mpeg Industry Forum

VIDEO CONVERGENCE FORUM

Standard API for Encryption Key Exchange

Working Group

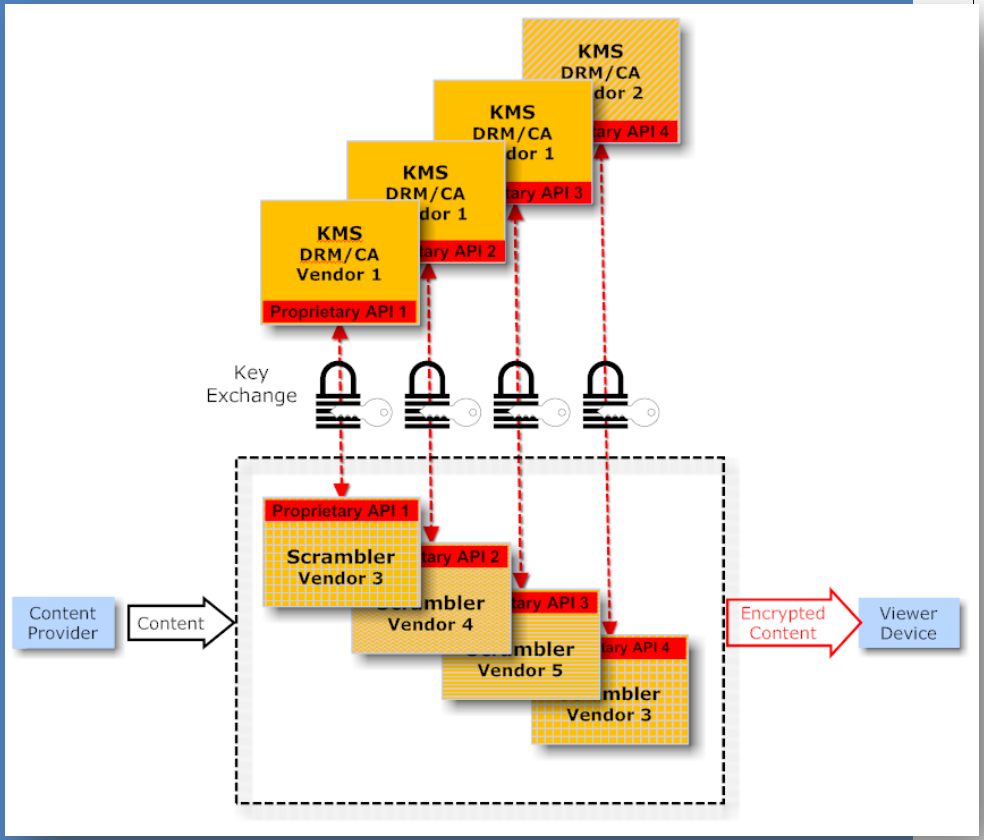
January 2011

This Presentation

- Aimed at all
  - DRM/CA (KMS) vendors
  - Scrambler (e.g. transcoder) vendors
- Purpose
  - Additional participants in Working Group Phase II
  - Submissions of draft APIs
  - Broader industry awareness
- Topics
  - Value Proposition
  - High level overview of completed Requirements Documents

Proprietary Key Exchange APIs

- High value video protected by encryption prior to online distribution
- Encryption implemented in scramblers - often embedded in transcoding solutions
- Encryption keys typically managed by Key Management Servers (KMS)
- Keys exchanged between KMS and Scrambler via API
- Lack of standardization of API leading to more and more proprietary APIs (per vendor partnership)

