Security solutions in MPEG family of standards

Touradj Ebrahimi
Touradj.Ebrahimi@epfl.ch

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- MPEG-1 (1992): MP3, Video CD, first generation set-top box, …
- MPEG-2 (1994): Digital TV, HDTV, DVD, DVB, Professional, …
- MPEG-4 (1998, 99, ongoing): Coding of Audiovisual Objects
- MPEG-7 (2001, ongoing): Description of Multimedia Content
- MPEG-21 (2002, ongoing): Multimedia Framework

- Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s
  - Part 1 Systems - Program Stream
  - Part 2 Video
  - Part 3 Audio
  - Part 4 Conformance
  - Part 5 Reference software

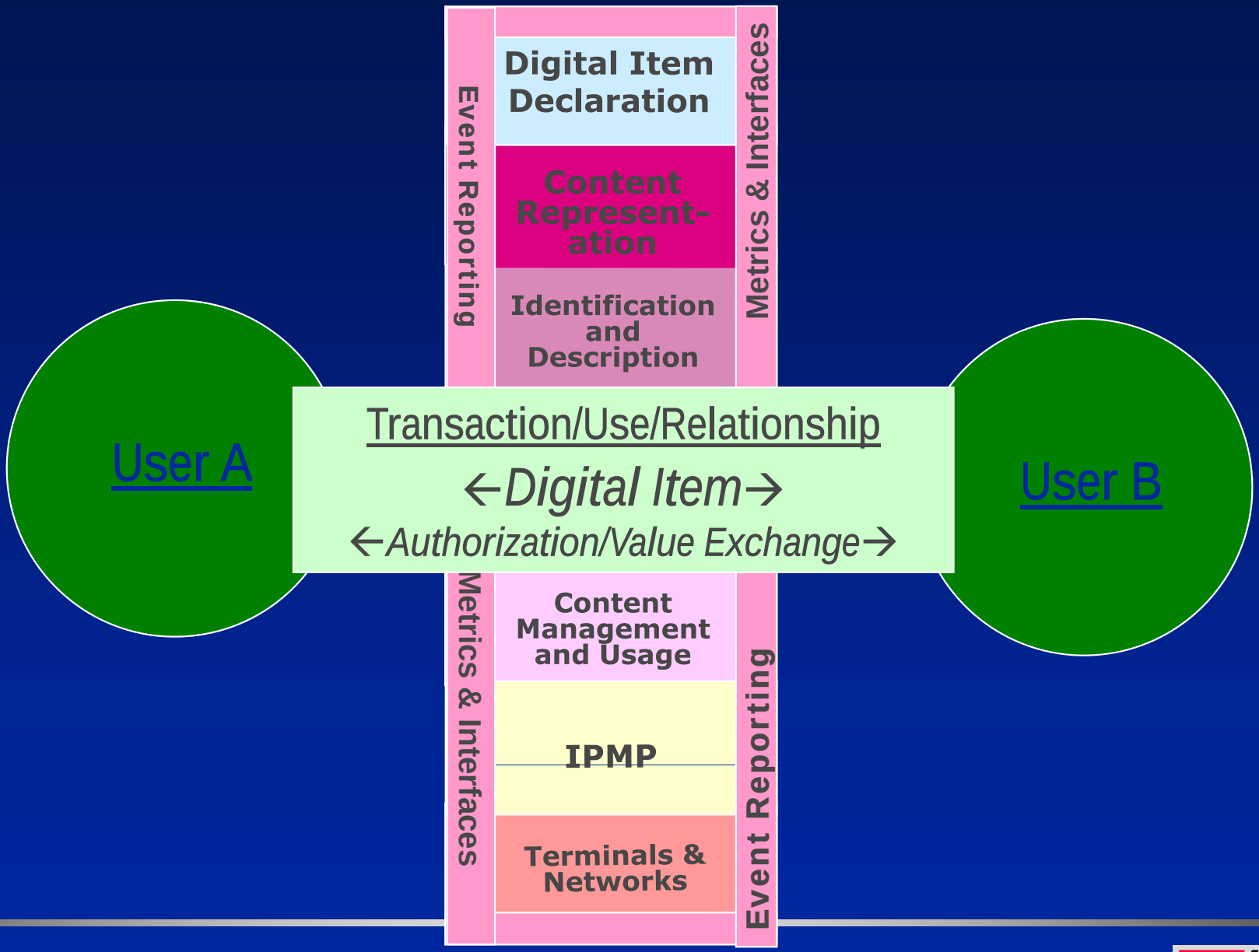
- Generic coding of moving pictures and associated audio
  - Part 1 Systems - joint with ITU
  - Part 2 Video - joint with ITU
  - Part 3 Audio
  - Part 4 Conformance
  - Part 5 Reference software
  - Part 6 DSM CC
  - Part 7 AAC - Advanced Audio Coding
  - Part 9 RTI - Real Time Interface
  - Part 10 Conformance extension - DSM-CC
  - Part 11 IPMP on MPEG-2 Systems

