ETSI TS 124 547 V17.1.0 (2022-05)

5G;
Identity management -
Service Enabler Architecture Layer for Verticals (SEAL);
Protocol specification
(3GPP TS 24.547 version 17.1.0 Release 17)

Reference
RTS/TSGC-0124547vh10

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies the protocol aspects for the identity management capability of SEAL to support vertical applications (e.g. V2X) over the 3GPP system.

The present document is applicable to the User Equipment (UE) supporting the identity management client functionality as described in 3GPP TS 23.434 [2], to the application server supporting the identity management server functionality as described in 3GPP TS 23.434 [2] and to the application server supporting the vertical application server (VAL server) functionality as defined in specific vertical application service (VAL service) specifications.

NOTE: The specification of the VAL server for a specific VAL service is out of scope of the present document.

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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows;".

[3] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[4] OMA OMA-TS-XDM_Group-V1_1_1-20170124-A: "Group XDM Specification".

[5] Void.

[6] W3C.REC-html401-19991224: "HTML 4.01 Specification".

[7] 3GPP TS 33.434: "Service Enabler Architecture Layer (SEAL); Security aspects for Verticals".

[8] IETF RFC 8693: "OAuth 2.0 Token Exchange".

[9] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[10] IETF RFC 7159: "The JavaScript Object Notation (JSON) Data Interchange Format".

[11] "OpenID Connect Core 1.0 incorporating errata set 1".

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

[13] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[14] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[15] IETF RFC 7230 (June 2014): "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[16] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[17] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[18] IETF RFC 8323: "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets".

[19] Internet draft draft-ietf-ace-oauth-authz-45: "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)".

[20] Internet draft draft-ietf-ace-dtls-authorize-18: "Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)".

[21] Internet draft draft-ietf-ace-oscore-profile-19: "OSCORE Profile of the Authentication and Authorization for Constrained Environments Framework"

3 Definitions of terms and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

Authorisation endpoint: A SEAL identity management server protocol endpoint used by the SEAL identity management client to obtain an authorisation grant, as specified in IETF RFC 6749 [9].

SEAL identity management client: An entity that provides the client side functionalities corresponding to the identity management SEAL service.

SEAL identity management server: An entity that provides the server side functionalities corresponding to the identity management SEAL service.

Token endpoint: A SEAL identity management server protocol endpoint used by the SEAL identity management client to exchange an authorisation grant for an access token, as specified in IETF RFC 6749 [9] for HTTP and Internet draft ACE-OAUTH [19] for CoAP.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.434 [2] apply:

SEAL client
SEAL server
SEAL service
VAL server
VAL service
VAL user
Vertical
Vertical application

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

ACE	Authentication and Authorization for Constrained Environments
SEAL	Service Enabler Architecture Layer for verticals
SIM-C	SEAL Identity Management Client
SIM-S	SEAL Identity Management Server
VAL	Vertical Application Layer

4 General description

Identity management is a SEAL service that provides the identity management related capabilities to one or more vertical applications. The present document enables a SEAL identity management client and a VAL server to communicate with a SEAL identity management server. The SEAL identity management server authenticates the VAL

user's identity by verifying the credentials provided by the VAL user. When the VAL user is authenticated it is provided with an access token which is used for accessing different SEAL services.

5 Functional entities

5.1 SEAL identity management client (SIM-C)

The SIM-C is a functional entity that acts as the application client for VAL user identity related transactions.

To be compliant with the HTTP procedures in the present document the SIM-C shall:

- support the user authentication procedure specified in clause 6.2.2; and
- support the token exchange procedure specified in clause 6.2.3.

To be compliant with the CoAP procedures in the present document the SIM-C:

- shall support the role of CoAP client as specified in IETF RFC 7252 [17];
- should support CoAP over TCP and Websocket as specified in IETF RFC 8323 [18];
- shall support Internet draft ACE-OAUTH [19];
- shall support OSCORE profile of ACE-OAUTH [21];
- should support DTLS profile of ACE-OAUTH [20]; and
- shall support the procedures in clause 6.2.2.