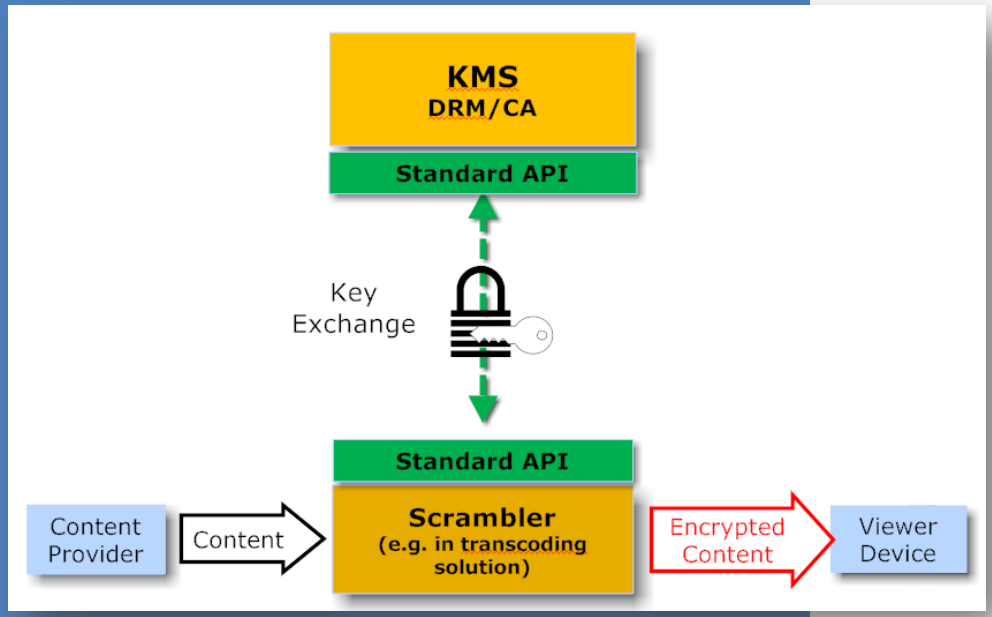


Proprietary means

- Increased time to market
- Increased costs of operation and maintenance

Standardized Key Exchange API

- Single API requires less
  - Development
  - Testing
  - Maintenance
- MPEGIF Working Group set up to transition industry to standardized API
- **Value proposition** for KMS and Scrambler vendors
  - Elimination of duplicate APIs
  - 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



