**3GPP TSG-SA3 Meeting #115AdHoc-e *S3-241508***

Electronic meeting, online, 15 - 19 April 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.310** | **CR** | **draftCR** | **rev** |  | **Current version:** | **19.0.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network | **x** | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Living document for CryptoSP: draftCR to TS 33.310, Updates to cryptographic profiles |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | CryptoSP |  | ***Date:*** | 2024-04-22 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-19 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | **From SA3#115Adhoce-e:****From the rationale of S3-241319:**RFC 2252 has been obsoleted by RFC 4510, 4517, 4523 and RFC 4512.**From the coverpage of S3-241306:**There are several advantages for using ECDSA signatures. For example, RFC 4754 states that "*For any given level of security against the best attacks known, ECDSA signatures are smaller than RSA signatures, and ECDSA keys require less bandwidth than DSA keys [LV]….*" In addition, the ECDSA signatures are also widely used in many areas (e.g. blockchain), and supported by crypto libraries. Currently, Method 14 as in RFC 7427 is specified in TS 33.310 to support ECDSA. The key idea for RFC 7427 is to support flexiblilty to include all signature methods (RSA, DSA, ECDSA, RSASSA-PSS, etc.) and the hash algorithms. To achieve this, additional negotiation method is required. Considering the algorithms in Method 14 specified in TS 33.310 are limited to only ECDSA, RSASSA-PSS. Such flexibility is not significant. In addition to method 14, method 9/10/11 to support ECDSA with fixed hash algorithm are also recommended by BSI. “<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-3.pdf?__blob=publicationFile&v=5>”It’s proposal to add addtionl methods to support ECDSA with fixed hash algorithm. With this, additional negotiation method for selecting the signature method and hash algorithm is not needed. |
|  |  |
| ***Summary of change:*** | Addition of ECDSA Digital Signature-based authentication methods in the IKEv2 profile |
|  |  |
| ***Consequences if not approved:*** | Outdated and limited authentication methods in the IKEv2 profile |
|  |  |
| ***Clauses affected:*** | 2, 5.2.1, 6.1a, 6.2.1b |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** | **SA3#115Ahdoc-e:** S3-241306, S3-241319 |

\*\*\* Start of 1st Change \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[2] IETF RFC 2986: "PKCS#10 Certification Request Syntax Specification Version 1.7".

[3] Void.

[4] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol".

[5] Void[6] Void.

[7] "PKI basics – A Technical Perspective", November 2002, http://www.oasis-pki.org/pdfs/PKI\_Basics-A\_technical\_perspective.pdf.

[8] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[9] 3GPP TS 33.203: "Access security for IP-based services".

[10] 3GPP TS 33.220: "Generic Authentication Architecture: Generic Bootstrapping Architecture".

[11] Void.

[12] Void.

[13] Void.

[14] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[15] IETF RFC 4945: "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX".

[16] Void.

[17] Void.

[18] IETF RFC 6712: "Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)".

[19] IETF RFC 4211: "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)".

[20] IETF RFC 2818: "HTTP Over TLS".

[21] IETF RFC 5922: "Domain Certificates in the Session Initiation Protocol (SIP)".

[22] IETF RFC 5924: "Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates".

[23] Void.

[24] Void.

[25] IETF RFC 1035: "Domain Names - Implementation and Specification".

[26] Void.

[27] Void.

[28] Void.

[29] Void.

[30] Void.

[31] 3GPP TS 23.251: "Network sharing; Architecture and functional description".

[32] 3GPP TS 32.508: "Telecommunication management; Procedure flows for multi-vendor plug-and-play eNode B connection to the network".

[33] 3GPP TS 32.509: "Telecommunication management; Data formats for multi-vendor plug and play eNode B connection to the network".

[34] Void.

[35] Void.

[36] Void.

[37] Void.

[38] Void.

[39] Void.

[40] Void.

[41] Void.

[42] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[43] IETF RFC 7427: "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)".

[44] Void.

[45] Void.

[46] Void.

[47] IETF RFC 6960: " X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[48] IETF RFC 8201: "Path MTU Discovery for IP version 6".

[49] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[50] IETF RFC 9113: "HTTP/2".

[51] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[52] IETF RFC 6125: "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)".

[53] IETF RFC 7633: "X.509v3 Transport Layer Security (TLS) Feature Extension".

[54] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[55] 3GPP TS 23.003: "Numbering, addressing and identification".

[56] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[57] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[58] IETF RFC 6979: " Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)".

[59] CA-Browser-Forum-BR-1.8.0, August 2021, https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.0.pdf.

[60] GSMA FS.34 Key Management for 4G and 5G inter-PLMN Security, https://www.gsma.com/security/resources/fs-34-key-management-for-4g-and-5g-inter-plmn-security/.

[61] IETF RFC 9310: "X.509 Certificate Extension for 5G Network Function Types".

[62] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[63] IETF draft-ietf-lamps-nf-eku-01: "X.509 Certificate Extended Key Usage (EKU) for 5G Network Functions".

[aa] IETF RFC 4510: "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map".

[bb] IETF RFC 4517: “Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules”[cc] IETF RFC 4523: "Lightweight Directory Access Protocol (LDAP): Schema Definitions for X.509 Certificates".

[dd] IETF RFC 4512: " Lightweight Directory Access Protocol (LDAP): Directory Information Models".

[xx] RFC 4754: "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)".

