**3GPP TSG-SA3 Meeting #123 draft\_S3-252937-r1**

Goteborg, Sweden, 25 – 29 August 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.310** | **CR** | **0216** | **rev** | **1** | **Current version:** | **19.4.0** |  |
|  | | | | | | | | |
| *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 |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | IANA registration information for ACME | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Google, Cisco System, Johns Hopkins University APL, US National Security Agency, Deutsche Telekom, NCSC, AT&T | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | ACME\_SBA | | | | |  | ***Date:*** | | | 2025-08-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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 can be 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:*** | | Address Editor's Notes for IANA registrations | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Address information resulting from the successfully completed IANA registrations for ACME. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | IANA registration will be missing and there is a risk of duplicate IANA registration. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, J.3.3.1, J.3.3.2, J.X (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\* \* \* First 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] Void

[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-2.0.4, April 2024, <https://cabforum.org/working-groups/server/baseline-requirements/documents/TLSBRv2.0.4.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 RFC 9509: "X.509 Certificate Extended Key Usage (EKU) for 5G Network Functions".

[64] IETF RFC 4122:" A Universally Unique Identifier (UUID) URN Namespace".

[65] IETF RFC 9110: " HTTP Semantics".

[66] IETF RFC 9525: "Service Identity in TLS".

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

[68] IETF RFC 4517: "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules".[69] IETF RFC 4523: "Lightweight Directory Access Protocol (LDAP): Schema Definitions for X.509 Certificates".

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

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

[72] IETF RFC 8555: "Automatic Certificate Management Environment (ACME)".

[73] IETF RFC 9447: "Automated Certificate Management Environment (ACME) Challenges Using an Authority Token".

[74] IETF RFC 7519: " JSON Web Token (JWT)".

[75] IETF RFC 7515: "JSON Web Signature (JWS)".

[76] IETF RFC 9448: "TNAuthList Profile of Automated Certificate Management Environment (ACME) Authority Token".

[XX] IANA Automated Certificate Management Environment (ACME) Protocol <https://www.iana.org/assignments/acme/>.

\* \* \* Next Change \* \* \* \*

## J.3.3 Challenge validation

### J.3.3.1 Introduction

The ACME challenge-type used for validation is the ACME Authority Token challenge type, "tkauth-01", as specified in RFC 9447 [73]. The validation method assumes a trust relationship between a CA and a Token Authority, i.e., that a CA is willing to accept the attestation of a Token Authority for particular types of identifiers as sufficient proof to issue a credential. When using ACME, the OAM system acts as a Token Authority that is trusted by the operator CA/RA. As such, the OAM is trusted to act as the authority for the NF Instance ID namespace within the 5GC.

### J.3.3.2 "NfInstanceId" identifier type

A new ACME identifier type, "NfInstanceId", is defined in this clause. A NF uses its NF Instance ID as the value of the “NfInstanceId". The format of the value of the "NfInstanceId" is that of the NfInstanceId, as defined in TS 29.571 [57]:

- NfInstanceId: string: String uniquely identifying a NF instance. The format of the NF Instance ID shall be a Universally Unique Identifier (UUID) version 4, as described in RFC 4122 [64]. The hexadecimal letters should be formatted as lower-case characters by the sender, and they shall be handled as case-insensitive by the receiver.

- Example: "4ace9d34-2c69-4f99-92d5-a73a3fe8e23b"

An example of an ACME order object "identifiers" field containing a "NfInstanceId" is as follows:

- "identifiers": [{"type":"NfInstanceId","value":"4ace9d34-2c69-4f99-92d5-a73a3fe8e23b"}]

NOTE: The “NfInstanceId” type and the “tkauth-01” validation method have been registered as documented in clause J.X.

In NF certificates, both client and server, the subjectAltName extension contains the NfInstanceId as a "uniformResourceIdentifier" formatted as a URN as described in clause 5.3.2 of TS 29.571 [57]. For example, "urn:uuid:4ace9d34-2c69-4f99-92d5-a73a3fe8e23b" is the string representation of the NF Instance ID "4ace9d34-2c69-4f99-92d5-a73a3fe8e23b" as a URN.

When processing a certificate order containing an identifier of type "NfInstanceId", a CA uses the Authority Token challenge type of "tkauth-01" with a "tkauth-type" of "atc", as defined in RFC 9447 [73], to verify that the requesting ACME client has authenticated and authorized control over the requested resources represented by the "NfInstanceId" value as well as any other NF profile parameters included in the certificate order.

The NF's ACME client responds to the challenge by posting the Authority Token, as received from the OAM system, to the challenge URL identified in the returned ACME authorization object, an example of which follows:

POST /acme/chall/prV\_B7yEyA4 HTTP/1.1

Host: boulder.example.com

Content-Type: application/jose+json

{

"protected": base64url({

"alg": "ES256",

"kid": "https://example.com/acme/acct/evOfKhNU60wg",

"nonce": "Q\_s3MWoqT05TrdkM2MTDcw",

"url": "https://boulder.example.com/acme/authz/asdf/0"

}),

"payload": base64url({

"tkauth": "DGyRejmCefe7v4N...vb29HhjjLPSggwiE"

}),

"signature": "9cbg5JO1Gf5YLjjz...SpkUfcdPai9uVYYQ"

}

The "tkauth" field is, as defined in RFC 9448 [76], a field in the challenge object specific to the tkauth-01 challenge type that contains an Authority Token as defined in the next clause.

\* \* \* End of Changes \* \* \* \*