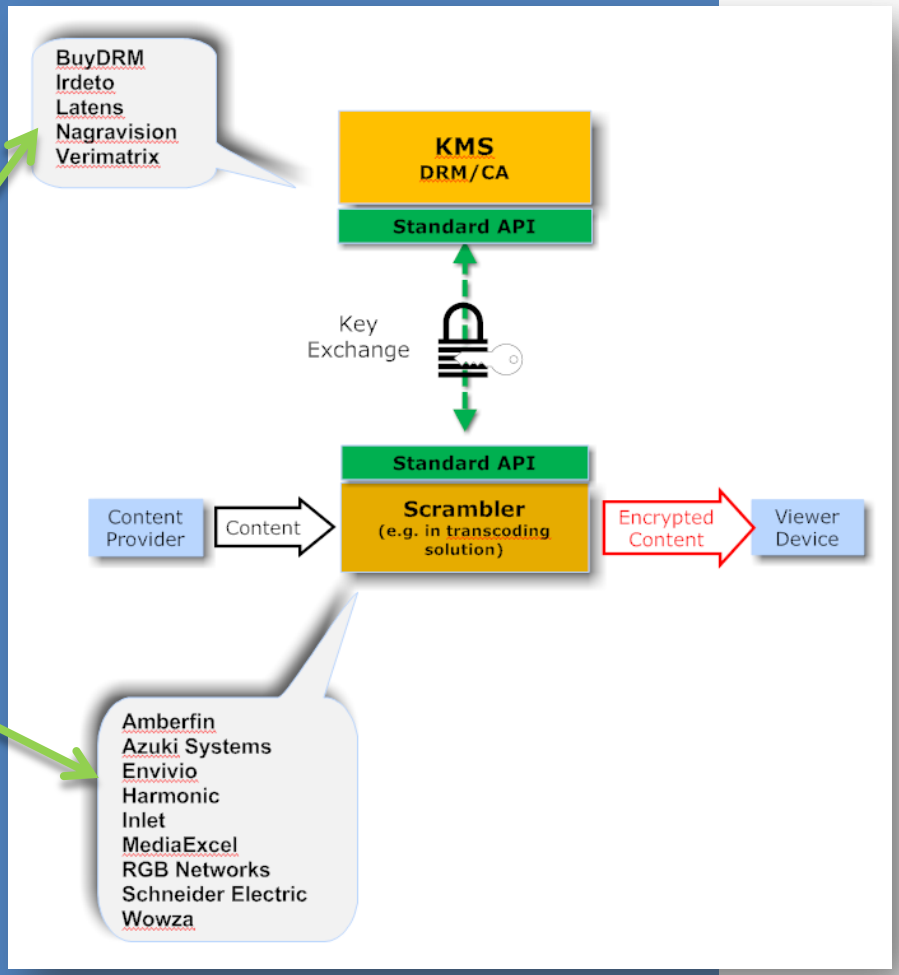
Standardized means

⇨ Reduced time to market

⇨ Reduced costs of operation and maintenance

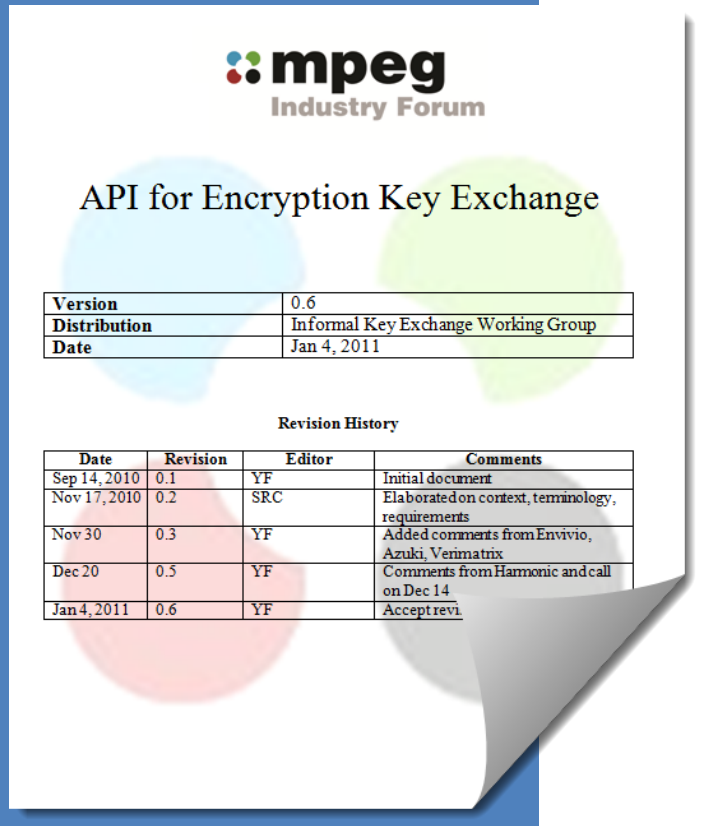
Working Group Phase I (completed)

- Requirements Document covering
  - Protocols
  - KMS
  - Scramblers
  - Type of data exchanged
  - I/O
  - Authentication
- 14 active participants
- Due for publication – Feb 2011



Protocol Requirements

- *API to be published openly*
- *Protocol stateless in nature – except for underlying state mechanisms*
- *Support for redundant configurations*
- *Scrambler*
  - *initiates sessions*
  - *requests for keys*
  - *determines interval of key requests*
  - *manages primary and redundant delivery*
  - *determines content identifier*
  - *time stamp in request*



