Namespace Prefixes 6
5.6 Reference Architectures 7
6 Security Application Requirements 7
6.1 Security Constraints 8
6.1.1 Log Record Header 8
6.1.2 Log Record Body 8
6.1.3 Log Record Signature 9
6.2 Security Log Record Authentication and Chaining 10
7 Security Event Definitions 10
7.1 ReferenceID Scope 10
7.2 Event Types 11
7.3 Event Sub Types 12
7.3.1 Playout Event Sub Types 12
7.3.2 Validation Event Sub Types 14
7.3.3 Key Event Sub Types 15
7.3.4 ASM Event Sub Types 16
7.3.5 Operations Event Sub Types 18
7.4 Exception Tokens and Definitions 22
8 Examples (Informative) 23
8.1 Example 1 23
9 Glossary of Acronyms 23
Annex A Proxy Logging (Informative) 24
Annex B Security Log Report Filtering (Informative) 25

Copyright © 2008 by THE SOCIETY OF
MOTION PICTURE AND TELEVISION ENGINEERS
595 W. Hartsdale Ave., White Plains, NY 10607
(914) 761-1100

Approved
March 3, 2008

Foreword

SMPTE (the Society of Motion Picture and Television Engineers) is an internationally-recognized standards developing organization. Headquartered and incorporated in the United States of America, SMPTE has members in over 80 countries on six continents. SMPTE's Engineering Documents, including Standards, Recommended Practices and Engineering Guidelines, are prepared by SMPTE's Technology Committees. Participation in these Committees is open to all with a bona fide interest in their work. SMPTE cooperates closely with other standards-developing organizations, including ISO, IEC and ITU.

SMPTE Engineering Documents are drafted in accordance with the rules given in Part XIII of its Administrative Practices.

SMPTE Standard 430-5 was prepared by Technology Committee DC28.

Introduction

A general specification for D-Cinema Log Records and Log Reports is specified in [LogRecord]. This Security Class standard defines a class, and an associated namespace, for Log Records for security logging. Additionally, this standard constrains the use and application of that format to Security Log Records and Reports. More specifically, this document specifies the format of Log Records produced by security devices within D-Cinema systems. Typically these records are produced by the Security Manager component of the system, which produces records of security events for consumption by systems external to the security system. When the Security Manager produces these records, they are constructed to support authentication and non-repudiation by and for the device that produces them. Support is included for authenticating chains of records in a manner that reduces the overhead that would otherwise result if each record were to be authenticated individually.

1 Scope

The purpose of this document is to specify a Security Event Class and namespace for Security Log Records; and to constrain individual Log Records and sequences of such records (Log Reports) as they are used for security event logging purposes in D-Cinema applications. The items covered contain descriptions of events logged by the security system, which are intended to provide forensic information regarding security critical events. This document does not specify the means of communication or the format of messaging between security devices in a system. Neither does this document define the format for storage of Log Events within the protected storage of a security device. The Security Log Records and Security Log Record Sequences (Log Reports) described herein are intended for reporting of Security Events previously recorded by the security system to consumers of that information which are external to the security system.

2 Conformance Notation

Normative text is text that describes elements of the design that are indispensable or contains the conformance language keywords: "shall", "should", or "may". Informative text is text that is potentially helpful to the user, but not indispensable, and can be removed, changed, or added editorially without affecting interoperability. Informative text does not contain any conformance keywords.

All text in this document is, by default, normative, except: the Introduction, any section explicitly labeled as "Informative" or individual paragraphs that start with "Note:"

The keywords "shall" and "shall not" indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.

The keywords, "should" and "should not" indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.

The keywords "may" and "need not" indicate courses of action permissible within the limits of the document.

The keyword “reserved” indicates a provision that is not defined at this time, shall not be used, and may be defined in the future. The keyword “forbidden” indicates “reserved” and in addition indicates that the provision will never be defined in the future.

A conformant implementation according to this document is one that includes all mandatory provisions ("shall") and, if implemented, all recommended provisions ("should") as described. A conformant implementation need not implement optional provisions ("may") and need not implement them as described.

3 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent edition of the standards indicated below.

