MXF AS-07 Application Specification (work in progress)

Working draft of sections pertaining to content integrity, aka fixity

Draft 2-18-2014. For more information, contact Carl Fleischhauer cfle@loc.gov

This is an excerpt from the main body of the application specification. Since this draft is being circulated for review, it begins with an extensive explanatory informative section. Tables in an appendix referenced in the text are appended to this excerpt.

6.6.2 Content Integrity

6.6.2.1 Content Integrity Objective and Relevant Standards (informative)

Content in AS-07 files will often be destined for long term archiving-and-preservation management. This objective is supported by a number of actions, including the creation of fixity or hash values and the monitoring of those values for change over time. In other MXF Application Specifications, this objective is called media integrity.

For digital library specialists, content or media integrity usually turns on whole-file fixity values, critical for a well-run asset management system. But whole-file fixity data cannot be embedded in the file itself: that action would change the file, making the hash value "next time" different, thus invalidating it for comparison and monitoring. Whole-file checksums are a critical part of storage and repository systems but have no place in a file-wrapper specification. For file wrappers, a good fit is provided by specifying a carriage location for hash values on segments of the file, e.g., on a frame or some other small unit of video.

AS-07 calls for the embedding of fixity data on the *V* or *value* data in the KLV triplets that represent frame-wrapped essences. Similar approaches are used in other standards and specifications and, writing informally, this is often referred to as *frame-level* or *edit-unit-level* fixity; the latter term is defined in SMPTE ST 377-1:2011. It is worth noting that frame-level hash values (often referred to as *checksums* or *Cyclic Redundancy Checks, CRCs*) are sometimes employed for use cases such as monitoring production. For example, some specialists use ffmpeg's *framecrc* and *framemd5* checksums to judge the success of lossless compression processes. Process monitoring, however, is not a goal for the AS-07 specification.

AS-07 files will generally be frame-wrapped, with the exception of files that carry long-GOP D-10 essences. For D-10, content integrity systems native to long-GOP are to be retained in AS-07 files.

Frame-wrapped picture may be progressive-scanned or interlaced. Picture data for progressive-scanned content will be represented as the *V* in a KLV triplet, and the calculation of fixity is straightforward. Picture data for interlaced video will very often be carried with the data from both fields represented as a single *V* in a KLV triplet. This is the case for uncompressed video mapped according to SMPTE ST 384 and ST 377-1 (annex G.2.25), and also for JPEG 2000 compressed video *case I2* (frame wrapping, interlaced two fields per KLV triplet) mapped according to SMPTE ST 422:2013.

The exception to the general rule outlined in the preceding paragraph is the JPEG 2000 interlaced picture wrapping identified as *case I1* in SMPTE ST 422:2013, where each field is

wrapped as a separate KLV triplet. In this case, AS-07 requires that the concatenated *V* values for pairs of KLV triplets be hashed as one. AS-07 uses this approach so that the integrity data for interlaced video is always at the frame (edit unit) level. The same hash value would be calculated as from *case I2*, and this outcome supports integrity monitoring if an essence is re-wrapped from I1 to I2 or vice versa.

The AS-07 approach borrows from two important precedents: (1) SMPTE ST 429-6:2006 (D-Cinema Packaging -- MXF Track File Essence Encryption) and (2) the BBC Archive Preservation File Format described in section 5 in the BBC White Paper 233: http://downloads.bbc.co.uk/rd/pubs/whp/whp-pdf-files/WHP233.pdf.

From SMPTE ST 429-6:2006, AS-07 re-uses the equivalent of a DMS (Descriptive Metadata Scheme) system for fixity data. In the digital cinema context represented by this standard, fixity data is conjoined with data pertaining to the encryption of the triplet.

Although the use of encryption will be very rare in AS-07 files, in order to allow for this rare use and also to remain consistent with ST 429-6:2006, AS-07 files use that standard's terminology: *Cryptographic Context Set* (like a DM Scheme), *Cryptographic Framework* (like a DM Framework), and *Cryptographic Framework DM Tracks*. The Cryptographic Context Set implemented in AS-07 includes three adaptations from the ST 429-6:2006 implementation: (1) the addition of the optional *MICContainer* item, (2) specifying the permitted *Null* value as the default value for the *CipherAlgorithm* item and (3) specifying *0 (zero)* as the default value for the *CryptographicKeyID* item.

