SMPTE STANDARD

D-Cinema Operations — Security Log Event Class and Constraints

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

Approved March 3, 2008
Correction to Title made on June 26, 2009

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.

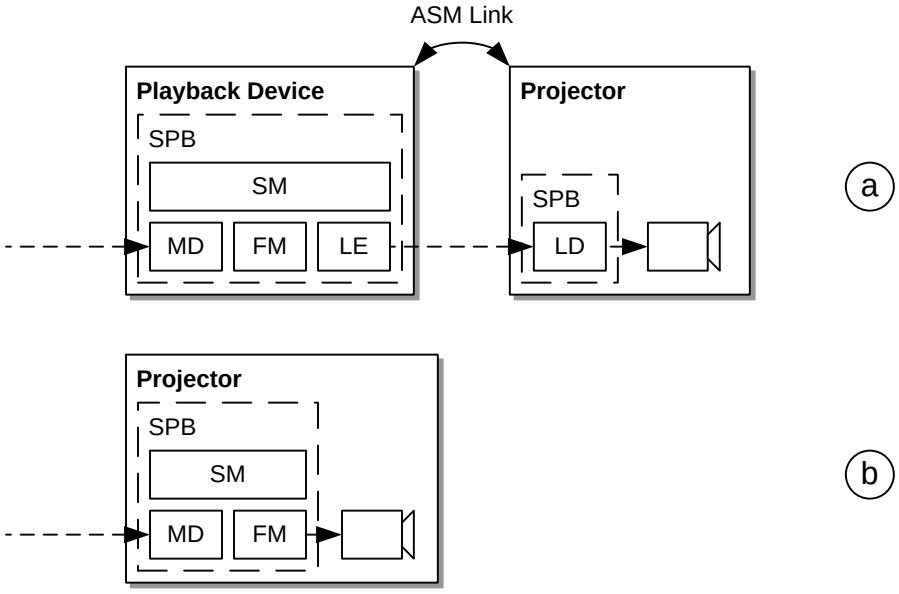

Figure 1 – Reference Architectures. Architecture (a) consists of two distinct Secure Processing Blocks sharing an Auditorium Security Link. Architecture (b) consists of a single Secure Processing Block.

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.

6.1.2.1 Event Types, Sub Types, and Parameters

If the EventClass field in the record header is set to the Security class, the EventType element of the associated Log Record Body shall be one of the Security Event Types defined in this document. If that Security Event Type has a required subtype, the EventSubType element shall be present, and shall contain an Event Sub Type defined in this document. If that Security Event Type or Subtype requires parameters, the Parameters element of the Log Record Body shall be present, and those parameters shall be supplied in the Parameters list of the Log Record Body.

Note: Types, Subtypes, Parameters, and Type Scopes for Security Log Messages are specified in the Security Event Definitions section of this document.

6.1.2.2 Key Delivery Message Identifier

If the event recorded in the Log Record is a Security Event, and that Security Event involves the usage or verification of a Key Delivery Message, the KeyDeliveryMessageID element of the Log Record Body shall be present. The contents of the MessageId element of the instant Key Delivery Message (KDM) shall be provided as the value of this element.

6.1.2.3 Composition and Track File Identification

If a Security Log Event relates to the processing of a Composition or a Track File, the Log Record Body shall include a ReferencedIDs list that shall contain a name/value pair whose IDName element shall contain either the token “CompositionID” or the token “TrackfileID” , and whose IDValue element shall contain the Composition Playlist Identifier or Track File Identifier respectively. In the case of a Composition Playlist identifier, this value shall be the UUID taken from the Id element of the Composition Playlist Structure [CPL]. In the case of a Track File Identifier, this value shall be a UUID which is taken from the Package UID of the (sole) Top-level File Package of the identified Track File [TRK], or the contents of the Id element of the Subtitle Reel element of a subtitle track file, or from such other unique identifiers as SMPTE may designate in Track Files defined in future standards.

A device that is not processing one of these entities directly, such as a Link Decryptor, may not know the identity of the content that it is processing. In that case, the composition or trackfile associated with that content may be inferred from the Log Record sequence, but the associated fields in the Log Record Body may be omitted by the reporting device.