[RFC 3280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile URL: http://www.ietf.org/rfc/rfc3280.txt

[DCMLTypes] SMPTE 433-2008, XML Data Types for Digital Cinema)

[LogRecord] SMPTE 430-4-2008, Log Record Format Specification for D-Cinema

[KDM] SMPTE 430-1-2006, D-Cinema Operations — Key Delivery Message

[D-Cert] SMPTE 430-2-2006 D-Cinema Operations — Digital Certificate

[ETM] SMPTE 430-3-2006, D-Cinema Operations — Generic Extra-Theater Message Format

[ASM] SMPTE 430-6-2008, D-Cinema Operations — Auditorium Security Messages for Intra-Theater Communications

[TFE] SMPTE 429-6-2006, D-Cinema Packaging — MXF Track File Essence Encryption

[CPL] SMPTE 429-7-2006, D-Cinema Packaging — Composition Playlist

[PKL] SMPTE 429-8-2007, D-Cinema Packaging — Packing List

[TRK] SMPTE 429-3-2007, D-Cinema Packaging — Sound and Picture Track File

[RFC 4051] Additional XML Security Uniform Resource Identifiers (URIs) http://www.ietf.org/rfc/rfc4051.txt

[RFC 2253] Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names. URL: http://www.ietf.org/rfc/rfc2253.txt

4 Overview

The fundamental purpose of security logging in D-Cinema systems is to assure that access to clear-text content, and the use of decryption keys to accomplish this, can be tracked in trusted reports from the security system. An important corollary of this requirement is to record that the security system itself is functioning properly. The Security Manager component of the security system is the trusted device, which collects information as the system operates, then processes that information to compose Security Log Records and potentially Log Reports. While communication of Log Event data between devices in a security system must be performed securely, such communications are outside of the scope of this document. This document does not specify any particular security system architecture, and so uses the term "Security Device" to refer to components of the security system generically.

The general requirements for Security Log Records external to the security system are that the records be verifiable as to the integrity of their content, verifiable as to the completeness of a report, and verifiable as to their source. An additional requirement is that sequences of log records must support filtering of potentially sensitive information, while maintaining sequential integrity, i.e. the filtering of an individual record must leave verifiable evidence of the record's existence and position in the sequence. Filtering is described in [LogRecord].

When a system external to the security system, such as a general-purpose log management system, is instructed to retrieve records from the security system, this standard describes how those records should be generated and represented. The [LogRecord] standard is constructed to support filtering of log records by omitting the body part of a record. The security system may support the generation of pre-filtered log record sequences (with selected record bodies omitted), or filtering may be performed after the log records are retrieved.

The Security Application Requirements section of this document constrains the application of the log format defined in the Log Record Specification for D-Cinema [LogRecord]. These constraints ensure that this format is applied to the expression of Log Records and Reports in a manner that provides for authentication of the log data.

It is important to note that [LogRecord] does not actually specify the Event Types, Event Subtypes, Parameters, or scopes for the Event Classes that it denotes, but provides a framework for doing so. The Security Event Definitions section of this document defines the “security” Event Class as called for in [LogRecord], including all of the detail necessary to create fully defined Log Records for security.

5 Definitions

5.1 Definition of Terms

Security Log Event – Any event that has security implications or forensic value. Such an event results in the recording of log data.

Security Log Data – Security event information that is recorded and stored within a security device, where such an event took place or was observed.

Security Log Record – A Log Record, containing Security Log Data, describing a Security Log Event.

Security Log Report - A sequence of Log Records as specified in [LogRecord] and subject to the constraints specified in this document.

Security Device – A generic term, which refers to a physical or logical device which contains or uses a D-Cinema security certificate, and which performs a D-Cinema security function.

Security Entity (SE) – A logical entity that implements one or more d-cinema security-related processes. (e.g. a media Decryptor or a forensic marker)

Secure Processing Block (SPB) – A tamper-resistant, -evident and -responsive perimeter associated with a Digital Certificate around security-critical information. The specific characteristics of the perimeter are outside the scope of this specification.

Image Media Block (IMB) – The combination of Image Decryptor, Audio Decryptor, Forensic Marker(s), Security Manager and (optionally) Link Encryptor Security Entities contained within a single Secure Processing Block.

Remote Secure Processing Block (Remote SPB) – A Secure Processing Block other than the Image Media Block.

