UE
AMF/ SEAF
AUSF
UDM
AAA-H
1. Registration Request (SUCI in NAI format)
2. Nausf_UEAuthentication_AuthenticateRequest (SUC, SN-nameI)
3. Nudm_UEAuthentication_Get_Request (SUCI, SN-name)
4. Authentication Method Selection
5. Nudm_UEAuthentication_Get_Response (SUPI, indicator(EAP-TTLS, CdP-UEID), [CdP address)
6. Nausf_UEAuthentication_AuthenticateResponse (EAP Request[EAP-TTLS, Start=1])
7. Authentication Request (EAP Request[EAP-TTLS, Start=1], ngKSI, ABBA)
8. Authentication Response (EAP Response[EAP-TTLS, Client_Hello])
9. Nausf_UEAuthentication_AuthenticateRequest (EAP Response[EAP-TTLS, Client_Hello])
10. Nausf_UEAuthentication_AuthenticateResponse (EAP Request[EAP-TTLS, ServerHello, ServerCertificate, ServerKeyExchange, CertificateRequest*, ServerHelloDone])
11. Authentication Request (EAP Request[EAP-TTLS, ServerHello, ServerCertificate, ServerKeyExchange, CertificateRequest*, ServerHelloDone], ngKSI, ABBA)
12. Verify Server Certificate
13. Authentication Response (EAP Response[EAP-TTLS, ClientCertificate*, ClientKeyExchange, CertificateVerify*, ChangeCiperSpec, Finished])
14. Nausf_UEAuthentication_AuthenticateRequest (EAP Response[EAP-TTLS, ClientCertificate*, ClientKeyExchange, CertificateVerify*, ChangeCiperSpec, Finished])
15a. Verify Client Certificate
15b. Nausf_UEAuthentication_AuthenticateResponse (EAP Request[EAP-TTLS, ChangeCiperSpec, Finished])
16. Authentication Request (EAP Request[EAP-TTLS, ChangeCiperSpec, Finished], ngKSI, ABBA)
17. EAP-TTLS 2nd phase
18. K_{AUSF} derived from EMSK
19. Nausf_UEAuthentication_AuthenticateResponse (EAP Success, K_{SEAF}, SUPI)
20. Authentication Result (EAP Success, ngKSI, ABBA)
21. K_{AUSF} derived from EMSK