



HKEP Capability



Version 1.0 DRAFT (2026/08)

Published by the Alliance for IP Media Solutions (AIMS)

<https://aimsalliance.org>

<https://ipmx.io>

Copyright & Permissions Notice

© 2026 Alliance for IP Media Solutions (AIMS).

This document is licensed under the Creative Commons Attribution–NoDerivatives 4.0 International License (CC BY-ND 4.0).

You are free to copy and redistribute this document in any medium or format, **provided that**:

- You give appropriate credit to AIMS,
- You do not modify the document, and
- You do not imply endorsement by AIMS for any use of this material.

No derivatives or adaptations of this document are permitted.

A copy of the license is available at:

<https://creativecommons.org/licenses/by-nd/4.0/>

IPMX and the IPMX logo are trademarks of AIMS and may not be used except as permitted by AIMS Brand Usage Guidelines.

1. Introduction (Informative)	3
2. Scope (Normative)	4
3. Normative References (Normative)	4
4. Terms and Definitions (Informative)	5
5. General Provisions (Normative)	5
6. Capability Evaluation Requirements (Normative)	6
6.1 Device Role, Topology, and Identifiers	7
6.2 SDP Signaling of HKEP Connection Parameters	7
6.3 HKEP Preamble and Session Establishment	7
6.4 Receiver Protocol Modes	8
6.5 Capability Inspection by Non-Receivers	8
6.6 HKEP Session Lifetime, Caching, and Failure Handling	9
6.7 Locality Check Constraints	9
6.8 HKEP Sequencing Constraints on Authentication with Repeaters	10
6.9 Receiver_AuthStatus Handling	10
6.10 Null Topology Handling	11
6.11 Stream Management Construction Constraints	11
6.12 RTP Header-Extension Presence and streamCtr Signaling	11
6.13 HKEP Media Info Block in RTCP Sender Reports	12
7. Out-of-Scope (Informative)	12
7.1 HDCP Cryptographic Behavior	12
7.2 HDCP Licensing and DCP Administrative Requirements	12
7.3 Non-IP HDCP Interface Behavior	13
7.4 Vendor-Specific Baseband Bridging	13
7.5 Generalized Topology-Limit Enforcement	13
7.6 Rejection of Non-HDCP Receivers	13
7.7 Certification-Lab Mechanics Not Defined by TR-10-5	13
8. Conformance Statement (Normative)	14
Appendix A: Mapping to VSF TR-10-5 (Informative)	14
Appendix B: Change Log	15

1. Introduction (Informative)

This document defines the IPMX HKEP Capability, which is the requirements an IPMX device must implement to claim support for HDCP-protected content over IP networks using the HDCP Key Exchange Protocol (HKEP), as defined in VSF TR-10-5, and the behaviors evaluated for conformance.

This capability builds upon:

- The IPMX baseline requirements that every conforming IPMX device must follow, as defined in the **IPMX Product Qualification and Certification Requirements (PQCR) document**.
- **VSF TR-10-5**, which defines HKEP and the HKEP-imposed constraints on HDCP RTP v2.3 behavior for IPMX devices.

It does not restate those specifications or redefine their behavior. Instead, it:

- Defines the scope of evaluation for the HKEP capability.
- Specifies which HKEP behaviors defined in TR-10-5 are evaluated, and where in TR-10-5 each requirement lives.
- Identifies matters that are explicitly outside the scope of this capability evaluation.

All uses of *shall*, *should*, and *may* follow the conformance notation of TR-10-5 section 2 and form the normative portion of this document.

2. Scope (Normative)

This capability evaluates HKEP and the HKEP-imposed constraints on HDCP RTP v2.3 behavior defined by TR-10-5 for IPMX devices. The behaviors evaluated are enumerated in section 6. Items outside the evaluation scope are enumerated in section 7.

This capability does not test HDCP compliance. HDCP compliance is the vendor's responsibility and is verified through Digital Content Protection LLC's processes. This capability evaluates only HKEP and the HKEP-imposed constraints on HDCP RTP v2.3 messaging defined by TR-10-5. It does not evaluate the correctness of HDCP cryptographic operations, key derivation, or HDCP RTP v2.3 behavior outside those constraints.

