PEP Capability Requirements

Version 1.0 (2026-05)

Published by the Alliance for IP Media Solutions (AIMS)
https://aimsalliance.org
https://ipmx.io

Copyright & Permissions Notice

1. Introduction (Informative)

This document defines the IPMX PEP Capability, the requirements an IPMX device must implement to claim support for the Privacy Encryption Protocol (PEP) over IP networks, as defined in VSF TR-10-13, 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-10-13, which defines PEP, including the privacy key derivation construction, the SDP and NMOS parameter exchange, the privacy cipher composition, the RTP protocol adaptation, and the PEP Media Info Block.

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

- Defines the scope of evaluation for the PEP capability.
- Specifies which PEP behaviors defined in TR-10-13 are evaluated, and where in TR-10-13 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-10-13 Section 6 and form the normative portion of this document.

2. Scope (Normative)

This capability evaluates the PEP behaviors defined by TR-10-13 for IPMX devices, across all PEP transport protocol adaptations defined by the TR-10 series. The transport-independent PEP core behaviors are enumerated in Section 6. The transport protocol adaptations are enumerated in Section 7, with RTP defined in TR-10-13 and USB defined in TR-10-14. Optional features within the capability are enumerated in Section 8, and items outside the evaluation scope in Section 9.

This capability does not test the cryptographic correctness of the underlying primitive implementations. PEP composes its key derivation, encryption, authentication, and key

agreement from primitives whose mathematical correctness is defined outside the TR-10 series (the AES block cipher, the CMAC and HMAC message authentication functions, the SHA-2 hash family, the underlying ECDH elliptic curve arithmetic, and the SEC1 public-key encoding). This capability evaluates that the device composes those primitives correctly per TR-10-13 (the KDF construction, the cipher input composition, the per-curve key encoding, the parameter exchange, and end-to-end stream interoperation), and that PEP itself interoperates correctly across senders and receivers. The mathematical correctness of the primitive implementations themselves is the vendor's responsibility, verified through cryptographic-module validation processes or equivalent vendor processes.

3. Normative References (Normative)

This document references these specifications:

- **VSF TR-10-1:** System Timing and Definitions.
- **VSF TR-10-5:** HDCP Key Exchange Protocol.
- **VSF TR-10-8:** NMOS Requirements.
- **VSF TR-10-13:** Privacy Encryption Protocol (PEP). This document is the primary reference for the PEP capability.
- **VSF TR-10-14:** IPMX USB. Referenced for the USB transport adaptation of PEP.
- **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-10-13 itself references material outside the TR-10 series (for example, the NIST cryptographic specifications, the IETF RTP header extension framing, or the SEC1 elliptic curve public key encoding), implementers reach that material transitively through TR-10-13. 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-10-13
  VSF TR-10-14
- 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 PEP behavior defined in VSF TR-10-13, applied to each PEP transport protocol adaptation the device implements.

Parameter	Requirement
Protocol	PEP, as defined by VSF TR-10-13
Required transport adaptations	At least one TR-10-series PEP transport adaptation: video RTP (TR-10-13 Section 20) and USB (if present, TR-10-14 Section 12), evaluated per Section 7 of this document for each adaptation the device implements. If audio and video are present, then one of each shall be supported. However, not all audio or video (RTP) flows are required to support PEP.
Mandatory cipher mode	AES-128-CTR, as required by TR-10-13 Section 15 and Section 20
Mandatory PSK target size	128 bits, as required by TR-10-13 Section 17
Parameter exchange	SDP privacy attribute and NMOS extended transport parameters, as defined in TR-10-13 Section 13 and TR-10-8

Parameter	Requirement
Privacy key derivation	KDF in counter mode using CMAC or HMAC-SHA-512/256 as the PRF, as TR-10-13 Section 12 prescribes
RTP header extensions	CTR Full and CTR Short Privacy RTP Extension Headers, as defined in TR-10-13 Section 20.1
PEP Media Info Block	As defined in TR-10-13 Section 22
USB message fields	CTR, KEYVERSION, and MAC fields of the IPMX USB TCP message, as defined in TR-10-14 Section 12
USB cipher mode	AES-128-CTR_CMAC-64-AAD, as required by TR-10-14 Section 12. Encryption and authentication are mandatory for the USB adaptation under this capability.
USB SDP signaling	USB_KV protocol value in the SDP privacy attribute, as defined in TR-10-14 Section 14

Per-adaptation requirements (mandatory cipher mode, header extension format, payload encoding, and adaptation-specific signaling) are defined in Section 7.

