3GPP TR 24.890 V16.0.0 (2020-07)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Core Network and Terminals;

5G System – Phase 1;

CT WG1 Aspects

(Release 16)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

5G, 5GS, EPS, layer 3, LTE, network, stage 3, user equipment

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [19](#__RefHeading___Toc510099256)

1 Scope [20](#__RefHeading___Toc510099257)

2 References [20](#__RefHeading___Toc510099258)

3 Definitions and abbreviations [22](#__RefHeading___Toc510099259)

3.1 Definitions [22](#__RefHeading___Toc510099260)

3.2 Abbreviations [23](#__RefHeading___Toc510099261)

4 Architecture [25](#__RefHeading___Toc510099262)

4.1 General [25](#__RefHeading___Toc510099263)

4.2 Architecture reference model [25](#__RefHeading___Toc510099264)

4.3 Architecture for interworking with E-UTRAN connected to EPC [26](#__RefHeading___Toc510099265)

5 Network selection procedures [27](#__RefHeading___Toc510099266)

5.1 Concepts [27](#__RefHeading___Toc510099267)

5.2 Procedures [28](#__RefHeading___Toc510099268)

5.2.1 General [28](#__RefHeading___Toc510099269)

5.2.2 Procedures for 3GPP radio access networks [28](#__RefHeading___Toc510099270)

5.2.2.1 General [28](#__RefHeading___Toc510099271)

5.2.2.2 PLMN selection in 5GMM-CONNECTED mode with RRC inactive indication [29](#__RefHeading___Toc510099272)

5.2.3 Procedures for non-3GPP access networks [29](#__RefHeading___Toc510099273)

5.2.4 Procedure for steering of UE in VPLMN [29](#__RefHeading___Toc510099274)

5.2.4.1 Alternative 1 for steering of UE in VPLMN [29](#__RefHeading___Toc510099275)

5.2.4.1.1 General [29](#__RefHeading___Toc510099276)

5.2.4.1.2 Procedure for steering of UE in VPLMN during registration [29](#__RefHeading___Toc510099277)

5.2.4.1.2.1 Initiation of the procedure for steering of UE in VPLMN during registration [29](#__RefHeading___Toc510099278)

5.2.4.1.2.2 Procedure for steering of UE in VPLMN during registration accepted by the UE [30](#__RefHeading___Toc510099279)

5.2.4.1.2.3 Procedure for steering of UE in VPLMN not accepted by the UE during registration [30](#__RefHeading___Toc510099280)

5.2.4.1.3 Procedure for steering of UE in VPLMN after registration [30](#__RefHeading___Toc510099281)

5.2.4.1.3.1 Initiation of the procedure for steering of UE in VPLMN after registration [30](#__RefHeading___Toc510099282)

5.2.4.1.3.2 Procedure for steering of UE in VPLMN after registration accepted by the UE [30](#__RefHeading___Toc510099283)

5.2.4.1.3.3 Procedure for steering of UE in VPLMN after registration not accepted by the UE [31](#__RefHeading___Toc510099284)

5.2.4.1.4 Completion of the procedure for steering of UE in VPLMN at the network [31](#__RefHeading___Toc510099285)

5.2.4.1.5 Stage-2 flow [31](#__RefHeading___Toc510099286)

5.2.4.1.5.1 Stage-2 flow for steering of UE in VPLMN during registration. [31](#__RefHeading___Toc510099287)

5.2.4.1.5.2 Stage-2 flow for steering of UE in VPLMN after registration [33](#__RefHeading___Toc510099288)

5.2.4.1.6 Stage-3 encoding of the list of preferred PLMN/access technology combinations [34](#__RefHeading___Toc510099289)

5.2.4.2 Alternative 2 for steering of UE in VPLMN [34](#__RefHeading___Toc510099290)

5.2.4.2.1 General [34](#__RefHeading___Toc510099291)

5.2.4.2.2 Initiation of the procedure for steering of UE in VPLMN [35](#__RefHeading___Toc510099292)

5.2.4.2.3 Procedure for steering of UE in VPLMN accepted by the UE [35](#__RefHeading___Toc510099293)

5.2.4.2.4 Procedure for steering of UE in VPLMN not accepted by the UE [35](#__RefHeading___Toc510099294)

5.2.4.2.5 Stage-2 flow [35](#__RefHeading___Toc510099295)

5.2.4.3 Void [37](#__RefHeading___Toc510099296)

5.2.4.3.1 Void [37](#__RefHeading___Toc510099297)

5.2.4.3.2 Void [37](#__RefHeading___Toc510099298)

5.2.4.3.3 Void [37](#__RefHeading___Toc510099299)

5.2.4.3.4 Void [37](#__RefHeading___Toc510099300)

6 Stage 3 protocol, general aspects [37](#__RefHeading___Toc510099301)

6.1 General [37](#__RefHeading___Toc510099302)

6.2 Protocols and peer to peer communication [37](#__RefHeading___Toc510099303)

6.3 Basic groups of functions [38](#__RefHeading___Toc510099304)

6.4 Protocol architecture [38](#__RefHeading___Toc510099305)

6.5 Standard L3 messages [41](#__RefHeading___Toc510099306)

6.6 General message format and information elements coding [41](#__RefHeading___Toc510099307)

6.6.1 Overview [41](#__RefHeading___Toc510099308)

6.6.2 Extended protocol discriminator [42](#__RefHeading___Toc510099309)

6.6.3 Security header type [42](#__RefHeading___Toc510099310)

6.6.4 PDU session identity [42](#__RefHeading___Toc510099311)

6.6.5 Spare half octet [42](#__RefHeading___Toc510099312)

6.6.6 Procedure transaction identity [42](#__RefHeading___Toc510099313)

6.6.7 Message type [42](#__RefHeading___Toc510099314)

6.7 Handling of unknown, unforeseen, and erroneous protocol data [42](#__RefHeading___Toc510099315)

6.7.1 General [42](#__RefHeading___Toc510099316)

6.7.2 Message too short [43](#__RefHeading___Toc510099317)

6.7.3 Unknown or unforeseen procedure transaction identity or PDU Session identity [43](#__RefHeading___Toc510099318)

6.7.3.1 Procedure transaction identity [43](#__RefHeading___Toc510099319)

6.7.3.2 PDU Session identity [43](#__RefHeading___Toc510099320)

6.7.4 Unknown or unforeseen message type [43](#__RefHeading___Toc510099321)

6.7.5 Non-semantical mandatory information element errors [43](#__RefHeading___Toc510099322)

6.7.5.1 Common procedures [43](#__RefHeading___Toc510099323)

6.7.5.2 5GS mobility management [44](#__RefHeading___Toc510099324)

6.7.5.3 5GS session management [44](#__RefHeading___Toc510099325)

6.7.6 Unknown and unforeseen IEs in the non-imperative message part [44](#__RefHeading___Toc510099326)

6.7.6.1 IEIs unknown in the message [44](#__RefHeading___Toc510099327)

6.7.6.2 Out of sequence IEs [44](#__RefHeading___Toc510099328)

6.7.6.3 Repeated IEs [44](#__RefHeading___Toc510099329)

6.7.7 Non-imperative message part errors [45](#__RefHeading___Toc510099330)

6.7.7.1 Syntactically incorrect optional IEs [45](#__RefHeading___Toc510099331)

6.7.7.2 Conditional IE errors [45](#__RefHeading___Toc510099332)

6.7.8 Messages with semantically incorrect contents [45](#__RefHeading___Toc510099333)

7 Coordination between the protocols for 5GS mobility management and 5GS session management [45](#__RefHeading___Toc510099334)

8 5GS mobility management [46](#__RefHeading___Toc510099335)

8.1 Overview [46](#__RefHeading___Toc510099336)

8.1.1 General [46](#__RefHeading___Toc510099337)

8.1.2 Domain selection [46](#__RefHeading___Toc510099338)

8.1.2.1 UE’s usage setting [46](#__RefHeading___Toc510099339)

8.1.2.2 Domain selection for UE originating sessions / calls [46](#__RefHeading___Toc510099340)

8.1.2.3 Change of UE’s usage setting [47](#__RefHeading___Toc510099341)

8.1.2.4 Change or determination of IMS voice availability [47](#__RefHeading___Toc510099342)

8.1.3 Types of 5GMM procedures [48](#__RefHeading___Toc510099343)

8.1.4 5GMM sublayer states [49](#__RefHeading___Toc510099344)

8.1.4.1 General [49](#__RefHeading___Toc510099345)

8.1.4.2 5GMM sublayer states [49](#__RefHeading___Toc510099346)

8.1.4.2.1 General [49](#__RefHeading___Toc510099347)

8.1.4.2.2 5GMM sublayer states in the UE [49](#__RefHeading___Toc510099348)

8.1.4.2.2.1 General [49](#__RefHeading___Toc510099349)

8.1.4.2.2.2 Main states [50](#__RefHeading___Toc510099350)

8.1.4.2.2.2.1 5GMM-NULL [50](#__RefHeading___Toc510099351)

8.1.4.2.2.2.2 5GMM-DEREGISTERED [50](#__RefHeading___Toc510099352)

8.1.4.2.2.2.3 5GMM-REGISTERED-INITIATED [50](#__RefHeading___Toc510099353)

8.1.4.2.2.2.4 5GMM-REGISTERED [50](#__RefHeading___Toc510099354)

8.1.4.2.2.2.5 5GMM-DEREGISTERED-INITIATED [50](#__RefHeading___Toc510099355)

8.1.4.2.2.2.6 5GMM-SERVICE-REQUEST-INITIATED [50](#__RefHeading___Toc510099356)

8.1.4.2.2.3 Substates of state 5GMM-DEREGISTERED [51](#__RefHeading___Toc510099357)

8.1.4.2.2.3.1 General [51](#__RefHeading___Toc510099358)

8.1.4.2.2.3.2 5GMM-DEREGISTERED.NORMAL-SERVICE [51](#__RefHeading___Toc510099359)

8.1.4.2.2.3.3 5GMM-DEREGISTERED.LIMITED-SERVICE [51](#__RefHeading___Toc510099360)

8.1.4.2.2.3.4 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION [51](#__RefHeading___Toc510099361)

8.1.4.2.2.3.5 5GMM-DEREGISTERED.PLMN-SEARCH [51](#__RefHeading___Toc510099362)

8.1.4.2.2.3.6 5GMM-DEREGISTERED.NO-SUPI [51](#__RefHeading___Toc510099363)

8.1.4.2.2.3.7 5GMM-DEREGISTERED.NO-CELL-AVAILABLE [51](#__RefHeading___Toc510099364)

8.1.4.2.2.3.8 5GMM-DEREGISTERED.eCALL-INACTIVE [51](#__RefHeading___Toc510099365)

8.1.4.2.2.4 Substates of state 5GMM-REGISTERED [52](#__RefHeading___Toc510099366)

8.1.4.2.2.4.1 General [52](#__RefHeading___Toc510099367)

8.1.4.2.2.4.2 5GMM-REGISTERED.NORMAL-SERVICE [52](#__RefHeading___Toc510099368)

8.1.4.2.2.4.3 5GMM-REGISTERED.NON-ALLOWED-SERVICE [52](#__RefHeading___Toc510099369)

8.1.4.2.2.4.4 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE [52](#__RefHeading___Toc510099370)

8.1.4.2.2.4.5 5GMM-REGISTERED.LIMITED-SERVICE [52](#__RefHeading___Toc510099371)

8.1.4.2.2.4.6 5GMM-REGISTERED.PLMN-SEARCH [52](#__RefHeading___Toc510099372)

8.1.4.2.2.4.7 5GMM-REGISTERED.NO-CELL-AVAILABLE [53](#__RefHeading___Toc510099373)

8.1.4.2.3 5GS update status [53](#__RefHeading___Toc510099374)

8.1.4.2.4 5GMM sublayer states in the network [53](#__RefHeading___Toc510099375)

8.1.4.2.4.1 General [53](#__RefHeading___Toc510099376)

8.1.4.2.4.2 5GMM-DEREGISTERED [54](#__RefHeading___Toc510099377)

8.1.4.2.4.3 5GMM-COMMON-PROCEDURE-INITIATED [54](#__RefHeading___Toc510099378)

8.1.4.2.4.4 5GMM-REGISTERED [54](#__RefHeading___Toc510099379)

8.1.4.2.4.5 5GMM-DEREGISTERED-INITIATED [54](#__RefHeading___Toc510099380)

8.1.4.3 Behaviour of the UE in state 5GMM-DEREGISTERED and state 5GMM-REGISTERED [54](#__RefHeading___Toc510099381)

8.1.4.3.1 General [54](#__RefHeading___Toc510099382)

8.1.4.3.2 UE behaviour in state 5GMM-DEREGISTERED [55](#__RefHeading___Toc510099383)

8.1.4.3.2.1 General [55](#__RefHeading___Toc510099384)

8.1.4.3.2.2 Detailed description of UE behaviour in state 5GMM-DEREGISTERED [55](#__RefHeading___Toc510099385)

8.1.4.3.2.2.1 NORMAL-SERVICE [55](#__RefHeading___Toc510099386)

8.1.4.3.2.2.2 LIMITED-SERVICE [55](#__RefHeading___Toc510099387)

8.1.4.3.2.2.3 ATTEMPTING-REGISTRATION [55](#__RefHeading___Toc510099388)

8.1.4.3.2.2.4 PLMN-SEARCH [55](#__RefHeading___Toc510099389)

8.1.4.3.2.2.5 NO-SUPI [55](#__RefHeading___Toc510099390)

8.1.4.3.2.2.6 NO-CELL-AVAILABLE [56](#__RefHeading___Toc510099391)

8.1.4.3.2.2.7 eCALL-INACTIVE [56](#__RefHeading___Toc510099392)

8.1.4.3.3 UE behaviour in state 5GMM-REGISTERED [56](#__RefHeading___Toc510099393)

8.1.4.3.3.1 General [56](#__RefHeading___Toc510099394)

8.1.4.3.3.2 Detailed description of UE behaviour in state 5GMM-REGISTERED [56](#__RefHeading___Toc510099395)

8.1.4.3.3.2.1 NORMAL-SERVICE [56](#__RefHeading___Toc510099396)

8.1.4.3.3.2.2 NON-ALLOWED-SERVICE [56](#__RefHeading___Toc510099397)

8.1.4.3.3.2.3 ATTEMPTING-REGISTRATION-UPDATE [56](#__RefHeading___Toc510099398)

8.1.4.3.3.2.4 LIMITED-SERVICE [57](#__RefHeading___Toc510099399)

8.1.4.3.3.2.5 PLMN-SEARCH [57](#__RefHeading___Toc510099400)

8.1.4.3.3.2.6 NO-CELL-AVAILABLE [57](#__RefHeading___Toc510099401)

8.1.5 Permanent identifiers [57](#__RefHeading___Toc510099402)

8.1.6 Temporary identities [57](#__RefHeading___Toc510099403)

8.1.7 Mobile initiated connection only mode [58](#__RefHeading___Toc510099404)

8.1.8 Handling of the periodic registration update timer and implicit de-registration timer [58](#__RefHeading___Toc510099405)