3. Normative References (Normative)

Devices conforming to this capability shall comply with:

- [VSF TR-10-1](#): Internet Protocol Media Experience (IPMX): System Timing and Definitions.
- [VSF TR-10-5](#): Internet Protocol Media Experience (IPMX): HDCP Key Exchange Protocol (HKEP). This document is the primary reference for the HKEP capability.
- [VSF TR-10-8](#): Internet Protocol Media Experience (IPMX): NMOS Requirements.
- [IPMX Product Qualification and Certification Requirements \(PQCR\)](#): The IPMX baseline requirements that every conforming IPMX device must follow.

This capability does not redefine concepts already defined in the documents above. Where TR-10-5 itself references material outside the TR-10 series (for example, the HDCP RTP v2.3 specification), implementers reach that material transitively through TR-10-5 and through their HDCP licensing process. This capability does not introduce a normative reference to material outside the TR-10 series.

4. Terms and Definitions (Informative)

The terms used in this document are as defined in:

- VSF TR-10-1
- VSF TR-10-5
- VSF TR-10-8
- IPMX Product Qualification and Certification Requirements (PQCR)

This capability introduces no additional terms.

5. General Provisions (Normative)

A device claiming this capability shall implement the HKEP behavior defined in VSF TR-10-5 for protected content transported over IPMX.

Parameter	Requirement
Protocol	HKEP, as defined by VSF TR-10-5
Protocol layering	HKEP messages over TCP/IP; encrypted content over RTP/UDP/IP. The relationship between the two channels shall be as defined in TR-10-5 section 9.3.
Minimum device key set	An HDCP Device Key Set indicating HDCP v2.2+, as required by TR-10-5 section 9.3.
Protocol constants	As per the values defined in TR-10-5 section 11.
Locality-check parameters	As per the values defined in TR-10-5 section 13.1.
SDP signaling	As defined in TR-10-5 section 10 and section 17.
Key set provenance	A production HDCP Device Key Set. Test or facsimile key sets shall not be used during evaluation.

6. Capability Evaluation Requirements (Normative)

This section enumerates the HKEP behaviors evaluated for this capability. Each subsection identifies a behavior area, references the TR-10-5 clauses that define it, and states the meaning in summary form. Implementers shall refer to TR-10-5 for the authoritative definitions.

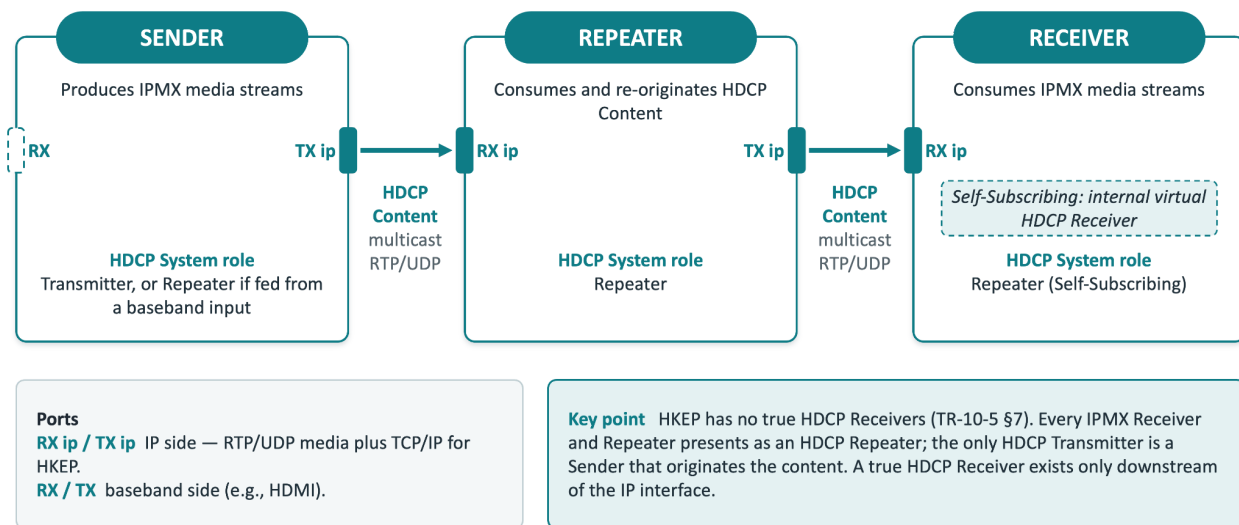
6.1 Device Role, Topology, and Identifiers