6. Capability Evaluation Requirements (Normative)

This section enumerates the transport-independent PEP core behaviors evaluated for every conforming device, regardless of which transport protocol adaptations the device implements. Adaptation-specific behaviors are enumerated in Section 7. Each subsection identifies a behavior area, references the TR-10-13 clauses that define it, and states the meaning in summary form. Implementers shall refer to TR-10-13 for the authoritative definitions.

6.1 Privacy Key Derivation Construction

References: **TR-10-13 Section 12.**

A Sender or Receiver claiming this capability shall derive a privacy key for every privacy-encrypted stream and sub-stream using the KDF in counter mode construction TR-10-13 Section 12 defines, with the PRF selection that TR-10-13 ties to the PSK size and with the inputs (PSK, key generator, key version, and the Perfect Forward Secrecy shared secret when applicable) TR-10-13 enumerates. The privacy key size shall match the AES variant the device implements, as TR-10-13 Section 12 prescribes.

When the device does not implement the Perfect Forward Secrecy mode, the PFS input to the key derivation shall be the empty value TR-10-13 Section 12 defines.

6.2 SDP Signaling of PEP Parameters

References: **TR-10-13 Section 13, Section 23.**

A Sender producing a privacy-encrypted stream over a transport protocol that uses an SDP transport file shall communicate the PEP parameters TR-10-13 Section 13 requires through the SDP privacy attribute, at the session level or the media level as TR-10-13 Section 23 defines. When the Sender does not perform privacy encryption, the SDP privacy attribute shall be omitted, as TR-10-13 Section 13 prescribes for the NULL case.

The SDP privacy attribute shall follow the syntax TR-10-13 Section 13 prescribes, including parameter ordering, separator characters, and line termination.

6.3 NMOS Transport Parameter Communication

References: **TR-10-13 Section 13, TR-10-8.**

In an NMOS environment, a Sender or Receiver shall communicate the PEP parameters TR-10-13 Section 13 enumerates through the extended NMOS transport parameters defined there, using the naming convention TR-10-13 Section 13 prescribes and following the constraint rules TR-10-13 imposes. Each transport parameter shall carry the constraint TR-10-13 requires

for that parameter's role on the device, and the device shall reject Controller attempts to set a transport parameter to a value outside its constraint.

The values exchanged simultaneously through the SDP transport file and the NMOS transport parameters shall be identical, as TR-10-13 Section 13 prescribes.

A Sender in an NMOS environment shall expose its PEP parameters through the SDP transport file and the NMOS transport parameters, as TR-10-13 Section 13 defines; subscribed Receivers obtain them through those mechanisms.

6.4 Parameter Stability and Activation Boundaries

References: **TR-10-13 Section 13.**

The PEP parameters TR-10-13 Section 13 enumerates shall not change while a Sender or Receiver is active. The single exception is the key version under an in-band dynamic-key-version protocol, where the SDP and NMOS values reflect the activation value and the in-band value may change during the activation, as TR-10-13 Section 13 prescribes.

When using redundancy as TR-10-13 Section 13 describes, all legs of the redundant set shall use identical PEP parameters.

Disabling privacy encryption on a device configured to perform privacy encryption shall not be possible through the NMOS transport parameters. Only a vendor-specific configuration mechanism shall be permitted to perform that change, as TR-10-13 Section 13 prescribes.

6.5 Privacy Cipher Input Uniqueness

References: **TR-10-13 Section 14.**

The per-sub-stream initial vector value shall equal the base initial vector value for a standalone unidirectional stream, as TR-10-13 Section 14 prescribes. The combination of per-sub-stream initial vector, key generator, key version, and key identifier shall be unique among all streams and sub-streams encrypted by the device, as TR-10-13 Section 14 requires.