mpeg Industry Forum

API for Encryption Key Exchange

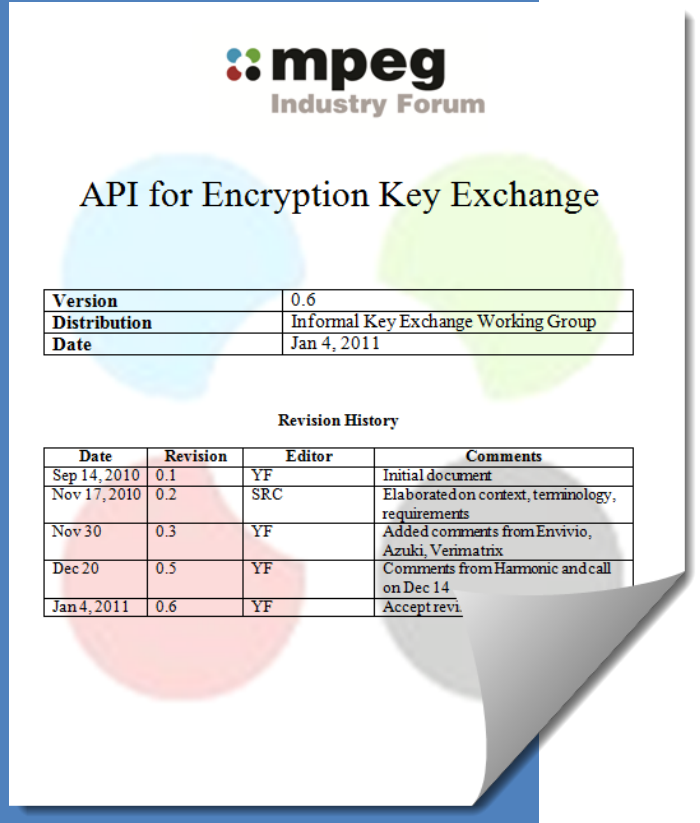
Version	0.6
Distribution	Informal Key Exchange Working Group
Date	Jan 4, 2011

Revision History

Date	Revision	Editor	Comments
Sep 14, 2010	0.1	YF	Initial document
Nov 17, 2010	0.2	SRC	Elaborated on context, terminology, requirements
Nov 30	0.3	YF	Added comments from Envivio, Azuki, Verimatrix
Dec 20	0.5	YF	Comments from Harmonic and call on Dec 14
Jan 4, 2011	0.6	YF	Accept revi

KMS Requirements

- *Capability of*
  - *creating encryption keys on demand*
  - *storing encryption keys together with an associated content ID reference*
  - *creating keys for both VoD and live content*
  - *signaling which types of encryption algorithm and keys it supports*
- *Support for rotating keys*



mpeg Industry Forum

API for Encryption Key Exchange

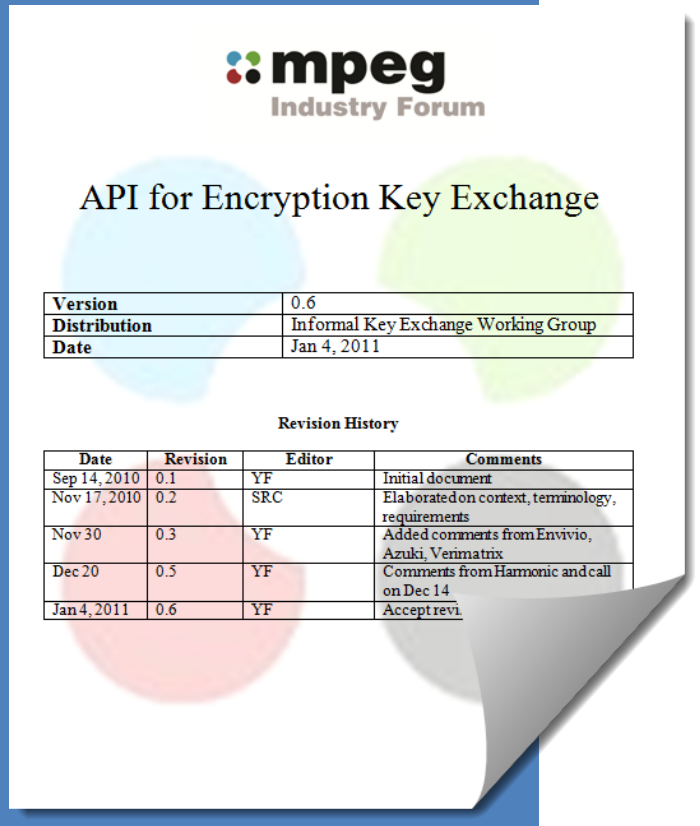
Version	0.6
Distribution	Informal Key Exchange Working Group
Date	Jan 4, 2011