References: **TR-10-5 section 6, section 7, section 8, section 9, section 9.3, section 9.3.1, section 9.3.2, section 9.3.3.**

TR-10-5 defines three device roles, and this document uses them with the same meaning. A Sender produces IPMX media streams. A Receiver consumes IPMX media streams. A Repeater does both: it consumes HDCP Content from an upstream Sender and re-originates that content to downstream devices. TR-10-5 section 8 describes a Repeater as a Receiver when only its RX ip side is considered, and as a Sender when only its TX ip side is considered, so a requirement written for a Sender or a Receiver applies to the corresponding side of a Repeater.

These are IPMX roles, and they are not the same as the role a device presents inside an HDCP System. A Sender appears in an HDCP System either as an HDCP Transmitter, when it originates the HDCP Content, or as an HDCP Repeater, when it takes HDCP Content in over a baseband RX Port and re-originates it onto IP. A Receiver always appears as an HDCP Repeater, because HKEP does not support true HDCP Receivers (TR-10-5 section 7); a Receiver with no active, authenticated downstream HDCP Device behaves as a Self-Subscribing HDCP Repeater. A Repeater appears as an HDCP Repeater. The practical consequence is that on the HDCP side of an HKEP system nearly every IPMX device is an HDCP Repeater, and a true HDCP Receiver appears only downstream of the IP interface.

A device claiming this capability shall present a Sender, Receiver, or Repeater role with the IP-side port topology TR-10-5 prescribes for that role (TR-10-5 section 6, section 7, and section 8), and shall associate the identifiers TR-10-5 requires: a globally unique node identifier (NodeId) for Sender and Repeater roles, an HDCP Receiver ID for Receiver and Repeater roles, and a locally unique port identifier (PortId) for each HDCP Content group originating at a Sender or Repeater.



Source: VSF TR-10-5 (2026-02-17), sections 6–8; HDCP RTP v2.3 (DCP LLC).

IPMX Device Roles and Their HDCP-System Equivalents

HDCP Content flows from the HDCP Transmitter (root) through Repeaters to a Receiver (leaf).

On IP, nearly every device presents as an HDCP Repeater.

All IP-side receive ports of a given Receiver or Repeater shall share a single HDCP Device Key Set, as required by TR-10-5 section 9.3.1 and section 9.3.2. A Receiver shall use a single TCP/IP connection for all HDCP Content streams produced by a given Sender, as required by TR-10-5 section 9.3.3.

6.1.1 Profile Testing Scope

The device shall be exercised against exactly one IPMX video profile and, where the device also supports audio, exactly one IPMX audio profile, each selected by the vendor. Where the device supports both audio and video, both are exercised; where it supports only one media type, only that media type is exercised. Where the device supports more than one IPMX profile, only the nominated profile is exercised, and this capability does not report which profile was tested. Because HKEP governs protocol behavior that is independent of the media profile

carried, a vendor may represent HKEP support for the device's other IPMX profiles; this capability does not exercise or verify those additional claims.

6.2 SDP Signaling of HKEP Connection Parameters

References: **TR-10-5 section 10, section 17.**

When the associated IPMX media stream carries HDCP Content, the Sender shall include at least one HKEP session attribute in the SDP transport file, populated as TR-10-5 section 10 prescribes. The Sender shall deliver the SDP through the method defined in VSF TR-10-8.

When the SDP transport file lists multiple HKEP connection endpoints, the Receiver shall attempt them in the listed order, fall back on connection failure, and — after a successful connection — continue with the chosen endpoint until a subsequent connection attempt fails, at which point the Receiver shall restart from the first listed entry. The HKEP attribute is permitted at both session and media levels of the SDP, as TR-10-5 section 17 defines.

