ETSI TS 124 382 V13.0.1 (2016-05)

LTE;
Mission Critical Push To Talk (MCPTT) identity management;
Protocol specification
(3GPP TS 24.382 version 13.0.1 Release 13)

Reference
DTS/TSGC-0124382vd01

Keywords
LTE

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 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.

1 Scope

This document specifies the identity management and authentication protocols needed to support Mission Critical Push To Talk (MCPTT). Identity management applies only to on-network operation.

Mission critical communication services are services that require preferential handling compared to normal telecommunication services, e.g. in support of police or fire brigade.

The MCPTT service can be used for public safety applications and also for general commercial applications (e.g., utility companies and railways).

This document is applicable to User Equipment (UE) supporting the identity management client functionality, and to application servers supporting the identity management server functionality.

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 33.179: "Security of Mission Critical Push-To-Talk (MCPTT)".

[3] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT) over LTE".

[4] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".

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

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

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

[8] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services".

[9] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services; Stage 2".

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

[11] 3GPP TS 24.383: "Mission Critical Push To Talk (MCPTT) Management Object (MO)".

[12] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control Protocol specification".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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].

IdM client id: The client_id as specified in 3GPP TS 33.179 [2] which is used to identify the IdM client to the IdM server.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.179 [3] apply:

MCPTT UE

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].

HTTP	Hypertext Transfer Protocol
IdM	Identity Management
LTE	Long Term Evolution
MC ID	Mission Critical User Identity
MCPTT	Mission Critical Push To Talk
OIDC	OpenID Connect
TLS	Transport Layer Security
UE	User Equipment

4 General

4.1 Identity management

The Identity Management functional model for MCPTT is shown in figure 4.1-1 below and consists of the identity management server located in the MCPTT common services core and the identity management client located in the MCPTT UE. The IdM server and the IdM client in the MCPTT UE establish the foundation for MCPTT user authentication and user authorisation.

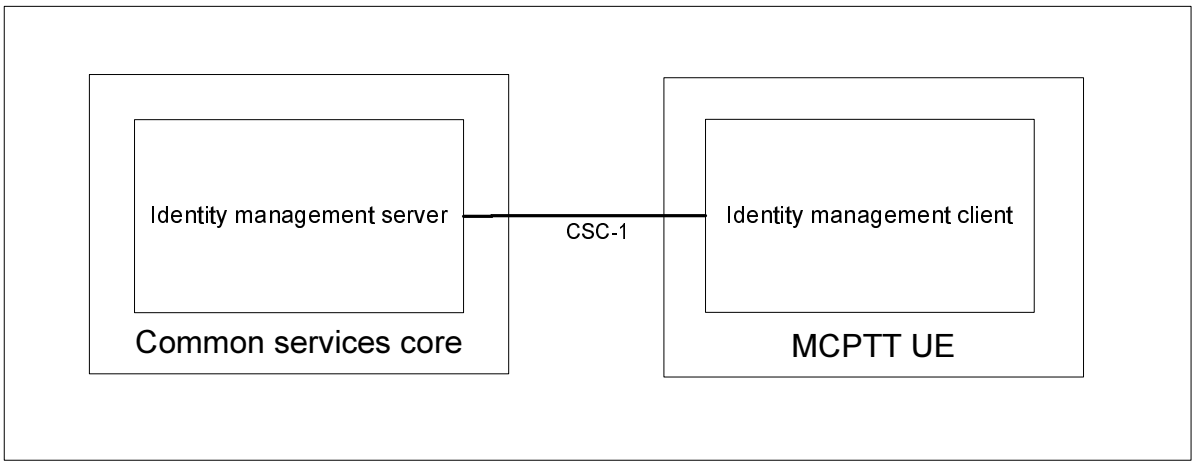

Figure 4.1-1: Functional model for MCPTT identity management

The CSC-1 reference point, between the MCPTT IdM client in the UE and the Identity Management server, provides the interface for user authentication. CSC-1 uses the HTTP-1 reference point and supports OpenID Connect Core 1.0 [6] and IETF RFC 6749 [5].