5.2 SEAL identity management server (SIM-S)

The SIM-S is a functional entity that authenticates the VAL user's identity by verifying the credentials provided by the VAL user.

To be compliant with the procedures in the present document the SIM-S shall:

- support the user authentication procedure specified in clause 6.2.2; and
- support the token exchange procedure specified in clause 6.2.3.

To be compliant with the CoAP procedures in the present document the SIM-S:

- shall support the role of CoAP server as specified in IETF RFC 7252 [17];
- should support CoAP over TCP and Websocket as specified in IETF RFC 8323 [18];
- shall support Internet draft ACE-OAUTH [19];
- shall support OSCORE profile of ACE-OAUTH [21];
- should support DTLS profile of ACE-OAUTH[20]; and
- shall support the procedures in clause 6.2.2.

6 Identity management procedures

6.1 General

6.2 On-network procedures

6.2.1 General

6.2.2 User authentication procedure

6.2.2.1 SIM-C procedure

6.2.2.1.1 HTTP based procedure

Upon receiving a request from VAL user to initiate authentication for VAL services, the SIM-C shall:

a) establish a TLS tunnel to the authorisation endpoint of the SIM-S as specified in 3GPP TS 33.434 [7] using the URL of authorisation endpoint of the SIM-S as provided by the specific VAL service; and

b) send an OIDC Authentication Request message as specified in the OpenID Connect 1.0 [11] and IETF RFC 6749 [9] using an HTTP GET request method towards the SIM-S according to IETF RFC 7231 [16]. The SIM-C shall include the following parameters as specified in 3GPP TS 33.434 [7] in the query component of the authorization endpoint's URI using the "application/x-www-form-urlencoded" format as specified in W3C.REC-html401-19991224 [6]:

   - response_type;
   - client_id;
   - scope;
   - redirect_uri;
   - state;
   - acr_values;
   - code_challenge; and
   - code_challenge_method.

Upon receiving an HTTP 200 (OK) response from the SIM-S, the SIM-C shall:

a) prompt the VAL service user for their username and password;

b) generate an HTTP POST request method containing the VAL service user's username and password; and

c) send the HTTP POST request method towards the SIM-S.

Upon receiving an OIDC Authentication Response message, the SIM-C shall:

a) establish a TLS tunnel to the token endpoint of the SIM-S as specified in 3GPP TS 33.434 [7]; and

b) send an OIDC Token Request message as specified in OpenID Connect 1.0 [11] and IETF RFC 6749 [9] using an HTTP POST request method towards the SIM-S according to IETF RFC 7231 [16]. The SIM-C shall include the following parameters in the entity body of the HTTP POST request using the "application/x-www-form-urlencoded" format as specified in W3C.REC-html401-19991224 [6] as specified in 3GPP TS 33.434 [7]:

   - grant_type;

- code;
- client_id;
- redirect_uri; and
- code_verifier.

Upon receiving an OIDC Token response message from the SIM-S, the SIM-C shall:

a) validate the id_token, access_token and refresh token in the received OIDC Token Response message as specified in the OpenID Connect 1.0 [11] specification; and

b) provide the id_token and access_token in the received OIDC Token Response message to the VAL user.

The SIM-C may repeat the entire procedure in this subclause as needed to obtain the necessary authorisation tokens for the VAL service clients, depending on the scope parameter in the Authentication Request message as specified in 3GPP TS 33.434 [7].

6.2.2.1.2 CoAP based procedure

Editor's note: The method to protect CoAP-based procedure will be decided by SA3, and necessary alignment with SA3 is FFS.