6.3 HKEP Preamble and Session Establishment

References: **TR-10-5 section 9.3, section 12, section 12.2, section 12.3, section 12.4, section 12.6.**

A Receiver subscribing to HDCP Content shall establish a TCP/IP connection to the Sender's listening HKEP endpoint and shall execute the HKEP preamble defined in TR-10-5 section 12.4 as the first exchange on that connection. The preamble carries the HDCP RTP v2.3 protocol messages over TCP/IP, including the pairing, receiver, and restart flags, as TR-10-5 section 12.2 through section 12.4 define.

6.4 Receiver Protocol Modes

References: **TR-10-5 section 12.6.1, section 12.6.2, section 12.6.3.**

A Receiver shall execute the receiver protocol in one of the three modes TR-10-5 defines:

- **Explicit pairing (TR-10-5 section 12.6.1)** — used to perform only the AKE stage and terminate, so that pairing information may be cached for accelerated future authentication.
- **Implicit pairing (TR-10-5 section 12.6.2)** — used to perform the full HDCP RTP v2.3 protocol, with the Sender's status response selecting between a fresh authentication path, a restart at the Authentication-with-Repeaters stage, or a parameter-invalid failure.
- **Reconnect (TR-10-5 section 12.6.3)** — used after the HKEP session has become valid, when the Receiver needs to update topology, refresh stream-management information after observing an unfamiliar `streamCtr`, or make the HKEP session inactive.

The Sender shall respond as TR-10-5 section 12.6.1 and section 12.6.2 prescribe for each mode, including the status-response, pairing-information storage, and message-sequence behaviors defined there.

6.5 Capability Inspection by Non-Receivers

References: **TR-10-5 section 12.7.**

When contacted by a non-Receiver client (for example, an NMOS controller checking capability), the Sender shall execute the non-receiver protocol defined in TR-10-5 section 12.7, including the restricted message exchange and the status response that advertises the Sender's maximum pairing and session slot capacities.

6.6 HKEP Session Lifetime, Caching, and Failure Handling

References: **TR-10-5 section 12.6, section 13.2.2.**

Senders and Receivers shall cache their active HKEP sessions and reuse them as TR-10-5 section 12.6.2 prescribes, including the LRU caching behavior, key composition, and slot-count signaling defined there.

The HKEP session lifetime model defined in TR-10-5 section 12.6 and section 13.2.2 distinguishes between behavior before and after the session becomes valid:

- **Before the HKEP session becomes valid:** if the HKEP or HDCP RTP v2.3 protocol fails, both the Sender and the Receiver shall close the TCP/IP connection and shall expire the associated HKEP session, which remains invalid.
- **After the HKEP session becomes valid:** timeouts, disconnects, or protocol errors shall not invalidate the session. A Sender shall not invalidate an active HKEP session unless it also invalidates the associated HDCP RTP v2.3 session key.

A Sender shall mark the HKEP session as valid after the first successful exchange of topology and stream-management information with the Receiver, as TR-10-5 section 13.2.2 prescribes; a Receiver shall do likewise on its side.

Note: Per TR-10-5 section 13.2.2, a Receiver shall not decrypt an encrypted HDCP Content stream until its HKEP session becomes valid. Verifying this behavior is not part of this capability evaluation because it requires observing HDCP decryption state, which is outside HKEP scope.

6.7 Locality Check Constraints

References: **TR-10-5 section 13.1.**

A device claiming this capability shall implement the HDCP RTP v2.3 locality check under the constraints TR-10-5 section 13.1 imposes, including:

- Setting the locality-precompute support flags as TR-10-5 section 13.1 requires;
- Retrying the locality check up to the maximum number of trials TR-10-5 section 13.1 defines, with a fresh challenge on each retry;
- Sending a new locality-check initiation message immediately upon observing a locality mismatch;
- Aborting the protocol and closing the TCP/IP connection when the locality response does not arrive within the timeout TR-10-5 section 11 defines.