The OpenID Connect profile for MCPTT is implemented as described in 3GPP TS 33.179 [2]. The MCPTT user authentication, the MCPTT user authorisation, the OpenID Connect Core 1.0 [6] and the OpenID Connect profile described in 3GPP TS 33.179 [2] for MCPTT forms the basis of the MCPTT identity management architecture.

Subclause 6.3 describes the procedures for the MCPTT user authentication. OIDC is flexible with respect to the user authentication mechanism used. As 3GPP TS 33.179 [2] has indicated that username and password authentication is mandatory to support, that mechanism is included in subclause 6.3, although other mechanisms are possible.

When the MCPTT user is authenticated, the procedure will provide an id token, an access token and a refresh token, which are all described in 3GPP TS 33.179 [2]. The access token is scoped to the services the MCPTT user is authorised for, e.g., group management services, key management services and MCPTT services. The access token will be utilized for MCPTT service authorisation, the procedure which is documented in 3GPP TS 24.379 [12].

5 Entities

5.1 Identity management client

The identity management client acts as the application user agent for MC ID transactions. It interacts with the identity management server. The identity management client:

- shall support identity management registration to the identity management server;
- shall support the MCPTT user authentication framework as specified in 3GPP TS 33.179 [2];
- shall support a username and password method of authentication as specified in 3GPP TS 33.179 [2]; and
- may support additional methods of authentication.

5.2 Identity management server

The identity management server is a functional entity that is capable of authenticating the MC ID. It contains the knowledge and means to do authentication by verifying the credentials supplied by the user. The identity management server:

- shall support identity management registration of the identity management client;
- shall support the MCPTT user authentication framework as specified in 3GPP TS 33.179 [2];
- shall support a username and password method of authentication as specified in 3GPP TS 33.179 [2]; and
- may support additional methods of authentication.

5.3 MCPTT client

The MCPTT client shall interact with the IdM client as specified in subclause 6.2:

- to trigger initiation of the user authentication procedure; and
- to receive the credentials obtained from the IdM server.

5.4 HTTP proxy

The HTTP proxy acts as the proxy for all hypertext transactions between the HTTP client and the HTTP server. The HTTP proxy terminates the TLS session with the HTTP client of the MCPTT UE in order to allow the HTTP client to

establish a single TLS session for hypertext transactions with multiple HTTP servers as specified in 3GPP TS 23.179 [9].

NOTE: The HTTP proxy is in the same trust domain as the HTTP servers that are located within a MCPTT service provider"s network.

6 Authentication procedures

6.1 General

6.2 Identity management client procedures

6.2.1 User authentication

Upon an indication from the MCPTT client to initiate MCPTT user authentication, the IdM client shall perform the user authentication procedure according to 3GPP TS 33.179 [2] with the following clarifications:

1) shall establish a TLS tunnel to the HTTP proxy as specified in 3GPP TS 33.179 [2] using the configured URL of the HTTP proxy specified in 3GPP TS 24.383 [11] and the clarifications in Annex A;

Editor's Note [CT1#96, C1-161228]: While 3GPP TS 33.179 indicates that the interface from IdM client to IdM server is CSC-1 and CSC-1 uses HTTP-1, there is a question as to whether the TLS session should terminate on the HTTP proxy or be end-to-end from IdM client to IdM server. This is the only interface where the MCPTT user exposes primary credentials and thus the security concerns are heightened, and IETF RFC 6749 specifies the use of TLS as MUST.

2) shall generate an OIDC Authentication Request message as specified in the OpenID Connect 1.0 [6] and IETF RFC 6749 [5] with the following clarifications:

   a) shall generate an HTTP GET request method according to IETF RFC 2616 [4];

   b) shall include the configured parameter IdM client id as the client_id parameter specified in 3GPP TS 33.179 [2] 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 [7]; and

NOTE 1: The configuration of client_id is specified in 3GPP TS 24.383 [11].

   c) shall include the remaining required parameters as specified in 3GPP TS 33.179 [2] 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 [7]; and

3) shall send the HTTP GET request method towards the IdM server.

NOTE 2: The OpenID Connect 1.0 [6] specification allows for an alternative mechanism for sending the OIDC Authentication request message using an HTTP POST request method which can be used in place of steps 1, 2, and 3 above.

