



Towards true DRM Interoperability

**PIFF, Ultraviolet, and the dream of portable
digital content**

Mark Jeffrey

Mark.Jeffrey@microsoft.com

Microsoft Corporation

14 January, 2011

Microsoft[®]

Requirements for Interop

- Container formats
 - Legacy support for MPEG2 TS
 - Support for one or more MP4 code-points
 - DRM interoperability
 - Late binding of additional media tracks
- HTTP Streaming
 - Support for both MPEG2 TS and MP4 wire formats
 - Support for live, protected streaming
 - Support for emerging standards
- General
 - Supply-side optimization
 - Alignment with emerging industry standards
 - Support for a broad range of PC and embedded clients

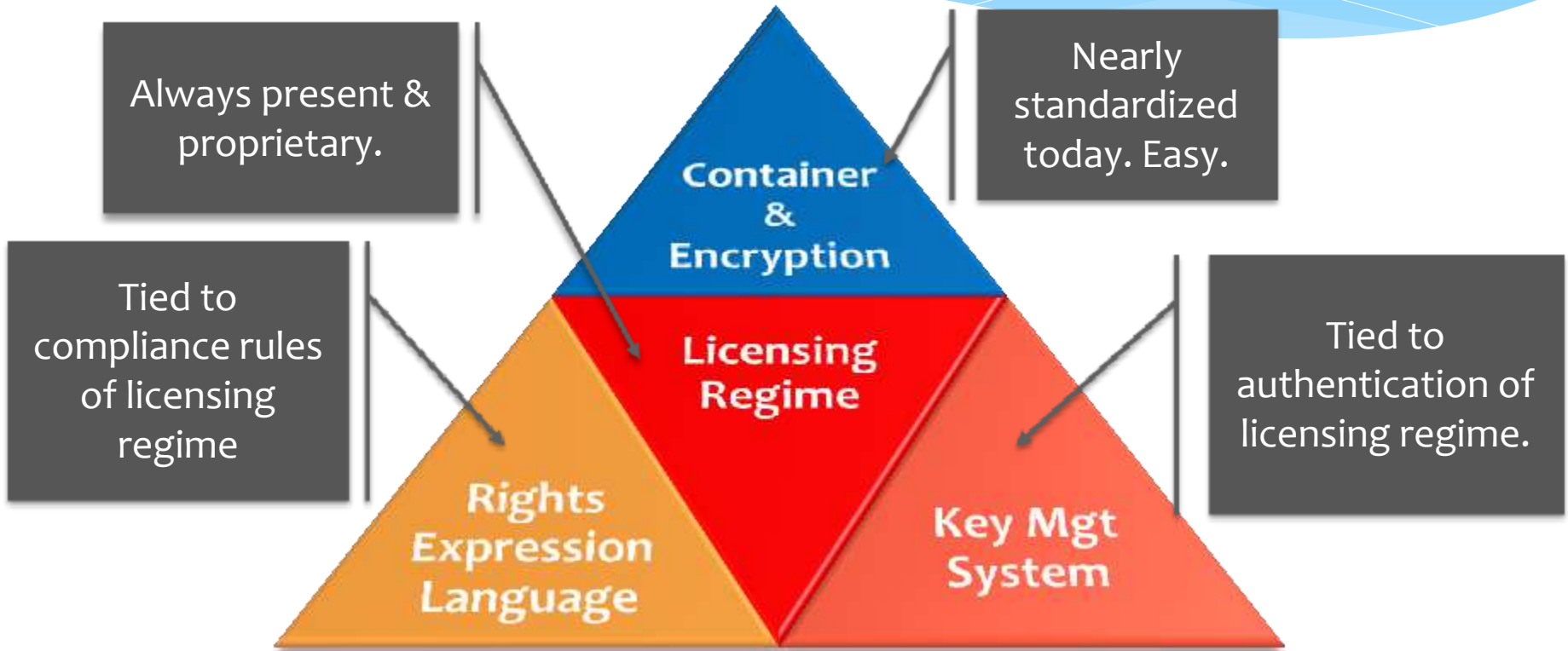
DRM Interoperability Requirement

Implementations are always proprietary, so how to make interoperable?