Devices that support multiplexed or bidirectional sub-streams are evaluated additionally under Section 7.5 of this document.

6.6 Privacy Cipher Operation

References: **TR-10-13 Section 15, Section 20.**

A device claiming this capability shall apply the privacy cipher to the protected portion of each stream or sub-stream using AES in CTR or GCM mode, with the key, the composed initial-vector-and-counter input, and the encryption boundary that TR-10-13 Section 15 and the relevant adaptation in Section 7 of this document define for the implemented mode.

The composed initial-vector-and-counter input shall not be used more than once with a given key, as TR-10-13 Section 15 requires.

For modes that authenticate a portion of the stream, the device shall follow the construction TR-10-13 Section 15 defines for that mode, including the mac-then-encrypt or encrypt-then-mac order and the truncated-MAC selection rule.

6.7 PSK Programming and Revocation

References: **TR-10-13 Section 17.**

A device claiming this capability shall accept PSK programming for the PSK sizes TR-10-13 Section 17 defines, with the 128-bit size mandatory and the 256-bit and 512-bit sizes optional. The device shall clearly indicate to the administrator which PSK sizes it supports.

The PSK programming interface shall accept PSK values expressed in the Octet String notation TR-10-13 Section 10 defines.

A Sender Device that needs to revoke a Receiver's access to a stream shall stop using the corresponding key identifier, as TR-10-13 Section 17 prescribes.

The mechanism by which PSKs are provisioned into a device is out of scope of TR-10-13 and of this capability.

6.8 Forward-Progress Verification of the In-band Counter

References: **TR-10-13 Section 18, Section 20.**

A device that consumes a privacy-encrypted stream carrying an in-band counter as part of its transport adaptation shall verify forward progress on the received counter value, including the modular wrap-around rule TR-10-13 Section 18 defines, except for the first counter value received after subscription, which TR-10-13 explicitly exempts. The specifics of how the counter is conveyed in-band depend on the transport adaptation and are evaluated under Section 7.

Forward-progress verification on the in-band dynamic key version, when implemented, is evaluated under Section 8.4 of this document.

7. Transport Protocol Adaptations (Normative)

A device claiming this capability shall implement at least one TR-10-series PEP transport protocol adaptation, and shall conform to the requirements of each adaptation it implements. The adaptations defined today are the RTP adaptation in TR-10-13 Section 20 and the USB adaptation in TR-10-14 Section 12. Future adaptations defined in companion TR-10 documents are evaluated under this section as they are added.

A device claiming this capability shall implement PEP on at least one content stream. If audio and video are both present on the device, then at least one of each must support PEP. When the USB capability is present, then implementation of the USB adaptation is required; a device that implements it shall conform to Section 7.2 of this document.

Evaluation of this capability exercises one stream of each content type the device supports. A device that supports video, audio, and USB is evaluated on one video stream, one audio stream, and one USB connection.

7.1 RTP Transport Adaptation

References: **TR-10-13 Section 20.**

A device that implements PEP for the RTP transport shall apply the RTP-specific PEP behavior TR-10-13 Section 20 defines, as enumerated in this subsection.

7.1.1 RTP Protocol Adaptation Baseline

References: **TR-10-13 Section 20.**

A device implementing the RTP adaptation shall support the RTP protocol adaptation defined in TR-10-13 Section 20. Support for the RTP_KV protocol adaptation is optional and is evaluated under Section 8.4 of this document.

The device shall apply the encryption-boundary rules TR-10-13 Section 20 defines, including the requirement that the RTP Header, RTP Header Extensions, and RTP Payload Header remain unencrypted, and the rule that determines whether the complete RTP Payload is encrypted when no RTP Payload Header is defined for the payload format.

The composed initial-vector-and-counter input under the RTP adaptation shall be constructed from the per-sub-stream initial vector and the per-slice counter as TR-10-13 Section 20 prescribes. The counter shall start at zero for a new key and shall increment by one per encrypted slice, with the wrap-around behavior TR-10-13 defines.