AS-07 does not, however, use the *Encrypted Triplet Variable Length Pack* specified by ST 429-6:2006 to carry the hash values; instead AS-07 employs the System Item in the Generic Container, like the BBC and as described in the following paragraphs. It is also the case that ST 429-6:2006 specifies the SHA-1 algorithm for integrity; for its preservation use case, AS-07 specifies the more easily created Castagnoli CRC-32C. The Encrypted Triplet Variable Length Pack from ST 429-6:2006 also carries an element called *Sequence Number*, defined as "Sequence number of this Triplet within the Track File." In AS-07, the required carriage of the Master Timecode in a System Item (see section 6.3.4.4) provides a one-up set of numbers that can be consulted to the same effect. To allow decoders to differentiate between AS-07 use of System Items and ST429-6:2006 Encrypted Triplets, AS-07 defines an optional item *MICContainer* in the Cryptographic Context Set in which a *SystemItem value* indicates the AS-07 usage and whose absence indicates use of Encrypted Triplets.

The BBC Archive Preservation File Format provides AS-07 with the structure that carries the fixity data itself, as specified in BBC White Paper 233, which refers to the approach as a *frame-level* checksum. There is one small variation: BBC calls for the use of the PNG CRC-32 Cyclic Redundancy Code algorithm; instead, we specify Castagnoli CRC-32C.

It is beyond the scope of a wrapper specification to specify when in an organization's workflow the initial MIC hash value should be calculated. It is worth noting, however, that many experts counsel that hash creation should occur at the moment of initial encoding, a possibility enhanced by the selection of the Castagnoli CRC-32C hash, which is easy and fast to calculate. Generating

the initial hash at the time of encoding means that a sophisticated file-creation system can use this data to verify that the file has been correctly written to media the first time file-writing occurs, thereby supporting quality control at an early stage in the life cycle.

6.6.2.2 CRC-32C values per KLV essence triplets

When required by a shim, AS-07 encoders shall calculate a Castagnoli CRC-32C Cyclic Redundancy Code (IETF RFC 3385) value for every *V* or *value* data unit in the KLV triplets that represent frame-wrapped essences, with the exception of interlaced JPEG 2000 that is wrapped according the *case I1* specified in SMPTE ST 422:2013, the case in which each field is wrapped as a separate KLV triplet. In the latter case, when integrity data is required by a shim, AS07 encoders shall calculate the Castagnoli CRC-32C for the concatenated values of the two *Vs* in the pair of KLVs.

For non-frame-wrapped D-10 essences, AS-07 encoders shall retain the integrity elements that are native to that essence.

6.6.2.3 Content integrity values carried in arrays in Essence Container System Items (informative)

The structure of data arrays of the type described here, and in the section devoted to Timecode (6.3), are governed by the batch syntax for KLV values specified in ST 2003:2012. For AS-07, the TimecodeArray is a single property whose value is an array, with the first element *MasterTC*, and with second and subsequent elements representing other Historical Source Timecodes. The integrity data is represented in a HashArray with a single property whose value is an array, with the first element *EssenceTrack Hash*, and with second and subsequent *Hashes* for other EssenceTracks. Generally speaking the first EssenceTrack is picture and the second and subsequent elements are sound, as in the BBC illustrative example in section 6.6.2.1 above. However, the actual identifiers for these essence tracks are contained in the structural metadata for the FilePackage, and also in the Descriptors contained in or strongly referenced by the FilePackage.

In the illustrative example that follows, the system item bytes for Timecode are a value equal to 09:58:10:12, and the hash values for video and four audio elements are bytes shown in hexadecimal notation with the start of each array item highlighted in bold text:

ITEM	ILLUSTRATIVE VALUE	COMMENT
Key	06.0e.2b.34.02.53.01.01.0d.01.03.01.14.02.01.00	
Len	83.00.00.3c	
Timecode array	01.02	
Local len	00.18	
Array len	00.00.00.02	
Array element len	00.00.00.08	
MasterTC	12.10.58.09.00.00.00.00	Value is actual bytes that represent a Timecode (in this case 09:58:10:12).
VITC element	12.10.58.09.00.00.00.00	Value is actual bytes that represent a Timecode.
LTC element	12.10.58.09.00.00.00.00	Value is actual bytes that represent a Timecode.
Hash array	ff.ff	

Local len	00.1c	
Array len	00.00.00.05	
Array element len	00.00.00.04	
EssenceTrack Hash	8b.cf.fa.3c	First hash is typically picture
EssenceTrack Hash	89.45.12.55	Second hash typically audio 1
EssenceTrack Hash	6f.89.01.06	Third hash typically audio 2
EssenceTrack Hash	32.cc.10.9a	Fourth hash typically audio 3
EssenceTrack Hash	32.cc.10.9a	Fifth hash typically audio 4

6.6.2.4 Content integrity array in Essence Container System Items

The CRC-32C values shall be stored in essence System Items as arrays that comply with SMPTE ST 2003:2012.