8.2 5GS mobility functions in IDLE and CONNECTED mode [59](#__RefHeading___Toc510099406)

8.2.1 Registration areas in the 5GS [59](#__RefHeading___Toc510099407)

8.2.1.1 General [59](#__RefHeading___Toc510099408)

8.2.1.2 Open issues on registration areas in the 5GS [59](#__RefHeading___Toc510099409)

8.2.2 Service area restrictions [60](#__RefHeading___Toc510099410)

8.2.3 UE NAS mobility functions in 5GMM-IDLE mode [61](#__RefHeading___Toc510099411)

8.2.4 UE NAS mobility functions in 5GMM-CONNECTED mode [62](#__RefHeading___Toc510099412)

8.2.5 5GMM-CONNECTED mode with RRC inactive indication [62](#__RefHeading___Toc510099413)

8.2.6 Disabling and re-enabling of UE's N1 mode radio capabilities [63](#__RefHeading___Toc510099414)

8.3 Establishment of the N1 NAS signalling connection [64](#__RefHeading___Toc510099415)

8.4 Release of the N1 NAS signalling connection [65](#__RefHeading___Toc510099416)

8.5 5GS mobility management procedures [66](#__RefHeading___Toc510099417)

8.5.1 5GMM common procedures [66](#__RefHeading___Toc510099418)

8.5.1.1 Primary authentication and key agreement procedure [66](#__RefHeading___Toc510099419)

8.5.1.1.1 General [66](#__RefHeading___Toc510099420)

8.5.1.1.2 EAP based primary authentication and key agreement procedure [66](#__RefHeading___Toc510099421)

8.5.1.1.2.1 General [66](#__RefHeading___Toc510099422)

8.5.1.1.2.2 EAP-AKA' related procedures [68](#__RefHeading___Toc510099423)

8.5.1.1.2.2.1 General [68](#__RefHeading___Toc510099424)

8.5.1.1.2.2.2 Initiation [68](#__RefHeading___Toc510099425)

8.5.1.1.2.2.3 UE successfully authenticates network [68](#__RefHeading___Toc510099426)

8.5.1.1.2.2.4 Errors when handling EAP-request/AKA'-challenge message [68](#__RefHeading___Toc510099427)

8.5.1.1.2.2.5 Network successfully authenticates UE [68](#__RefHeading___Toc510099428)

8.5.1.1.2.2.6 UE handling EAP-AKA' notification [69](#__RefHeading___Toc510099429)

8.5.1.1.2.2.7 Network sending EAP-success message [69](#__RefHeading___Toc510099430)

8.5.1.1.2.2.8 UE handling EAP-success message [69](#__RefHeading___Toc510099431)

8.5.1.1.2.2.9 Network not successfully authenticates UE [69](#__RefHeading___Toc510099432)

8.5.1.1.2.2.10 Network sending EAP-failure message [69](#__RefHeading___Toc510099433)

8.5.1.1.2.2.11 UE handling EAP-success [69](#__RefHeading___Toc510099434)

8.5.1.1.2.3 EAP message reliable transport procedure [69](#__RefHeading___Toc510099435)

8.5.1.1.2.3.1 General [69](#__RefHeading___Toc510099436)

8.5.1.1.2.3.2 EAP message reliable transport procedure initiation by the network [69](#__RefHeading___Toc510099437)

8.5.1.1.2.3.3 EAP message reliable transport procedure accepted by the UE [70](#__RefHeading___Toc510099438)

8.5.1.1.2.3.4 Abnormal cases on the network side [70](#__RefHeading___Toc510099439)

8.5.1.1.2.3.5 Abnormal cases in the UE [70](#__RefHeading___Toc510099440)

8.5.1.1.3 5G AKA based primary authentication and key agreement procedure [70](#__RefHeading___Toc510099441)

8.5.1.1.3.1 General [70](#__RefHeading___Toc510099442)

8.5.1.1.3.2 Authentication initiation by the network [71](#__RefHeading___Toc510099443)

8.5.1.1.3.3 Authentication response by the UE [71](#__RefHeading___Toc510099444)

8.5.1.1.3.4 Authentication completion by the network [72](#__RefHeading___Toc510099445)

8.5.1.1.3.5 Authentication not accepted by the network [72](#__RefHeading___Toc510099446)

8.5.1.1.3.6 Authentication not accepted by the UE [73](#__RefHeading___Toc510099447)

8.5.1.1.3.7 Abnormal cases [73](#__RefHeading___Toc510099448)

8.5.1.2 Security mode control procedure [73](#__RefHeading___Toc510099449)

8.5.1.2.1 General [73](#__RefHeading___Toc510099450)

8.5.1.2.2 NAS security mode control initiation by the network [73](#__RefHeading___Toc510099451)

8.5.1.2.3 NAS security mode command accepted by the UE [75](#__RefHeading___Toc510099452)

8.5.1.2.4 NAS security mode control completion by the network [76](#__RefHeading___Toc510099453)

8.5.1.2.5 NAS security mode command not accepted by the UE [76](#__RefHeading___Toc510099454)

8.5.1.2.6 Abnormal cases in the UE [77](#__RefHeading___Toc510099455)

8.5.1.2.7 Abnormal cases on the network side [77](#__RefHeading___Toc510099456)

8.5.1.3 NAS transport procedures [78](#__RefHeading___Toc510099457)

8.5.1.3.1 General [78](#__RefHeading___Toc510099458)

8.5.1.3.2 Alternative 1 for NAS transport [78](#__RefHeading___Toc510099459)

8.5.1.3.2.1 SM transport procedures [78](#__RefHeading___Toc510099460)

8.5.1.3.2.1.1 UE-initiated SM message transport procedure [78](#__RefHeading___Toc510099461)

8.5.1.3.2.1.1.1 General [78](#__RefHeading___Toc510099462)

8.5.1.3.2.1.1.2 UE-initiated SM message transport initiation [78](#__RefHeading___Toc510099463)

8.5.1.3.2.1.1.3 UE-initiated SM message transport of messages [79](#__RefHeading___Toc510099464)

8.5.1.3.2.1.1.4 Abnormal cases on the network side [81](#__RefHeading___Toc510099465)

8.5.1.3.2.1.3 Network-initiated SM message transport procedure [81](#__RefHeading___Toc510099466)

8.5.1.3.2.1.3.1 General [81](#__RefHeading___Toc510099467)

8.5.1.3.2.1.3.2 Network-initiated SM message transport initiation [81](#__RefHeading___Toc510099468)

8.5.1.3.2.1.3.3 Network-initiated SM message transport of messages [82](#__RefHeading___Toc510099469)

8.5.1.3.2.2 Non-SM message transport procedures [82](#__RefHeading___Toc510099470)

8.5.1.3.2.2.1 General [82](#__RefHeading___Toc510099471)

8.5.1.3.2.2.2 UE-initiated non-SM message transport procedure [82](#__RefHeading___Toc510099472)

8.5.1.3.2.2.2.1 General [82](#__RefHeading___Toc510099473)

8.5.1.3.2.2.2.2 UE-initiated non-SM message transport initiation [82](#__RefHeading___Toc510099474)

8.5.1.3.2.2.2.3 UE-initiated non-SM message transport of messages [83](#__RefHeading___Toc510099475)

8.5.1.3.2.2.3 Network-initiated non-SM message transport procedure [83](#__RefHeading___Toc510099476)

8.5.1.3.2.2.3.1 General [83](#__RefHeading___Toc510099477)

8.5.1.3.2.2.3.2 Network-initiated non-SM message transport initiation [83](#__RefHeading___Toc510099478)

8.5.1.3.2.2.3.3 Network-initiated non-SM message transport of messages [84](#__RefHeading___Toc510099479)

8.5.1.3.3 Alternative 2 for NAS transport [84](#__RefHeading___Toc510099480)

8.5.1.3.3.1 General [84](#__RefHeading___Toc510099481)

8.5.1.3.3.2 UE-initiated NAS transport procedure [85](#__RefHeading___Toc510099482)

8.5.1.3.3.2.1 General [85](#__RefHeading___Toc510099483)

8.5.1.3.3.2.2 UE-initiated NAS transport procedure initiation [85](#__RefHeading___Toc510099484)

8.5.1.3.3.2.3 UE-initiated NAS transport of messages [86](#__RefHeading___Toc510099485)

8.5.1.3.3.3 Network-initiated NAS transport procedure [89](#__RefHeading___Toc510099486)

8.5.1.3.3.3.1 General [89](#__RefHeading___Toc510099487)

8.5.1.3.3.3.2 Network-initiated NAS transport procedure initiation [89](#__RefHeading___Toc510099488)

8.5.1.3.3.3.3 Network-initiated NAS transport of messages [90](#__RefHeading___Toc510099489)

8.5.1.3.4 Criteria for evaluation of alternatives for NAS transport [90](#__RefHeading___Toc510099490)

8.5.1.3.5 Evaluation of the alternatives for NAS transport [90](#__RefHeading___Toc510099491)

8.5.1.3.5.1 Message size [90](#__RefHeading___Toc510099492)

8.5.1.3.5.2 Scalability [91](#__RefHeading___Toc510099493)

8.5.1.3.5.3 Implementation and specification impact [91](#__RefHeading___Toc510099494)

8.5.1.3.5.4 Extensibility [91](#__RefHeading___Toc510099495)

8.5.1.3.6 Selection of the NAS transport mechanism [91](#__RefHeading___Toc510099496)

8.5.1.4 Generic UE configuration update procedure [91](#__RefHeading___Toc510099497)

8.5.1.4.1 General [91](#__RefHeading___Toc510099498)

8.5.1.4.2 Generic UE configuration update procedure initiated by the network [92](#__RefHeading___Toc510099499)

8.5.1.4.3 Generic UE configuration update accepted by the UE [93](#__RefHeading___Toc510099500)

8.5.1.4.4 Generic UE configuration update completion by the network [94](#__RefHeading___Toc510099501)

8.5.1.4.5 Abnormal cases in the UE [94](#__RefHeading___Toc510099502)

8.5.1.4.6 Abnormal cases on the network side [94](#__RefHeading___Toc510099503)

8.5.1.5 Identification procedure [95](#__RefHeading___Toc510099504)

8.5.1.5.1 General [95](#__RefHeading___Toc510099505)

8.5.1.5.2 Identification initiation by the network [95](#__RefHeading___Toc510099506)

8.5.1.5.3 Identification response by the UE [95](#__RefHeading___Toc510099507)

8.5.1.5.4 Identification completion by the network [95](#__RefHeading___Toc510099508)

8.5.1.5.5 Abnormal cases in the UE [95](#__RefHeading___Toc510099509)

8.5.1.5.6 Abnormal cases on the network side [95](#__RefHeading___Toc510099510)

8.5.1.6 5GMM status procedure [96](#__RefHeading___Toc510099511)

8.5.1.6.1 General [96](#__RefHeading___Toc510099512)

8.5.1.6.2 5GMM status received in the UE [96](#__RefHeading___Toc510099513)

8.5.1.6.3 5GMM status received in the network [96](#__RefHeading___Toc510099514)

8.5.2 5GMM specific procedures [96](#__RefHeading___Toc510099515)

8.5.2.1 Registration procedure [96](#__RefHeading___Toc510099516)

8.5.2.1.1 General [96](#__RefHeading___Toc510099517)

8.5.2.1.2 Registration procedure for initial registration [97](#__RefHeading___Toc510099518)

8.5.2.1.2.1 General [97](#__RefHeading___Toc510099519)

8.5.2.1.2.2 Initial registration initiation [97](#__RefHeading___Toc510099520)

8.5.2.1.2.3 5GMM common procedure initiation [98](#__RefHeading___Toc510099521)

8.5.2.1.2.4 Initial registration accepted by the network [98](#__RefHeading___Toc510099522)

8.5.2.1.2.5 Initial registration not accepted by the network [100](#__RefHeading___Toc510099523)

8.5.2.1.2.6 Initial registration for emergency services not accepted by the network [101](#__RefHeading___Toc510099524)

8.5.2.1.2.7 Abnormal cases in the UE [101](#__RefHeading___Toc510099525)

8.5.2.1.2.8 Abnormal cases on the network side [102](#__RefHeading___Toc510099526)

8.5.2.1.3 Registration procedure for mobility and periodic registration update [102](#__RefHeading___Toc510099527)

8.5.2.1.3.1 General [102](#__RefHeading___Toc510099528)

8.5.2.1.3.2 Mobility and periodic registration update initiation [102](#__RefHeading___Toc510099529)

8.5.2.1.3.3 5GMM common procedure initiation [104](#__RefHeading___Toc510099530)

8.5.2.1.3.4 Mobility and periodic registration update accepted by the network [104](#__RefHeading___Toc510099531)

8.5.2.1.3.5 Mobility and periodic registration update not accepted by the network [106](#__RefHeading___Toc510099532)

8.5.2.1.3.6 Abnormal cases in the UE [107](#__RefHeading___Toc510099533)

8.5.2.1.3.7 Abnormal cases on the network side [107](#__RefHeading___Toc510099534)

8.5.2.2 De-registration procedure [107](#__RefHeading___Toc510099535)

8.5.2.2.1 General [107](#__RefHeading___Toc510099536)

8.5.2.2.2 UE-initiated de-registration procedure [108](#__RefHeading___Toc510099537)

8.5.2.2.2.1 UE-initiated de-registration procedure initiation [108](#__RefHeading___Toc510099538)

8.5.2.2.2.2 UE-initiated de-registration procedure completion for 5GS services over 3GPP access [109](#__RefHeading___Toc510099539)

8.5.2.2.2.3 UE-initiated de-registration procedure completion for 5GS services over both 3GPP access and non-3GPP access [109](#__RefHeading___Toc510099540)