7.1.2 Privacy RTP Header Extension Format and Usage

References: **TR-10-13 Section 20.1, Section 20.2.**

A Sender producing privacy-encrypted RTP shall embed the Privacy RTP Extension Headers in each protected stream, using the Full and Short forms TR-10-13 Section 20.1 defines and the URN values TR-10-13 prescribes for their identification in the SDP transport file. The header fields shall be populated as TR-10-13 Section 20.1 defines, including endianness, reserved-bit settings, and the partitioning of the counter value across the Full and Short forms.

A Sender shall use the Full form of the Privacy RTP Extension Header in the first RTP packet of each video frame, video field, video frame or field slice, and audio packet, and shall use the Full form on every RTP packet not categorized as video or audio. The Short form shall be used in the other RTP packets. The distance between two consecutive Full form headers in a stream shall not exceed the bound TR-10-13 Section 20.2 defines, ensuring that a Receiver can recover the full counter value from the Short form using the algorithm TR-10-13 prescribes.

A Receiver shall recover the full counter value from the Full and Short forms using the concatenation and wrap-handling rules TR-10-13 Section 20 defines.

7.1.3 RTP Payload Encoding and MAC Storage

References: **TR-10-13 Section 20.2.**

A Sender shall encode the encrypted portion of the RTP Payload as a sequence of 16-byte slices, optionally terminated by a partial slice, with the zero-fill behavior TR-10-13 Section 20.2 defines for the partial slice.

In the modes that authenticate the payload, the Sender shall reserve the trailing bytes of the RTP Payload for the truncated MAC, as TR-10-13 Section 20.2 prescribes, and shall reduce the effective payload size accordingly so that the resulting RTP packet remains within the maximum length permitted by the payload format.

7.1.4 PEP Media Info Block in RTCP Sender Reports

References: **TR-10-13 Section 22.**

A Sender producing privacy-encrypted RTP shall include the PEP Media Info Block in its RTCP Sender Reports as TR-10-13 Section 22 prescribes, and shall omit the block when the associated SDP transport file carries no privacy attribute. The block shall be populated with the fields TR-10-13 Section 22 defines, including the privacy version field that increments when the privacy attribute value changes and the identifiers for the Privacy RTP header extensions.

7.2 USB Transport Adaptation

References: **TR-10-14 Section 12, Section 14.**

A device that implements PEP for the USB transport defined in TR-10-14 shall apply the USB-specific PEP behavior TR-10-14 Section 12 defines, as enumerated in this subsection.

7.2.1 USB Adaptation Cipher Mode Baseline

References: **TR-10-14 Section 12.**

A USB Sender and a USB Receiver shall support the AES-128-CTR_CMAC-64-AAD cipher mode, as TR-10-14 Section 12 requires. The cipher mode in use shall be one of the values TR-10-14 Section 12 enumerates. The CMAC function used for authentication shall use the privacy cipher key, with the AES block-cipher size selected to match the key size, as TR-10-14 Section 12 prescribes.

The encryption boundary, slice structure, and MAC storage shall follow the construction TR-10-14 Section 12 defines, including the mac-then-encrypt order, the 16-byte slice subdivision with zero-fill of any partial slice, and the encrypted MAC stored as the trailing bytes of the message.

7.2.2 USB Sub-stream Identifier Assignment

References: **TR-10-14 Section 12.**

A USB Sender and a USB Receiver shall assign sub-stream identifiers to the USB control channel and the USB data channels as TR-10-14 Section 12 prescribes, including the bidirectional pairing convention TR-10-14 defines for the Sender-to-Receiver and Receiver-to-Sender directions. The per-sub-stream initial vector value derived from these identifiers shall preserve the uniqueness invariant under Section 6.5 of this document.

7.2.3 Per-TCP-Session Key Version and Counter Reset

References: **TR-10-14 Section 12.**

At each TCP session, when the connection is accepted, the USB Sender shall increment the key version and shall reset the counter value to zero, as TR-10-14 Section 12 prescribes. The forward-progress evaluation under Section 6.8 of this document applies to the counter value as it advances within a TCP session.