6.1.2.4 Exceptions

If one of the Exceptions identified in the Event Sub Type Record descriptions in this document is detected, the Security Device shall include an Exception record as specified in the Event Sub Type definitions in Section 7.3 of this document.

6.1.3 Log Record Signature

Authenticated Log Records shall be required for all Security class Log Records in Log Reports. Thus Log Record Signatures shall be included as specified in [LogRecord] and related sections of this document, either on individual Log Records or on sequences of Log Records in Log Reports. Log Record Signatures placed at the end of a sequence or in a single record shall include the RecordAuthData element and its sub-elements, and shall include the Signature element. The Digest Method for the RecordAuthData element shall be SHA-1. The Signature Method for the SignedInfo element of the Signature shall be RSA-SHA-256.

In the Log Record Signature, the KeyInfo element shall be present and shall contain the entire certificate chain for the signer. The Object element shall not be present and the URI attribute of the Reference element shall be set to: " " (empty string), as the signature is enveloped. The Reference element shall contain a single DigestMethod element, with its Algorithm attribute set to the URI value “`http://www.w3.org/2000/09/xmldsig#sha1`".

The Reference element shall contain a single Transform element, with its Algorithm attribute set to the URI value "`http://www.w3.org/2000/09/xmldsig#envelopedsignature`".

The CanonicalizationMethod shall be set to the URI value "`http://www.w3.org/TR/2001/REC-xml-c14n-20010315`".

The SignatureMethod shall be set to the URI value "`http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`" [RFC 4051].

The entire certificate chain shall be carried in the KeyInfo element as a sequence of X509Data elements. Each of the X509Data elements shall correspond to one certificate in the chain, and contain one X509IssuerSerial element and one X509Certificate element. The Distinguished Name value in all X509IssuerName elements shall be compliant with RFC 2253 per [XML-Signature Syntax and Processing].

6.2 Security Log Record Authentication and Chaining

Security Log Records and Reports shall be authenticated using the mechanisms described in [LogRecord]. Individual Log Records may be authenticated by signing each record individually. Security Log Reports shall consist of one or more sequences of Log Records in authenticated chains. Each sequence shall be signed by a Log Record Signature at the end of each sequence. Each Signature shall be signed with the Digital Cinema Certificate of the Security Device that generates the Log Record or sequence of Log Records.

7 Security Event Definitions

The Log Record Format Specification for D-Cinema [LogRecord] defines a general format for Log Records. While that specification defines Event Classes, it leaves the specific definition of the content of the Event Classes to application specifications such as this one. In this section, the Event Types, Event Sub Types, their scope identifiers, and Event Parameters for the Security Class are defined.

Each Security Log Record shall contain at least the following elements:

- **EventClass** – This element shall contain the Security Class Namespace Name specified in Section 5.4.
- **EventType** – This element shall contain an Event Type token as specified in this section.
- **EventSubType** – This element shall contain an Event Sub Type token from the list specified in this section for the corresponding EventType.

Within the "security" event class, the following types, subtypes, scopes, and parameters shall represent a hierarchy of security event identifiers, which shall be used in the EventType, EventSubType, and Parameters elements of Security Log Record Body elements.

Note: See the definition of the Named Parameter Type and the Parameter List Type in [DCMLTypes] for a more complete explanation of XML Parameter Lists, and additional examples.

When parameters are specified in the Event Sub Type sections below, a Security Log Record may include a RecordTextExtention element to additionally frame the parameters in a textual description of the Log Event. A logging device may also include additional parameters beyond the ones specified in the tables.

7.1 ReferencedID Scope

Within the ReferencedIDs element of the Log Record Body, The IDName element of each ReferencedID is a scopedTokenType. These tokens are defined in this section. These tokens shall comprise a scope, which shall be represented by the following scope identifier in URI form:

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

Instance documents shall either use this scope for ReferenceID IDNames, or may create an extended scope which contains the same members as this scope, with the same meanings, as the basis for the extended scope. If no scope identifier is present in the IDName elements of the ReferenceID elements of the ReferenceIDs element of the Log Record Body, then this scope shall be taken as the default scope.

