**3GPP TSG-SA3 Meeting #115AdHoc-e *S3-241281-r1***

Electronic meeting, online, 15 - 19 April 2024

**Source: Ericsson**

**Title: Clarifying vulnerabilities in DTLS over SCTP**

**Document for: Approval**

**Agenda Item: 4.8**

# 1 Decision/action requested

***This document proposes changes for TS 33.501 and add to the living document [1] to clarify the vulnerabilities in using DTLS over SCTP***

# 2 References

[1] <https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_115AdHoc-e/Docs/S3-241108.zip>

[2] 3GPP TS 33.501 Security architecture and procedures for 5G system

[3] https://datatracker.ietf.org/meeting/115/materials/slides-115-tsvwg-sctp-auth-security-issues-00

# 3 Rationale

## 3.1 Reason for Change

As pointed out in LSs from RAN3, DTLS/SCTP has significant message size limitations which means that it does not work in many current networks. As pointed out in LSs from IETF [3], SCTP-AUTH and DTLS/SCTP have significant security issues affecting integrity, replay protection, and availability.

## 3.2 Summary of Change

The issues with DTLS over SCTP (RFC 6083) is described

3.3 Consequences if not agreed

May create lack of awareness.

# 4 Detailed proposal

## \*\*\*\*\*\* START OF CHANGES **\*\*\*\***

## 9.2 Security mechanisms for the N2 interface

N2 is the reference point between the AMF and the 5G-AN. It is used, among other things, to carry NAS signalling traffic between the UE and the AMF over 3GPP and non-3GPP accesses.

The transport of control plane data over N2 shall be integrity, confidentiality and replay-protected.

In order to protect the N2 reference point, it is required to implement IPsec ESP and IKEv2 certificates-based authentication as specified in sub-clause 9.1.2 of the present document. IPsec is mandatory to implement on the gNB and the ng-eNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

Mutual authentication shall be supported over the N2 interface between the AMF and the 5G-AN using DTLS and/or IKEv2.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect N2 is an operator's decision. In case the NG-RAN node (gNB or ng-eNB) has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the NG-RAN node.

NOTE 3: DTLS over SCTP as described in RFC 6083 [53] has significant message size limitations which means that it does not work in many current networks. SCTP-AUTH and DTLS over SCTP have significant security issues affecting integrity, replay protection, and availability. When RFC 6083 is used for DTLS over SCTP with DTLS 1.3, rekeying and reauthentication is not possible.

## \*\*\*\*\*\* NEXT CHANGE **\*\*\*\***

## 9.4 Security mechanisms for the Xn interface

Xn is the interface connecting NG-RAN nodes. It consists of Xn-C and Xn-U. Xn-C is used to carry signalling and Xn-U user plane data.

The transport of control plane data and user data over Xn shall be integrity, confidentiality and replay-protected.

In order to protect the traffic on the Xn reference point, it is required to implement IPsec ESP and IKEv2 certificate- based authentication as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection. IPsec shall be supported on the gNB and ng-eNB.

In addition to IPsec, for the Xn-C interface, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

Mutual authentication shall be supported over the Xn interface between the NG-RAN nodes using DTLS and/or IKEv2.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding..

NOTE 2: The use of cryptographic solutions to protect Xn is an operator's decision. In case the NG-RAN node (gNB or ng-eNB) has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the NG-RAN node.

NOTE 3: DTLS over SCTP as described in RFC 6083 [53] has significant message size limitations which means that it does not work in many current networks. SCTP-AUTH and DTLS over SCTP have significant security issues affecting integrity, replay protection, and availability. When RFC 6083 is used for DTLS over SCTP with DTLS 1.3, rekeying and reauthentication is not possible.

QoS related aspects are further described in sub-clause 9.1.3 of the present document.

## \*\*\*\*\*\* NEXT CHANGE **\*\*\*\***

### 9.8.2 Security mechanisms for the F1 interface

The F1 interface connects the gNB-CU to the gNB-DU. It consists of the F1-C for control plane and the F1-U for the user plane. The security mechanisms for the F1 interface connecting the IAB-node to the IAB-donor-CU are detailed in clause M.3.3 of this document.

In order to protect the traffic on the F1-U interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In order to protect the traffic on the F1-C interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

IPsec is mandatory to implement on the gNB-DU and on the gNB-CU. On the gNB-CU side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, for the F1-C interface, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks..

Mutual authentication shall be supported over the F1-C interface between the gNB-CU and the gNB-DU using DTLS and/or IKEv2.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect F1 is an operator's decision. In case the gNB or the IAB-node has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB or the IAB-node.

NOTE 3: The security considerations for DTLS over SCTP are documented in RFC 6083 [58].

NOTE 4: The support of DTLS (with mutual authentication) for F1-C, between the IAB-node (gNB-DU) and the IAB-donor-CU, is optional for the IAB-node and the IAB-donor-CU.

NOTE 5: DTLS over SCTP as described in RFC 6083 [53] has significant message size limitations which means that it does not work in many current networks. SCTP-AUTH and DTLS over SCTP have significant security issues affecting integrity, replay protection, and availability. When RFC 6083 is used for DTLS over SCTP with DTLS 1.3, rekeying and reauthentication is not possible.

## \*\*\*\*\*\* NEXT CHANGE **\*\*\*\***

### 9.8.3 Security mechanisms for the E1 interface

The E1 interface connects the gNB-CU-CP to the gNB-CU-UP. It is only used for the transport of signalling data.

In order to protect the traffic on the E1 interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In addition to IPsec, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

Mutual authentication shall be supported over the E1interface between the gNB-CU-CP and the gNB-CU-UP using DTLS and/or IKEv2.

IPsec is mandatory to support on the gNB-CU-UP and the gNB-CU-CP. Observe that on both the gNB-CU-CP and the gNB-CU-UP sides, a SEG may be used to terminate the IPsec tunnel.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect E1 is an operator's decision. In case the gNB has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB.

NOTE 3: DTLS over SCTP as described in RFC 6083 [53] has significant message size limitations which means that it does not work in many current networks. SCTP-AUTH and DTLS over SCTP have significant security issues affecting integrity, replay protection, and availability. When RFC 6083 is used for DTLS over SCTP with DTLS 1.3, rekeying and reauthentication is not possible.

## \*\*\*\*\*\* END OF CHANGES **\*\*\*\***