7.2.4 SDP Signaling for the USB Adaptation

References: **TR-10-14 Section 14.**

A USB Sender shall use the USB_KV protocol value in the SDP privacy attribute, with one of the cipher mode values TR-10-14 Section 14 prescribes for the USB adaptation. The SDP privacy attribute itself follows the requirements under Section 6.2 of this document.

8. Optional Features (Normative)

This section enumerates the optional features TR-10-13 defines within the PEP capability. When a device implements an optional feature, it shall implement the additional behaviors TR-10-13 prescribes for that feature, as summarized below. Optional features that apply only within a specific transport adaptation are flagged in the subsection that defines them.

8.1 Perfect Forward Secrecy ECDH Mode

References: **TR-10-13 Section 12, Section 13.**

A device that implements one of the cipher modes with the ECDH prefix TR-10-13 Section 20 enumerates or TR-10-14 Section 12 enumerates shall implement the Perfect Forward Secrecy mechanism TR-10-13 Section 12 and Section 13 define. The device shall implement the elliptic curve and the two public-key NMOS transport parameters TR-10-13 Section 13 requires, with the per-curve encoding rules TR-10-13 prescribes. The device shall generate a fresh, ephemeral public key randomly at initialization and at each transition out of the active state, and shall regenerate the keypair under the conditions TR-10-13 Section 12 defines. Under redundancy, all legs shall use the same ECDH keypair, as TR-10-13 Section 12 requires.

A Controller that participates in a Perfect Forward Secrecy ECDH exchange shall exchange the Sender's public key and the Receiver's public key prior to activation, as TR-10-13 Section 13 prescribes.

8.2 AES-256 Support

References: **TR-10-13 Section 12, Section 15, Section 20.**

A device that implements any of the AES-256 cipher modes TR-10-13 Section 20 or TR-10-14 Section 12 enumerates shall meet the additional PSK size, key derivation, and cipher key size requirements TR-10-13 Section 12 and Section 15 define for AES-256. The device shall accept

the additional PSK target sizes TR-10-13 Section 17 permits for AES-256 (256 bits and 512 bits) when the administrator selects them.

8.3 Authenticated Cipher Modes

References: **TR-10-13 Section 15, Section 20.**

A device that implements one of the authenticated cipher modes TR-10-13 Section 20 enumerates (the CMAC-64 and CMAC-64-AAD variants) shall implement the authentication construction TR-10-13 Section 15 defines for that mode, including the truncated-MAC size, the CMAC key selection rule that ties the CMAC block cipher to the cipher key size, and the MAC storage location TR-10-13 Section 20.2 prescribes within the RTP Payload. For the AAD variants, the device shall compute the MAC over the additional authenticated data input TR-10-13 Section 20 defines for the Full or Short form, in addition to the payload data.

Within the USB adaptation, the authenticated CMAC-64-AAD construction is mandatory rather than optional and is evaluated under Section 7.2.1 of this document.

8.4 In-band Dynamic Key Version (RTP_KV)

References: **TR-10-13 Section 18, Section 20, Section 20.3.**

This feature applies only within the RTP transport adaptation. A Sender or Receiver that implements the RTP_KV protocol adaptation shall convey the current key version in the dedicated field of the Full form of the Privacy RTP Extension Header, as TR-10-13 Section 20.3 prescribes, and shall use the value received in that field to derive the decryption key for the associated RTP Payload.

A device implementing RTP_KV shall verify forward progress on the received in-band key version, including the modular wrap-around and bounded-distance rules TR-10-13 Section 18 defines, except for the first value received after subscription.

The RTP_KV protocol adaptation should be used with an authenticated cipher mode under Section 7.3 of this document, as TR-10-13 Section 18 recommends.

8.5 Multiplexed and Bidirectional Sub-streams

References: **TR-10-13 Section 14, Section 20.**

A device that supports multiplexed or bidirectional sub-streams shall derive the per-sub-stream initial vector value from the base initial vector and the sub-stream identifier as TR-10-13 Section 14 prescribes, using the sub-stream identifier range TR-10-13 defines and, for bidirectional streams, the even-and-odd partitioning by direction. The uniqueness invariant under Section 6.5 of this document continues to apply across all sub-streams.