6.8 HKEP Sequencing Constraints on Authentication with Repeaters

References: **TR-10-5 section 13.2, section 13.2.1, section 13.2.3.**

A device claiming this capability shall implement the HKEP-imposed sequencing on the HDCP RTP v2.3 Authentication-with-Repeaters exchange as TR-10-5 section 13.2 prescribes. The intent of these constraints, as TR-10-5 section 13.2 states, is to ensure that an HKEP session becomes valid on a Receiver only if it is also valid on the Sender.

The evaluation includes:

- The initial-message exchange between Sender and Receiver and the timeout behavior on that exchange (TR-10-5 section 13.2.1);
- The conditions under which subsequent exchanges are considered successful (TR-10-5 section 13.2.3);
- The parallel operation of Authentication with Repeaters with the flow of encrypted content and HDCP link synchronization (TR-10-5 section 13.2).

This evaluation does not test the correctness of AKE, locality check, or SKE behavior beyond the constraints TR-10-5 imposes; those run as per the HDCP RTP v2.3 specification.

6.9 Receiver_AuthStatus Handling

References: **TR-10-5 section 13.2.1.**

A device claiming this capability shall handle the HDCP RTP v2.3 Receiver_AuthStatus message under the constraints TR-10-5 section 13.2.1 imposes. The evaluation includes the Sender's obligation to disregard Receiver_AuthStatus for purposes of establishing HKEP or HDCP RTP v2.3 session validity, the Receiver's behavior with respect to the REAUTH state, and the Receiver's restriction on sending Receiver_AuthStatus in the unsolicited case.

6.10 Null Topology Handling

References: **TR-10-5 section 13.2.4.**

A Receiver that no longer subscribes to a Sender's HDCP Content may make its HKEP session inactive at that Sender by presenting a Null Topology, as TR-10-5 section 13.2.4 defines. This evaluation does not assess enforcement of maximum topology size or any other HDCP topology policy that lies outside TR-10-5.

6.11 Stream Management Construction Constraints

References: **TR-10-5 section 13.3.**

A Sender shall construct stream-management messages under the HKEP-imposed constraints TR-10-5 section 13.3 defines, including the requirement that each content stream in a session be associated with a unique stream counter, the immutability of the association between that counter and its content-stream identifiers for the duration of the session, and the practical size bound TR-10-5 section 13.3 places on the message.

6.12 RTP Header-Extension Presence and streamCtr Signaling

References: **TR-10-5 section 14, section 14.1.**

A Sender producing protected HDCP Content over IPMX shall embed the HDCP RTP v2.3 IV-counter header extensions in each protected media stream, in the position TR-10-5 section 14 requires.

A Receiver shall monitor the stream counter on each protected stream it consumes. On observing a stream-counter value for which it does not hold the corresponding stream-management information, the Receiver shall connect or reconnect to the Sender and execute the HDCP RTP v2.3 protocol as TR-10-5 section 14.1 prescribes. A Sender shall change the stream counter when its associated stream-management information changes, as TR-10-5 section 14.1 prescribes.

This evaluation does not test the use of the stream counter or the input counter by the HDCP stream cipher itself; those are HDCP cryptographic behaviors verified elsewhere.

6.13 HKEP Media Info Block in RTCP Sender Reports

References: **TR-10-5 section 16.**

A Sender producing HDCP Content shall include the HKEP Media Info Block in its RTCP Sender Reports as TR-10-5 section 16 prescribes, and shall omit the block when the associated SDP transport file carries no HKEP session attribute. The block shall be populated with the

fields TR-10-5 section 16 defines, including the version field that increments when the HKEP session attribute value changes and the identifiers for the HKEP RTP header extensions.

7. Out-of-Scope (Informative)

This capability evaluation does not test or certify matters outside the behavioral scope of TR-10-5. In particular:

7.1 HDCP Cryptographic Behavior

It does not test HDCP cryptographic behavior, including key derivation, session-key and initialization-vector usage across streams, or the correctness of content encryption and decryption. HDCP cryptographic correctness is governed by HDCP RTP v2.3 and is verified through Digital Content Protection LLC's processes.

7.2 HDCP Licensing and DCP Administrative Requirements

It does not test compliance with HDCP licensing agreements, commercial entitlement, or broader DCP administrative requirements. TR-10-5 states the minimum device-key-set requirement for participating IPMX devices, but it is not itself a licensing-audit procedure.