The Tokens that comprise this scope and the definitions of the UUIDs contained in the IDValue part of the corresponding name/value pair shall be as defined in the following table.

ReferencedID IDName Scope	
Token	**Description of Value**
KeyDeliveryMessageID	If present, the KeyDeliveryMessageID value shall be the UUID that identifies the Key Delivery Message currently being processed by the reporting device, if the event is related to key usage or key validation. This UUID shall be taken from the MessageId element of the Authenticated Public section of the KDM.
CompositionID	If present, the CompositionID value shall contain the UUID of the current composition at the time of the event, if any. This UUID shall be taken from the Id element of the Composition Playlist structure.
TrackFileID	If present, the TrackFileID value shall be the UUID of the current Track File which is the subject of the Log Event. As appropriate, this UUID shall either be the Package UID value of the (sole) Top-level File Package of the identified Track File, per [SMPTE 429.3], or the contents of the Id element of the SubtitleReel element of a subtitle track file per [SMPTE 429.5], or the designated unique identifier of other track file types that SMPTE may define.

7.2 Event Types

The content of the EventType element in the Log Record Body shall be a token from the following table. The set of tokens listed in this table shall be represented by the following scope identifier in URI form:

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

When a Security Log Record is created, the EventType element of the Log Record Body should include this scope attribute. If no scope attribute is included, but the EventClass element of the Log Record Header contains the value of the URI specified in Section 5.4 of this document, then this scope shall be taken to be the default scope. If a different scope attribute is included in the EventType element, that scope shall define the meaning of the EventType value. Any such alternate scope, where defined, shall also define Event Sub Types and Parameters for the tokens defined in that scope.

Security Log Event Type Tokens	
Token	**Description**
Playout	Playout security Event type. Events related to content playout.
Validation	Security System Validation
Key	Key Related Event
ASM	Auditorium Security Message Event
Operations	An Event related to the operation of an SPB or an SPB's contents.

7.3 Event Sub Types

Each of the following Subtype tables defines the subtypes and parameters for one of the Event Types defined in the previous section.

7.3.1 Playout Event Sub Types

If the content of the EventType element is the "Playout" token, the content of the EventSubType element shall be a token from the following table. The set of tokens listed in this table shall be represented by the following scope identifier in URI form:

"http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-playout"

Security Log Event --Playout-- Event Subtype Tokens	
Token	**Description**
FrameSequencePlayed	A specified sequence of frames from a track file has been played as defined in Section 5.2.2 of this standard
CPLStart	The first edit unit of the Main Asset of the first reel of a target CPL has been played by a device
CPLEnd	The last edit unit of the Main Asset of the last Reel of a target CPL has been played by a device
PlayoutComplete	The target CPL has been played without interruption of exception by a device as per Section 5.2.3 of this standard

7.3.1.1 FrameSequencePlayed Record

Each FrameSequencePlayed Record shall at a minimum contain the following elements with values as specified below. Note that this record will never be created for track files which are not encrypted per [TFE].

Note: If an attempt to play a sequence of frames fails, this Record should be generated with an appropriate exception.

- The ContentID element shall contain the ID of the CPL that specified the playout of the track file that has been played
- The TimeStamp element shall contain the time at which the frame sequence playout completed.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the device that played the frame sequence
- The ReferencedIDs list shall contain a name/value pair whose IDName element shall contain the token “TrackFileID” and whose IDValue element shall contain the ID of the track file that was played.
- The ReferencedIDs list shall contain a name/value pair whose IDName element shall contain the token “KeyDeliveryMessageID” and whose IDValue element shall contain the MessageID of the KDM from which the content decryption key was obtained to decrypt the track file.
- The Parameters list shall contain a name/value pair whose Name element shall contain the token “AuthId” and whose Value element shall contain the identifier of the entity that authorized the action that triggered the Event logged in this Record.

- The Parameters list shall contain a name/value pair whose Name element shall contain the token “FirstFrame” and whose Value element shall contain the Sequence Number of the first frame played in the sequence. Sequence Number is defined in Section 5.1.