← Ease of Standardisation →

Difficult

Easy



What ordinary consumers want from DRM

- * No hassles!
- * Buy once play anywhere
- * Move files between devices
- * Just play, without needing special software
- * Re-download if the file is lost
- * Buying, renting, sharing within the family

Supply Side Optimization

Reducing encoding costs to enable large scale growth of Internet TV

- * Common container format for download-to-own, progressive download and HTTP streaming
- * Common encryption for DRM Interoperability
- * Late binding or alternate track files to reduce combinatorial complexity
- * Common container for HD, SD, PD versions
- * Common streaming standard for all networks

Protected Interoperable File Format

- * Code point on the ISO base media file format – like MP4 – entirely standards based.
- * PIFF uses the fragmented movie form of the ISO Base media file format (fMP4)
- * One encoding to cover all key consumer scenarios promotes supply chain optimization
- * Can be easily converted (only re-containerizing needed) for Apple-style MPEG2-TS HTTP Streaming
- * Can be easily packaged for progressive download

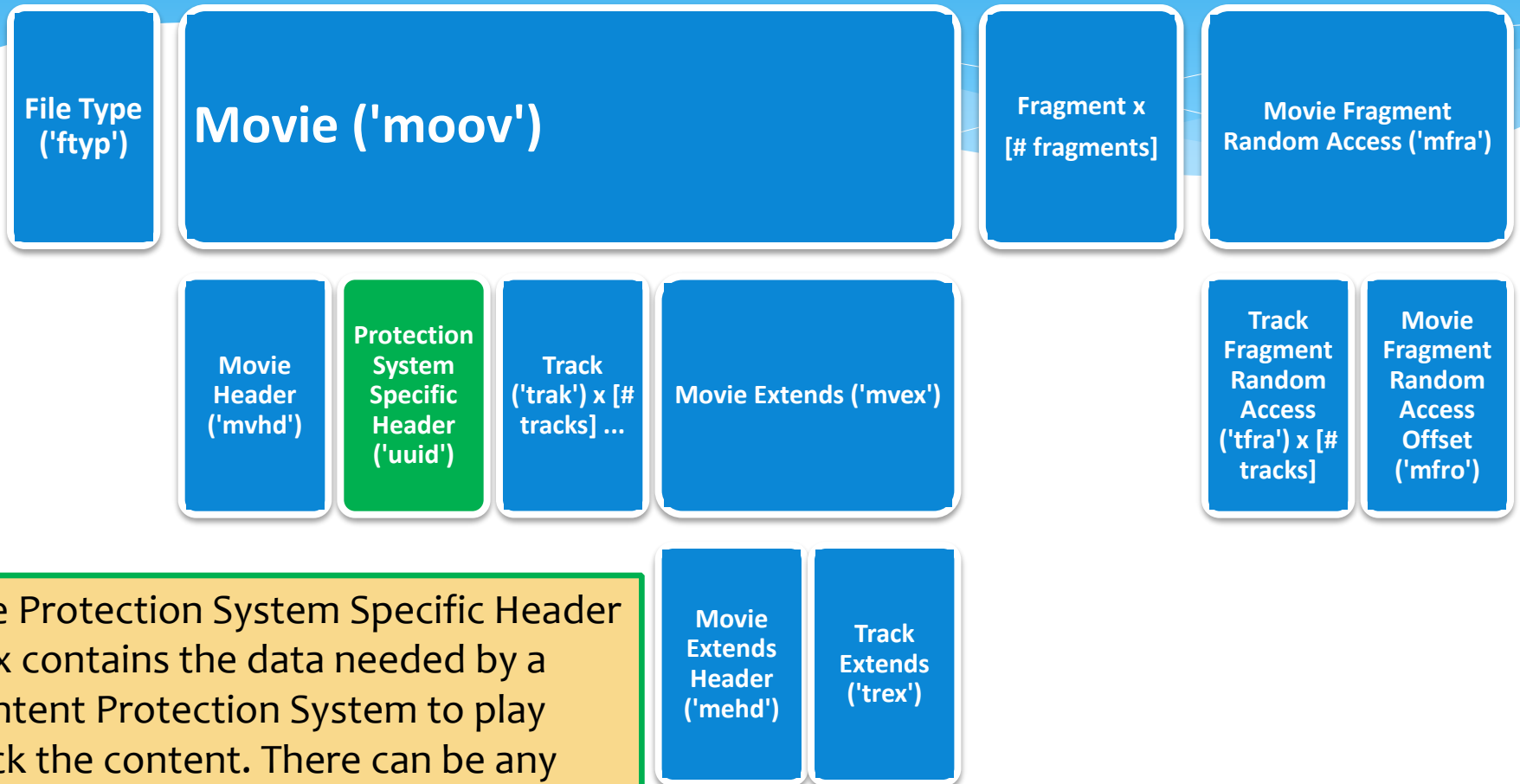
DECE / Ultraviolet Common Container Format

- * Extends PIFF into a full container format specification
 - * Adds rules for Codecs, picture formats, metadata, etc.
 - * Adds SMPTE-TT subtitles
- * Uses PIFF mechanism for multi-DRM portability
- * Mandates inclusion of five DRM headers in all Ultraviolet files:
 - * Adobe Flash Access, Google Widevine, Marlin, Microsoft PlayReady, OMA DRM
- * Standardised usage rules
 - * Family groups of individual accounts
 - * Use on up to 12 UV devices, plus streaming to others
 - * Re-download rights

Content Protection Scheme

- * PIFF uses a standard encryption algorithm
 - * AES-128 in Counter (CTR) mode
- * ISO base media file format “scheme signalling” is generalized to signal multiple DRM systems
- * PIFF multi-DRM signalling and common encryption of the fragmented movie format are the foundation of the Digital Entertainment Content Ecosystem (DECE) Common File Format (CFF).

