

SMPTE STANDARD

D-Cinema Operations —
Security Log Event
Class and Constraints



Table of Contents	Page
Foreword	2
Intellectual Property	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 SubTypes	12
7.3.1 Playout Event SubTypes	12
7.3.2 Validation Event SubTypes	14
7.3.3 Key Event SubTypes	15
7.3.4 ASM Event SubTypes	16
7.3.5 Operations Event SubTypes	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

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 ST 430-5 was prepared by Technology Committee 21DC.

Intellectual Property

At the time of publication no notice had been received by SMPTE claiming patent rights essential to the implementation of this Standard. However, attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. SMPTE shall not be held responsible for identifying any or all such patent rights.

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

Note: All references in this document to other SMPTE documents use the current numbering style (e.g. SMPTE ST 433:2008) although, during a transitional phase, the document as published (printed or PDF) may bear an older designation (such as SMPTE 433-2008). Documents with the same root number (e.g. 433) and publication year (e.g. 2008) are functionally identical.

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>