- Coding of audio-visual objects
  - Part 1 Systems
  - Part 2 Visual
  - Part 3 Audio
  - Part 4 Conformance
  - Part 5 Reference Software
  - Part 6 DMIF - Delivery Multimedia Integration Framework
  - Part 7 Optimized Software
  - Part 8 4 on IP Framework
  - Part 9 Reference Hardware
  - Part 10 Advanced Video Coding
  - Part 11 Scene Description and Application Engine
  - Part 12 ISO Base Media File Format
  - Part 13 IPMP Extensions
  - Part 14 MP4 File Format
  - Part 15 AVC File Format
  - Part 16 Animation Framework eXtension (AFX)
  - Part 17 Streaming text format
  - Part 18 Font compression and streaming

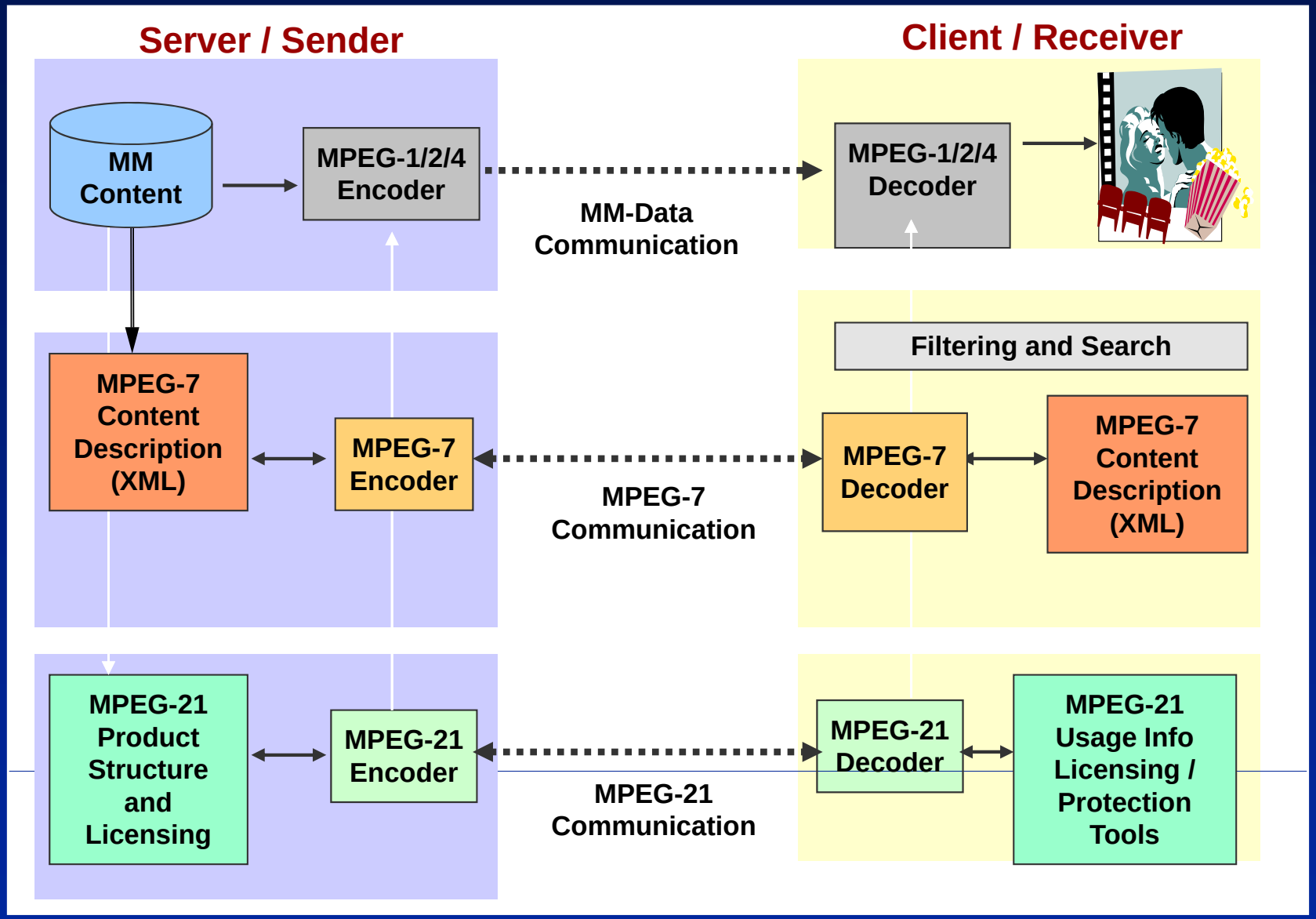
- Multimedia content description interface
  - Part 1 Systems
  - Part 2 DDL - Description definition language
  - Part 3 Visual
  - Part 4 Audio
  - Part 5 Multimedia description schemes
  - Part 6 Reference software
  - Part 7 Conformance
  - Part 8 Extraction and Use of MPEG-7 Descriptions
  - Part 9 Profiles
  - Part 10 Schema Definition