Protection System Specific Header Box



The Protection System Specific Header Box contains the data needed by a Content Protection System to play back the content. There can be any number of these boxes, added at any time.

Track Encryption Box

Original Sample Entry with protected type

Protection Scheme Info ('sinf')

Original Format Box
('frma')

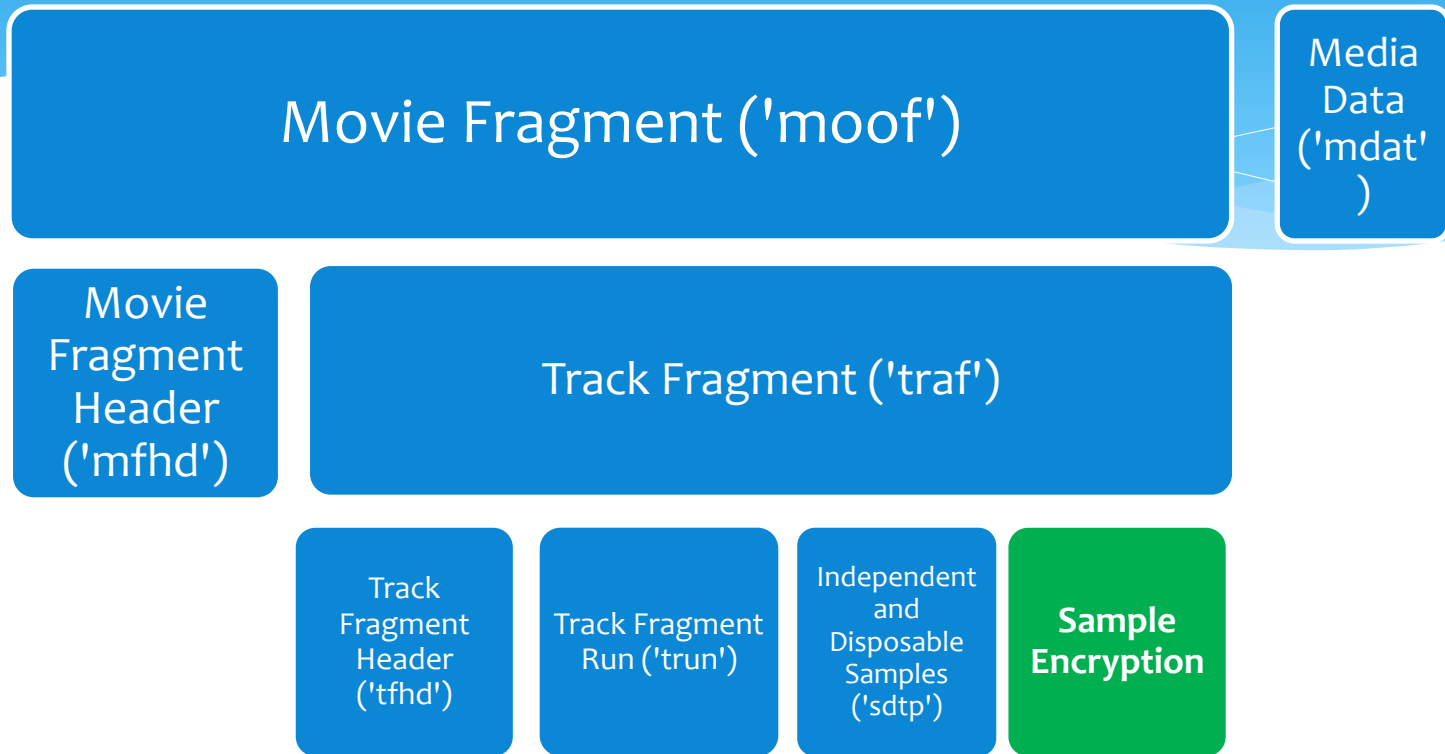
Scheme Type Box
('schm')

Scheme Information
Box ('schi')

The Track Encryption box contains default values for the AlgorithmID, IV_size, and KID for the entire track. All Content Protection Systems use the same encryption algorithm. There is no DRM-Specific metadata at the track or sample level.

Track Encryption Box

Sample Encryption Box



The Sample Encryption Box contains the sample specific encryption data, including whether the sample is encrypted or not.

Conclusions

- * With some exceptions, industry is increasingly aligning on:
 - * fMP4 and MPEG2 TS containers
 - * MPEG DASH standard for adaptive streaming over IP networks
 - * AES-128 encryption of content
 - * DRM interoperability using PIFF mechanisms
- * Keep your eyes on:
 - * Ultraviolet (for DRM interop)
 - * MPEG DASH (for streaming)

Thank you