- The Parameters list shall contain a name/value pair whose Name element shall contain the token “LastFrame” and whose Value element shall contain the Sequence Number of the last frame played in the sequence.

- If the track file is an image track file, the Parameters list shall contain a name/value pair whose name element shall contain the token ImageMark, and whose Value element shall contain one of two tokens, either “true” or “false”, indicating that a forensic mark was or was not inserted during playout.

- If the track file is an audio track file, the Parameters list shall contain a name/value pair whose name element shall contain the token AudioMark, and whose Value element shall contain one of two tokens, either “true” or “false”, indicating that a forensic mark was or was not inserted during playout.

- If the decrypted content was sent to a downstream device which has a Security Certificate, the Parameters list shall contain a name/value pair whose Name element shall contain the token “DownstreamDevice” and whose Value element shall contain the Certificate Thumbprint of the downstream device.

In addition to the minimum elements, the following exceptions are defined in the case of a exception or playout failure. One or more exceptions may be listed in the Exceptions element of the Log Record. The following exceptions apply to FrameSequencePlayed records:

CheckValueError, FrameMICError, FrameSequenceError, TrackFileIDError, ContentAuthenticatorError, TDLError, KeyTypeError, ValidityWindowError. See Section 7.4 for definitions of these exceptions.

7.3.1.2 CPLStart Record

This record indicates that the first edit unit of the Main Asset of the first Reel of a Composition has been processed by a device. Each CPLStart record shall at a minimum contain the following elements with values as specified below.

- The ContentID element shall contain the ID of the CPL that specified the playout of the track file that the first edit unit was played from.

- The TimeStamp element shall contain the time at which the edit unit was played.

- The DeviceSourceID element shall contain the Certificate Thumbprint of the device that processed the edit unit.

No specific Exceptions are defined for this Record.

7.3.1.3 CPLEnd Record

This record indicates that the last edit unit of the Main Asset of the last Reel of a Composition has been processed by a device. Each CPLEnd record shall at a minimum contain the following elements with values as specified below.

- The ContentID element shall contain the ID of the CPL that specified the playout of the track file that the last edit unit was played from.

- The TimeStamp element shall contain the time at which the edit unit was played.

- The DeviceSourceID element shall contain the Certificate Thumbprint of the device that processed the edit unit.

No specific Exceptions are defined for this record.

Informative Note: The events that generate the CPLStart and CPLEnd records can be detected by noting a change in the ContentID elements of successive FrameSequencePlayed events, except in the case where the same CPL is played twice in sequence.

7.3.1.4 PlayoutComplete Record

This record indicates that a CPL has been processed without interruption or exception by a device as per section 0 of this standard. Each PlayoutComplete Record shall at a minimum contain the following elements with values as specified below.

- The ContentID element shall contain the ID of the CPL that specified the Composition.
- The TimeStamp element shall contain the time at which the playout process completed.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the device that performed the playout process.
- The Parameters list shall contain a name/value pair whose Name element shall contain the token “AuthId” and whose Value element shall contain the identifier of the entity that authorized the action that triggered the Event logged in this Record.

No specific Exceptions are defined for this Record.

7.3.2 Validation Event Subtypes

If the content of the EventType element is the "Validation" token, the content of the EventSubType element shall be a token from the following table. The set of tokens listed in this table shall be represented by the following scope identifier in URI form:

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

Security Log Event --Validation-- Event Subtype Tokens	
Token	**Description**
CPLCheck	A CPL has been validated according to Section 5.2.1 of this document.

7.3.2.1 CPLCheck Record

Each CPLCheck Record shall at a minimum contain the following elements with values as specified below.

- The TimeStamp element shall contain the time at which the validation process completed.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the Device Certificate of the validating entity.
- The ContentID element shall contain the CPL ID as specified in [LogRecord].

- If the CPL contains a valid signature, the Parameters list shall contain a name/value pair with the Name set to SignerID and the Value containing the Certificate Thumbprint of the certificate that was used to sign the CPL.

