# Standard API for Encryption Key Exchange - Working Group

**Moving from proprietary to standardized Key Exchange APIs**

The online distribution of high-value video requires encryption and careful management of the associated encryption keys. Keys for encryption in the online content ecosystem are delivered by DRM/CA vendors and typically managed by Key Management Servers (KMS), which are designed to distribute keys to client devices for controlled decryption of content. The encryption itself often takes place in separate scrambler components created by encoder (and stream-segmentor) vendors that use encryption keys ultimately managed by the KMS. The exchange of keys for this purpose between scramblers and key management servers takes place over APIs - which today are proprietary.

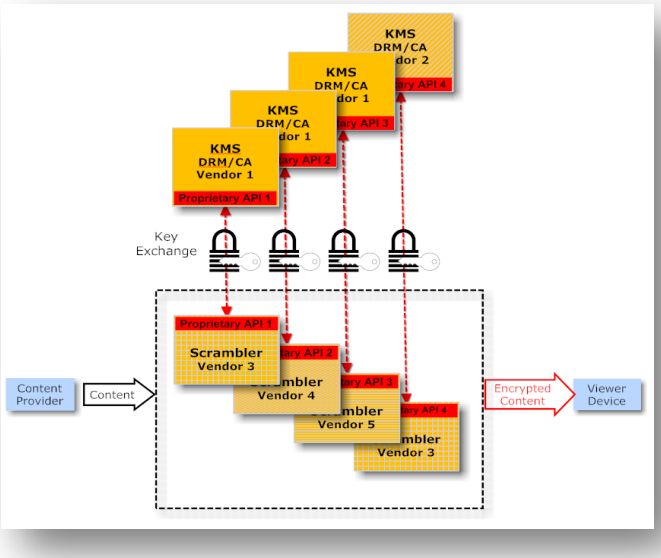



Figure 1: Current proprietary approach

Although these APIs are relatively simple, the development, testing and maintenance of multiple proprietary interfaces (for each pair of vendors) is costly in time and money for all concerned. The solution is to define a single industry-standard API for key exchange which can be adopted by KMS and scrambling solution providers across the industry.

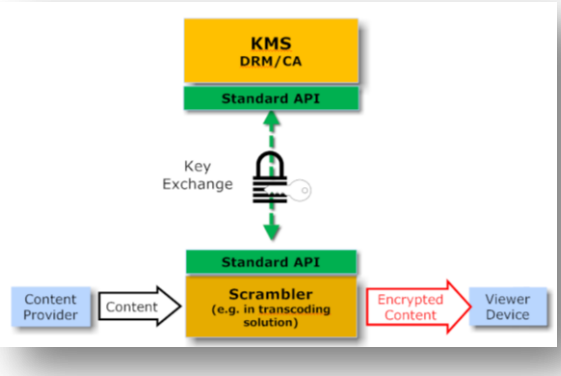
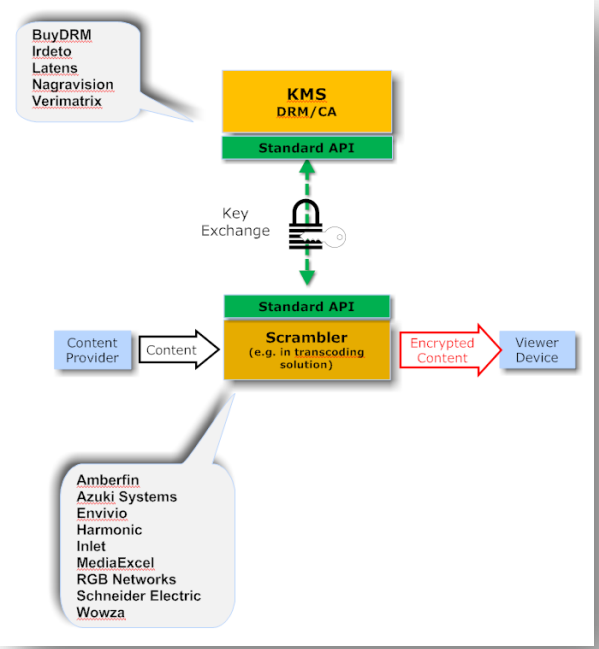



Figure 2: Target standardized approach

The **value proposition** of this work for DRM and scrambling vendors is: elimination of duplicate APIs reducing costs and time to market; reduction of potential interoperability problems through the use of a robust, tested API; increased availability of use-cases based on industry-wide consensus during the creation of the API.

**Industry Working Group**

MPEG Industry Forum (MPEGIF) and the Video Convergence Forum (VCF) have collaborated to organize and promote an open industry working group that brings together members of the online content ecosystem that have technical expertise in the area of KMS, scrambling and key exchange. Companies participating in this work include AmberFin, Azuki Systems, BuyDRM, Envivio, Harmonic, Inlet, Irdeto, Latens, MediaExcel, NagraVision, RGB Networks, Schneider Electric, Verimatrix and Wowza.




**Phase 1 Completed - Requirements document**

The working group has recently completed a draft set of requirements for the standardized API which is due for public release in February 2011. Topics covered in the Requirements Document include requirements for protocols, KMS, scramblers, type of data exchanged, I/O and authentication.

The goal of this document is to list requirements for an API for exchanging keys between key management servers and scramblers - requirements that can scale from the simplest situations to the most complex and demanding that are envisioned.

**Phase 2 – Invitation to submit API proposals**

The working group's next milestone is a draft standardized API based on submissions provided by some of the working group members in February 2011. The draft API will be developed over the course of around six months, and will be made available for review and comments prior to IBC 2011.

MPEGIF and VCF wish to invite any company that is involved in KMS-scrambler key exchange to join the Working Group and actively participate in developing and/or reviewing the draft API in the lead up to the next milestone in the group's work. For more information, please contact Nicola Wissler, MPEGIF Coordinator at nicola.wissler@mpegif.org or 510-492-4028 or visit http://bit.ly/gFCIZk.