8.5.2.2.2.4 Abnormal cases in the UE [109](#__RefHeading___Toc510099541)

8.5.2.2.2.5 Abnormal cases in the network side [109](#__RefHeading___Toc510099542)

8.5.2.2.3 Network-initiated de-registration procedure [109](#__RefHeading___Toc510099543)

8.5.2.2.3.1 Network-initiated de-registration procedure initiation [109](#__RefHeading___Toc510099544)

8.5.2.2.3.2 Network-initiated de-registration procedure completion by the UE [110](#__RefHeading___Toc510099545)

8.5.2.2.3.3 Network-initiated de-registration procedure completion by the network [111](#__RefHeading___Toc510099546)

8.5.2.2.3.4 Abnormal cases in the UE [111](#__RefHeading___Toc510099547)

8.5.2.2.3.5 Abnormal cases in the network side [111](#__RefHeading___Toc510099548)

8.5.3 5GMM connection management procedures [111](#__RefHeading___Toc510099549)

8.5.3.1 Service request procedure [111](#__RefHeading___Toc510099550)

8.5.3.1.1 General [111](#__RefHeading___Toc510099551)

8.5.3.1.2 Service request procedure initiation [113](#__RefHeading___Toc510099552)

8.5.3.1.3 Common procedure initiation [114](#__RefHeading___Toc510099553)

8.5.3.1.4 Service request procedure accepted by the network [114](#__RefHeading___Toc510099554)

8.5.3.1.5 Service request procedure not accepted by the network [114](#__RefHeading___Toc510099555)

8.5.3.1.6 Abnormal cases in the UE [115](#__RefHeading___Toc510099556)

8.5.3.1.7 Abnormal cases on the network side [116](#__RefHeading___Toc510099557)

8.5.3.2 Paging procedure [116](#__RefHeading___Toc510099558)

8.5.3.2.1 General [116](#__RefHeading___Toc510099559)

8.5.3.2.2 Paging for 5GS services [116](#__RefHeading___Toc510099560)

8.5.3.2.2.1 General [116](#__RefHeading___Toc510099561)

8.5.3.2.2.2 Abnormal cases on the network side [117](#__RefHeading___Toc510099562)

8.5.3.2.2.3 Abnormal cases in the UE [117](#__RefHeading___Toc510099563)

8.5.3.3 Notification procedure [117](#__RefHeading___Toc510099564)

8.5.3.3.1 General [117](#__RefHeading___Toc510099565)

8.5.3.3.2 Notification procedure initiation [117](#__RefHeading___Toc510099566)

8.5.3.3.3 Notification procedure completion [118](#__RefHeading___Toc510099567)

8.5.3.3.4 Abnormal cases on the network side [118](#__RefHeading___Toc510099568)

8.6 5GS mobility management message coding [119](#__RefHeading___Toc510099569)

8.6.1 Authentication failure [119](#__RefHeading___Toc510099570)

8.6.1.1 Message definition [119](#__RefHeading___Toc510099571)

8.6.2 Authentication reject [119](#__RefHeading___Toc510099572)

8.6.2.1 Message definition [119](#__RefHeading___Toc510099573)

8.6.3 Authentication request [120](#__RefHeading___Toc510099574)

8.6.3.1 Message definition [120](#__RefHeading___Toc510099575)

8.6.3.2 EAP message [120](#__RefHeading___Toc510099576)

8.6.4 Authentication response [120](#__RefHeading___Toc510099577)

8.6.4.1 Message definition [120](#__RefHeading___Toc510099578)

8.6.4.2 EAP message [121](#__RefHeading___Toc510099579)

8.6.5 Registration request [121](#__RefHeading___Toc510099580)

8.6.5.1 Message definition [121](#__RefHeading___Toc510099581)

8.6.5.2 NonceUE [122](#__RefHeading___Toc510099582)

8.6.5.3 5GMM capability [122](#__RefHeading___Toc510099583)

8.6.5.4 UE security capability [122](#__RefHeading___Toc510099584)

8.6.5.5 Requested NSSAI [122](#__RefHeading___Toc510099585)

8.6.5.6 Last visited registered TAI [122](#__RefHeading___Toc510099586)

8.6.5.7 S1 UE network capability [122](#__RefHeading___Toc510099587)

8.6.5.8 Uplink data status [123](#__RefHeading___Toc510099588)

8.6.5.9 PDU session status [123](#__RefHeading___Toc510099589)

8.6.6 Registration accept [123](#__RefHeading___Toc510099590)

8.6.6.1 Message definition [123](#__RefHeading___Toc510099591)

8.6.6.2 5G-GUTI [123](#__RefHeading___Toc510099592)

8.6.6.3 Equivalent PLMNs [123](#__RefHeading___Toc510099593)

8.6.6.4 TAI list [124](#__RefHeading___Toc510099594)

8.6.6.5 Allowed NSSAI [124](#__RefHeading___Toc510099595)

8.6.6.6 Rejected NSSAI [124](#__RefHeading___Toc510099596)

8.6.6.7 Dual registration supported [124](#__RefHeading___Toc510099597)

8.6.6.8 5GMM network feature support [124](#__RefHeading___Toc510099598)

8.6.6.8 PDU session status [124](#__RefHeading___Toc510099599)

8.6.6.8 PDU session reactivation result [124](#__RefHeading___Toc510099600)

8.6.6.8 LADN information [124](#__RefHeading___Toc510099601)

8.6.7 Registration complete [124](#__RefHeading___Toc510099602)

8.6.7.1 Message definition [124](#__RefHeading___Toc510099603)

8.6.8 Registration reject [125](#__RefHeading___Toc510099604)

8.6.8.1 Message definition [125](#__RefHeading___Toc510099605)

8.6.8.2 T3346 value [125](#__RefHeading___Toc510099606)

8.6.9 UL SM message transport for Alternative 1 [125](#__RefHeading___Toc510099607)

8.6.9.1 Message definition [125](#__RefHeading___Toc510099608)

8.6.10 DL SM message transport for Alternative 1 [126](#__RefHeading___Toc510099609)

8.6.10.1 Message definition [126](#__RefHeading___Toc510099610)

8.6.11 UL generic transport for Alternative 1 [126](#__RefHeading___Toc510099611)

8.6.11.1 Message definition [126](#__RefHeading___Toc510099612)

8.6.12 UL NAS transport for Alternative 2 [127](#__RefHeading___Toc510099613)

8.6.12.1 Message definition [127](#__RefHeading___Toc510099614)

8.6.12.2 PDU session ID [128](#__RefHeading___Toc510099615)

8.6.12.3 Old PDU session ID [128](#__RefHeading___Toc510099616)

8.6.12.4 Request type [128](#__RefHeading___Toc510099617)

8.6.12.5 S-NSSAI [128](#__RefHeading___Toc510099618)

8.6.12.6 DNN [128](#__RefHeading___Toc510099619)

8.6.12.7 Additional information [128](#__RefHeading___Toc510099620)

8.6.13 DL generic transport for Alternative 1 [129](#__RefHeading___Toc510099621)

8.6.13.1 Message definition [129](#__RefHeading___Toc510099622)

8.6.14 DL NAS transport for Alternative 2 [129](#__RefHeading___Toc510099623)

8.6.14.1 Message definition [129](#__RefHeading___Toc510099624)

8.6.14.2 PDU session ID [130](#__RefHeading___Toc510099625)

8.6.14.3 Additional information [130](#__RefHeading___Toc510099626)

8.6.15 De-registration request (UE originating de-registration) [130](#__RefHeading___Toc510099627)

8.6.15.1 Message definition [130](#__RefHeading___Toc510099628)

8.6.16 De-registration accept (UE originating de-registration) [131](#__RefHeading___Toc510099629)

8.6.16.1 Message definition [131](#__RefHeading___Toc510099630)

8.6.17 De-registration request (UE terminated de-registration) [131](#__RefHeading___Toc510099631)

8.6.17.1 Message definition [131](#__RefHeading___Toc510099632)

8.6.17.2 5GMM cause [132](#__RefHeading___Toc510099633)

8.6.17.3 T3346 value [132](#__RefHeading___Toc510099634)

8.6.18 De-registration accept (UE terminated de-registration) [132](#__RefHeading___Toc510099635)

8.6.18.1 Message definition [132](#__RefHeading___Toc510099636)

8.6.19 Service request [132](#__RefHeading___Toc510099637)

8.6.19.1 Message definition [132](#__RefHeading___Toc510099638)

8.6.19.2 Uplink data status [133](#__RefHeading___Toc510099639)

8.6.19.3 PDU session status [133](#__RefHeading___Toc510099640)

8.6.19.4 Allowed PDU session status [133](#__RefHeading___Toc510099641)

8.6.20 Service accept [133](#__RefHeading___Toc510099642)

8.6.21.1 Message definition [133](#__RefHeading___Toc510099643)

8.6.21.2 PDU session status [134](#__RefHeading___Toc510099644)

8.6.21.3 PDU session reactivation result [134](#__RefHeading___Toc510099645)

8.6.22 Service reject [134](#__RefHeading___Toc510099646)

8.6.22.1 Message definition [134](#__RefHeading___Toc510099647)

8.6.22.2 PDU session status [134](#__RefHeading___Toc510099648)

8.6.22.3 T3346 value [134](#__RefHeading___Toc510099649)

8.6.23 Configuration update command [135](#__RefHeading___Toc510099650)

8.6.23.1 Message definition [135](#__RefHeading___Toc510099651)

8.6.24 Configuration update complete [135](#__RefHeading___Toc510099652)

8.6.24.1 Message definition [135](#__RefHeading___Toc510099653)

8.6.25 Identity request [136](#__RefHeading___Toc510099654)

8.6.25.1 Message definition [136](#__RefHeading___Toc510099655)

8.6.26 Identity response [136](#__RefHeading___Toc510099656)

8.6.26.1 Message definition [136](#__RefHeading___Toc510099657)

8.6.27 Notification [137](#__RefHeading___Toc510099658)

8.6.27.1 Message definition [137](#__RefHeading___Toc510099659)

8.6.28 5GMM status [137](#__RefHeading___Toc510099660)

8.6.28.1 Message definition [137](#__RefHeading___Toc510099661)

8.6.29 Security mode command [138](#__RefHeading___Toc510099662)

8.6.29.1 Message definition [138](#__RefHeading___Toc510099663)

8.6.29.2 Allowed NSSAI [138](#__RefHeading___Toc510099664)

8.6.29.3 IMEISV request [139](#__RefHeading___Toc510099665)

8.6.29.4 Replayed nonceUE [139](#__RefHeading___Toc510099666)

8.6.29.5 NonceAMF [139](#__RefHeading___Toc510099667)

8.6.29.6 HashAMF [139](#__RefHeading___Toc510099668)

8.6.30 Security mode complete [139](#__RefHeading___Toc510099669)

8.6.30.1 Message definition [139](#__RefHeading___Toc510099670)

8.6.30.2 IMEISV [140](#__RefHeading___Toc510099671)

8.6.30.3 NAS message container [140](#__RefHeading___Toc510099672)

8.6.31.1 Message definition [140](#__RefHeading___Toc510099673)

8.7 5GMM information elements [140](#__RefHeading___Toc510099674)

8.7.1 5GMM cause [140](#__RefHeading___Toc510099675)

8.7.2 NAS key set identifier [141](#__RefHeading___Toc510099676)

8.7.3 Authentication parameter RAND [142](#__RefHeading___Toc510099677)

8.7.4 Authentication parameter AUTN [142](#__RefHeading___Toc510099678)

8.7.5 SM message container (for alternative 1) [142](#__RefHeading___Toc510099679)

8.7.6 Request type [143](#__RefHeading___Toc510099680)

8.7.7 S-NSSAI [143](#__RefHeading___Toc510099681)

8.7.8 DNN [143](#__RefHeading___Toc510099682)

8.7.9 Message container type (for alternative 1) [144](#__RefHeading___Toc510099683)

8.7.10 Message container (for alternative 1) [144](#__RefHeading___Toc510099684)

8.7.14 Additional information (for alternative 2) [145](#__RefHeading___Toc510099685)

8.7.15 Configuration update indication [146](#__RefHeading___Toc510099686)

8.7.16 5GS mobile identity [146](#__RefHeading___Toc510099687)

8.7.17 Tracking area identity list [147](#__RefHeading___Toc510099688)

8.7.18 Service area list [147](#__RefHeading___Toc510099689)

8.7.19 Network name [151](#__RefHeading___Toc510099690)

8.7.20 Time zone [151](#__RefHeading___Toc510099691)

8.7.21 Time zone and time [151](#__RefHeading___Toc510099692)

8.7.22 Daylight saving time [151](#__RefHeading___Toc510099693)

8.7.23 Identity type 2 [151](#__RefHeading___Toc510099694)

8.7.24 Sequence number [151](#__RefHeading___Toc510099695)

8.7.25 Message authentication code [151](#__RefHeading___Toc510099696)

8.7.26 Uplink data status [152](#__RefHeading___Toc510099697)

8.7.27 PDU session status [152](#__RefHeading___Toc510099698)

8.7.28 De-registration type [153](#__RefHeading___Toc510099699)

8.7.29 NSSAI [154](#__RefHeading___Toc510099700)

8.7.30 EAP message [154](#__RefHeading___Toc510099701)

8.7.31 5GMM capability [155](#__RefHeading___Toc510099702)

8.7.32 LADN information [155](#__RefHeading___Toc510099703)

8.7.33 PDU session reactivation result [156](#__RefHeading___Toc510099704)

8.7.34 Old PDU session identity [157](#__RefHeading___Toc510099705)

8.7.35 GPRS timer 2 [157](#__RefHeading___Toc510099706)

8.7.36 Allowed PDU session status [157](#__RefHeading___Toc510099707)

8.7.37 5GS registration type [158](#__RefHeading___Toc510099708)

8.7.38 Tracking area identity [158](#__RefHeading___Toc510099709)

8.7.39 S1 UE network capability [158](#__RefHeading___Toc510099710)

8.7.40 Registration result [158](#__RefHeading___Toc510099711)

8.7.41 PLMN list [158](#__RefHeading___Toc510099712)

8.7.42 5GS network feature support [158](#__RefHeading___Toc510099713)

8.7.43 UE status [159](#__RefHeading___Toc510099714)

8.7.44 IMEISV request [159](#__RefHeading___Toc510099715)

8.7.45 NAS security algorithms [159](#__RefHeading___Toc510099716)

8.7.46 Nonce [160](#__RefHeading___Toc510099717)

8.7.47 UE security capability [160](#__RefHeading___Toc510099718)

8.7.48 HashAMF [164](#__RefHeading___Toc510099719)

8.7.49 NAS message container [164](#__RefHeading___Toc510099720)

8.8 3GPP specific coding information defined within present document [165](#__RefHeading___Toc510099721)

