**3GPP TSG-CT WG1 Meeting #133-eC1-21abcd**

**E-meeting, 11-19 November 2021 (was C1-217057)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.547** | **CR** | **0011** | **rev** | **1** | **Current version:** | **16.2.0** |  |
|  |
| *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 | **x** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Addition of CoAP entities annex |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | eSEAL |  | ***Date:*** | 2021-11-04 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *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:*** | To introduce support for CoAP for SEAL Identity Management, specification and requirements for CoAP entities needs to be added. It is proposed to add this in a new annex of the TS. |
|  |  |
| ***Summary of change:*** | CoAP entity annex is added |
|  |  |
| ***Consequences if not approved:*** | SEAL IM does not support CoAP as required by stage 2. |
|  |  |
| ***Clauses affected:*** | Annex 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 \* \* \* \*

Annex X (normative):
CoAP entities

# X.1 Scope

This annex describes the functionality expected from the CoAP entities (i.e. the CoAP client, the CoAP proxy and the CoAP server) defined by RFC 7252 [7252] and 3GPP TS 23.434 [2].

# X.2 General

When the VAL UE is authenticating directly to the SEAL/VAL server without proxies, then the DTLS profile of ACE-OAUTH [dtls] may be used. In order to authorize clients and protect communication across proxies, the OSCORE profile of ACE-OAUTH [oscore] shall be used.

The client shall support UDP transport defined in IETF RFC 7252 [7252] and should support TCP transport defined in IETF RFC 8323 [8323]:

a) when UDP transport and OSCORE profile of ACE-OAUTH [oscore] are used, datagram transport layer security (DTLS) may be used;

b) when TCP transport and OSCORE profile of ACE-OAUTH [oscore] are used, transport layer security (TLS) may be used;

c) when UDP transport and DTLS profile of ACE-OAUTH [dtls] are used, datagram transport layer security (DTLS) shall be used; and

d) when TCP transport and DTLS profile of ACE-OAUTH [dtls] are used, transport layer security (TLS) shall be used.

Proof-of-Possession token type is used with ACE-OAUTH [oauth].

# X.3 Procedures

## X.3.1 CoAP client

The CoAP client in the UE shall support the client role defined in IETF RFC 7252 [7252].

If the communication is via proxies, the CoAP client in the UE:

a) shall be configured with a home CoAP proxy FQDN parameter;

b) shall be configured with a home CoAP proxy port parameter; and

c) may be configured with one of the following (D)TLS tunnel authentication method along with its parameters as specified in 3GPP TS 33.434 [7]:

1) one-way authentication of the CoAP proxy based on the server certificate;

2) mutual authentication based on certificates, along with (D)TLS tunnel authentication based on X.509 certificate; and

3) mutual authentication based on pre-shared key, along with (D)TLS tunnel authentication based on pre-shared key.

## X.3.2 CoAP proxy

### X.3.2.1 General

The CoAP proxy shall support CoAP-to-CoAP, CoAP-to-HTTP proxy and HTTP-to-CoAP roles defined in IETF RFC 7252 [15].

CoAP proxy shall support UDP transport in IETF RFC 7252 [7252] and shall support TCP transport defined in IETF RFC 8323 [8323].

### X.3.2.2 CoAP request method from CoAP client in UE

The CoAP proxy shall support the server role defined in IETF RFC 7252 [7252].

The CoAP proxy may support datagram transport layer security (DTLS) or transport layer security (TLS) as specified in clause 6 of 3GPP TS 33.434 [7].

The CoAP proxy is configured with the following CoAP proxy parameters:

a) an FQDN of an CoAP proxy for UEs; and

b) a port of an CoAP proxy for UEs.

The CoAP proxy may support establishing transport connections on the FQDN of CoAP proxy for UEs and the port of CoAP proxy for UEs. The CoAP proxy shall support establishing a (D)TLS tunnel via each such transport connection as specified in 3GPP TS 33.434 [7]. When establishing the (D)TLS tunnel, the CoAP proxy shall act as the (D)TLS server.

### X.3.2.3 CoAP request method from CoAP client in network entity within trust domain

The CoAP proxy is configured with the following parameters:

a) a FQDN of an CoAP proxy for trusted entities; and

b) a port of an CoAP proxy for trusted entities.

Upon receiving an CoAP request method via a transport connection established on the FQDN of CoAP proxy for UEs and the port of CoAP proxy for UEs, if the transport connection is between network elements within trusted domain as specified in 3GPP TS 33.434 [7], then:

a) if the CoAP request contains a CoAP URI identifying a resource in a partner's VAL service provider, the CoAP proxy shall forward the CoAP request according to the CoAP URI; and

b) if an CoAP request contains CoAP URI identifying a resource in own VAL service provider, the CoAP proxy shall act as reverse proxy for the CoAP request and shall forward the CoAP request according to VAL service provider's policy.

## X.4.2 CoAP server

The CoAP server shall support the server role defined in IETF RFC 7252 [7252].

Upon reception of an ACE-OAuth Token Provisioning Request message containing an access token, the CoAP server:

1. shall verify the integrity of the access token; and
2. shall verify that the key included in the access token belongs to the authenticated requesting party.

Upon reception of a resource request, the CoAP server:

1. shall verify that the requesting party is authorized according to the access token as specified in the corresponding ACE-OAuth profile; the DTLS profile of ACE-OAUTH [dtls] or the OSCORE profile of ACE-OAUTH [oscore].

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