9. Conformance Statement (Normative)

Successful evaluation of this capability indicates that the device correctly implements the PEP behavior defined by VSF TR-10-13 within the scope described in this document, including each TR-10-series transport protocol adaptation under Section 7 the device implements and any optional features under Section 8 the device claims. It does not imply certification of the underlying cryptographic primitive implementations or of product behavior beyond that scope.

Appendix A: Mapping to VSF TR-10-13 (Informative)

The following table maps each Section 6 and Section 7 subsection of this document to the TR-10-13 clauses that define its normative behavior.

Section	TR-10 clauses
6.1 Privacy key derivation construction	TR-10-13 Section 12
6.2 SDP signaling of PEP parameters	TR-10-13 Section 13, Section 23
6.3 NMOS transport parameter communication	TR-10-13 Section 13
6.4 Parameter stability and activation boundaries	TR-10-13 Section 13
6.5 Privacy cipher input uniqueness	TR-10-13 Section 14
6.6 Privacy cipher operation	TR-10-13 Section 15
6.7 PSK programming and revocation	TR-10-13 Section 17
6.8 Forward-progress verification of the in-band counter	TR-10-13 Section 18
7.1.1 RTP protocol adaptation baseline	TR-10-13 Section 20

Section	TR-10 clauses
7.1.2 Privacy RTP Header Extension format and usage	TR-10-13 Section 20.1, Section 20.2
7.1.3 RTP Payload encoding and MAC storage	TR-10-13 Section 20.2
7.1.4 PEP Media Info Block in RTCP Sender Reports	TR-10-13 Section 22
7.2.1 USB adaptation cipher mode baseline	TR-10-14 Section 12
7.2.2 USB sub-stream identifier assignment	TR-10-14 Section 12
7.2.3 Per-TCP-session key version and counter reset	TR-10-14 Section 12
7.2.4 SDP signaling for the USB adaptation	TR-10-14 Section 14
8.1 Perfect Forward Secrecy ECDH mode	TR-10-13 Section 12, Section 13
8.2 AES-256 support	TR-10-13 Section 12, Section 15, Section 20
8.3 Authenticated cipher modes	TR-10-13 Section 15, Section 20
8.4 In-band dynamic key version (RTP_KV)	TR-10-13 Section 18, Section 20, Section 20.3

Section	TR-10 clauses
8.5 Multiplexed and bidirectional sub-streams	TR-10-13 Section 14, Section 20

Appendix B: Change Log

Version	Date	Summary of Changes
1.0	2026-08	Clarified USB support requirements. Clarified that one audio and one video flow (if present) must support PEP.
1.0 DRAFT	2026-05	Initial draft of the PEP Capability Requirements document. Coverage of Section 6 organized around 12 always-mandatory behavior areas spanning TR-10-13 Sections 12 through 22, each referencing TR-10-13 by meaning and section rather than by field or value. Section 7 enumerates six optional features TR-10-13 defines within the capability (Perfect Forward Secrecy ECDH mode, AES-256 support, authenticated cipher modes, RTP_KV protocol with in-band dynamic key version, multiplexed and bidirectional sub-streams, HDCP coexistence), each carrying its own dependent requirements. Scope boundary in Section 2 carves out the correctness of the underlying cryptographic primitives (AES, CMAC, HMAC, SHA, KDF construction, ECDH) as a vendor responsibility verified through cryptographic-module validation processes. Normative References restricted to the TR-10 series and PQCR. Section 8 Out-of-Scope covers the cryptographic primitive carve-out, PSK provisioning and administrative key management, RTCP privacy encryption, non-RTP transport adaptations, HDCP behavior in coexistence scenarios, vendor-specific configuration and bridging, and certification-lab mechanics. Mapping table in Appendix A covers both Section 6 and Section 7 entries with section numbers only and no line-number suffixes.