In addition to the minimum elements, the following exceptions are defined in the case of a validation failure. One or more exceptions may be listed in the Exceptions element of the Log Record. The following exceptions apply to CPLCheck records:

CPLFormatError, CertFormatError, AssetHashError, AssetMissingError, SignatureError. Refer to Section 7.4 for descriptions of these exceptions.

7.3.3 Key Event Sub Types

If the content of the EventType element is the "Key" token, the content of the EventSubType element shall be a token from the following table. The set of tokens listed in this table shall be represented by the following scope identifier in URI form:

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

Security Log Event --Key-- Event Subtype Tokens	
Token	**Description**
KDMKeysReceived	Indicates that a device has retrieved a list of plaintext keys from a given KDM.
KDMDeleted	Indicates that a device has permanently purged a KDM and its associated Keys.

7.3.3.1 KDMKeysReceived Record

Each KDMKeysReceived Record shall at a minimum contain the following elements with values as specified below.

- The ContentID element shall contain the Id of the CPL associated with the KDM.
- The TimeStamp element shall contain the time at which the process completed.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the device that retrieved the plaintext keys.
- The ReferencedIDs list shall contain a name/value pair whose IDName element shall contain the token “KeyDeliveryMessageID” and whose IDValue element shall contain the Message ID of the KDM.
- If the KDM signature is valid, the Parameters list shall contain a name/value pair with the Name set to SignerID and the Value containing the Certificate Thumbprint of the certificate that was used to sign the KDM.

In addition to the minimum elements, the following exceptions are defined in the case of a processing failure. One or more exceptions may be listed in the Exceptions element of the Log Record. The following exceptions apply to KDMKeysReceived records:

KDMFormatError, CertFormatError, SignatureError. Refer to Section 7.4 for descriptions of these exceptions.

7.3.3.2 KDMDeleted Record

Each KDMDeleted Record shall at minimum contain the following elements with values as specified below.

- The ContentID element shall contain the Id of the Composition Playlist associated with the KDM.
- The TimeStamp element shall contain the time at which the deletion process was completed.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the device that deleted the KDM.
- The ReferencedIDs list shall contain a name/value pair whose IDName element shall contain the token “KeyDeliveryMessageID” and whose IDValue element shall contain the Message ID of the KDM

No specific exceptions are defined for this record.

7.3.4 ASM Event Sub Types

If the content of the EventType element is the "ASM" token, the content of the EventSubType element shall be a token from the following table. The set of tokens listed in this table shall be represented by the following scope identifier in URI form:

"http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-ASM"

Security Log Event –ASM-- Event Subtype Tokens	
Token	**Description**
LinkOpened	A link has been opened between two devices using the [ASM] protocol
LinkClosed	An [ASM] link between two devices has been closed
LinkException	An exception occurred on an open [ASM] link
LogTransfer	A device has transferred a log record or records to another device on an [ASM] link
KeyTransfer	A device has transmitted a key to another device on an [ASM] link

7.3.4.1 ASM LinkOpened Record

Each LinkOpened record shall at a minimum contain the following elements with values as specified below.

- The TimeStamp element shall contain the time at which the link was opened.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the device logging the event.
- The Parameters list shall contain a name/value pair with the Name element containing the token “DeviceConnectedID” and the Value element containing the Certificate Thumbprint of the device at the other end of the [ASM] link.

In addition to the minimum elements, the following exceptions are defined in the case of a link opening failure. One or more exceptions may be listed in the Exceptions element of the Log Record. The following exceptions apply to LinkOpened records:

CertFormatError, TLSError. Refer to Section 7.4 for the descriptions of these exceptions.

Note: The DeviceSourceID element in a LinkOpened Record may identify either the initiator or responder in an ASM connection.

7.3.4.2 ASM LinkClosed Record

Each LinkClosed record shall at a minimum contain the following elements with values as specified below.

- The TimeStamp element shall contain the time at which the link was closed.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the device logging the event.
- The Parameters list shall contain a name/value pair with the Name element containing the token "DeviceConnectedID" and the Value element containing the Certificate Thumbprint of the device at the other end of the [ASM] link.