Upon receiving a request from VAL user to initiate authentication for VAL services, the SIM-C:

a) may establish a (D)TLS tunnel to the token endpoint of the SIM-S as specified in 3GPP TS 33.434 [7] using the URL of token endpoint of the SIM-S as provided by the specific VAL service; and

b) shall send an ACE-OAUTH Token Request message with client credentials grant type as specified in Internet draft ACE-OAUTH [19] using an CoAP POST request towards the SIM-S. The SIM-C shall use the "application/ace+cbor" format and:

   a) shall include grant type parameter;

   b) shall include scope parameter;

   c) may include req_cnf parameter; and

   d) may include ace_profile parameter,

   in the message payload as specified in Internet draft ACE-OAUTH [19].

Upon receiving an CoAP 2.01 (Created) response from the SIM-S, the SIM-C shall:

a) validate the access token as specified in the Internet draft ACE-OAUTH [19]; and

b) provide the access token in the received ACE-OAUTH Token Response message to the VAL user.

The SIM-C may repeat the entire procedure in this subclause as needed to obtain the necessary access tokens for the VAL service clients, depending on the scope parameter in the Token Request message as specified in 3GPP TS 33.434 [7].

6.2.2.2 SIM-S procedure

6.2.2.2.1 HTTP based procedure

Upon receiving an OIDC Authentication Request message as specified in the OpenID Connect 1.0 [11] and IETF RFC 6749 [9] via a secure TLS tunnel between the SIM-C and the authorisation endpoint of the SIM-S, the SIM-S shall:

a) validate the received OIDC Authentication Request message as specified in the OpenID Connect 1.0 [11] and IETF RFC 6749 [9];

b) generate an HTTP 200 (OK) response according to IETF RFC 7231 [16] including form data to prompt the VAL service user for their username and password credentials; and

c) send the HTTP 200 (OK) response towards the SIM-C.

Upon receiving an HTTP POST request method from the SIM-C containing the VAL service user's username and password, the SIM-S authenticates the VAL service user and shall:

a) generate an OIDC Authentication Response message as specified in OpenID Connect 1.0 [11] and IETF RFC 6749 [9] with the following clarifications:

   1) shall generate an HTTP 302 (FOUND) response according to IETF RFC 7231 [16]; and

   2) shall include the following parameters as specified in 3GPP TS 33.434 [7]:

      - code; and

      - state,

      in the query component of the redirection URI contained in the Location header field of the HTTP FOUND request method using the "application/x-www-form-urlencoded" format as specified in W3C.REC-html401-19991224 [6]; and

b) send the HTTP 302 (FOUND) response towards the SIM-C.

Upon receiving an OIDC Token Request message via a secure TLS tunnel established between the SIM-C and the token endpoint of the SIM-S, the SIM-S shall:

a) validate the OIDC Token Request message and if valid shall generate an OIDC Token Response message as specified in OpenID Connect 1.0 [11] and IETF RFC 6749 [9] with the following clarifications:

   1) shall generate an HTTP 200 (OK) response according to IETF RFC 7231 [16];

   2) shall based on the received VAL user ID obtained from the received user authentication credentials, determine the VAL service ID of the VAL service user;

   3) shall include the:

      - access_token;

      - token_type; and

      - expires_in.

      parameters and may include the:

      - id_token; and

      - refresh_token.

      parameters as specified in 3GPP TS 33.434 [7]; and

   4) shall include the other required parameters as specified in OpenID Connect 1.0 [11] and IETF RFC 6749 [9]; and

b) shall send the HTTP 200 (OK) response towards the SIM-C.