8.8.1 Serving network name (SNN) [165](#__RefHeading___Toc510099722)

8.9 Timers of 5GS mobility management [165](#__RefHeading___Toc510099723)

8.10 Cause values for 5GS mobility management [168](#__RefHeading___Toc510099724)

8.10.1 Causes related to UE identification [168](#__RefHeading___Toc510099725)

8.10.2 Cause related to subscription options [168](#__RefHeading___Toc510099726)

8.10.3 Causes related to PLMN specific network failures and congestion/authentication failures [169](#__RefHeading___Toc510099727)

8.10.4 Causes related to invalid messages [169](#__RefHeading___Toc510099728)

9 5GS session management [170](#__RefHeading___Toc510099729)

9.1 General [170](#__RefHeading___Toc510099730)

9.2 Overview [170](#__RefHeading___Toc510099731)

9.2.1 PDU session types [170](#__RefHeading___Toc510099732)

9.2.2 PDU session management [170](#__RefHeading___Toc510099733)

9.2.3 Local area data network [171](#__RefHeading___Toc510099734)

9.3.4 Types of 5GSM procedures [171](#__RefHeading___Toc510099735)

9.3 5GSM sublayer states [172](#__RefHeading___Toc510099736)

9.3.1 General [172](#__RefHeading___Toc510099737)

9.3.2 5GSM sublayer states in the UE [172](#__RefHeading___Toc510099738)

9.3.2.1 Overview [172](#__RefHeading___Toc510099739)

9.3.2.2 PDU SESSION INACTIVE [172](#__RefHeading___Toc510099740)

9.3.2.3 PDU SESSION ACTIVE PENDING [172](#__RefHeading___Toc510099741)

9.3.2.4 PDU SESSION ACTIVE [173](#__RefHeading___Toc510099742)

9.3.2.5 PDU SESSION INACTIVE PENDING [173](#__RefHeading___Toc510099743)

9.3.2.6 PDU SESSION MODIFICATION PENDING [173](#__RefHeading___Toc510099744)

9.3.2.7 PDU SESSION ACTIVE PENDING [173](#__RefHeading___Toc510099745)

9.3.2.8 PDU SESSION ACTIVE [173](#__RefHeading___Toc510099746)

9.3.2.9 PDU SESSION INACTIVE PENDING [173](#__RefHeading___Toc510099747)

9.3.2.10 PDU SESSION MODIFICATION PENDING [173](#__RefHeading___Toc510099748)

9.3.2.11 PROCEDURE TRANSACTION INACTIVE [173](#__RefHeading___Toc510099749)

9.3.2.12 PROCEDURE TRANSACTION PENDING [173](#__RefHeading___Toc510099750)

9.3.3 5GSM sublayer states in the network [173](#__RefHeading___Toc510099751)

9.3.3.1 Overview [173](#__RefHeading___Toc510099752)

9.3.3.2 PDU SESSION INACTIVE [174](#__RefHeading___Toc510099753)

9.3.3.3 PDU SESSION ACTIVE [174](#__RefHeading___Toc510099754)

9.3.3.4 PDU SESSION INACTIVE PENDING [174](#__RefHeading___Toc510099755)

9.3.3.5 PDU SESSION MODIFICATION PENDING [174](#__RefHeading___Toc510099756)

9.3.3.6 PROCEDURE TRANSACTION INACTIVE [174](#__RefHeading___Toc510099757)

9.3.3.7 PROCEDURE TRANSACTION PENDING [175](#__RefHeading___Toc510099758)

9.4 IP address allocation [175](#__RefHeading___Toc510099759)

9.4.1 General [175](#__RefHeading___Toc510099760)

9.4.2 IP address allocation via NAS signalling [175](#__RefHeading___Toc510099761)

9.5 5GS session management procedures [176](#__RefHeading___Toc510099762)

9.5.1 General [176](#__RefHeading___Toc510099763)

9.5.1.1 Principles of PTI handling for 5GSM procedures [176](#__RefHeading___Toc510099764)

9.5.2 Local PDU session release without NAS signalling [177](#__RefHeading___Toc510099765)

9.5.3 UE-requested PDU session establishment procedure [178](#__RefHeading___Toc510099766)

9.5.3.1 General [178](#__RefHeading___Toc510099767)

9.5.3.2 UE-requested PDU session establishment procedure initiation [178](#__RefHeading___Toc510099768)

9.5.3.3 UE-requested PDU session establishment procedure accepted by the network [180](#__RefHeading___Toc510099769)

9.5.3.4 UE requested PDU session establishment procedure not accepted by the network [182](#__RefHeading___Toc510099770)

9.5.3.4.1 General [182](#__RefHeading___Toc510099771)

9.5.3.4.2 Handling of network rejection due to 5GSM cause #26 [185](#__RefHeading___Toc510099772)

9.5.3.4.3 Handling of network rejection due to 5GSM cause other than 5GSM cause #26 [185](#__RefHeading___Toc510099773)

9.5.3.5 Abnormal cases in the UE [185](#__RefHeading___Toc510099774)

9.5.3.6 Abnormal cases on the network side [185](#__RefHeading___Toc510099775)

9.5.4 PDU session establishment authentication and authorization procedure [186](#__RefHeading___Toc510099776)

9.5.4.1 General [186](#__RefHeading___Toc510099777)

9.5.4.2 PDU session establishment authentication and authorization procedure initiation [187](#__RefHeading___Toc510099778)

9.5.4.3 PDU session establishment authentication and authorization procedure accepted [188](#__RefHeading___Toc510099779)

9.5.4.4 Abnormal cases on the network side [188](#__RefHeading___Toc510099780)

9.5.4.5 Abnormal cases in the UE [188](#__RefHeading___Toc510099781)

9.5.5 UE-requested PDU session modification procedure [188](#__RefHeading___Toc510099782)

9.5.5.1 General [188](#__RefHeading___Toc510099783)

9.5.5.2 UE-requested PDU session modification procedure initiation [188](#__RefHeading___Toc510099784)

9.5.5.3 UE-requested PDU session modification procedure accepted by the network [189](#__RefHeading___Toc510099785)

9.5.5.4 UE-requested PDU session modification procedure not accepted by the network [189](#__RefHeading___Toc510099786)

9.5.5.5 Abnormal cases in the UE [191](#__RefHeading___Toc510099787)

9.5.5.6 Abnormal cases on the network side [192](#__RefHeading___Toc510099788)

9.5.6 Network-requested PDU session modification procedure [192](#__RefHeading___Toc510099789)

9.5.6.1 General [192](#__RefHeading___Toc510099790)

9.5.6.2 Network-requested PDU session modification procedure initiation [192](#__RefHeading___Toc510099791)

9.5.6.3 Network-requested PDU session modification procedure accepted by the UE [193](#__RefHeading___Toc510099792)

9.5.6.4 Network-requested PDU session modification procedure not accepted by the UE [194](#__RefHeading___Toc510099793)

9.5.6.5 Abnormal cases on the network side [194](#__RefHeading___Toc510099794)

9.5.6.6 Abnormal cases in the UE [194](#__RefHeading___Toc510099795)

9.5.7 UE-requested PDU session release procedure [195](#__RefHeading___Toc510099796)

9.5.7.1 General [195](#__RefHeading___Toc510099797)

9.5.7.2 UE-requested PDU session release procedure initiation [195](#__RefHeading___Toc510099798)

9.5.7.3 UE-requested PDU session release procedure accepted by the network [195](#__RefHeading___Toc510099799)

9.5.7.4 UE-requested PDU session release procedure rejected by the network [195](#__RefHeading___Toc510099800)

9.5.7.5 Abnormal cases in the UE [196](#__RefHeading___Toc510099801)

9.5.7.6 Abnormal cases on the network side [196](#__RefHeading___Toc510099802)

9.5.8 Network-requested PDU session release procedure [196](#__RefHeading___Toc510099803)

9.5.8.1 General [196](#__RefHeading___Toc510099804)

9.5.8.2 Network-requested PDU session release procedure initiation [196](#__RefHeading___Toc510099805)

9.5.8.3 Network-requested PDU session release procedure accepted by the UE [197](#__RefHeading___Toc510099806)

9.5.8.4 N1 SM delivery skipped [198](#__RefHeading___Toc510099807)

9.5.8.5 Abnormal cases on the network side [198](#__RefHeading___Toc510099808)

9.5.8.6 Abnormal cases in the UE [198](#__RefHeading___Toc510099809)

9.5.9 5GSM status procedure [198](#__RefHeading___Toc510099810)

9.5.9.1 General [198](#__RefHeading___Toc510099811)

9.5.9.2 5GSM status received in the UE [198](#__RefHeading___Toc510099812)

9.5.9.3 5GSM status received in the SMF [199](#__RefHeading___Toc510099813)

9.6 5GS session management coding [199](#__RefHeading___Toc510099814)

9.6.1 PDU session establishment request [199](#__RefHeading___Toc510099815)

9.6.1.1 Message definition [199](#__RefHeading___Toc510099816)

9.6.1.2 PDU session type [200](#__RefHeading___Toc510099817)

9.6.1.3 SSC mode [200](#__RefHeading___Toc510099818)

9.6.1.4 UE SM capability [200](#__RefHeading___Toc510099819)

9.6.1.5 SM PDU DN request container [200](#__RefHeading___Toc510099820)

9.6.1.6 Extended protocol configuration options [200](#__RefHeading___Toc510099821)

9.6.2 PDU session establishment accept [200](#__RefHeading___Toc510099822)

9.6.2.1 Message definition [200](#__RefHeading___Toc510099823)

9.6.2.2 5GSM cause [201](#__RefHeading___Toc510099824)

9.6.2.3 PDU address [201](#__RefHeading___Toc510099825)

9.6.2.4 EAP message [201](#__RefHeading___Toc510099826)

9.6.2.5 RQ timer value [201](#__RefHeading___Toc510099827)

9.6.2.6 Extended protocol configuration options [201](#__RefHeading___Toc510099828)

9.6.3 PDU session establishment reject [202](#__RefHeading___Toc510099829)

9.6.3.1 Message definition [202](#__RefHeading___Toc510099830)

9.6.3.2 Extended protocol configuration options [202](#__RefHeading___Toc510099831)

9.6.3.3 EAP message [202](#__RefHeading___Toc510099832)

9.6.4 PDU session authentication request [202](#__RefHeading___Toc510099833)

9.6.4.1 Message definition [202](#__RefHeading___Toc510099834)

9.6.4.2 EAP message [203](#__RefHeading___Toc510099835)

9.6.4.3 Extended protocol configuration options [203](#__RefHeading___Toc510099836)

9.6.5 PDU session authentication accept [203](#__RefHeading___Toc510099837)

9.6.5.1 Message definition [203](#__RefHeading___Toc510099838)

9.6.5.2 EAP message [204](#__RefHeading___Toc510099839)

9.6.5.3 Extended protocol configuration options [204](#__RefHeading___Toc510099840)

9.6.7 PDU session modification request [204](#__RefHeading___Toc510099841)

9.6.7.1 Message definition [204](#__RefHeading___Toc510099842)

9.6.7.2 Extended protocol configuration options [204](#__RefHeading___Toc510099843)

9.6.7.3 Requested QoS rules [204](#__RefHeading___Toc510099844)

9.6.8 PDU session modification reject [204](#__RefHeading___Toc510099845)

9.6.8.1 Message definition [204](#__RefHeading___Toc510099846)

9.6.8.2 Extended protocol configuration options [205](#__RefHeading___Toc510099847)

9.6.9 PDU session modification command [205](#__RefHeading___Toc510099848)

9.6.9.1 Message definition [205](#__RefHeading___Toc510099849)

9.6.9.2 5GSM cause [206](#__RefHeading___Toc510099850)

9.6.9.3 Authorized QoS rules [206](#__RefHeading___Toc510099851)

9.6.9.4 Session-AMBR [206](#__RefHeading___Toc510099852)

9.6.9.5 PDU session release time [206](#__RefHeading___Toc510099853)

9.6.9.6 Extended protocol configuration options [206](#__RefHeading___Toc510099854)

9.6.10 PDU session modification accept [206](#__RefHeading___Toc510099855)

9.6.10.1 Message definition [206](#__RefHeading___Toc510099856)

9.6.10.2 Extended protocol configuration options [206](#__RefHeading___Toc510099857)

9.6.11 PDU session modification command reject [207](#__RefHeading___Toc510099858)

9.6.11.1 Message definition [207](#__RefHeading___Toc510099859)

9.6.11.2 Extended protocol configuration options [207](#__RefHeading___Toc510099860)

9.6.12 PDU session release request [207](#__RefHeading___Toc510099861)

9.6.12.1 Message definition [207](#__RefHeading___Toc510099862)

9.6.12.2 Extended protocol configuration options [208](#__RefHeading___Toc510099863)

9.6.13 PDU session release reject [208](#__RefHeading___Toc510099864)

9.6.13.1 Message definition [208](#__RefHeading___Toc510099865)

9.6.13.2 Extended protocol configuration options [208](#__RefHeading___Toc510099866)

9.6.14 PDU session release command [209](#__RefHeading___Toc510099867)

9.6.14.1 Message definition [209](#__RefHeading___Toc510099868)

9.6.1.2 Extended protocol configuration options [209](#__RefHeading___Toc510099869)

9.6.15 PDU session release accept [209](#__RefHeading___Toc510099870)

9.6.15.1 Message definition [209](#__RefHeading___Toc510099871)

9.6.15.2 Extended protocol configuration options [210](#__RefHeading___Toc510099872)

9.6.16 5GSM status [210](#__RefHeading___Toc510099873)

9.6.16.1 Message definition [210](#__RefHeading___Toc510099874)

9.7 5GSM information elements [210](#__RefHeading___Toc510099875)

9.7.1 PDU session type [210](#__RefHeading___Toc510099876)

9.7.2 SSC mode [211](#__RefHeading___Toc510099877)

9.7.3 Extended protocol configuration options [211](#__RefHeading___Toc510099878)

9.7.4 SM PDU DN request container [211](#__RefHeading___Toc510099879)

9.7.5 PDU address [211](#__RefHeading___Toc510099880)

9.7.6 5GSM cause [212](#__RefHeading___Toc510099881)