In addition to the minimum elements, the following exception is defined in the case of a link close failure. One or more exceptions may be listed in the Exceptions element of the Log Record. The following exception applies to LinkClosed records:

TLSError. Refer to Section 7.4 for the description of this exception.

Note: The DeviceSourceID element in a LinkClosed Record may identify either the initiator or responder in an ASM connection.

7.3.4.3 ASM LinkException Record

Each LinkException record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the time at which the exception was noted.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the device logging the event.
- The Parameters list shall contain a name/value pair with the Name element containing the token "DeviceConnectedID" and the Value element containing the Certificate Thumbprint of the device at the other end of the [ASM] link.

In addition to the minimum elements, the following exceptions are defined in the case of a link exception. One or more exceptions may be listed in the Exceptions element of the Log Record. The following exceptions apply to LinkException records:

QuerySPBError, QuerySPBAlert, ASMMessageError. Refer to Section 7.4 for the description of these exceptions.

7.3.4.4 ASM LogTransfer Record

Each LogTransfer record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the time at which the Log Transfer completed.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the initiating device.
- The Parameters list shall contain a name/value pair with the Name element containing the token "DeviceConnectedID" and the Value element containing the Certificate Thumbprint of the device at the other end of the [ASM] link. (The responder in this case.)

In addition to the minimum elements, the following exceptions are defined in the case of a LogTransfer error. One or more exceptions may be listed in the Parameters of the Log Message. The following exceptions apply to LogTransfer records:

ASMLogRequestFailed. Refer to Section 7.4 for the description of this exception.

Note: The DeviceSourceID element in a LogTransfer Record may identify either the initiator or responder in an ASM connection.

7.3.4.5 ASM KeyTransfer Record

Each KeyTransfer record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the time at which the Key Transfer completed.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the initiator device.
- The Parameters list shall contain a name/value pair with the Name containing the token “DeviceConnectedID” and the Value containing the Certificate Thumbprint of the device at the other end of the [ASM] link, in this case, the responder.

No specific exceptions are defined for this record.

Note: The DeviceSourceID in a KeyTransfer Record may identify either the initiator or responder in an ASM connection.

7.3.5 Operations Event Sub Types

If the content of the EventType element is the "Operations" token, the content of the EventSubType element shall be a token from the following table. The set of tokens listed in this table shall be represented by the following scope identifier in URI form:

"http://www.smpte-ra.org/430-5/2008/SecurityLog/#EventSubTypes-operations"

Security Log Event --Operations-- Event Subtype Tokens	
Token	**Description**
SPBOpen	An SPB perimeter has been opened
SPBClose	An SPB perimeter has been closed
SPBMarriage	Two SPBs have been “Married” per the definition in Section 5.1 of this standard.
SPBDivorce	Two SPBs have been “Divorced” per the definition in Section 5.1 of this standard.
SPBShutdown	The operating software of an SPB has shut down per the definition in Section 5.1
SPBStartup	The operating software of an SPB has been started per the definition in Section 5.1
SPBClockAdjust	The time of a secure clock within an SPB was adjusted.
SPBSoftware	The operating software of an SPB was modified..
SPBSecurityAlert	An SPB is reporting a Security Log Event not listed in this document.

7.3.5.1 SPBOpen Record

Each SPBOpen record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The Timestamp element shall contain the time at which the SPB perimeter was opened.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the SPB.
- The Parameters list shall contain a name/value pair whose Name element shall contain the token "AuthId" and whose Value element shall contain the identifier of the entity that authorized the action that triggered the Event logged in this Record.

No specific exceptions are defined for this record.

7.3.5.2 SPBClose Record

Each SPBClose record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the time at which the SPB perimeter was closed.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the SPB.
- The Parameters list shall contain a name/value pair whose Name element shall contain the token "AuthId" and whose Value element shall contain the identifier of the entity that authorized the action that triggered the Event logged in this Record.

No specific exceptions are defined for this record.

7.3.5.3 SPBMarriage Record

Each SPBMarriage record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the time at which the marriage occurred.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the SPB that logs this event.
- The Parameters list shall contain a name/value pair with the Name set to DeviceConnectedID and the Value containing the Certificate Thumbprint of the device which is the other partner in the marriage.
- The Parameters list shall contain a name/value pair whose Name element shall contain the token "AuthId" and whose Value element shall contain the identifier of the entity that authorized the action that triggered the Event logged in this Record.