Revision History

Date	Revision	Editor	Comments
Sep 14, 2010	0.1	YF	Initial document
Nov 17, 2010	0.2	SRC	Elaborated on context, terminology, requirements
Nov 30	0.3	YF	Added comments from Envivio, Azuki, Verimatrix
Dec 20	0.5	YF	Comments from Harmonic and call on Dec 14
Jan 4, 2011	0.6	YF	Accept revi

Scrambler Requirements

- *Communicate and accept keys from at least two distinct KMS service points*
- *Ability to create encryption keys*
- *Independent of underlying content encoding/segmentation mechanism*



mpeg Industry Forum

API for Encryption Key Exchange

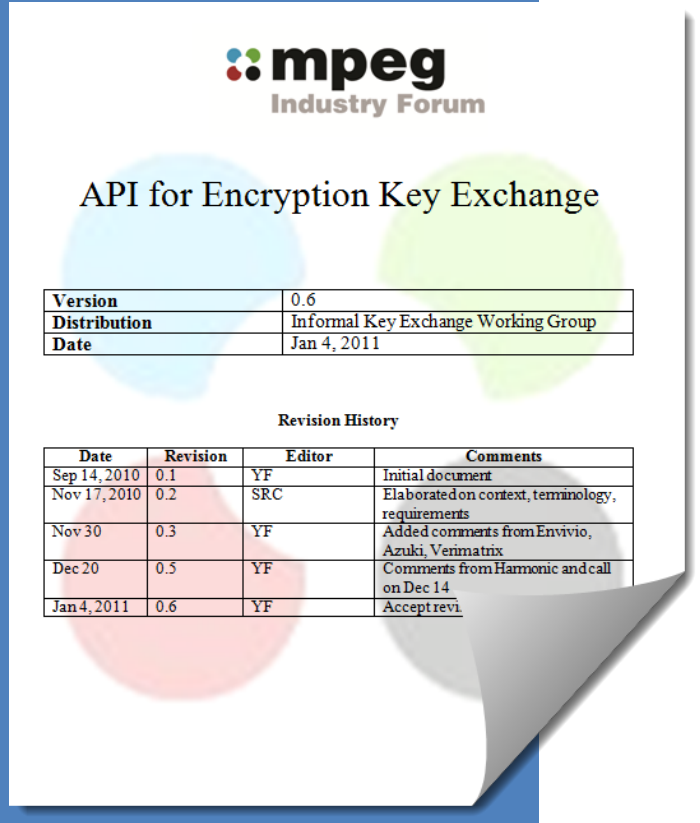
Version	0.6
Distribution	Informal Key Exchange Working Group
Date	Jan 4, 2011

Revision History

Date	Revision	Editor	Comments
Sep 14, 2010	0.1	YF	Initial document
Nov 17, 2010	0.2	SRC	Elaborated on context, terminology, requirements
Nov 30	0.3	YF	Added comments from Envivio, Azuki, Verimatrix
Dec 20	0.5	YF	Comments from Harmonic and call on Dec 14
Jan 4, 2011	0.6	YF	Accept revi