9.7.7 GPRS timer [213](#__RefHeading___Toc510099882)

9.7.8 UE SM capability [213](#__RefHeading___Toc510099883)

9.8 Timers of 5GS session management [214](#__RefHeading___Toc510099884)

9.9 Cause values for 5GS session management [215](#__RefHeading___Toc510099885)

9.9.1 Causes related to nature of request [215](#__RefHeading___Toc510099886)

9.9.2 Protocol errors (e.g., unknown message) [216](#__RefHeading___Toc510099887)

10 Access to the 5G core network via non-3GPP access networks [217](#__RefHeading___Toc510099888)

10.1 General [217](#__RefHeading___Toc510099889)

10.2 Protocol stack [217](#__RefHeading___Toc510099890)

10.2.1 Control plane protocol stacks [217](#__RefHeading___Toc510099891)

10.2.2 User plane protocol stacks [219](#__RefHeading___Toc510099892)

10.3 NAS over non-3GPP access [219](#__RefHeading___Toc510099893)

10.3.1 General [219](#__RefHeading___Toc510099894)

10.3.2 Mobility management over non-3GPP access [219](#__RefHeading___Toc510099895)

10.3.3 Session management over non-3GPP access [220](#__RefHeading___Toc510099896)

10.4 Registration over non-3GPP access [220](#__RefHeading___Toc510099897)

10.4.1 General [220](#__RefHeading___Toc510099898)

10.4.2 Registration over non-3GPP access [220](#__RefHeading___Toc510099899)

10.4.3 Registration over non-3GPP access and 3GPP access [221](#__RefHeading___Toc510099900)

10.4.4 De-registration over non-3GPP access [221](#__RefHeading___Toc510099901)

10.5 Selection of N3IWF [222](#__RefHeading___Toc510099902)

10.6 Procedures between UE and N3IWF [222](#__RefHeading___Toc510099903)

10.7.1 IKE SA creation procedure for UE registration via untrusted non-3GPP access [222](#__RefHeading___Toc510099904)

10.7.1.1 General [222](#__RefHeading___Toc510099905)

10.7.1.2 IKE SA and signalling IPsec SA establishment procedure [222](#__RefHeading___Toc510099906)

10.7.1.3 EAP-5G procedure for registration over non-3GPP access [223](#__RefHeading___Toc510099907)

10.7.1.4 Abnormal cases in the UE [224](#__RefHeading___Toc510099908)

10.7.1.5 Abnormal cases in the N3IWF [224](#__RefHeading___Toc510099909)

10.7.2 User plane Ipse SA creation procedure for UE-requested PDU session establishment [225](#__RefHeading___Toc510099910)

10.7.2.1 General [225](#__RefHeading___Toc510099911)

10.7.2.2 Child SA creation procedure initiation [225](#__RefHeading___Toc510099912)

10.7.2.3 Child SA creation procedure accepted by the UE [225](#__RefHeading___Toc510099913)

10.7.2.4 Child SA creation procedure not accepted by the UE [225](#__RefHeading___Toc510099914)

10.7.2.5 Abnormal cases in the UE [226](#__RefHeading___Toc510099915)

10.7.2.6 Abnormal cases in the N3IWF [226](#__RefHeading___Toc510099916)

10.7.3 Child SA change procedure for PDU session modification [226](#__RefHeading___Toc510099917)

10.7.4 Child SA deletion procedure for PDU session release [226](#__RefHeading___Toc510099918)

10.7.4.1 General [226](#__RefHeading___Toc510099919)

10.7.4.2 Child SA deletion procedure initiation [226](#__RefHeading___Toc510099920)

10.7.4.3 Child SA deletion procedure accepted by the UE [226](#__RefHeading___Toc510099921)

10.7.4.5 Abnormal cases in the UE [226](#__RefHeading___Toc510099922)

10.7.4.6 Abnormal cases in the N3IWF [226](#__RefHeading___Toc510099923)

10.7.5 IKE SA deletion for de-registration via untrusted non-3GPP access [226](#__RefHeading___Toc510099924)

10.7.5.1 General [227](#__RefHeading___Toc510099925)

10.7.5.2 IKE SA deletion procedure initiation [227](#__RefHeading___Toc510099926)

10.7.5.3 IKE SA deletion procedure accepted by the UE [227](#__RefHeading___Toc510099927)

10.7.5.5 Abnormal cases in the UE [227](#__RefHeading___Toc510099928)

10.7.5.6 Abnormal cases in the N3IWF [227](#__RefHeading___Toc510099929)

10.8 IKEv2 payload extensions [227](#__RefHeading___Toc510099930)

11 Interworking with E-UTRAN connected to EPC [227](#__RefHeading___Toc510099931)

11.1 General [227](#__RefHeading___Toc510099932)

11.2 Single-registration mode [227](#__RefHeading___Toc510099933)

11.2.1 General [227](#__RefHeading___Toc510099934)

11.2.2 Coordination between 5GMM and EMM with N26 interface [227](#__RefHeading___Toc510099935)

11.2.3 Coordination between 5GMM and EMM without N26 interface [228](#__RefHeading___Toc510099936)

11.2.4 Coordination between 5GSM and ESM [229](#__RefHeading___Toc510099937)

11.3 Dual-registration mode [230](#__RefHeading___Toc510099938)

11.4 Core Network selection [231](#__RefHeading___Toc510099939)

12 5G System core network impact on services, network functions and capabilities [231](#__RefHeading___Toc510099940)

12.1 Specific services [231](#__RefHeading___Toc510099941)

12.1.1 Public warning system [231](#__RefHeading___Toc510099942)

12.1.1.1 General [231](#__RefHeading___Toc510099943)

12.1.1.1.1 Service Requirements [231](#__RefHeading___Toc510099944)

12.1.1.1.2 Technology Framework Assumptions [231](#__RefHeading___Toc510099945)

12.1.1.2 Architecture alternative 1: Supporting PWS in 5GS via Service based Interface [231](#__RefHeading___Toc510099946)

12.1.1.2.1 Overview [231](#__RefHeading___Toc510099947)

12.1.1.2.2 Architecture description [231](#__RefHeading___Toc510099948)

12.1.1.2.2.1 PWS architecture [231](#__RefHeading___Toc510099949)

12.1.1.2.2.2 AMF functionality [232](#__RefHeading___Toc510099950)

12.1.1.2.2.3 CBCF functionality [232](#__RefHeading___Toc510099951)

12.1.1.2.2.4 NG-RAN functionality [232](#__RefHeading___Toc510099952)

12.1.1.2.3 Protocol Stack Overview [233](#__RefHeading___Toc510099953)

12.1.1.2.4 CBCF-AMF interface operations [233](#__RefHeading___Toc510099954)

12.1.1.3 Architecture alternative 2: Supporting PWS in 5GS via SBc like Interface [234](#__RefHeading___Toc510099955)

12.1.1.3.1 Overview [234](#__RefHeading___Toc510099956)

12.1.1.3.2 Architecture description [234](#__RefHeading___Toc510099957)

12.1.1.3.2.1 PWS architecture [234](#__RefHeading___Toc510099958)

12.1.1.3.2.2 AMF functionality [235](#__RefHeading___Toc510099959)

12.1.1.3.2.3 CBC functionality [235](#__RefHeading___Toc510099960)

12.1.1.3.2.4 NG-RAN functionality [235](#__RefHeading___Toc510099961)

12.1.1.3.3 NG-RAN Protocol Overview [236](#__RefHeading___Toc510099962)

12.1.1.3.4 CBC-AMF interface [236](#__RefHeading___Toc510099963)

12.1.1.4 Architecture alternative 3: Supporting PWS in 5GS to CBCF and via PWS-IWF to CBC [237](#__RefHeading___Toc510099964)

12.1.1.4.1 Overview [237](#__RefHeading___Toc510099965)

12.1.1.4.2 Architecture description [237](#__RefHeading___Toc510099966)

12.1.1.4.2.1 PWS architecture [237](#__RefHeading___Toc510099967)

12.1.1.4.2.2 AMF functionality [237](#__RefHeading___Toc510099968)

12.1.1.4.2.3 CBCF functionality [238](#__RefHeading___Toc510099969)

12.1.1.4.2.4 CBC functionality [238](#__RefHeading___Toc510099970)

12.1.1.4.2.5 PWS-IWF functionality [238](#__RefHeading___Toc510099971)

12.1.1.4.2.6 NG-RAN functionality [238](#__RefHeading___Toc510099972)

12.1.1.4.3 Protocol Stack Overview [239](#__RefHeading___Toc510099973)

12.1.1.5 Overall evaluation [239](#__RefHeading___Toc510099974)

12.1.2 SMS over NAS [241](#__RefHeading___Toc510099975)

12.1.2.1 Registration requirements [241](#__RefHeading___Toc510099976)

12.1.2.1.1 Initial registration initiation [241](#__RefHeading___Toc510099977)

12.1.2.1.2 Initial registration accepted by the network [241](#__RefHeading___Toc510099978)

12.1.2.1.3 Mobility and periodic registration update initiation [242](#__RefHeading___Toc510099979)

12.1.2.1.4 Mobility and periodic registration update accepted by the network [242](#__RefHeading___Toc510099980)

12.1.3 Emergency services [242](#__RefHeading___Toc510099981)

12.1.3.1 Indication of support of emergency services [242](#__RefHeading___Toc510099982)

12.1.3.2 Handling of emergency service for the UE in limited service state [243](#__RefHeading___Toc510099983)

12.1.3.3 Emergency PDU session setup [243](#__RefHeading___Toc510099984)

12.1.3.4 Handling of local emergency numbers [243](#__RefHeading___Toc510099985)

12.1.3.5 Security procedures for handling emergency services [244](#__RefHeading___Toc510099986)

12.1.3.6 IMS emergency call reattempt [244](#__RefHeading___Toc510099987)

12.1.4 Location services [244](#__RefHeading___Toc510099988)

12.1.5 Multimedia priority services [244](#__RefHeading___Toc510099989)

12.1.5.1 General [244](#__RefHeading___Toc510099990)

12.1.5.2 5GS mobility management priority mechanisms [244](#__RefHeading___Toc510099991)

12.1.5.3 5GS session management priority mechanisms [245](#__RefHeading___Toc510099992)

12.2 Access control [245](#__RefHeading___Toc510099993)

12.2.1 Unified access control (Alternative 1) [245](#__RefHeading___Toc510099994)

12.2.1.1 General [245](#__RefHeading___Toc510099995)

12.2.1.2 Operator-specific access categories [246](#__RefHeading___Toc510099996)

12.2.1.3 Mapping of an access attempts to access category [247](#__RefHeading___Toc510099997)

12.2.2 Access categories, access categorization and access control checking (combined Alternative 2 and Alternative 1) [249](#__RefHeading___Toc510099998)

12.2.2.1 General [249](#__RefHeading___Toc510099999)

12.2.2.2 Determination of the access identities and access category associated with a request for access [250](#__RefHeading___Toc510100000)

12.2.2.3 Operator-defined access categories [251](#__RefHeading___Toc510100001)

12.2.2.4 Access control and checking [252](#__RefHeading___Toc510100002)

12.2.2.4.1 Access control and checking in 5GMM-IDLE mode [252](#__RefHeading___Toc510100003)

12.2.2.4.2 Access control and checking in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication [253](#__RefHeading___Toc510100004)

12.2.2.5 Exception handling and avoiding double barring [254](#__RefHeading___Toc510100005)

12.2.3 Alternative 3 [255](#__RefHeading___Toc510100006)

12.2.3.1 General [255](#__RefHeading___Toc510100007)

12.2.3.2 Access attempts for standardized access categories [255](#__RefHeading___Toc510100008)

12.2.3.2A Operator specific access categories [259](#__RefHeading___Toc510100009)

12.2.3.3 Layers detecting the access attempts [259](#__RefHeading___Toc510100010)

12.2.3.4 Access category selection assistance information [260](#__RefHeading___Toc510100011)

12.2.3.5 Enforcement of unified access control [261](#__RefHeading___Toc510100012)

12.3 Security [263](#__RefHeading___Toc510100013)

12.3.1 General [263](#__RefHeading___Toc510100014)

12.3.2 NAS security mode command [263](#__RefHeading___Toc510100015)

12.3.3 5G NAS security context [263](#__RefHeading___Toc510100016)

12.4 Quality of service (QoS) [263](#__RefHeading___Toc510100017)

12.4.1 General [263](#__RefHeading___Toc510100018)

12.4.1.1 QoS rules [264](#__RefHeading___Toc510100019)

12.4.1.1.1 General [264](#__RefHeading___Toc510100020)

12.4.1.1.2 Signalled QoS rules [264](#__RefHeading___Toc510100021)

12.4.1.1.3 Derived QoS rules [265](#__RefHeading___Toc510100022)

12.4.1.2 Session-AMBR [265](#__RefHeading___Toc510100023)

12.4.1.3 UL user data packet matching [265](#__RefHeading___Toc510100024)

12.4.1.4 Reflective QoS [266](#__RefHeading___Toc510100025)

12.4.1.4.1 General [266](#__RefHeading___Toc510100026)

12.4.1.4.2 Derivation of packet filter for UL direction from DL user data packet [266](#__RefHeading___Toc510100027)

12.4.1.4.3 Creating a derived QoS rule by reflective QoS in the UE [267](#__RefHeading___Toc510100028)

12.4.1.4.4 fUpdating a derived QoS rule by reflective QoS in the UE [267](#__RefHeading___Toc510100029)

12.4.1.4.5 Deleting a derived QoS rule by reflective QoS in the UE [268](#__RefHeading___Toc510100030)

12.4.2 QoS coding [268](#__RefHeading___Toc510100031)

12.4.2.1 QoS rules coding [268](#__RefHeading___Toc510100032)

12.4.2.2 Session-AMBR coding [277](#__RefHeading___Toc510100033)

12.5 IM CN subsystem [279](#__RefHeading___Toc510100034)

12.5.1 IMS voice over PS Session supported Indication [279](#__RefHeading___Toc510100035)

12.5.2 P-CSCF address delivery [280](#__RefHeading___Toc510100036)

12.6 Network sharing [280](#__RefHeading___Toc510100037)

12.7 Congestion and overload control [280](#__RefHeading___Toc510100038)

12.7.1 Handling of NAS level mobility management congestion control [280](#__RefHeading___Toc510100039)

12.7.2 Handling of DNN based congestion control [281](#__RefHeading___Toc510100040)

12.7.3 Handling of S-NSSAI based congestion control [281](#__RefHeading___Toc510100041)

12.8 Charging [282](#__RefHeading___Toc510100042)

12.9 Mission critical services [282](#__RefHeading___Toc510100043)

13 Network slicing [282](#__RefHeading___Toc510100044)

13.1 General [282](#__RefHeading___Toc510100045)

13.2 Mobility management aspects [283](#__RefHeading___Toc510100046)

13.2.1 General [283](#__RefHeading___Toc510100047)

13.2.2 NSSAI storage [283](#__RefHeading___Toc510100048)

13.3 Session management aspects [284](#__RefHeading___Toc510100049)

13.3.1 General [284](#__RefHeading___Toc510100050)

13.3.2 NSSP [284](#__RefHeading___Toc510100051)

14 Conclusions and recommendations [285](#__RefHeading___Toc510100052)

14.1 Work plan and procedures [285](#__RefHeading___Toc510100053)

14.2 Alternatives on NAS transport mechanism [285](#__RefHeading___Toc510100054)

14.3 Mapping to 3GPP TS 24.501 [285](#__RefHeading___Toc510100055)

14.4 Mapping to 3GPP TS 24.502 [287](#__RefHeading___Toc510100056)

14.5 Alternatives on architecture for PWS in 5GS [287](#__RefHeading___Toc510100057)

14.6 Alternatives on unified access control [287](#__RefHeading___Toc510100058)

14.7 Alternatives on steering of UE in VPLMN [287](#__RefHeading___Toc510100059)

Annex A: Impacts to specifications [288](#__RefHeading___Toc510100060)

