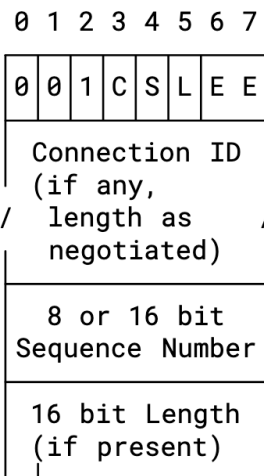
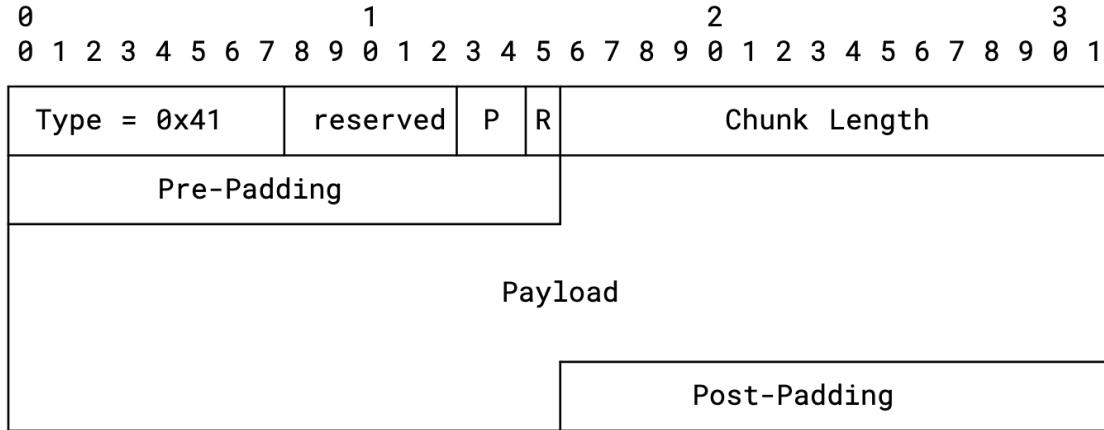


DTLS Chunk for SCTP

[draft-ietf-tsvwg-sctp-dtls-chunk-02](#)

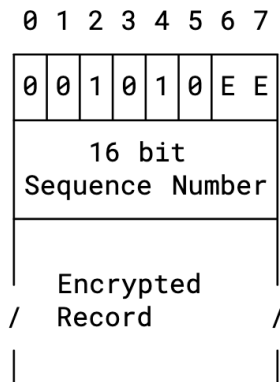
Magnus Westerlund
Claudio Porfiri
John Preuß Mattsson
Michael Tüxen

DTLS Chunk



Legend:

- C - Connection ID (CID) present
- S - Sequence number length
- L - Length present
- E - Epoch



DTLSCiphertext
Structure
(recommended)

- Standard Chunk Header
 - P: Indicate amount of Pre-Padding
 - R: Indicate Restart Security Context used to protect this Packet
- Payload is DTLS 1.3 Record layer per RFC 9147
- DTLS 1.3 Header Usage
 - E E: Epoch indicate key context (2 LSBs)
 - Don't use Connection ID, see next slide
 - Sequence Number: 16-bit recommended
- Expect 1 byte Pre-Padding to be common
 - No gain to use 8-bit sequence