7.3 Non-IP HDCP Interface Behavior

It does not test non-IP HDCP interface behavior, except insofar as such equipment may exist in a product outside the TR-10-5 IPMX interface model. TR-10-5 explicitly separates non-HDCP_{RTP} connections from HDCP_{RTP} / HKEP connections, with non-IP connections governed by their own interface-specific HDCP specifications.

7.4 Vendor-Specific Baseband Bridging

It does not test vendor-specific baseband bridging behavior between HDCP versions or other product-specific implementation choices outside the HKEP behavior defined for the IPMX side.

7.5 Generalized Topology-Limit Enforcement

It does not test maximum connected receiver count, maximum cascade depth, or generalized topology-limit enforcement as a separate certification objective. TR-10-5 defines Null Topology behavior and references topology-related fields within the HDCP RTP v2.3 flow, but this capability does not make "maximum receiver topology enforcement" a standalone evaluation item.

7.6 Rejection of Non-HDCP Receivers

It does not test rejection of "non-HDCP receivers" as a separate requirement. TR-10-5 defines the HKEP behavior of IPMX participants and explicitly notes (TR-10-5 section 7) that, in this system, an IP-based Receiver is an HDCP Repeater rather than a true HDCP Receiver. This capability therefore stays within the HKEP participant model defined by TR-10-5.

7.7 Certification-Lab Mechanics Not Defined by TR-10-5

It does not prescribe certification-lab mechanics that are not defined by TR-10-5, such as mandatory use of certification-authority reference devices, prohibition of vendor-paired test setups, or broader program rules outside the normative protocol behavior itself.

8. Conformance Statement (Normative)

Successful evaluation of this capability indicates that the device correctly implements the HKEP behavior defined by VSF TR-10-5 within the scope described in this document. It does not imply certification of HDCP compliance or of product behavior beyond that scope.

Appendix A: Mapping to VSF TR-10-5 (Informative)

The following table maps each section 6 subsection of this document to the TR-10-5 clauses that define its normative behavior.

section 6 subsection	TR-10-5 clauses
6.1 Device role, topology, and identifiers	section 6, section 7, section 8, section 9, section 9.3, section 9.3.1, section 9.3.2, section 9.3.3
6.2 SDP signaling of HKEP connection parameters	section 10, section 17
6.3 HKEP preamble and session establishment	section 9.3, section 12, section 12.2, section 12.3, section 12.4, section 12.6
6.4 Receiver protocol modes	section 12.6.1, section 12.6.2, section 12.6.3
6.5 Capability inspection by non-Receivers	section 12.7
6.6 HKEP session lifetime, caching, and failure handling	section 12.6, section 13.2.2
6.7 Locality check constraints	section 13.1
6.8 HKEP sequencing constraints on Authentication with Repeaters	section 13.2, section 13.2.1, section 13.2.3
6.9 Receiver_AuthStatus handling	section 13.2.1
6.10 Null Topology handling	section 13.2.4
6.11 Stream management construction constraints	section 13.3

section 6 subsection	TR-10-5 clauses
6.12 RTP header-extension presence and streamCtr signaling	section 14, section 14.1
6.13 HKEP Media Info Block in RTCP Sender Reports	section 16

Appendix B: Change Log

Version	Date	Summary of Changes
1.0	Aug 20, 2026	Published.
1.0 DRAFT	2026/05	Initial draft of the HKEP Capability Requirements document. Coverage of section 6 expanded against the full TR-10-5 SHALL surface (audited 2026-05-20). HKEP-only scope boundary stated in section 2. Normative References restricted to the TR-10 series and PQCR. Section 6 organized around 13 behavior areas, each referencing TR-10-5 by meaning and section rather than by field or value. Out-of-Scope expanded with an explicit HDCP cryptographic carve-out (section 7.1). Mapping table rebuilt without line-number

Version	Date	Summary of Changes
		suffixes; AKE / Locality entry corrected (AKE itself is not HKEP-constrained; the HKEP preamble lives in section 12.4 / section 12.6 and the locality check in section 13.1).