

RTP Field Considerations: Header Extensions and RTCP

Virtual Interim 2016-01-11

draft-westerlund-perc-rtp-field-considerations-00

Magnus Westerlund

Outline



- › RTP Header Extensions
 - Walk through of all existing ones
 - Classes
- › RTCP End-to-End

Header Extensions



- › Assumes RFC 5285
- › Header Extension Id values have the same properties as PTs:
 - Dynamically assigned
 - Depending on signalling
 - Can vary between conference legs
 - Malicious change of IDs could have substantial impact on application
- › Need for privacy and confidentiality depends on individual header extensions
- › MDD can consume and generate some header extensions
 - Which can and should be authenticated end-to-end
 - Which needs confidentiality end-to-end



Header Extensions

- › Transmission Time offsets (RFC5450)
 - › Gives Transmission time
 - Used by for example congestion control
 - End-to-End No rewrite
 - When using hop-by-hop adaptation
 - › Rewrite when sending from MDD
 - › Measure individual leg
 - › MDD Modify: ?
 - › Original value: ?
 - › End-to-End Auth: ?
 - › End-to-End Conf: No
- › SMPTE time-code mapping (RFC5484)
 - Unlikely to use by interactive media source
 - Would reveal source information if not continuously increasing
 - However, should come from source if used
 - › MDD Modify: No
 - › Original value: Yes
 - › End-to-End Auth: Yes
 - › End-to-End Conf: Probably



Header Extensions

- › Synchronisation metadata (RFC6051)
 - Provides the equivalent of RTCP SR NTP to TS mapping
 - Needed by MDD, especially if Switching Media Mixer
- › MDD Modify: No
 - May be created by MDD if Switching Mixer
- › Original value: Yes
- › End-to-End Auth: Yes
 - May not require forwarding (Switching Mixer)
- › End-to-End Conf: No
- › Client to Mixer Audio Level (RFC6464)
 - May be used by MDD to make stream forwarding decision
 - At the same time privacy sensitive, may leak media content [RFC6562]
- › MDD Modify: Remove?
- › Original value: Yes
- › End-to-End Auth: Yes, but conditionally on being present
- › End-to-End Conf: Desirable, but prevents its use in MDD

Header Extensions



- › Mixer-to-client audio level (RFC6465)
 - Provided for streams with mixed media
 - Does not appear likely in PERC context
 - › Not Relevant for MDD -> receiver
 - › Source endpoint Mixing
 - In that case privacy sensitive
 - › MDD Modify: No
 - › Original value: Yes
 - › End-to-End Auth: Yes
 - › End-to-End Conf: Yes
- › Coordination of video orientation (CVO) (3GPP TS 26.114 v 12.5.0)
 - Provides video streams orientation (Rotation)
 - Reveals end user actions
 - › How they rotate device
 - › Privacy sensitive
 - › MDD Modify: No
 - › Original value: Yes
 - › End-to-End Auth: Yes
 - › End-to-End Conf: Yes



Header Extensions

- › Region-of-interest (ROI) (3GPP TS 26.114 V 13.1.0)

- Identifies the sub-selection of the video picture provided
- Controlled by receiver
 - › Privacy sensitive

- › MDD Modify: No

- › Original value: Yes

- › End-to-End Auth: Yes

- › End-to-End Conf: Yes

- › SDES Information (draft-ietf-avtext-sdes-hdr-ext)

- › CNAME

- RTP Endpoint identification
- CNAME can be sensitive

- › Can be made safe (RFC7022)

- › MDD Modify: No

- › Original value: Yes

- › End-to-End Auth: Yes

- › End-to-End Conf: No

- (Maybe if badly created SDES values)



Header Extensions

› SDES MID

([draft-ietf-mmusic-sdp-bundle-negotiation-23](#))

- Provides receiver with Media Source identification (SDP m= line)
 - Signalling specific scope
 - Application dependent what a m= represents
 - Original value meaningless without source to MDD signalling context
- › MDD Modify: Yes
 - › Original value: No
 - › End-to-End Auth: No
 - › End-to-End Conf: No

› SDES RID ([draft-roach-avtext-rid-00](#))

- Identifies what set of encoding and packetization constraints are applied to this RTP stream.

› MDD Modify: Yes (Value remapping)

› Original value: No

› End-to-End Auth: No

› End-to-End Conf: No



Header Extensions

- › Frame Marking ([draft-ietf-avtext-framemarking-00](#))
 - Information on Media Encoding in the Encrypted RTP Payload
 - Indicates independent starting points (I-frames), discardability, layering to MDD
- › MDD Modify: No
- › Original value: Yes
- › End-to-End Auth: Yes
- › End-to-End Conf: No



Header Extension

- › Treatment depends on header extensions:
 - MDD changeable
 - End-to-End Authenticated
 - End-to-End Confidentiality
- › The whole header extension framework can be added and removed
- › Notes that end-to-end authenticated header extension has an issue with ID of extensions

RTP Header Extension Summary



Extension	MDD Modify	Need Original	E2E Auth	E2E Conf
Transmission Time Offset	Y	N	N	N
SMPTE Time Codes	N	Y	Y	Y
Synchronization Metadata	N	Y	Y	N
Client to Mixer Audio Levels	Y	Y	Y*	Y*
Mixer to Client	N	Y	Y	Y
Coordination of video orientation	N	Y	Y	Y
Region-of-interest	N	Y	Y	Y
SDES:CNAME	N	Y	Y	N*
SDES:MID	Y	N	N	N
SDES:RID	Y	N	N	N
Frame Marking	N	Y	Y	N



Header Extension: Decision Time

› Magnus Proposal:

- End-to-End Authentication: **Required in Solution**
 - › Source originating data that needs to be trusted
 - › Needs to also detect removal of Authenticated E2E Header Extensions
 - › Solution for removing selected source authenticated header extensions is: Optional
 - Client to Mixer only to have possible need
- End-to-End Encryption: **Required in Solution**
 - › Several Header Extensions that can contain privacy sensitive data

RTCP



- › A lot of the RTCP information will be leg specific
 - RTCP SR/RR
 - RTCP FB messages related to transport
 - › NACK
 - › TMMBR/TMMBN
 - FB messages related to switching
 - › FIR
 - › LRR

- › RTCP SDES items
 - Some are privacy sensitive
 - › Name, Location,...
 - Some needed by MDD
 - › CNAME, MID, RID
 - CNAME
 - › If changeable by MDD
 - Miss-associate streams
 - Miss-sync with wrong streams
 - › Needs End-to-End authentication to prevent attacks

RTCP



› End-to-End Information

- RTCP SR
 - › Synchronization information
- RTCP Feedback Messages
 - › ROI requests
 - E2E
 - Privacy sensitive

› Unknown Scope

- AFB – Application Layer Feedback
 - › Unknown
- RTCP APP
 - › Unknown content

› To me it appear that we will have to define both:

- End-to-End authenticated
 - End-to-End confidential
- ## › Issue with End-to-End is that any source IDs (SSRC) needs to be common space
- No SSRC translation in MDD

RTP Summary Table



Field	MDD Modify	Need Original	E2E Auth	E2E Conf
Version	N	Y	Y	N
P Indicator	N	Y	Y	N
X Indicator bit	Y	N*	N*	N
CSRC Count	N	Y	Y	N
Marker Bit	N*	Y	Y	N
Payload Type	Y	Y*	Y*	N
Seq. Number	Y	Y	Y	N
Timestamp	Y	Y*	Y	N
SSRC	N	Y	Y	N
CSRC List	N	Y	Y	N
Payload	N	Y	Y	Y
Padding	N	Y	Y	Y