\*\*\* End of 1st Change \*\*\*

\*\*\* Start of 2nd Change \*\*\*

### 5.2.1 Operator Registration: Creation of interconnect agreement

SEGs or TLS entities of two different security domains need to establish a secure connection, when the operators make an interconnect agreement. The first technical step in creating the interconnect agreement between domains is the creation of cross-certificates by the Interconnection CAs of the two domains.

Inter-operator cross-certification can be done using different protocols, but the certification authority shall support the PKCS#10 method for certificate requests as specified in RFC 2986 [2]. The SEG CA, TLS client CA and TLS server CA create a PKCS#10 certificate request, and send it to the other operator's Interconnection CA. The method for transferring the PKCS#10 request is not specified, but the transfer method shall be secure. The PKCS#10 can be transferred e.g. HTTPS, in a flash drive, or be send in a signed email. The PKCS#10 request contains the public key of the authority and the name of the authority requesting the cross-certificate. When the Interconnection CA accepts the request, a new cross-certificate is created for the requesting CA. The Interconnection CA shall make the new cross-certificate available to SEGs and TLS entities in its own domain that need to use it. Cross-certificates on the other domain's SEG CA's are stored in a local CR (Certificate Repository) which all SEGs that need to communicate with the other domains shall access using LDAP as specified in RFC 4510, 4517, 4523 and RFC 4512  [aa][bb][cc][dd]. Cross-certificates on TLS client CAs and TLS server CAs are made available to TLS entities, e.g. by storing them in a file of trusted CAs on the TLS entity, or by storing them in a local CR (Certificate Repository) which all TLS entities that need to communicate with the other domain shall access e.g. using LDAP as specified in RFC 4510, 4517, 4523 and RFC 4512  [aa][bb][cc][dd].

\*\*\* End of 2nd Change \*\*\*

\*\*\* Start of 3rd Change \*\*\*

## 6.1a CRL profile

- Version 2 CRL according to RFC5280 [14].

- Hash algorithm for use before signing CRL: SHA-256 shall be supported SHA-384 should be supported, MD5 MD2, and SHA-1 shall not be supported.

NOTE: Void.

- Signature algorithm: RSAEncryption and ecdsa shall be supported. RSAEncryption is not recommended as it uses PKCS#1v1.5 padding.

- Parameters: For ecdsa, secp256r1 shall be supported, secp384r1 should be supported.

- ECDSA is recommended for newly created CRLs.

- The security level of the public key used to sign the CRL shall be at least the same as the public keys used to sign the revoked certificates.

- For RSA: The key length shall be at least 2048-bit. A key length of at least 4096-bit shall be supported. Key lengths of less than 2048-bit shall not be supported. PKCS#1v1.5 padding and key lengths less than 3072-bits should not be used in certificates that expire after 2030.

- For ECDSA: Except curve25519, ed25519, and W-25519, elliptic curve groups of less than 256 bits shall not be supported. A key length of at least 384-bit shall be supported.

NOTE 1: In practice, certificates often have a long lifetime, for example about ten years. The use of RSA with PKCS#1v1.5 padding and key lengths less than 3072-bits is planned to be prohibited by several organisations no later than 2030.

CRL retrieval with LDAPv3 [aa][bb][cc][dd] shall be supported as the primary method. HTTP may be used for checking the revocation status of TLS and NE certificates.

\*\*\* End of 3rd Change \*\*\*

\*\*\* Start of 4th Change \*\*\*

## 6.2 IKE negotiation and profiling

For certificate based establishment of IPsec SAs between NDS/IP elements, the IKE profile in this clause shall be used.

### 6.2.1 Void

### 6.2.1b IKEv2 profile

The following requirements on certificate based IKEv2 authentication in addition to those specified in NDS/IP [1] shall be applied:

For the IKE\_INIT\_SA and IKE\_AUTH exchanges:

- Following algorithms shall be supported:

- Authentication: Method 1 - RSA Digital Signature [42];

- Implementations shall support signatures that use SHA-256, should support signatures that use SHA-384, and shall not support signatures that use SHA-1. Implementations should use SHA-256 as the default hash function when generating signatures.

- Usage of Method 1 is not recommended as it uses PKCS#1v1.5 padding.

- Authentication: Method 9/10/11 - ECDSA Digital Signature [xx];

- Implementations should support ECDSA with SHA-256 on the P-256 curve.

- Implementations should support ECDSA with SHA-384 on the P-384 curve.

- Implementations should support ECDSA with SHA-512 on the P-521 curve.

- Hash Algorithm Notification [43]

- Implementations shall support SHA2-256, should support SHA2-384, and shall not support SHA1.

- Authentication: Method 14 - Digital Signature [43].

- Implementations shall support ecdsa-with-sha256 and should support ecdsa-with-sha384, and should support RSASSA-PSS with SHA-256. Implementations shall not support sha1WithRSAEncryption, dsa-with-sha1, ecdsa-with-sha1, RSASSA-PSS with Empty Parameters, and RSASSA-PSS with Default Parameters.

- The identity of the CERT payload (including the end entity certificate) shall be used for policy checks;

- Initiating/responding end entities are required to send certificate requests in the IKE\_INIT\_SA exchange for the responder and in the IKE\_AUTH exchange for the initiator;

- Cross-certificates shall not be sent by the peer end entity as they are pre-configured in the end entity;

- The certificates in the certificate payload shall be encoded as type 4 (X.509 Certificate – Signature);

- An end entity shall rekey the IKE SA when any used end entity certificate expires.

\*\*\* End of 4th Change \*\*\*