A.1 New specifications [288](#__RefHeading___Toc510100061)

A.2 Impacted existing specifications [288](#__RefHeading___Toc510100062)

Annex B (informative): Proposed changes to 3GPP TS 23.040 [290](#__RefHeading___Toc510100063)

B.1 First Change [290](#__RefHeading___Toc510100064)

1 Scope [290](#__RefHeading___Toc510100065)

B.2 Next Change [291](#__RefHeading___Toc510100066)

2 References [291](#__RefHeading___Toc510100067)

B.3 Next Change [293](#__RefHeading___Toc510100068)

Annex L (normative): SMS in 5GS [293](#__RefHeading___Toc510100069)

L.1 General [293](#__RefHeading___Toc510100070)

B.4 Next Change [295](#__RefHeading___Toc510100071)

L.2 Support for SMS when UE is registered to both 5GS and EPS [295](#__RefHeading___Toc510100072)

Annex C (informative): Proposed changes to 3GPP TS 24.011 [295](#__RefHeading___Toc510100073)

C.1 First Change [295](#__RefHeading___Toc510100074)

1 Scope [295](#__RefHeading___Toc510100075)

1.1 References [295](#__RefHeading___Toc510100076)

1.2 Abbreviations [296](#__RefHeading___Toc510100077)

C.2 Next Change [297](#__RefHeading___Toc510100078)

2 Overview of Short Message Service (SMS) support [297](#__RefHeading___Toc510100079)

2.1 Protocols and protocol architecture [298](#__RefHeading___Toc510100080)

C.3 Next Change [300](#__RefHeading___Toc510100081)

2.5B 5GSMS entity in N1 mode [300](#__RefHeading___Toc510100082)

C.4 Next Change [301](#__RefHeading___Toc510100083)

3.2 Service provided by the CM‑sublayer [301](#__RefHeading___Toc510100084)

C.5 Next Change [302](#__RefHeading___Toc510100085)

5 CM‑procedures [302](#__RefHeading___Toc510100086)

5.1 General [302](#__RefHeading___Toc510100087)

C.6 Next Change [302](#__RefHeading___Toc510100088)

5.2.2 SMC-GP, SMC-EP and SMC-5G states at the MS side of the radio interface [302](#__RefHeading___Toc510100089)

5.2.2.1 Mobile Originating Case [302](#__RefHeading___Toc510100090)

C.7 Next Change [302](#__RefHeading___Toc510100091)

5.2.4 SMC-GP, SMC-EP and SMC-5G states at the network side of the radio interface [302](#__RefHeading___Toc510100092)

5.2.4.1 Mobile Originating Case [302](#__RefHeading___Toc510100093)

C.8 Next Change [303](#__RefHeading___Toc510100094)

5.3.2.2 RPDU transfer for GPRS, EPS and 5GS [303](#__RefHeading___Toc510100095)

C.9 Next Change [305](#__RefHeading___Toc510100096)

5.4 Concatenating short message or notification transfers [305](#__RefHeading___Toc510100097)

Annex D (informative): Proposed changes to 3GPP TS 24.301 [306](#__RefHeading___Toc510100098)

D.1 Summary of changes [306](#__RefHeading___Toc510100099)

Annex E (informative): Proposed changes to 3GPP TS 24.007 [307](#__RefHeading___Toc510100100)

E.1 First change [307](#__RefHeading___Toc510100101)

11.2.3.1.X PDU session identity [307](#__RefHeading___Toc510100102)

Annex F (informative): Proposed changes to 3GPP TS 24.008 [308](#__RefHeading___Toc510100103)

Annex G: Change history [309](#__RefHeading___Toc510100104)

# Foreword

This Technical Report 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

The present document discusses and describes the CT1 aspects of the 5G System phase 1. In particular, these CT1 aspects include the non-access-stratum (NAS) functions to be performed by the user equipment (UE) in idle mode and the NAS signalling procedures between the UE and the 5G System (5GS) phase 1.

The present document also considers the requirements on the NAS between the UE and the core network which arise from specific services such as public warning system (PWS), SMS over NAS, emergency services, location services (LCS), multimedia priority services (MPS), and also network functions such as access control, security, QoS, IMS, network sharing, charging, congestion and overload control. In addition, the document considers the case of network slicing as well as interworking with E-UTRAN connected to EPC.

The present document is intended as a holding place for CT1 5GS material until it stabilises sufficiently to be moved to appropriate 3GPP technical specifications.

# 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 22.011: "Service accessibility".

[3] 3GPP TS 22.261: "Service requirements for the 5G system; Stage 1".

[4] 3GPP TS 22.268: "Public Warning System (PWS) Requirements".

[5] 3GPP TS 23.003: "Numbering, addressing and identification".

[6] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[7] 3GPP TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".

[8] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[9] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[10] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[11] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[12] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[13] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[14] 3GPP TS 24.250: "Protocol for Reliable Data Service between UE and SCEF; Stage 3".

[15] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[16] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3"

[17] 3GPP TS 24.501: "Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[18] 3GPP TS 24.502: "Access to the 3GPP 5G System (5GS) via non-3GPP access networks; Stage 3"

[19] 3GPP TS 24.568: "WLAN connectivity for 5GS Management Object (MO)"

[20] 3GPP TS 28.530: "Telecommunication management; Management of network slicing in mobile networks; Concepts, use cases and requirements".

[21] 3GPP TS 28.531: "Provisioning of network slicing for 5G networks and services".

[22] 3GPP TS 29.168: "Cell Broadcast Centre interfaces with the Evolved Packet Core".

[23] 3GPP TR 32.899: "Charging management; Study on charging aspects of 5G system architecture phase 1".

[24] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[25] 3GPP TS 36.355: "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP)".

[26] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[27] 3GPP TS 38.304: "New Generation Radio Access Network; User Equipment (UE) procedures in idle mode".

[28] 3GPP TS 38.413: "NG Radio Access Network (NG-RAN); NG Application Protocol (NGAP)".

[29] IETF RFC 3736: "Stateless DHCP Service for IPv6".

[30] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[31] IETF RFC 4191: "Default Router Preferences and More-Specific Routes".

[32] IETF RFC 4282: "The Network Access Identifier".

[33] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[34] IETF RFC 4960: "Stream Control Transmission Protocol".

[35] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

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

[37] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)".

[38] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

[39] 3GPP TS 31.116: "Remote APDU Structure for (U)SIM Toolkit applications".

# 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].

**5GMM-IDLE mode:** In this specification, if the term is used standalone, a UE in 5GMM-IDLE mode means the UE can be either in 5GMM-IDLE mode over 3GPP access or in 5GMM-IDLE mode over non-3GPP access.

**5GMM-CONNECTED mode:** In this specification, if the term is used standalone, a UE in 5GMM-CONNECTED mode means the UE can be either in 5GMM-CONNECTED mode over 3GPP access or in 5GMM-CONNECTED mode over non-3GPP access.

**5GMM-IDLE mode over 3GPP access:** A UE is in 5GMM-IDLE mode **over 3GPP access** when no N1 NAS signalling connection between the UE and network over 3GPP access exists. The term 5GMM-IDLE mode over 3GPP access used in the present document corresponds to the term CM-IDLE state for 3GPP access used in 3GPP TS 23.501 [9].

**5GMM-CONNECTED mode over 3GPP access:** A UE is in 5GMM-CONNECTED mode over 3GPP access when a N1 NAS signalling connection between the UE and network over 3GPP access exists. The term 5GMM-CONNECTED mode over 3GPP access used in the present document corresponds to the term CM-CONNECTED state for 3GPP access used in 3GPP TS 23.501 [9].

**5GMM-IDLE mode over non-3GPP access:** A UE is in 5GMM-IDLE mode over non-3GPP access no N1 NAS signalling connection between the UE and network over non-3GPP access exists. The term 5GMM-IDLE mode over non-3GPP access used in the present document corresponds to the term CM-IDLE state for non-3GPP access used in 3GPP TS 23.501 [9].

**5GMM-CONNECTED mode over non-3GPP access:** A UE is in 5GMM-CONNECTED mode over non-3GPP access when it has N1 NAS signalling connection between the UE and network over non-3GPP access exists. The term 5GMM-CONNECTED mode over non-3GPP access used in the present document corresponds to the term CM-CONNECTED state for non-3GPP access used in 3GPP TS 23.501 [9].

**Access stratum connection:** A peer to peer access stratum connection between either the UE and the NG-RAN for 3GPP access or the UE and the N3IWF for non-3GPP access. The access stratum connection for 3GPP access corresponds to an RRC connection via the Uu reference point. The creation of the access stratum connection for non-3GPP access corresponds to the completion of the IKE\_SA\_INIT exchange (see IETF RFC 7296 [36]) via the NWu reference point.

**DNN based congestion control:** Type of congestion control at session management level that is applied to reject session management requests from UEs or release PDU sessions when the associated DNN is congested.

**EAP-5G:** A vendor-specific EAP method which is used to encapsulate NAS messages between the UE and the N3IWF.

**General NAS level congestion control:** Type of congestion control at mobility management level that is applied at a general overload or congestion situation in the network, e.g. lack of processing resources.

**Last visited registered TAI:** A TAI which is contained in the registration area that the UE registered to the network and which identifies the tracking area last visited by the UE.

**N1 mode:** A mode of a UE allowing access to the 5G core network via the 5G access network.

**N1 NAS signalling connection:** A peer to peer N1 mode connection between UE and AMF. An N1 NAS signalling connection is either the concatenation of an RRC connection via the Uu reference point and an NG connection via the N2 reference point for 3GPP access, or the concatenation of an IPsec tunnel via the NWu reference point and an NG connection via the N2 reference point for non-3GPP access.

**PDU session for LADN:** A PDU session with a DNN associated with a LADN.

**S-NSSAI based congestion control:** Type of congestion control at session management level that is applied to reject session management requests from UEs for a particular S-NSSAI.

**Selected core network type information:** A type of core network (EPC or 5GCN) selected by the UE NAS layer in case of an E-UTRA cell connected to both EPC and 5GCN.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [9] apply:

**5G access network**

**5G core network**

**5G QoS flow**

**5G QoS identifier**

**5G-GUTI**

**5G System**

**5G-S-TMSI**

**Allowed area**

**Allowed NSSAI**

**AMF region**

**AMF set**

**Configured NSSAI**

**Local area data network**

**Network slice**

**NG-RAN**

**Non-allowed area**

**PDU session**

**PDU session type**

**PEI**

**Requested NSSAI**

**SUPI**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.301 [15] apply:

**UE configured to use AC11 – 15 in selected PLMN**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.501 [24] apply:

**5G security context**

**5G NAS security context**

**Current 5G security context**

**Full native 5G security context**

**Native 5G security context**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 38.413 [28] apply:

**NG connection**

## 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].

4G-GUTI 4G-Globally Unique Temporary Identifier

5GCN 5G Core Network

5G-GUTI 5G-Globally Unique Temporary Identifier

5GMM 5GS Mobility Management

5GS 5G System

5GSM 5GS Session Management

5G-S-TMSI 5G S-Temporary Mobile Subscription Identifier

5G-TMSI 5G Temporary Mobile Subscription Identifier

5QI 5G QoS Identifier

AKA Authentication and Key Agreement

AMF Access and Mobility Management Function

DL Downlink

DN Data Network

DNN Data Network Name

E-UTRA Evolved Universal Terrestrial Radio Access

E-UTRAN Evolved Universal Terrestrial Radio Access Network

EAP Extensible Authentication Protocol

EAP-AKA' Improved Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement

EPD Extended Protocol Discriminator

EMM EPS Mobility Management

EPC Evolved Packet Core Network

EPS Evolved Packet System

ESM EPS Session Management

GFBR Guaranteed Flow Bit Rate

GUAMI Globally Unique AMF Identifier

HRPD High Rate Packet Data

LADN Local Area Data Network

LMF Location Management Function

LPP LTE Positioning Protocol

MCS Mission Critical Service

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

N3IWF Non-3GPP Inter-Working Function

NAI Network Access Identifier

NR New Radio

NRAS New Radio Access Stratum

ngKSI Key Set Identifier for Next Generation Radio Access Network

NSSAI Network Slice Selection Assistance Information

NSSP Network Slice Selection Policy

QFI QoS Flow Identifier

QoS Quality of Service

QRI QoS Rule Identifier

RQA Reflective QoS Attribute

RQI Reflective QoS Indication

(R)AN (Radio) Access Network

S-NSSAI Single NSSAI

SA Security Association

SNN Serving Network Name

SMF Session Management Function

UL Uplink

TA Tracking Area

TAC Tracking Area Code

TAI Tracking Area Identity

# 4 Architecture

## 4.1 General

The 5GS architecture is specified in 3GPP TS 23.501 [9] and the stage 2 procedures and flows for 5GS are specified in 3GPP TS 23.502 [10].

## 4.2 Architecture reference model

The 5GS architecture reference model can be represented in two ways; a service-based representation and a reference point representation (see figures 4.2.1, 4.2.2). The service-based representation also includes point-to-point reference points where necessary. The 5GS architecture reference model covers both roaming and non-roaming scenarios in all aspects, including interworking between 5GS and EPS, mobility within 5GS, policy control and charging, and authentication.



