SA3 Crypto Inventory Protocol List (version 0.1), 19.03.2025, upd6

|  |  |  |  |
| --- | --- | --- | --- |
| Protocol / Function |  |  |  |
| DTLS | Asymmetric |  | TR 33.938 v0.1.0 |
| TLS | Asymmetric |  | TR 33.938 v0.1.0 |
| PDCP | Symmetric | TS 33.501, Clause 6.5 and 6.6 | Zander (Huawei) |
| EAP-AKA’5G AKA | Symmetric | TS 33.501, Clause 6.1 (Primary AuthN and Key Agreement)TS 24.501, Clause 4.6.2.4 (Network slice-specific authN and authZ)TS 24.501, Clause 5.4.1 (Primary AuthN and Key Agreement Procedure) | Andreas (Lenovo) |
| EAP-TLS | Symmetric | TS 33.501, Clause B.2 (Primary AuthN and Key Agreement), InformativeB.2.1.1 Security proceduresEAP-TLS is a mutual authentication EAP method that can be used by the EAP peer and the EAP server to authenticate each other. It is specified in RFC 5216 [38] and RFC 9190 [76]. The 3GPP TLS protocol profile related to supported TLS versions and supported TLS cipher suites in 3GPP networks is specified in clause 6.2 of TS 33.210 [3]. The 3GPP profile of TLS certificates is specified in clause 6.1.3a of TS 33.310 [5]. Guidance on the use of certificates in EAP-TLS is specified in RFC 9191 [119].I.2 Authentication in standalone non-public networks (normative)I.2.1 GeneralOne of the major differences of non-public networks is that authentication methods other than AKA based ones may be used in a standalone non-public network (SNPN). When an AKA-based authentication method is used, clause 6.1 shall apply. When an authentication method other than 5G AKA or EAP-AKA' is used, only the non-AKA specific parts of clause 6.1 shall apply. An example of running such an authentication method is given in Annex B with EAP-TLS. The choice of the supported authentication methods for access to SNPNs follows the principles described in clauses I.2.2 and I.2.3. Annex O (Informative):Authentication for non-5G capable devices behind residential gatewaysTS 24.501, Clause 5.4.1.2.3 (EAP-TLS related procedures)5.4.1.2.3 EAP-TLS related procedures5.4.1.2.3.1 GeneralThe UE may support acting as EAP-TLS peer as specified in 3GPP TS 33.501 [24]. The AUSF may support acting as EAP-TLS server as specified in 3GPP TS 33.501 [24]. The AAA server of the CH or the DCS may support acting as EAP server of such EAP method as specified in 3GPP TS 23.501 [8].The EAP-TLS enables mutual authentication of the UE and the network. | Yuto (KDDI) |
| ECIES | Symmetric, Asymmetric | TS 33.501 Annex C.3C.3 Elliptic Curve Integrated Encryption Scheme (ECIES)C.3.1 GeneralThe use of ECIES for concealment of the SUPI shall adhere to the SECG specifications [29] and [30]. Processing on UE side and home network side are described in high level in clauses C.3.2 and C.3.3.When the SUPI is of type IMSI, the subscription identifier part of the IMSI (i.e., MSIN) that is used to construct the scheme-input shall be coded as hexadecimal digits using packed BCD coding where the order of digits within an octet is same as the order of MSIN digits specified in Figure 9.11.3.4.3a of TS 24.501 [35]. If the MSIN is composed of an odd number of digits, then the bits 5 to 8 of final octet shall be coded as "1111".When the SUPI is of type network specific identifier, the subscription identifier part of the SUPI that is used to construct the scheme-input shall follow the encoding rules specified in Annex B.2.1.2 of TS 33.220 [28].IETF RFC 7748: "Elliptic Curves for Security". | Stawros (Nokia) |
| KDF | Symmetric | TS 33.501, Annex AThe KDF is a function. | Khishig (Accenture) |
| OAuth 2.0 | Asymmetric | TS 33.501, Clause 13.4TS 33.501, Annex X (normative)Annex X (normative):Security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) | Virendra (Qualcomm) |
| IPsec ESP, AH | Asymmetric | TS 33.501, Annex M (normative) 🡪 IABTS 33.210, Clause 5.3TS 33.310, Clause 5.1.1.1 | Ramesh (Samsung) |
| IKEv2 | Asymmetric | TS 33.210, Clause 5.4.2TS 33.310, Clause 6.2.1b | Zander (Huawei) |
| SEPP - PRINSSEPP - TLS | Asymmetric | PRINS = PRotocol for N32 INterconnect SecurityTS 33.501, Clause 5.9.3 and 13.2SEPP is defined in 3GPP specification TS 29.573 | Wiktor (Nokia) |
| MIKKEY- SAKKE |  | RFC65091. Clarify why TS 33.180 is not tagged with 5G; it mentions 5GS
2. If this is 5GS, then we would need contribution on this
 | Jeff (NIST) |
| CRL |  | Not a protocol; could be removed from the table | Jeff (NIST) |
| 802.1x (tbc) |  | MACsec | Stawros |
| PKI |  | TS 33.310 (Hint: many 3GPP specs have PKI mentioned, but all of them refer to the 33.310 spec)  | Stawros |
| QUIC |  | Is a protocol and is using the TLS1.3 -> please refer to TLS | Stawros |
| OCSP |  | TS 33.310TS 33.501 | Stawros |
| COSE |  | CBOR Object Signing and EncryptionRFC815233.434; Release: rel-18; Title: security aspects of service enabler architecture layer (seal) for verticals;33.220; Release: rel-18; Title: generic authentication architecture (gaa); generic bootstrapping architecture (gba) | Stawros |

*IKEv2, X.509 -> PKI, PKCS #10 -> CSR, CMP -> not a protocol, CRL -> not a protocol****,****OCSP over HTTP -> a protocol, TLS, DTLS****,****QUIC -> protocol, is using TLS1.3****,****JOSE -> not a protocol****,****COSE ->* ***,****EAP, MIKEY-SAKKE*