- Multimedia Framework
  - Part 1 Vision, Technologies and Strategy
  - Part 2 Digital Item Declaration
  - Part 3 Digital Item Identification and Description
  - Part 4 Intellectual Property Management and Protection
  - Part 5 Rights Expression Language
  - Part 6 Rights Data Dictionary
  - Part 7 Digital Item Adaptation
  - Part 8 Reference Software
  - Part 9 File Format
  - Part 10 Digital Item Processing
  - Part 11 Evaluation Tools for Persistent Association
  - Part 12 Test Bed for MPEG-21 Resource Delivery
  - Part 13 Scalable Video Coding
  - Part 14 Conformance

MPEG-21 Overview



Integrated view



- Security
  - Authentication and data integrity
  - Conditional access
  - Ownership protection
  - Digital Rights Management
  - …
- MPEG handles security through IPMP (Intellectual Property Management and Protection)
  - IP in content *and* in technology
  - IP protection *and* management
- MPEG has been moving from ‘hooks’ to truly interoperable security solutions

- Nothing!
- MP3 phenomenon

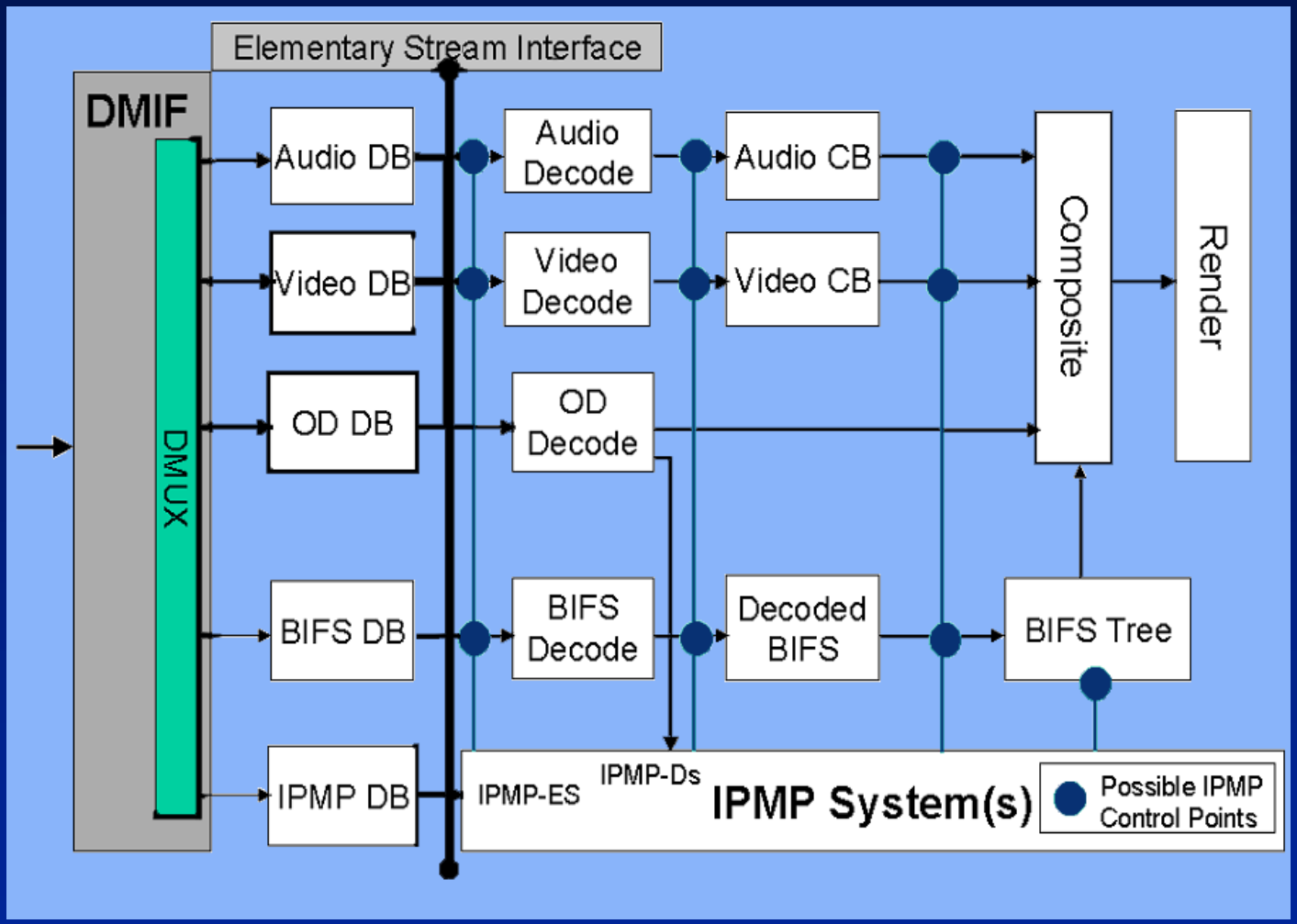
- Identification:
  - Copyright descriptor ID
  - Identifier refers to Registration Authority (similar to ISBN)
  - Number is unique ID handed out by authority
  - Removal or alteration of ID is prohibited by WIPO treaty

- Protection:
  - Encryption messages
  - Provisions for signaling the presence of encryption and the type of Conditional Access system used.
  - No standard DRM
  - (MPEG-4) IPMP on MPEG-2 systems

- Identification: IP dataset
  - content type ~ protected? (y/n) ~ registration authority ~ registration number ~ titles and supplementary information ~ references to IP info
  - Can be attached at any level of granularity

- Protection: standard interfaces to proprietary IPMP systems
  - In 1997 broad consensus NOT to specify IPMP System
    - *One size does not fit all (Cost-Benefit)*
    - *Fear of laundry of high value content through low protection devices*
  - Tight integration of 'hooks' with MPEG-4 Systems layer
    - *Special Descriptors and Stream Type for IPMP information*
    - *Special Registration Authority for registering IPMP Systems*
    - *Architecture allows management next to protection*
  - IPMP extensions