No specific exceptions are defined for this record.

Note: This record may be logged by both of the partner SPBs.

7.3.5.4 SPBDivorce Record

Each SPBDivorce record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the time at which the divorce occurred.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the SPB that logs this event.
- The Parameters list shall contain a name/value pair with the Name set to DeviceConnectedID and the Value containing the Certificate Thumbprint of the device which was the other partner in the marriage.
- The Parameters list shall contain a name/value pair whose Name element shall contain the token “AuthId” and whose Value element shall contain the identifier of the entity that authorized the action that triggered the Event logged in this Record.

No specific exceptions are defined for this record.

Note: This record may be logged by both of the partner SPBs.

7.3.5.5 SPBShutdown Record

Each SPBShutdown record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the approximate time at which the shutdown occurred to a tolerance of +/– ten seconds.
- The DeviceSourceID element shall contain the Certificate Thumbprint of the SPB that logs this event.

No specific exceptions are defined for this record.

7.3.5.6 SPBStartup Record

Each SPBStartup record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the time at which the initialization operation completed..
- The DeviceSourceID element shall contain the Certificate Thumbprint of the SPB that logs this event.

No specific exceptions are defined for this record.

7.3.5.7 SPBClockAdjust Record

Each SPBClockAdjust record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the time at which the adjustment took place, based on the new timeline after the adjustment..

- The DeviceSourceID element shall contain the Certificate Thumbprint of the SPB that logs this event.

- The Parameters list shall contain a name/value pair whose Name element shall contain the token “AuthId” and whose Value element shall contain the identifier of the entity that authorized the action that triggered the Event logged in this Record.

- The Parameters list shall contain a name/value pair with the Name containing the token “TimeOffset” and the Value containing the number of seconds by which the clock was adjusted.

In addition to the minimum elements, the following exceptions are defined in the case of a clock adjustment error. One or more exceptions may be listed in the Exceptions element of the Log Message. The following exceptions apply to SPBClockAdjust records:

AdjustmentRangeError. Refer to Section 7.4 for the description of this exception.

7.3.5.8 SPBSoftware Record

Each SPBSoftware record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more exceptions may be included, or the UnknownError exception may be included if none of the defined exceptions are appropriate.

- The TimeStamp element shall contain the time at which the software was modified.

- The DeviceSourceID element shall contain the Certificate Thumbprint of the SPB that logs this event.

- The Parameters list shall contain a name/value pair whose Name element shall contain the token “AuthId” and whose Value element shall contain the identifier of the entity that authorized the action that triggered the Event logged in this Record.

- The Parameters list shall contain a name/value pair with the Name set to SignerID and the Value containing the Certificate Thumbprint of the signer of the new software package.

- The Parameters list shall contain a name/value pair with the Name set to SoftwareVersion and the Value containing a string describing at least the version of the new software package.

In addition to the minimum elements, the following exceptions are defined in the case of an error. One or more exceptions may be listed in the Exceptions element of the Log Record. The following exceptions are defined for SPBSoftware records:

SoftwareFailure. Refer to Section 7.4 for the description of this exception.

7.3.5.9 SPBSecurityAlert Record

Each SPBSecurityAlert record shall at a minimum contain the following elements with values as specified below. In addition to these elements, one or more additional parameters and one or more exceptions may be included, or the UnknownError exception may be included.

- The TimeStamp element shall contain the time at which the event occurred.

- The DeviceSourceID element shall contain the Certificate Thumbprint of the SPB that logs this event.

No specific exceptions are defined for this record.

Note: This record is intended to be used as a generic exception for the purpose of logging events associated with SPB functional aberrations or intermittent failures. Details of such events are expected to be added by implementers as additional parameters or exceptions to this Record. It would be helpful if implementers included a RecordTextExtension element to describe the nature of the event.