Security Manager (SM) – A Security Entity responsible for parsing Key Delivery Messages and generating Log Records. It is implemented within the Image Media Block. There is a single Security Manager associated with each auditorium within an exhibition site.

Screen Management System (SMS) – A logical entity associated with a Digital Certificate responsible for content management and validation within an auditorium.

SPB Marriage and Divorce – SPB Marriage and Divorce consist in the creation and termination, respectively, of a persistent, monitored connection (electrical and physical) between two Secure Processing Blocks.

Forensic Marking – Forensic Marking (FM) is the embedding of tracking information into sound and/or image essence by the Image Media Block during playback.

SPB Shutdown and Initialization – SPB Shutdown and Initialization mean that execution of the firmware on the SPB has been terminated or started, respectively.

Sequence Number – refers to a count of KLV encrypted triplets in a track file, counted using the method defined in Section 7.9 “Sequence Number” of [TFE] (2006).

Main Asset – The Main Asset in a CPL shall be the Main Picture asset if present. If the Main Picture asset is not present, the Main Asset shall be the picture related asset that references the picture elements to be projected on the main screen. If no main screen picture related asset is present in the CPL, the Main Asset shall be the first asset — according to the Reel assets sequence order defined in SMPTE 429-7 — that is used in the CPL Reels.

5.2 Definitions of Processes and Validation

5.2.1 Composition Playlist Validity

A Composition Playlist is valid if all of the following conditions are satisfied.

- The message digest of all assets referenced by the Composition Playlist matches the corresponding message digest stored in the Hash element of the CPL, as defined in Section 8.2.2 of SMPTE 429-7.
- The digital signature recorded in the Signature element, including the certificates contained therein, is valid per the provisions of [D-Cert].

5.2.2 Frame Playback Process

The Frame Playback Process consists of

- The decryption of essence according to [TFE]; followed by:
- The validation of the integrity of essence using the Check Value and MIC, as defined in [TFE]; followed by:
- The optional forensic marking of essence; and finally followed by:
- The optional encryption of essence and transmission to a downstream device (i.e. link encryption).

5.2.3 Complete CPL Playback

A complete composition playlist (CPL) playback is the playback of a composition Playlist from the first edit unit of the first Reel to the last edit unit of the last Reel without exception, operator intervention or other interruptions.

5.3 Security Event Class

This document defines and constrains the Security Log Event Class. Log Records of this class shall conform to the specifications and constraints in this document. This document also definesEvent Types and Event Sub Types for the Security Event Class. Log Records in this class shall be identified by the URI of the Security Class Namespace Name defined in Section 5.4 appearing in the EventClass element of the Log Record Header as defined in [LogRecord].

Note: The Security Event Class only includes events which are specifically and clearly security related. Other events that occur in the system could be construed as security related or not, depending upon individual interpretation, and upon whether or not they can reasonably occur in normal operation or equipment service. For example, logging a short loss of power, or the theft of an entire system, is outside of the scope of this standard.

5.4 Security Class Namespace

This document declares fragment identifiers in an XML namespace, whose Namespace Name (URI) shall be:

```
"http://www.smpte-ra.org/430-5/2008/SecurityLog/"
```

There are no types defined in this namespace.

5.5 Namespace Prefixes

The following table defines the namespace prefixes used in the XSDL and XML examples in this document. Please refer to the normative references in this document and in [DCMLTypes] for specific references to the namespaces referred to in this table. Note that the prefixes themselves are not normative, and that instance documents may assign alternative prefixes in practice.

Prefix	Namespace Reference
xs	XMLSchema
ds	XMLDsig
xsi	XMLSchema-Instance
dcml	DcmlTypes
lr	LogRecord

5.6 Reference Architectures

This specification is based on the use of one of the two architectures depicted in Figure 1.

