

# ISO 26429-6:2008-07 (E)

## Digital cinema (D-cinema) packaging\_ - Part\_6: MXF\_track file, essence encryption

---

### Table of Contents

1	Scope .....	3
2	Normative References .....	3
3	Overview .....	4
4	Encrypted Essence Container .....	5
5	Cryptographic Framework.....	5
5.1	Cryptographic Framework Key .....	6
5.2	Length .....	6
5.3	Context SR.....	7
6	Cryptographic Context .....	7
6.1	Cryptographic Context Key .....	7
6.2	Length .....	8
6.3	Context ID .....	8
6.4	Source Essence Container Label .....	8
6.5	Cipher Algorithm .....	8
6.6	MIC Algorithm .....	8
6.7	Cryptographic Key ID .....	9
7	Encrypted Triplet.....	9
7.1	Encrypted Triplet Key.....	10
7.2	Length .....	10
7.3	Cryptographic Context Link.....	10
7.4	Plaintext Offset.....	10
7.5	Source Key.....	10
7.6	Source Length.....	10
7.7	Encrypted Source Value .....	11
7.8	TrackFile ID [optional] .....	11
7.9	Sequence Number [optional] .....	12
7.10	MIC [optional].....	12
8	Encrypted Track File Constraints.....	12
8.1	Encrypted Essence Track .....	12
8.2	Cryptographic Framework DM Track .....	12
8.3	Index Tables.....	13
9	Reference Decryption Processing Model.....	13
9.1	Overall Flow .....	13
9.2	Modules.....	14
10	Label and Key Structures .....	18
10.1	Encrypted Essence Container Label .....	18
10.2	Cryptographic Framework Label .....	19
10.3	Cryptographic Framework Key .....	20
10.4	Cryptographic Context Key.....	21
10.5	Encrypted Triplet Key .....	22
10.6	AES-CBC with 128-bit Key UL .....	22
10.7	HMAC-SHA1 with 128-bit Key UL .....	23
Annex A	Security Properties (Informative) .....	24
Annex B	Bibliography (Informative).....	25