Upon receipt of an HTTP POST request method from the IdM server, the MCPTT client:

1) shall prompt the MCPTT user for their username and password;

NOTE 3: Other types of authentication are supported and are not defined by the OIDC specifications. 3GPP TS 33.179 [2] has defined username and password as a mandatory authentication method to be supported, hence a procedure to realize that method is included here.

2) shall generate an HTTP POST request method containing the MCPTT user's username and password; and

3) shall send the HTTP POST request method towards the IdM server.

Upon receipt of an OIDC Authentication Response message, the IdM client:

1) shall generate an OIDC Token Request message as specified in OpenID Connect 1.0 [6] and IETF RFC 6749 [5] with the following clarifications:

   a) shall generate an HTTP POST request method according to IETF RFC 2616 [4]; and

   b) shall include the grant_type parameter set to a value of "authorization_code" and the other required parameters in the entity body of the HTTP POST request method using the using the "application/x-www-form-urlencoded" format as specified in 3GPP TS 33.179 [2]; and

2) shall send the HTTP POST request method towards the IdM server.

Upon receipt of an OIDC Token Response message, the IdM client:

1) shall validate the id_token, access_token and refresh token in the received OIDC Token Response message as specified in the OpenID Connect 1.0 [6] specification; and

2) shall provide the id_token and access_token in the received OIDC Token Response message to the MCPTT client.

NOTE 4: The method in which the IdM client provides the id_token and access_token to the MCPTT client is implementation specific.

6.3 Identity management server procedures

6.3.1 User authentication

Upon receipt of an OIDC Authentication Request message as specified in the OpenID Connect 1.0 [6] and IETF RFC 6749 [5] via a secure tunnel as specified in subclause 9, the IdM server:

Editor's Note [CT1#96, C1-161388]: It needs to be determined whether the secure tunnel towards the IdM client is NDS IPsec as specified in 3GPP TS 33.210 or TLS dependent on deployment . IETF RFC 6749 appears to mandate TLS.

1) shall validate the received OIDC Authentication Request message as specified in the OpenID Connect 1.0 [6] and IETF RFC 6749 [5];

2) shall generate an HTTP POST request method according to IETF RFC 2616 [4] including form data to prompt the MCPTT user for their username and password credentials; and

NOTE 1: The username will be the MCPTT user's MC ID.

3) shall send the HTTP POST request method towards the IdM client.

Upon receipt of an HTTP POST request method from the IdM client containing the MCPTT user's username and password, the IdM server authenticates the MCPTT user and:

NOTE 2: Other methods of authentication can be used by the MCPTT service provider and are not defined by the OIDC specifications. 3GPP TS 33.179 [2] has defined username and password as a mandatory authentication method to be supported for MCPTT, hence a procedure to realize that method is included here.

1) shall generate an OIDC Authentication Response message as specified in OpenID Connect 1.0 [6] and IETF RFC 6749 [5] with the following clarifications:

   a) shall generate an HTTP 302 (FOUND) response according to IETF RFC 2616 [4]; and

   b) shall include the required parameters including the authorization_code as specified in 3GPP TS 33.179 [2] 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 [7]; and

2) shall send the HTTP 302 (FOUND) response towards the IdM client.

Upon receipt of an OIDC Token Request message, the IdM server:

1) shall validate the OIDC Token Request message and if valid shall generate an OIDC Token Response message as specified in OpenID Connect 1.0 [6] and IETF RFC 6749 [5] with the following clarifications:

   a) shall generate an HTTP 200 (OK) response according to IETF RFC 2616 [4];

   b) shall based on the received MC ID obtained from the received user authentication credentials, determine the MCPTT ID of the MCPTT user;

   c) shall include an id_token, access_token and refresh_token and MCPTT ID as specified in 3GPP TS 33.179 [2]; and

   d) shall include the other required parameters as specified in OpenID Connect 1.0 [6] and IETF RFC 6749 [5]; and

2) shall send the HTTP 200 (OK) response towards the IdM client.