Data Exchange Requirements

- *Encryption keys, content identifiers and timestamps support character string representation*
- *Enables unambiguous key requests from client devices*
- *Support for exchange of auxiliary data*
- *Allows for the insertion of all data necessary for decryption*



mpeg Industry Forum

API for Encryption Key Exchange

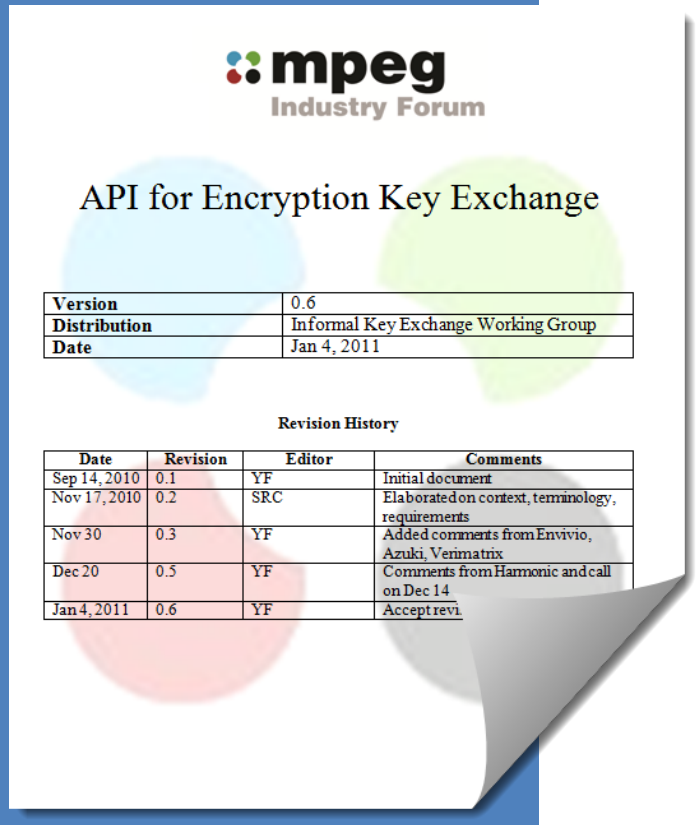
Version	0.6
Distribution	Informal Key Exchange Working Group
Date	Jan 4, 2011

Revision History

Date	Revision	Editor	Comments
Sep 14, 2010	0.1	YF	Initial document
Nov 17, 2010	0.2	SRC	Elaborated on context, terminology, requirements
Nov 30	0.3	YF	Added comments from Envivio, Azuki, Verimatrix
Dec 20	0.5	YF	Comments from Harmonic and call on Dec 14
Jan 4, 2011	0.6	YF	Accept revi

I/O Requirements

- *Uses HTTP in the clear or using SSL to protect the data exchange*



mpeg Industry Forum

API for Encryption Key Exchange

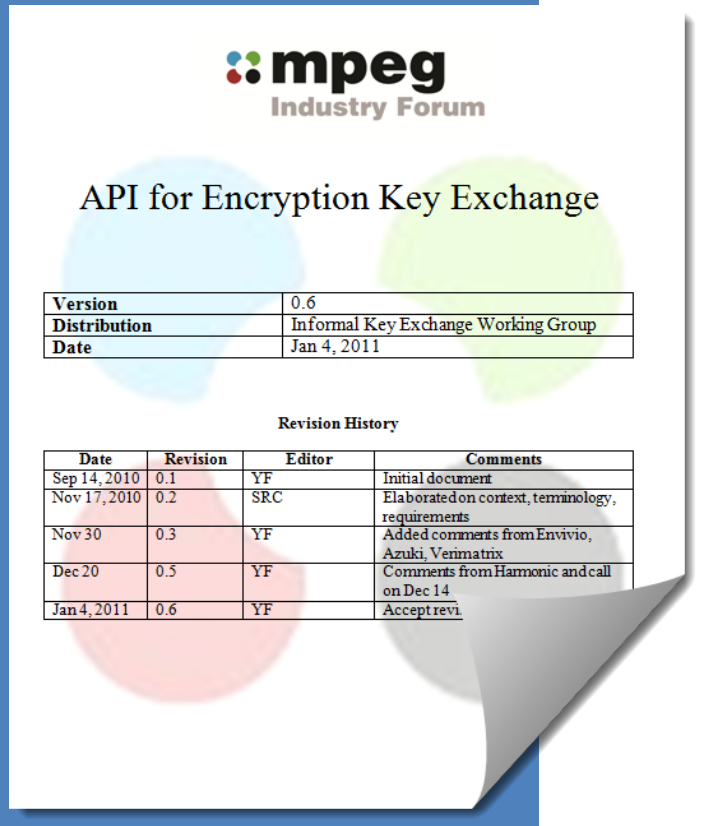
Version	0.6
Distribution	Informal Key Exchange Working Group
Date	Jan 4, 2011