7.4 Exception Tokens and Definitions

The following table defines standard tokens, which identify exceptions in Security Log Records, and describes the meaning of each exception when it is used. These standard tokens shall be used in the Name element of a name/value pair, and additional information about the exception may be provided in the Value element. If no additional information is available, the Value element of the name/value pair shall still be present. . These name/value pairs shall be included in the Exceptions element of the Log Record Body as specified in [LogRecord].

Token String	Description
CPLFormatError	Indicates that the CPL did not meet the normative language of SMPTE 429-7.
CertFormatError	Indicates that the Signer Certificate of the referenced object did not meet the normative language of SMPTE 430-2.
AssetHashError	Indicates that the computed hash of one of the assets referenced by the CPL did not match the value recorded in the optional Hash element of the Asset element of the CPL.
AssetMissingError	Indicates that one or more of the assets referenced in a CPL was not available.
SignatureError	Indicates that the digital signature of the referenced object did not validate.
KDMFormatError	Indicates that a KDM did not meet the normative Language of [KDM].
CheckValueError	At least one Check Value within a range of frames processed did not match the Check Value specified in [TFE] Table 11.
FrameMICError	Indicates that a MIC check failed on one or more frames of a track file.
FrameSequenceError	Indicates that a frame sequence check failed on two or more frames of a track file.
TrackFileIDError	Indicates that a TrackFileID check against the associated CPL failed.
ContentAuthenticatorError	Indicates that the Signer of a CPL does not match the Content Authenticator of a KDM that enables that CPL. See [KDM] Section 5.2.4.
TDLError	At least one downstream device from a media block did not appear on the TDL of the KDM that was to be used to decrypt content.
KeyTypeError	A KDM supplied a key of the wrong KeyType for a track file. (e.g. an image track file KeyID pointed to an audio KeyType in the KDM.) See [KDM].
ValidityWindowError	Indicates that decryption failed due to an attempt to use a KDM outside of its validity window.
TLSError	Indicates that an [ASM] connection detected an error in an underlying TLS session.
UnknownError	Indicates that an unspecified error occurred.
QuerySPBError	(Initiator Only) A responder failed to respond to a QuerySPB message per the requirements of [ASM].
QuerySPBAlert	(Initiator Only) A responder returned a “Security Alert” response to a QuerySPB command from an initiator per [ASM].
ASMMessageError	Either an initiator or a responder received a request or response that did not meet the normative requirements of [ASM].
ASMLogRequestFailed	A log transfer request did not result in a complete response per [ASM].
SoftwareFailure	Replacement or modification of software on an SPB failed.
AdjustmentRangeError	An attempt to make an adjustment outside of an allowable range failed.

8 Examples (Informative)

8.1 Example 1

Note: This Informative Example has been removed from this document to facilitate maintenance and processing with tools suitable to the purpose. If you are reviewing this document, you should have been provided with an up to date version of the informative example in electronic form. The name of the file should be "SecurityReportExampleSigned.xml".

9 Glossary of Acronyms

- SHA-1 – Secure Hash Algorithm revision 1
- TLS – Transport Layer Security protocol
- MIC – Message Integrity Code - used to check content integrity– see SMPTE 429-6
- TDL – Trusted Device List

Annex A (Informative)
Proxy Logging

A Security Device may produce Security Log Records for Security Log Events that are reported by another Security Device via an authenticated secure channel. The security properties of that authenticated secure channel are outside of the scope of this document. If a Security Device performs this function, it shall act as a Proxy for the logging function, By acting as a Proxy, it shall implicitly assert that it has authenticated the other Security Device, and has established a secure channel to receive the Security Log Data that constitutes the Proxy Logged Security Log Events.

Annex B (Informative)
Security Log Report Filtering

In order to support confidentiality requirements of Log Event reporting, while at the same time assuring that Log Report tampering is detected, this specification supports Log Report Filtering. Log Reports may be filtered to remove the Log Record Body section of any selected records, while preserving the associated Log Record Header for all Log Records in the report. Recipients may examine a filtered Log Report that records content key usage over a period of time, for example, and verify that no records have been deleted from the report, although not all record bodies may be present.

Verification of Log Report Header chaining and Log Body Data validation are described in [LogRecord].