7 Inter/intra domain interface security

Inter/intra domain interface security shall be provided as specified in 3GPP TS 33.179 [2];

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 23.179 [9] and 3GPP TS 33.179 [2].

A.2 Procedures

A.2.1 HTTP client

A.2.1.1 General

The HTTP client in the UE shall support the client role defined in IETF RFC 2616 [4].

A.2.1.2 HTTP client in UE

The HTTP client in the UE shall support the client role defined in IETF RFC 2818 [10].

The HTTP client in the UE shall support transport layer security (TLS) as specified in 3GPP TS 33.179 [2].

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

1) a home HTTP proxy FQDN;
2) a home HTTP proxy port;
3) a TLS tunnel authentication method. The TLS tunnel authentication method parameter is set to one of the following:
   a) one-way authentication of the HTTP proxy based on the server certificate;
   b) mutual authentication based on certificates; and
   c) mutual authentication based on pre-shared key;

   as specified in 3GPP TS 33.179 [2];
4) if the TLS tunnel authentication method is the mutual authentication based on certificates:
   a) TLS tunnel authentication X.509 certificate; and
5) if the TLS tunnel authentication method is the mutual authentication based on pre-shared key;
   a) TLS tunnel authentication 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 33.179 [2]. 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 33.179 [2]. The UE shall use the configured TLS tunnel authentication X.509 certificate and the configured TLS tunnel authentication pre-shared key when applicable for the used TLS authentication method. 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. The HTTP client in the UE shall not check the portion of dereferenced HTTP URL against the server's identity as presented in the received server's certificate message.

NOTE: the TLS tunnel is 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.

A.2.1.3 HTTP client in network entity

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

1) a home HTTP proxy FQDN; and

2) a home HTTP proxy port.

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

A.2.2 HTTP proxy

A.2.2.1 General

The HTTP proxy shall support proxy role of IETF RFC 2616 [4].

A.2.2.2 HTTP request method from HTTP client in UE

The HTTP proxy shall support the server role of IETF RFC 2616 [4], and IETF RFC 2818 [10].

The HTTP proxy shall support transport layer security (TLS) as specified in 3GPP TS 33.179 [2].

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

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

2) 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 33.179 [2]. When establishing the TLS tunnel, the HTTP proxy shall act as TLS server.

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

1) if the HTTP request method contains an X-3GPP-Asserted-Identity header field, the HTTP proxy shall reject the HTTP request method with an HTTP 403 (Forbidden) response and do not continue with rest of the steps;

2) if the HTTP proxy is able to authenticate the sender of an HTTP request method, the HTTP proxy shall insert an X-3GPP-Asserted-Identity header field containing the identity of the sender of an HTTP request method in the HTTP request method;

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

4) if an HTTP request method contains a Request-URI identifying a resource in own MCPTT provider, the HTTP proxy shall act as reverse proxy for the HTTP request method and shall forward the HTTP request method according to the MCPTT provider 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:

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

2) 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 33.179 [2]:

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

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

A.2.3 HTTP server

The HTTP server shall support the server role of IETF RFC 2616 [4].

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2015-07					Initial proposal to CT1#92-bis	-	0.0.0
2015-08					Contains the following agreed P-CRs from CT1#92-bis: C1ah-150013, C1ah-150033 Minor alignments by the rapporteur.	0.0.0	0.1.0
2015-09					Updated to include specification number after CT#69 allocation.	0.1.0	0.1.1
2016-02					Contains the following agreed P-CRs from CT1-on MCPTT: C1ah-160030, C1ah-160105, C1ah-160103, C1ah-160088	0.1.1	0.2.0
2016-02					Contains the following agreed P-CRs from CT1#96: C1-161040, C1-161222, C1-161228, C1-161229, C1-161260, C1-161300, C1-161301, C1-161388	0.2.0	0.3.0
2016-03	CT-71	CP-160055			Version 1.0.0 created for presentation for information and approval	0.3.0	1.0.0
2016-03	CT-71				Version 13.0.0 created after approval	1.0.0	13.0.0
2016-03	CT-71				Minor editorial changes by TS rapporteur	13.0.0	13.0.1

History

Document history		
V13.0.1	May 2016	Publication