6.2.2.2.2 CoAP based procedure

Upon receiving an ACE-OAUTH Token Request message with client credentials grant type as specified in the Internet draft ACE-OAUTH [19] optionally via a secure (D)TLS tunnel between the SIM-C and the token endpoint of the SIM-S, the SIM-S shall:

a) validate the ACE-OAuth Token Request message and if valid shall generate an ACE-OAuth Token Response message as specified in Internet draft ACE-OAUTH [19] with the following clarifications:

   1) shall generate an COAP 2.01 (Created) response according to Internet draft ACE-OAUTH [19];

2) based on the received client credentials, shall determine the VAL user ID, VAL service ID of the VAL service user;

3) shall include parameters:

- access_token;
- expires_in;
- ace_profile; and
- rs_cnf; and

4) shall include the other required parameters as specified in Internet draft ACE-OAUTH [19]; and

b) shall send the CoAP 2.01 (Created) response towards the SIM-C.

6.2.3 Token exchange procedure

6.2.3.1 SIM-C procedure

Upon receiving a request from the VAL user to acquire a security token for authentication of the VAL services, the SIM-C shall:

a) establish a TLS tunnel to the token endpoint of the SIM-S; and

b) send a Token Exchange Request message as specified in 3GPP TS 33.434 [7] and IETF RFC 8693 [8] using an HTTP POST request method towards the SIM-S according to IETF RFC 7231 [16]. The following parameters shall be included in the entity body of the HTTP POST request using the "application/x-www-form-urlencoded" format as specified in W3C.REC-html401-19991224 [6]:

- grant_type;
- code;
- client_id;
- redirect_uri; and
- code_verifier.

Upon receipt of an HTTP 200 (OK) response from SIM-S, the SIM-C shall extract the security token contained in the access_token parameter of the received Token Exchange Response message as specified in IETF RFC 8693 [8] and send it to the VAL user.

6.2.3.2 SIM-S procedure

Upon receiving a Token Exchange Request message as specified in IETF RFC 8693 [8] via a secure TLS tunnel between the SIM-C and the token endpoint of the SIM-S, the SIM-S shall:

a) validate the received Token Exchange Request message as specified in IETF RFC 8693 [8]; and

b) send a Token Exchange Response message as specified in IETF RFC 8693 [8] and IETF RFC 6749 [9] using an HTTP 200 (OK) response to the SIM-C according to IETF RFC 7231 [16]. The following parameters shall be included,

- access_token;
- token_type; and
- expires_in.

and the following parameters may be included,

- id_token; and

- refresh_token.

in the HTTP 200 (OK) response and are serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 8693 [8] and IETF RFC 7159 [10].

6.3 Off-network procedures

The off-network procedures are out of scope of the present document in this release of the specification.

Annex A (normative): HTTP entities

A.1 Scope

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

A.2 Procedures

A.2.1 HTTP client

A.2.1.1 General

The HTTP client shall support the client role defined in IETF RFC 7230 [15].

A.2.1.2 HTTP client in UE

The HTTP client in the U E shall support the client role defined in IETF RFC 2818 [12].

The HTTP client in the UE shall support transport layer security (TLS) as specified in clause 6 of 3GPP TS 33.434 [7].

The HTTP client in the UE is configured with the following parameters:

a) a home HTTP proxy FQDN;

b) a home HTTP proxy port;

c) One of the following TLS tunnel authentication method along with its parameters as specified in 3GPP TS 33.434 [7]:

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

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

   3) mutual authentication based on pre-shared key, along with TLS tunnel authentication based on pre-shared key;

The HTTP client in the UE shall establish a TCP connection towards the home HTTP proxy FQDN and the home HTTP proxy port.

The HTTP client in the UE shall establish a TLS tunnel via the TCP connection as specified in 3GPP TS 33.434 [7]. When establishing the TLS tunnel, the HTTP client in the UE shall act as a TLS client and the UE shall perform the TLS tunnel authentication using the TLS authentication method indicated by the TLS tunnel authentication method parameter according to 3GPP TS 33.434 [7]. In order to prevent man-in-the-middle attacks, the HTTP client in the UE shall check the home HTTP proxy FQDN against the server's identity as presented in the received server's certificate message if the TCP connection terminates on the HTTP proxy. The HTTP client in the UE shall check the portion of dereferenced HTTP URL against the server's identity as presented in the received server's certificate message only if the TCP connection terminates on the SIM-S.