Figure 4.2.1: Non-roaming 5GS architecture in reference point representation



Figure 4.2.2: Non-roaming architecture for 5GCN with untrusted non-3GPP access

A UE, which supports 5GS connectivity, can access the 5GCN via a NG-RAN or a standalone non-3GPP access or both. The NAS signalling with the 5GCN control-plane functions is over the N1 reference point. The N11 reference point is used to connect the core access and mobility management function (AMF) and the session management function (SMF). The SMF handles the session management part of the NAS signalling exchanged with the UE. The NWu reference point is used for establishing secure tunnel(s) between the UE and the N3IWF so that control-plane and user-plane exchanged between the UE and the 5GCN is transferred securely over untrusted non-3GPP access. CT1 will specify the N1 and NWu interfaces.

## 4.3 Architecture for interworking with E-UTRAN connected to EPC

Interworking between the 5GS and the EPC through E-UTRAN is supported and specified in 3GPP TS 23.501 [9] as illustrated by the figure 4.3.1. The system interworking procedures are specified in 3GPP TS 23.502 [10].



Figure 4.3.1: Non-roaming architecture for interworking between the 5GS and the EPC/E-UTRAN

The N26 interface is an inter-CN interface between the MME and the AMF used to enable interworking between the EPC and the 5GCN. Support of the N26 interface is optional. However, single-registration mode (see 3GPP TS 23.501 [9]) requires support for N26 interface between the AMF and the MME to enable seamless session continuity (e.g. for voice services) for N1 mode to S1 mode inter-system change and vice versa.

Editor's note: Whether to support the single-registration mode without N26 interface is FFS.

# 5 Network selection procedures

## 5.1 Concepts

The 5GS supports both 3GPP and non-3GPP access networks as specified in 3GPP TS 22.261 [3].

As per 3GPP TS 22.261 [3] the 5G system supports the concept of "network slices" where different 5G radio access networks potentially are connected to network slices of different SSTs. Network slicing is not taken into account for PLMN selection. The network slices are selected only after the UE has registered to a PLMN.

Editor's note: It is for further study how to support the concept of "network slices" of 5G radio access networks.

Requirements on PLMN selection for 3GPP access in 3GPP TS 22.011 [2], clause 3.2 apply together with new requirements specified by 3GPP TS 22.261 [3] subclause 6.19.2.

PLMN selection for 3GPP access does not depend on PLMN selection for non-3GPP access. If a UE is registered over non-3GPP access, the UE performs PLMN selection for 3GPP access independently of the PLMN to which the N3IWF belongs.

Editor's note: It is FFS whether PLMN selection for non-3GPP access depends on PLMN selection for 3GPP access, e.g. PLMN for 3GPP access can be taken into account for PLMN selection for non-3GPP access.

PLMNs selected for 3GPP access and non-3GPP access may be the same or different.

PLMN selection defines a UE-based procedure, whereby candidate PLMNs are selected, one at a time, for attempted registration. Once the PLMN selection has been performed, the UE follows the signalling procedures defined for the selected RAT.

Editor's note: It is for further study whether a common PLMN selection procedure can apply to both 3GPP access and non-3GPP access.

## 5.2 Procedures

### 5.2.1 General

The radio access technology (RAT) identifier associated with each entry in the "User controlled PLMN selector with Access Technology", "Operator controlled PLMN selector with Access Technology" and "HPLMN selector with Access Technology" data files can indicate any combination of the values: GSM, GSM COMPACT, UTRAN, E-UTRAN, cdma2000® 1xRTT, cdma2000® HRPD and NG-RAN access technologies.

NOTE: cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA).

Any signalling procedures after PLMN selection are defined in the specifications related with the radio access technology of the selected PLMN.

### 5.2.2 Procedures for 3GPP radio access networks

#### 5.2.2.1 General

The same procedures for PLMN selection applicable for the GSM, UTRAN and E-UTRAN access technologies as described in 3GPP TS 22.011 [2] and 3GPP TS 23.122 [7] also apply for NG-RAN, with the following additions and exceptions:

- when the UE is informed that an area is forbidden during a registration procedure or a generic UE configuration update procedure, the UE shall take the following action depending on the received 5GMM cause value:

1) #12 (tracking area not allowed);

The UE shall enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE and store the current TAI in the list of "5GS forbidden tracking areas for regional provision of service".

2) #13 (roaming not allowed in this tracking area);

The UE shall enter the state 5GMM-DEREGISTERED.PLMN-SEARCH, store the current TAI in the list of "5GS forbidden tracking areas for roaming" and shall perform PLMN selection according to 3GPP TS 23.122 [7].

The lists of "5GS forbidden tracking areas for roaming" and of "5GS forbidden tracking areas for regional provision of service" shall be erased when:

1) the UE is switched off;

2) the UICC containing the USIM is removed; and

3) periodically (with a period in the range 12 to 24 hours).

When the lists are erased, the UE performs cell selection.

One or more tracking areas are removed from the list of "5GS forbidden tracking areas for roaming" in the UE, as well as the list of "5GS forbidden tracking areas for regional provision of service" if, after a subsequent procedure e.g. registration procedure, one or more tracking areas in the lists are received from the network. If the UE has only one PDU session established which is for emergency services, the tracking areas shall not be removed from these lists if one or more tracking areas in the lists are received from the network.

Each list shall accommodate 40 or more TAIs. When the list is full and a new entry has to be inserted, the oldest entry shall be deleted.

- one single list of forbidden PLMNs ("forbidden PLMNs" list) is sufficient for 5GS. The existing "forbidden PLMNs for GPRS service" and "forbidden PLMNs for attach in S101 mode" lists are not used for 5GS.

Editor's note: It is FFS how RAT restriction is achieved.

#### 5.2.2.2 PLMN selection in 5GMM-CONNECTED mode with RRC inactive indication

The UE shall perform PLMN selection in 5GMM-CONNECTED mode with RRC inactive indication.

### 5.2.3 Procedures for non-3GPP access networks

Editor's note: Currently there are no new requirements available.

### 5.2.4 Procedure for steering of UE in VPLMN

#### 5.2.4.1 Alternative 1 for steering of UE in VPLMN

##### 5.2.4.1.1 General

The purpose of the procedure for steering of UE in VPLMN is to allow the HPLMN to update the list of preferred PLMN/access technology combinations at the UE via NAS signalling. The HPLMN updates the list of preferred PLMN/access technology combinations e.g. depending on the PLMN where the UE is registered or when required by HPLMN operator policies.

The VPLMN shall not be able to modify the list of preferred PLMN/access technology combinations sent by the HPLMN. The UE shall be able to verify that the received list of preferred PLMN/access technology combinations has not been modified.

The procedure for steering of UE in VPLMN can be initiated by the network while the UE is trying to register onto the VPLMN as described in subclause 5.2.4.1.2, or after the UE has registered onto the VPLMN as described in subclause 5.2.4.1.3.

Editor's note: SA3 needs to confirm whether it is feasible to ensure the VPLMN cannot alter the contents of the list of preferred PLMN/access technology combinations sent to the UE by the VPLMN.

Editor's note: End-to-end security between HPLMN and roaming UEs will be defined following SA3 recommendations.

##### 5.2.4.1.2 Procedure for steering of UE in VPLMN during registration

###### 5.2.4.1.2.1 Initiation of the procedure for steering of UE in VPLMN during registration

If the network decides to provide a list of preferred PLMN/access technology combinations to the UE it shall include the list as part of the authentication procedure (see subclause 8.5.1.1.3.2). The AMF shall include the received list of preferred PLMN/access technology combinations in the AUTHENTICATION REQUEST message. The UE shall check the indication included in an AV to determine whether a list of preferred PLMN/access technology combinations was provided by the HPLMN and then perform a security check on the received list of preferred PLMN/access technology combinations. If the list of preferred PLMN/access technology combinations is received and the check is successful, the UE shall proceed as described in subclause 5.2.4.1.2.2. If the indication included in an AV indicates a list of preferred PLMN/access technology combinations was provided by the HPLMN but no list is received, or if the list of preferred PLMN/access technology combinations is received but the security check is not successful, the UE shall proceed as described in subclause 5.2.4.1.2.3.

Editor's note: Additional information included in the NAS message to enable the UE to verify the integrity of the received list of preferred PLMN/access technology combinations needs to be specified in SA3.

###### 5.2.4.1.2.2 Procedure for steering of UE in VPLMN during registration accepted by the UE

Upon receiving an updated list of preferred PLMN/access technology combinations which successfully passes the security check, the UE shall:

- replace the highest priority entries in the "Operator Controlled PLMN Selector with Access Technology" list stored in the ME with the received list of preferred PLMN/access technology combinations;

- delete the PLMNs identified by the received list of preferred PLMN/access technology combinations from the Forbidden PLMN list, if they are present in this list. This includes any information stored in the USIM and the ME internal memory; and

- take the new information into account in subsequent attempts to access a higher priority PLMN.

If the UE determines that there is an available PLMN which is higher priority than the PLMN which the UE is currently camped on, then the UE shall respond with an AUTHENTICATION FAILURE message so that the AMF releases the current N1 NAS signalling connection and aborts the ongoing registration procedure. The UE shall then attempt to obtain service on a higher priority PLMN as specified in 3GPP TS 23.122 [7] by acting as if timer T that controls periodic attempts (see 3GPP TS 23.122 [7]) has expired.

###### 5.2.4.1.2.3 Procedure for steering of UE in VPLMN not accepted by the UE during registration

The UE shall discard the received list of preferred PLMN/access technology combinations and attempt to obtain service on a higher priority PLMN as specified in 3GPP TS 23.122 [7] by acting as if timer T that controls periodic attempts (see 3GPP TS 23.122 [7]) has expired, with an exception that the current PLMN is considered as lowest priority.

##### 5.2.4.1.3 Procedure for steering of UE in VPLMN after registration

###### 5.2.4.1.3.1 Initiation of the procedure for steering of UE in VPLMN after registration

The network intiates the procedure for steering of UE in VPLMN after registration using the NAS transport procedure specified in subclause 8.5.1.3.3, with the Payload container IE of the DL NAS TRANSPORT message set to the list of preferred PLMN/access technology combinations.

Editor's note: The encoding of the list of preferred PLMN/access technology combinations in the DL NAS TRANSPORT message is FFS.

Editor's note: How the need for the UE to send an acknowledgement for the list of preferred PLMN/access technology combinations is conveyed to the UE is FFS.

Editor's note: Additional information included in the NAS message to enable the UE to verify that the received list of preferred PLMN/access technology combinations has not been modified needs to be specified in SA3.

###### 5.2.4.1.3.2 Procedure for steering of UE in VPLMN after registration accepted by the UE

Upon receiving an updated list of preferred PLMN/access technology combinations, the UE shall verify that the received list of preferred PLMN/access technology combinations has not been modified by performing a security check. If the security check passes, the UE shall:

- if the UE needs to send an acknowledgement upon receipt of the list of preferred PLMN/access technology combinations, the UE shall initiate the NAS transport procedure specified in subclause 8.5.1.3.3, with the Payload container type IE of the UL NAS TRANSPORT message indicating that the Payload container IE contains an acknowledgment for a list of preferred PLMN/access technology combinations;

Editor's note: The encoding of the acknowledgement for the list of preferred PLMN/access technology combinations in the UL NAS TRANSPORT message is FFS.

Editor's note: Additional information included in the NAS message to enable the network to verify that the acknowledgement for the list of preferred PLMN/access technology combinations has not been modified and what kind of security check the network performs need to be specified in SA3.

- replace the highest priority entries in the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE with the received list of preferred PLMN/access technology combinations;

- delete the PLMNs identified by the received list of preferred PLMN/access technology combinations from the Forbidden PLMN list, if they are present in this list. This includes any information stored in the USIM and the ME internal memory;

- take the new information into account in subsequent attempts to access a higher priority PLMN; and

- attempt to obtain service on a higher priority PLMN as specified in 3GPP TS 23.122 [7] by acting as if timer T that controls periodic attempts (see 3GPP TS 23.122 [7]) has expired.

###### 5.2.4.1.3.3 Procedure for steering of UE in VPLMN after registration not accepted by the UE

If the security check of the received list of preferred PLMN/access technology combinations fails at the UE, the UE shall perform the following steps in the order in which they are listed:

- if the UE needs to send an acknowledgement upon receipt of the list of preferred PLMN/access technology combinations, the UE shall initiate the NAS transport procedure specified in subclause 8.5.1.3.3, with the Payload container type IE of the UL NAS TRANSPORT message indicating that the Payload container IE contains an acknowledgment for a list of preferred PLMN/access technology combinations;

Editor's note: The encoding of the acknowledgement for the list of preferred PLMN/access technology combinations in the UL NAS TRANSPORT message is FFS.

Editor's note: Additional information included in the NAS message to enable the network to verify that the acknowledgement for the list of preferred PLMN/access technology combinations has not been modified and what kind of security check the network performs need to be specified in SA3.

- discard the received list of preferred PLMN/access technology combinations; and

- attempt to obtain service on a higher priority PLMN as specified in 3GPP TS 23.122 [7] by acting as if timer T that controls periodic attempts (see 3GPP TS 23.122 [7]) has expired, with an exception that the current PLMN is considered as lowest priority. If the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication, the UE may locally release the established N1 NAS signalling connection so as not to delay PLMN selection.

##### 5.2.4.1.4 Completion of the procedure for steering of UE in VPLMN at the network

After initiating the procedure for steering of UE in VPLMN, the network may determine whether the UE has received the list of preferred PLMN/access technology combinations by:

- checking whether the UE has attempted registration on the highest priority VPLMN in the list available in the UE’s location within a timer set to an implementatation specific value; or

- if the network has requested the UE to send an acknowledgement for the list of preferred PLMN/access technology combinations, checking whether an acknowledgement from the UE is received within a timer set to an implementation specific value.