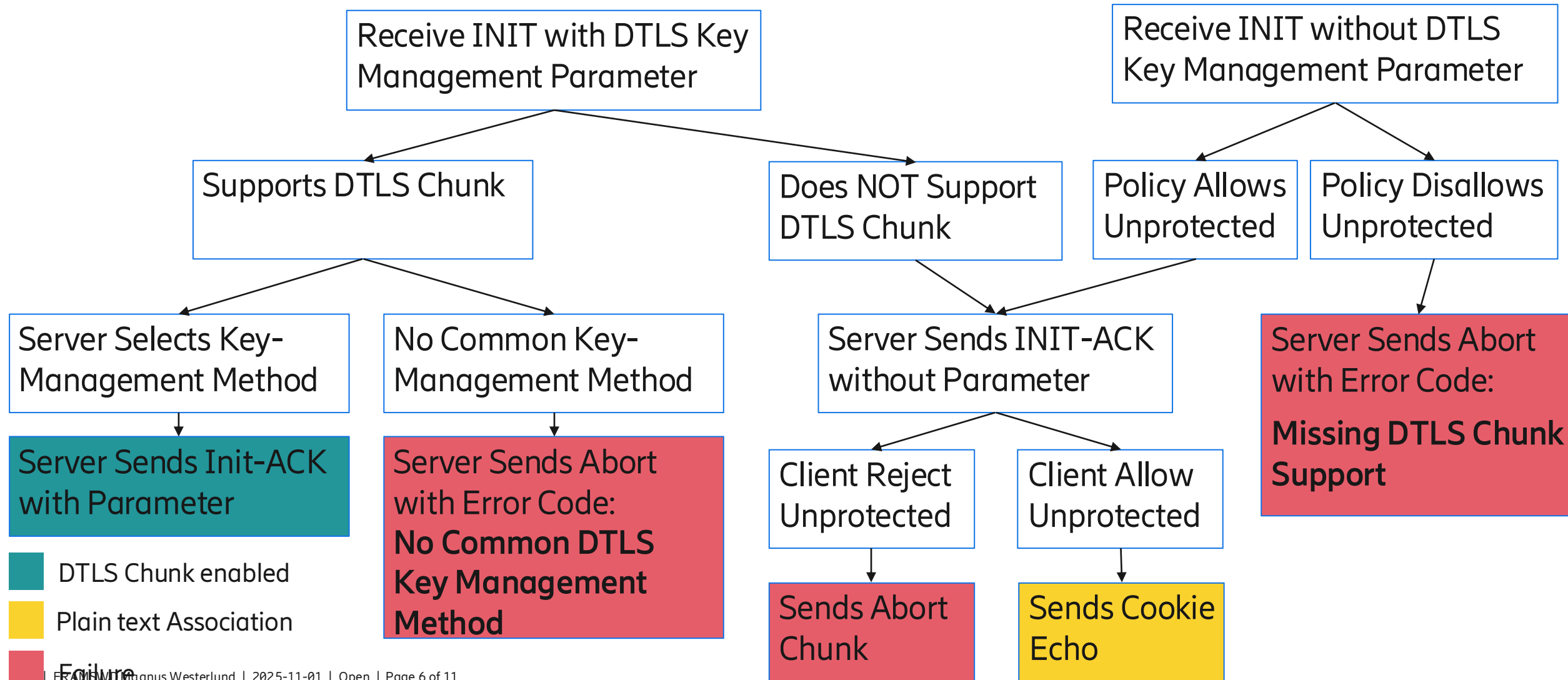
Removed DTLS Connection ID

- The design team decided to remove the possibility to use the DTLS Connection ID
- Unnecessary Complexity in API and specification
- No clear use cases in this SCTP context
- DTLS Connection ID field is negotiated length
 - A DTLS server is expected to keep this consistent for all incoming on the same port
 - Keying API would have to enforce using the same length for each SCTP association
- Conclusion was that there are no point of maintaining the functionality
- Now is the time to object against this change

Implemented Issues from last Meeting

- Mandatory to support pre-padding in DTLS Chunk.
- Require support of full DTLS record size
 - No requirement on supporting negotiation
- No Changes to number of Key Invocation API
- Now Proposes to update RFC 5061 when DTLS Chunk Security is used in a session
 - Remove requirement to use SCTP-AUTH and instead rely on DTLS Chunk for authentication

Establishing Association with DTLS Chunk Outcomes



- DTLS Chunk enabled
- Plain text Association
- Failure

Changes

- Massive changes to the text
 - Restructured and cut down duplication
- IANA Pre-Allocated values
 - DTLS Chunk:
 - 0x41 DTLS Chunk (DTLS)
 - Chunk Parameter Type:
 - 0x8006 DTLS Key Management
- DTLS Key Management Method Considerations
- API
 - Abstract: Added Key-Management
 - Set Supported Methods
 - Get Offered Methods
 - Socket API:
 - Redefined Data Structures in many calls

Liaison Statement

- After WG meeting at IETF-124 an LS was sent to 3GPP RAN3 and SA3 WG
 - <https://datatracker.ietf.org/liaison/2076/>
 - For Information
 - Reported on that WG was making progress on solution components
 - Plan to send next LS when publication request has been done
- No Reply LS received

Key-Managements

- [draft-ietf-tsvwg-dtls-chunk-key-management-01](#)
 - Has been updated
 - Still have a number of TBDs
- Progress in TLS WG on normative dependency
 - [draft-ietf-tls-extended-key-update-10](#)
 - Will be discussed in TLS WG meeting Friday 14:00-16:00 session
- Ericsson will update their proposal for key-management to align with the changes to DTLS Chunk
 - Important goal to verify that DTLS chunk's API and descriptions are usable to create methods

Next Steps

- Implementation Work still Catching up
 - Linux and FreeBSD
- Authors will work on editorial improvements
- Target WG last call prior to Vienna