NOTE: The TLS tunnel can be terminated in the HTTP proxy (rather than in the HTTP server providing the dereferenced HTTP URL).

The HTTP client in the UE shall send and receive all HTTP messages via the TLS tunnel.

If the HTTP client in the UE has an access token of the "bearer" token type as specified in IETF RFC 6750 [13], the HTTP client in the UE shall include an Authorization header field with the "Bearer" authentication scheme as specified in IETF RFC 6750 [13] in HTTP requests.

A.2.1.3 HTTP client in network entity

The HTTP client in the network entity is configured with the following parameters:

a) a home HTTP proxy FQDN; and

b) a home HTTP proxy port.

The HTTP client in the network entity shall send and receive all HTTP messages via the home HTTP proxy.

The HTTP client in the network entity shall insert an X-3GPP-Asserted-Identity header field as specified in 3GPP TS 24.109 [14] in the HTTP request and shall set X-3GPP-Asserted-Identity header field to the identity of the HTTP client in the network entity. The identity of the HTTP client in the network entity can be a public service identity, a VAL group ID, or a VAL service ID.

A.2.2 HTTP proxy

A.2.2.1 General

The HTTP proxy shall support proxy role defined in .

A.2.2.2 HTTP request method from HTTP client in UE

The HTTP proxy shall support the server role defined in IETF RFC 7230 [15] [5], and in IETF RFC 2818 [12].

The HTTP proxy shall support transport layer security (TLS) as specified in 3GPP TS 33.434 [7].

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

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

b) a TCP port of an HTTP proxy for UEs.

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

Upon reception of an HTTP request method via a TLS tunnel:

a) if the HTTP request method contains an X-3GPP-Asserted-Identity header field as specified in 3GPP TS 24.109 [14], the HTTP proxy shall reject the HTTP request method with an HTTP 403 (Forbidden) response and shall not continue with the below steps;

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

c) if the HTTP request method contains a Request-URI identifying a resource in its own VAL service provider, the HTTP proxy shall act as a reverse proxy for the HTTP request method and shall forward the HTTP request method according to the VAL service provider's policy.

A.2.2.3 HTTP request method from HTTP client in network entity within trust domain

The HTTP proxy is configured with the following parameters:

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

b) a TCP port of an HTTP proxy for trusted entities.

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

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

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

A.2.3 HTTP server

The HTTP server shall support the server role defined in IETF RFC 7230 [15].

Upon reception of an HTTP request:

a) if the received HTTP request does not contain an Authorization header field with the "Bearer" authentication scheme and a bearer access token as specified in IETF RFC 6750 [13] and the received HTTP request does not contain an X-3GPP-Asserted-Identity header field as specified in 3GPP TS 24.109 [14], the HTTP server shall reject the request with HTTP 403 (Forbidden) response;

b) if the received HTTP request contains an Authorization header field with the "Bearer" authentication scheme and a bearer access token as specified in IETF RFC 6750 [13];

   a) the HTTP server shall validate the bearer access token as specified in IETF RFC 6750 [13]; and

   b) the HTTP server shall consider the VAL service ID derived from the bearer access token as the identity of the sender of the HTTP request; and

c) if the received HTTP request does not contain an Authorization header field with the "Bearer" authentication scheme and a bearer access token as specified in IETF RFC 6750 [13] and the received HTTP request contains an X-3GPP-Asserted-Identity header field as specified in 3GPP TS 24.109 [14], the HTTP server shall consider the URI in the X-3GPP-Asserted-Identity header field as the identity of the sender of the HTTP request.

Annex B (normative): CoAP entities

B.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 [17] and 3GPP TS 23.434 [2].

B.2 General

When the VAL UE is authenticating directly to the SEAL/VAL server without proxies, then the DTLS profile of ACE-OAUTH [20] may be used. In order to authorize clients and protect communication across proxies, the OSCORE profile of ACE-OAUTH [21] shall be used.