Revision History

Date	Revision	Editor	Comments
Sep 14, 2010	0.1	YF	Initial document
Nov 17, 2010	0.2	SRC	Elaborated on context, terminology, requirements
Nov 30	0.3	YF	Added comments from Envivio, Azuki, Verimatrix
Dec 20	0.5	YF	Comments from Harmonic and call on Dec 14
Jan 4, 2011	0.6	YF	Accept revi

Authentication Requirements

- *Mutual authentication prior to any key exchange*
- *Announcing supported authentication schemes*
- *Negotiating a mutual scheme used for mutual authentication*



mpeg Industry Forum

API for Encryption Key Exchange

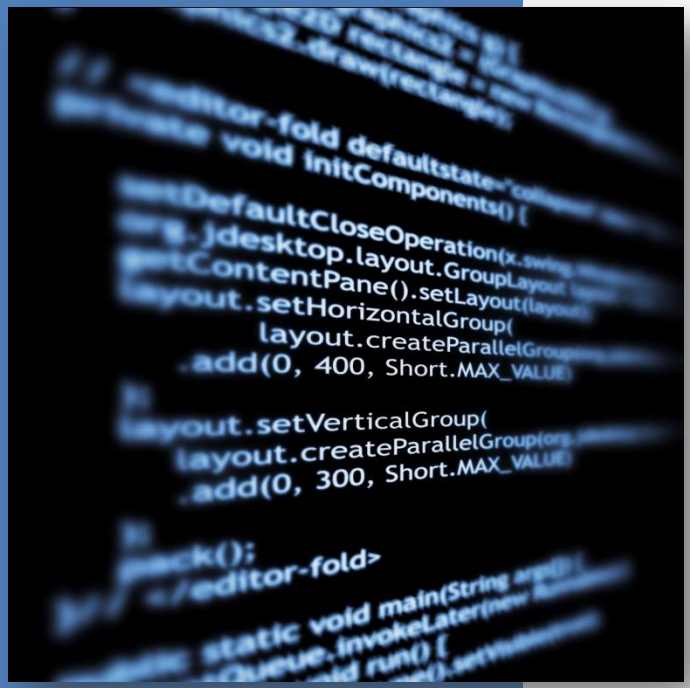
Version	0.6
Distribution	Informal Key Exchange Working Group
Date	Jan 4, 2011

Revision History

Date	Revision	Editor	Comments
Sep 14, 2010	0.1	YF	Initial document
Nov 17, 2010	0.2	SRC	Elaborated on context, terminology, requirements
Nov 30	0.3	YF	Added comments from Envivio, Azuki, Verimatrix
Dec 20	0.5	YF	Comments from Harmonic and call on Dec 14
Jan 4, 2011	0.6	YF	Accept revi

Working Group Phase II

- Draft API based on Requirements Document (Phase I)
- Invitation for API submissions to launch work
- Group open to all DRM/CA and scrambler vendors
- Target launch of work - February 2011
- Target release of draft API - 3Q2011



Contact Information

For more information on the Key Exchange API Working Group

Nicola Wissler
MPEGIF Coordinator

nicola.wissler@mpegif.org
Tel: +1 510 492-4028
http://bit.ly/gFCIZk