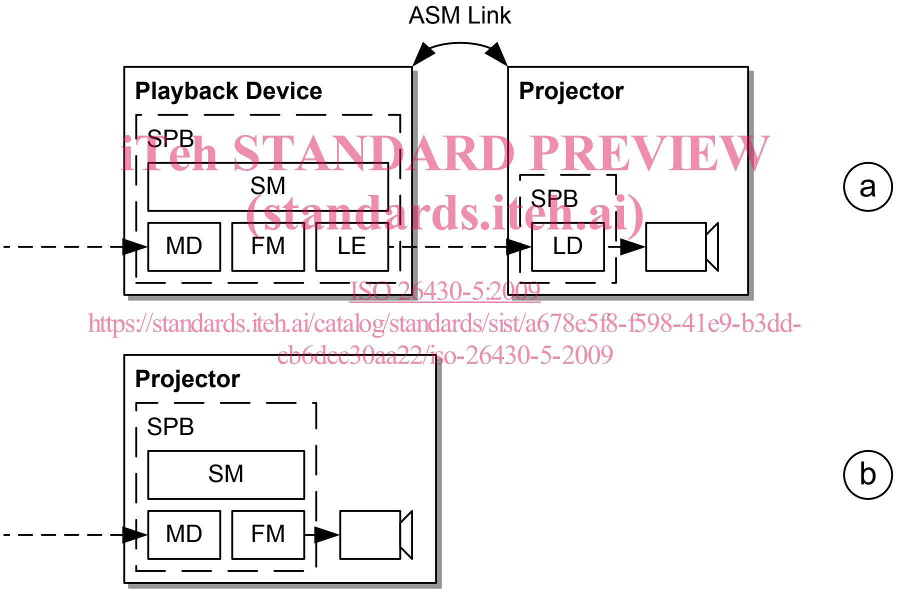

Figure 1 – Reference Architectures. Architecture (a) consists of two distinct Secure Processing Blocks sharing an Auditorium Security Link. Architecture (b) consists of a single Secure Processing Block.

6 Security Application Requirements

When a security system is requested to produce log records, that system should produce the records in a format based on the Log Record Specification for D-Cinema [LogRecord] as constrained by this document. Security Log Reports may contain any number of records. Security Devices may also provide status information through other means, such as real-time messaging, but such messages are not intended to be used as records of security events for forensic purposes, and are outside of the scope of this document.

6.1 Security Constraints

When Log Records are created in a security context, the following constraints and requirements shall be applied to the structure and content of each Log Record and Log Report containing those records. These constraints shall be applied in addition to the constraints specified in [LogRecord].

6.1.1 Log Record Header

The following constraints shall apply to the use of elements in the Log Record Header of a Security Log Record.

6.1.1.1 Time Stamp (Secure Time)

All time stamps shall be derived from a secure time source located in the Security Device which recorded the event. The source or reference for that time source is outside of the scope of this document. The TimeStamp element of the Log Record Header shall be set to a value corresponding to the time that the Security Log Event was detected.

6.1.1.2 Event Sequences

All Log Record Headers in a Security Log Report shall contain the EventSequence element. Within each signed sequence in a Security Log Report, the value of the EventSequence element in each Log Record shall increase strictly (i.e. shall never remain the same or decrease) throughout the sequence.

If a single Security Log Record is signed individually (not as part of a sequence), the EventSequence element of the Log Record Header shall not be present.

6.1.1.3 Device Source Identifiers

The DeviceSourceID list element in each Log Record Header shall contain the Certificate Thumbprint of the security device that reported or recorded the Security Log Event, i.e. the device that the Event applies to.

6.1.1.4 Event Classes

A Log Report may contain events which are not classified as Security Events. If such events are included, they shall be treated as part of the Log Record Sequence. When a logged event is a Security Event, the content of the EventClass element of the Log Record Header shall be the Security Class Namespace Name URI defined in Section 0 of this document.. Events which must be treated as Security Events are listed elsewhere in this document.

6.1.1.5 Hashes

The PreviousHeaderHash element shall be required in all Log Record Headers, except on the first record in a sequence. If the PreviousHeaderHash field is included in the first record in a sequence, its value shall be zero expressed as a valid message digest value (i.e the message digest of the value zero). The PreviousHeaderHash element shall be calculated according to the algorithm specified in [LogRecord].

The RecordBodyHash element shall be required in all Log Record Headers for all Security Events, whether the Log Record is part of a sequence or not. The RecordBodyHash element shall be calculated according to the algorithm specified in [LogRecord].

6.1.2 Log Record Body

The following constraints shall apply to the body of a Security Log Record defined in this class document.