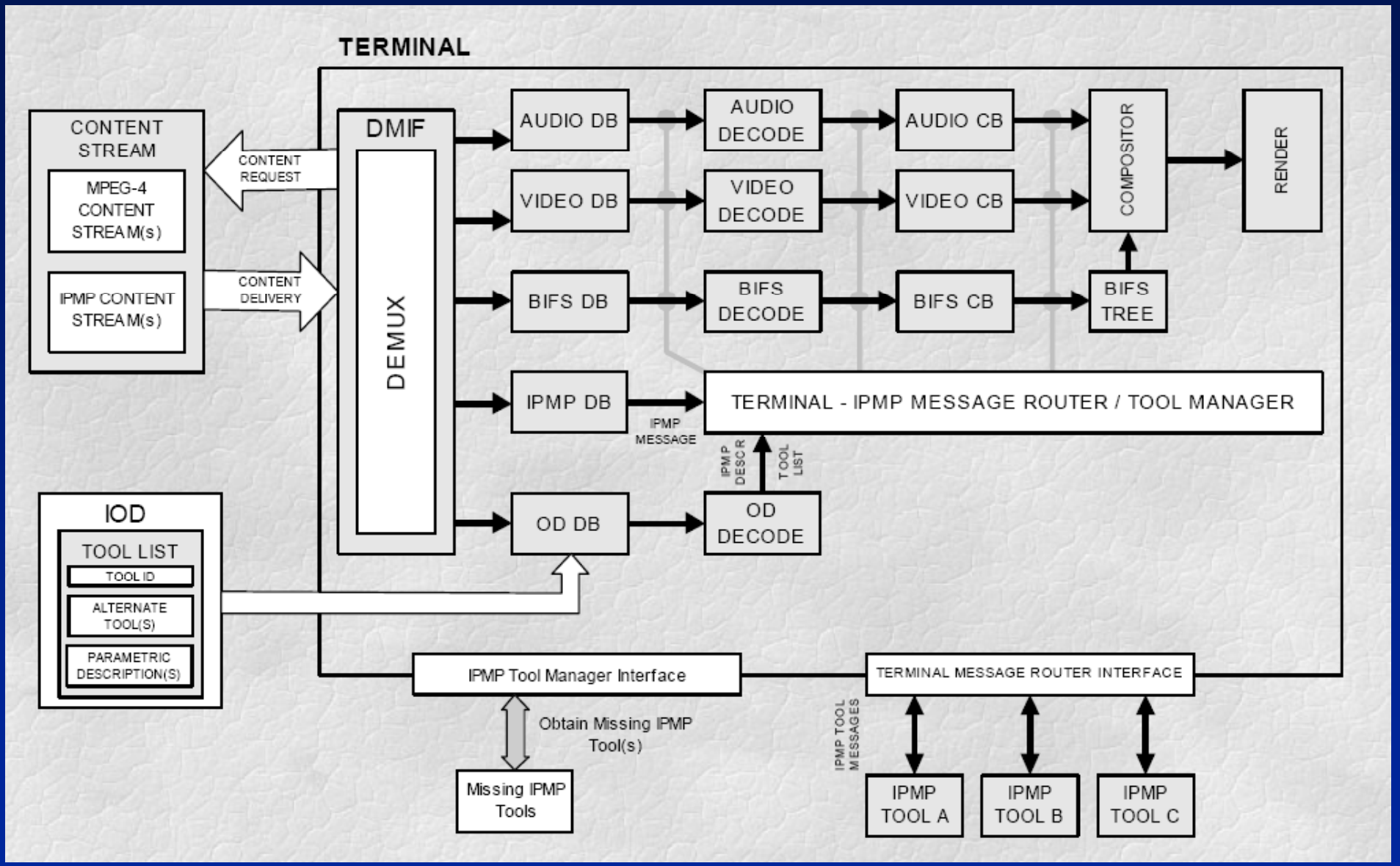
IPMP in MPEG-4



DB: Decoding Buffer / CB: Composition Buffer / OD: Object Descriptor
BIFS: Binary Format for Scenes / ES: Elementary Stream / Ds: Descriptors

- MPEG-4 IPMP Extensions
  - secure downloading protocol
  - IPMP message format
  - Message routing protocol between IPMP tools and system

MPEG-4 IPMP extensions



- Descriptions are as valuable as the content
- Identification
  - IPMP Descriptors
- Authentication
  - Digital signature
- Protection
  - Encryption: Crypto Binary Data Type

- Rights Expression Language (REL)
  - XrML (eXtensible rights Mark-up Language)
- Rights Data Dictionary (RDD)
  - Define terms for Rights Expression
- MPEG-21 IPMP requirements have been identified
- A call for proposals on MPEG-21 IPMP has been issued in March 2004

Conclusions

- MPEG has been active in proposing standardized security solutions for a broad range of applications since more than 10 years
- An explosion of such activities has taken place recently (IPMP-X, REL, RDD, MPEG-21 IPMP)
- Many challenges still remain
  - To successfully include all these in products and services
  - Relationship with other standardization activities (DMP, …)
  - …

- This presentation includes ideas and materials resulting from hard work of many MPEG experts. Their contribution is hereby acknowledged.

- More information available at:

  http://www.chiariglione.org/mpeg/