The client shall support UDP transport defined in IETF RFC 7252 [17] and should support TCP transport defined in IETF RFC 8323 [18]:

a) when UDP transport and OSCORE profile of ACE-OAUTH [21] are used, datagram transport layer security (DTLS) may be used;

b) when TCP transport and OSCORE profile of ACE-OAUTH [21] are used, transport layer security (TLS) may be used;

c) when UDP transport and DTLS profile of ACE-OAUTH [20] are used, datagram transport layer security (DTLS) shall be used; and

d) when TCP transport and DTLS profile of ACE-OAUTH [20] are used, transport layer security (TLS) shall be used.

Proof-of-Possession token type is used with ACE-OAUTH [19].

B.3 Procedures

B.3.1 CoAP client

The CoAP client in the UE shall support the client role defined in IETF RFC 7252 [17].

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.

B.3.2 CoAP proxy

B.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 [17].

CoAP proxy shall support UDP transport in IETF RFC 7252 [17] and shall support TCP transport defined in IETF RFC 8323 [18].

B.3.2.2 CoAP request method from CoAP client in UE

The CoAP proxy shall support the server role defined in IETF RFC 7252 [17].

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.

B.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.

B.4.2 CoAP server

The CoAP server shall support the server role defined in IETF RFC 7252 [17].

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

a) shall verify the integrity of the access token; and

b) 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:

a) 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 [20] or the OSCORE profile of ACE-OAUTH [21].

Annex C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-10	CT1#120	C1-196093				Draft skeleton provided by the rapporteur.	0.0.0
2019-10	CT1#120					Implementing the following p-CRs agreed by CT1: C1-196850, C1-196865, C1-196866, C1-196867	0.1.0
2019-11	CT1#121					Implementing the following p-CRs agreed by CT1: C1-198600, C1-198601, C1-198602, C1-198603	0.2.0
2019-12	CT-86	CP-193154				Presentation for information at TSG CT	1.0.0
2020-03	CT1#122-e					Implementing the following p-CRs agreed by CT1: C1-200450, C1-200609, C1-200611, C1-200612, C1-200818, C1-201003	1.1.0
2020-03	CT-87e	CP-200171				Presentation for approval at TSG CT	2.0.0
2020-03	CT-87e					Version 16.0.0 created after approval	16.0.0
2020-06	CT-88e	CP-201129	0001		F	Updates to User Authentication Client (SIM-C) procedure	16.1.0
2020-06	CT-88e	CP-201129	0002		F	Updates to User Authentication Server (SIM-S) procedure	16.1.0
2020-06	CT-88e	CP-201129	0003	3	F	Updates to Token Exchange Client (SIM-C) procedure	16.1.0
2020-06	CT-88e	CP-201129	0004	3	F	Updates to Token Exchange Server (SIM-S) procedure	16.1.0
2020-06	CT-88e	CP-201129	0005	1	F	draft-ietf-oauth-token-exchange has been published as RFC8693	16.1.0
2020-09	CT-89e	CP-202163	0006	1	F	Correcting a reference	16.2.0
2021-12	CT-94e	CP-213031	0007	-	B	Reference update for HTTP/1.1 protocol	17.0.0
2021-12	CT-94e	CP-213052	0008	1	B	SEAL IM FE requirements	17.0.0
2021-12	CT-94e	CP-213052	0009	-	B	Token endpoint reference for CoAP support	17.0.0
2021-12	CT-94e	CP-213052	0010	1	B	Addition of CoAP user authentication procedure	17.0.0
2021-12	CT-94e	CP-213052	0011	1	B	Addition of CoAP entities annex	17.0.0
2022-03	CT-95e	CP-220255	0012	-	F	Correction of CR implementation issues	17.1.0

History

Document history		
V17.1.0	May 2022	Publication