6.6.2.5 Encryption data (informative)

This version of the AS-07 specification does not offer specifications pertaining to encryption, reserving this topic for a future version. The approach to be adopted is anticipated to follow the guidance provided by SMPTE ST 429-6:2006 and will take into account additional or refined guidance that may result from the development of the Interoperable Master Format (IMF).

6.6.2.6 Cryptographic Context Set, Cryptographic Framework, and Cryptographic Framework DM Tracks.

When CRC-32C hash values are created for frame-wrapped essences, AS-07 encoders shall also create and populate Cryptographic Context Set, Cryptographic Framework, and Cryptographic Framework DM Tracks as specified in SMPTE ST 429-6:2006, with the optional item *MICContainer* in the Cryptographic Context Set in which a *SystemItem value* indicates the AS-07 usage and whose absence indicates use of Encrypted Triplets. Detailed information and requirements on this interrelated set of metadata elements is provided in appendix I.

6.6.2.7 Decoder requirements

AS-07 decoders shall provide the ability to output the CRC-32C data to applications external to the decoder.

Decoders shall provide the ability to select and display the metadata in the Cryptographic Context Set, Cryptographic Framework, and Cryptographic Framework DM Tracks before and during playback, but shall not depend on the presence of this data for the handoff of the CRC data.

This capability shall extend to CRC-32 data in non-Castagnoli formats, thus permitting AS-07 decoders to support "legacy" BBC archive files, which do not have Cryptographic Context Set, Cryptographic Framework, and Cryptographic Framework DM Tracks.

6.6.2.8 Shim parameter table for content integrity

Dimension	Description	Shim parameter	AS-07 Constraint	AS-07 Values
Content integrity	Content integrity data required	content_integrity	Strong	y/n

Appendix I Cryptographic Structures

Appendix I.1 AS-07-Cryptographic Framework

Item Name	Type	Len	Rec	Meaning	Compare to SMPTE ST 429-6:2006 (informative)
Cryptographic Framework Key	Set Key	16	Req	Defines the Cryptographic Framework Set	No change
Length	BER Length	var	Req	Set length	No change
InstanceID	UUID	16	Req	Unique identifier for the framework.	No change
GenerationUID	UUID	16	Opt	Optional Generation Identifier	No change
Context SR	Strong Ref	16	Req	Strong reference to the associate Cryptographic Context	No change

Appendix I.2 AS-07-Cryptographic Context Set

Item Name	Type	Len	Rec	Meaning	Compare to SMPTE ST 429-6:2006 (informative)
Cryptographic Context Key	Set Key	16	Req	Defines the Cryptographic Context Set	No change
Length	BER Length	var	Req	Set length	No change
InstanceID	UUID	16	Req	Unique identifier for the context used by Cryptographic Framework to refer to the Context.	No change
GenerationUID	UUID	16	Opt	Optional Generation Identifier	No change
Context ID	UUID	16	Req	Unique identifier used by Encrypted Triplets to refer to the Context.	No change
Source Essence Container Label	UL	16	Req	Essence Container Label for the source essence,	No change

				prior to encryption	
Cipher Algorithm	UL or zero	16	Req	Algorithm used for Triplet encryption, if any.	Use SMPTE ST 429-6:2006 option for Null value as default.
MIC Algorithm	UL or zero	16	Req	Algorithm used for Triplet integrity, if any.	Replace SHA-1 with CRC-32C.
Cryptographic Key ID	UUID	16	Req	Unique identifier for the cryptographic key.	Use a Zero value
MICContainer	UL	16	Opt	Informs decoder where to find MIC value	Added item for AS-07. Value = SystemItem indicates AS-07 usage; absent Value indicates use of Encrypted Triplets