##### 5.2.4.1.5 Stage-2 flow

###### 5.2.4.1.5.1 Stage-2 flow for steering of UE in VPLMN during registration.

The stage-2 flow for the case when the UE registers with VPLMN AMF is described below in figure 5.2.4.1.5.1.1:



Figure 5.2.4.1.5.1.1: Procedure for providing list of preferred PLMN/access technology combinations

1) The UE to the VPLMN AMF: The UE initiates registration by sending REGISTRATION REQUEST message to the VPLMN AMF, and the VPLMN AMF initiates the authentication procedure as defined in 3GPP TS 33.501 [24];

2) The VPLMN AMF to the HPLMN AUSF: The VPLMN AMF sends Authentication Initiation Request (5G-AIR) message to HPLMN AUSF;

3) The HPLMN AUSF to the HPLMN UDM: The HPLMN AUSF sends Auth Info-Req request message to the HPLMN UDM;

4) The HPLMN UDM decides to provide the list of preferred PLMN/access technology combinations to the UE,based on operator policy, and then set an indication in an AV to indicate the UE that the list of preferred PLMN/access technology combinations are provided;

5) The HPLMN UDM to the HPLMN AUSF: The HPLMN UDM sends the list of preferred PLMN/access technology combinations in Auth Info-Resp message along with other existing parameters;

6) The HPLMN AUSF to the VPLMN AMF: The HPLMN AUSF sends the 5G Authentication Initiation Answer (5G-AIA) message to the VPLMN AMF, which includes the protected list of preferred PLMN/access technology combinations and the AV(s);

7) The VPLMN AMF to the UE: The VPLMN AMF transparently sends the list of preferred PLMN/access technology combinations and the AV(s) to the UE in the NAS AUTHENTICATION REQUEST message; and

8) If the UE has successfully authenticated the network(see 3GPP TS 33.501 [24]), after receiving the NAS AUTHENTICATION REQUEST message:

a) The UE checks the indication included in an AV to determine whether a list of preferred PLMN/access technology combinations was provided by the HPLMN and then performs security check on the received preferred PLMN/access technology combinations; and

b) If the list of preferred PLMN/access technology combinations is received and the check is successful in step  8a, then the UE proceeds as described in subclause 5.2.4.1.2.2. If the UE determines that there is a higher priority PLMN than currently camped chosen VPLMN, then the UE shall respond with AUTHENTICATION FAILURE message indicating VPLMN AMF to release the current N1 NAS signalling connection and abort the ongoing registration procedure before performing PLMN selection.If the current chosen PLMN is the highest priority PLMN, the UE shall respond with AUTHENTICATION RESPONSE message and may include a protected acknowledgement IE, if HPLMN requested it. If the indication included in an AV indicates a list of preferred PLMN/access technology combinations was provided by the HPLMN but no list is received; or if the list of preferred PLMN/access technology combinations is received but the security check is not successful in step 8a then the UE shall respond with AUTHENTICATION FAILURE message and proceeds as described in subclause 5.2.4.1.2.3.

NOTE 1: The mechanism in which UE determines there is a higher priority PLMN than currently campend VPLMN in step 8b is UE implementation issue.

NOTE 2: The above procedure shows incremental changes required in authentication procedure(for both EAP-AKA' and 5G AKA) as defined in 3GPP TS 33.501 [24], for sending list of preferred PLMN/access technology combinations to the UE.

NOTE 3: The HPLMN UDM decides to provide the list of preferred PLMN/access technology combinations to the UE,based on operator policy, it is preferred to use it only for first registration in VPLMN otherwise VPLMN may avoid periodic re-authentication of the UE for commercial reasons.

Editor's note: End-to-end security between HPLMN and roaming UEs will be defined following SA3 recommendations.

Editor's note: CT1 will change above procedure to service based interface once SA3 adopts it in their specifications.

###### 5.2.4.1.5.2 Stage-2 flow for steering of UE in VPLMN after registration

The stage-2 flow for the steering of UE in VPLMN after registration is indicated in figure 5.2.4.1.5.2.1.



Figure 5.2.4.1.5.2.1: Procedure for providing list of preferred PLMN/access technology combinations after registration

1. The UDM to the AMF: The UDM notifies the changes of the user profile to the affected AMF by the means of invoking Nudm\_SubscriberDataManagement\_UpdateNotification service operation. The Nudm\_SubscriberDataManagement\_UpdateNotification service operation contains the list of preferred PLMN/access technology combinations that needs to be delivery transparently to the UE over NAS. If the HPLMN decided that the UE is to acknowledge successful security check of the received list of preferred PLMN/access technology combinations, the Nudm\_SubscriberDataManagement\_UpdateNotification service operation also contains an indication that the UDM requests an acknowledgement from the UE.

2. The AMF to the UE: the AMF sends a DL NAS TRANSPORT message to the served UE. The AMF includes in the DL NAS TRANSPORT message the transparent container received from the UDM. If the UE verifies that the list of preferred PLMN/access technology combinations included in the DL NAS TRANSPORT message is provided by HPLMN, the UE stores the list of preferred PLMN/access technology combinations.

Editor's note: How the need for the UE to provide an acknowledgment is encoded in the DL NAS TRANSPORT is FFS.

3. The UE to the AMF: if the UDM has requested an acknowledgement from the UE in the DL NAS TRANSPORT message and the UE verified that the list of preferred PLMN/access technology combinations has been provided by HPLMN, the UE sends an UL NAS TRANSPORT message to the serving AMF with a transparent container including the UE acknowledgement.

4. The AMF to the UDM: the AMF sends an N8 message. If a transparent container with a UE acknowledgement was received in the UL NAS TRANSPORT message, the AMF includes the transparent container in the N8 message. If the HPLMN decided that the UE is to acknowledge successful security check of the received list of preferred PLMN/access technology combinations in step 1, the UDM verifies that the acknowledgement is provided by the UE.

Editor's note: Further messages and further entities might be involved in order to secure the solution.

Editor's note: FFS whether the N8 message is the Nudm\_SubscriberDataManagement\_UpdateNotification response or other N8 message.

##### 5.2.4.1.6 Stage-3 encoding of the list of preferred PLMN/access technology combinations

Editor’s note: It is ffs whether one possibility to encode the list of preferred PLMN/access technology combinations is the secured packet mechanism as specified in 3GPP TS 31.111 [37], 3GPP TS 31.115 [38], and 3GPP TS31.116 [39].

Editor’s note: Other encoding mechanisms are ffs

#### 5.2.4.2 Alternative 2 for steering of UE in VPLMN

##### 5.2.4.2.1 General

The purpose of the procedure for steering of UE in VPLMN is to allow the HPLMN to update the list of preferred PLMN/access technology combinations at the UE via NAS signalling. The HPLMN updates the list of preferred PLMN/access technology combinations e.g. depending on the PLMN where the UE is registered or when required by HPLMN operator policies. The HPLMN may request the UE to acknowledge successful integrity verification of the received list of preferred PLMN/access technology combinations.

The VPLMN shall not be able to modify the list of preferred PLMN/access technology combinations sent by the HPLMN.

The ME of the UE shall be able to verify the integrity of the received list of preferred PLMN/access technology combinations. If the HPLMN requests the UE to acknowledge successful integrity verification of the received list of preferred PLMN/access technology combinations, the ME of the UE shall send a steering acknowledgement to the HPLMN.

The HPLMN shall be able to verify the integrity of the received steering acknowledgement from the UE.

Editor's note: SA3 needs to confirm whether it is feasible to ensure the VPLMN cannot alter the contents of the list of preferred PLMN/access technology combinations sent to the UE by the VPLMN and the steering acknowledgement sent to the HPLMN by the UE via the VPLMN.

Editor's note: End-to-end security between HPLMN and roaming UEs will be defined following SA3 recommendations.

Editor's note: Whether the UE needs to maintain a per PLMN counter to track the number of times the integrity check of the received information has failed is FFS.

##### 5.2.4.2.2 Initiation of the procedure for steering of UE in VPLMN

In order to provide the list of preferred PLMN/access technology combinations to the UE, the AMF shall perform the generic UE configuration update procedure as specified in subclause 8.5.1.3. The AMF shall include the list of preferred PLMN/access technology combinations in the CONFIGURATION UPDATE COMMAND message. The AMF shall require a confirmation response in order to ensure that the list of preferred PLMN/access technology combinations has been updated by the UE.

Editor's note: Additional information included in the NAS message to enable the UE to verify the integrity of the received list of preferred PLMN/access technology combinations needs to be specified in SA3.

##### 5.2.4.2.3 Procedure for steering of UE in VPLMN accepted by the UE

Upon receiving a CONFIGURATION UPDATE COMMAND message with an updated list of preferred PLMN/access technology combinations, the ME of the UE shall verify the integrity of the received list of preferred PLMN/access technology combinations.

If the integrity check of the received list of preferred PLMN/access technology combinations passes, the UE shall:

- if the HPLMN requests the UE to acknowledge successful integrity verification of the received list of preferred PLMN/access technology combinations, the UE shall send a steering acknowledgement to the AMF;

- replace the highest priority entries in the "Operator Controlled PLMN Selector with Access Technology" list stored in the ME with the received list of preferred PLMN/access technology combinations;

- delete the PLMNs identified by the received list of preferred PLMN/access technology combinations from the Forbidden PLMN list, if they are present in this list. This includes any information stored in the USIM and the ME internal memory;

- take the new information into account in subsequent attempts to access a higher priority PLMN; and

- attempt to obtain service on a higher priority PLMN as specified in 3GPP TS 23.122 [7] by acting as if timer T that controls periodic attempts (see 3GPP TS 23.122 [7]) has expired.

##### 5.2.4.2.4 Procedure for steering of UE in VPLMN not accepted by the UE

If the integrity check of the received list of preferred PLMN/access technology combinations fails, the UE shall discard the received list of preferred PLMN/access technology combinations and attempt to obtain service on a higher priority PLMN as specified in 3GPP TS 23.122 [7] by acting as if timer T that controls periodic attempts (see 3GPP TS 23.122 [7]) has expired, with an exception that the current PLMN is considered as lowest priority PLMN.

##### 5.2.4.2.5 Stage-2 flow

The stage-2 flow for the procedure is indicated in figure 5.2.4.2.5.

Figure 5.2.4.2.5: Procedure for providing list of preferred PLMN/access technology combinations

1. The UDM to the AMF: The UDM notifies the changes of the user profile to the affected AMF by the means of invoking Nudm\_SubscriberDataManagement\_UpdateNotification service operation. The Nudm\_SubscriberDataManagement\_UpdateNotification service operation contains the list of preferred PLMN/access technology combinations. If the HPLMN decided that the UE is to acknowledge successful integrity verification of the received list of preferred PLMN/access technology combinations, the Nudm\_SubscriberDataManagement\_UpdateNotification service operation also contains the steering acknowledgement requested indication.

2. The AMF to the UE: the AMF sends a UE configuration update command to the served UE. The AMF includes in the UE configuration update command a UE configuration update cause indicating that the UE is to acknowledge the UE configuration update command. The UE configuration update command contains the list of preferred PLMN/access technology combinations and, if received from UDM, the steering acknowledgement requested indication. If the ME of the UE verifies that the list of preferred PLMN/access technology combinations included in the UE configuration update command is provided by HPLMN, the UE stores the list of preferred PLMN/access technology combinations.

3. The UE to the AMF: the UE sends a UE configuration update command ack to the serving AMF. If the steering acknowledge requested indication was included in the UE configuration update command and the UE verified that the list of preferred PLMN/access technology combinations had been provided by HPLMN, the UE includes the steering acknowledgement in the UE configuration update command ack.

4. The AMF to the UDM: the AMF sends a N12 message. If the steering acknowledgement was received in the UE configuration update command ack, the AMF includes the steering acknowledgement in the N12 message. If the HPLMN decided that the UE is to acknowledge successful integrity verification of the received list of preferred PLMN/access technology combinations in step 1, the UDM verifies that the steering acknowledgement is provided by the ME of the UE.

Editor's note: Further messages and further entities might be involved in order to secure the solution.

Editor's note: FFS whether the N12 message is the Nudm\_SubscriberDataManagement\_UpdateNotification response or other N12 message.

#### 5.2.4.3 Void

##### 5.2.4.3.1 Void

##### 5.2.4.3.2 Void

##### 5.2.4.3.3 Void

##### 5.2.4.3.4 Void

# 6 Stage 3 protocol, general aspects

## 6.1 General

This subclause defines the principal architecture of the 5GS NAS layer 3 protocol and its sublayers, including the message format applied by layer 3.

The layer 3 for 5GS services is composed of three sublayers comprising:

- the 5GS radio resource management (5GRR) functions for NAS over 3GPP access;

- the non-3GPP access functions for NAS over non-3GPP access;

- the 5GS mobility management (5GMM) functions; and

- the 5GS connection management (5GCM) functions.

The 5GS mobility management (5GMM) sublayer is composed of a functional block for:

- the 5GS mobility management (5GMM) functions.

The 5GS connection management (5GCM) sublayer is composed of a functional block for:

- the 5GS session management (5GSM) functions.

NOTE: For NAS over non-3GPP access, the non-3GPP access functions can be supported through functionalities defined in IETF RFC 7296 [36].

## 6.2 Protocols and peer to peer communication

In the model used in the present document, there are:

1) for 5GS services:

- one 5GRR entity in the MS and one 5GRR entity in the network for NAS over 3GPP access;

- one non-3GPP access management entity in the MS and one non-3GPP access interworking entity in the N3IWF for the NAS over non-3GPP access;

- one 5GMM entity in the MS and one 5GMM entity in the network;

- for each functional block of the 5GCM sublayer as defined in subclause 6.1 which is supported in the MS (in the network), there are, depending on the protocol, one or more entities in the MS (in the network). Two different entities of the same functional block in the MS (in the network) are called parallel entities. The entities of the same functional block in the MS correspond in a one-to-one relation to the entities of the functional block in the network. The corresponding entities are called peer entities.

## 6.3 Basic groups of functions

Most functions of layer 3 and its sub-layers are described by the service specifications and protocol specifications of the (sub-)layers.

These functions are in the model realized by protocol control entities, see subclause 6.2.

In addition, routing functions are contained in layer 3 which are related to the transport of messages, e.g. multiplexing and splitting. These routing functions are defined in the 5GRR (for NAS over 3GPP access) or non-3GPP access management (for NAS over non-3GPP access) and 5GMM sub-layers.

1) They have the task to pass the messages from upper (sub-)layers to lower (sub-)layers.

2) They also have the task to pass messages provided by lower (sub-)layers to the appropriate (sub-)layer and, if applicable, entity.

The routing functions with task 2 make use of the extended protocol discriminator (EPD) which is part of the message header, or PDU session identity.

A 5GCM sublayer protocol may also define a procedure transaction identity (PTI) as a part of the message header. This is at least the case if there are parallel entities of the same functional block, see subclause 6.2.

- The 5GMM-sublayer routing function passes the messages of the 5GCM entities as well as of the 5GMM entities of its own sublayer to the service access point of 5GRR. Furthermore, it multiplexes them in case of parallel transactions.

- For NAS over 3GPP access, the new radio access stratum (NRAS) sublayer routing function distributes the messages to be sent according to their message type and protocol discriminator (PD), to the actual channel configuration, and, if applicable, to further information received from upper sub-layers to the appropriate service access point of layer 2. Paging messages received from the PCH are always routed to 5GMM.

- For NAS over 3GPP access, the messages provided at the different service access points of layer 2 are distributed by the 5GRR sublayer routing function according to their protocol discriminator (PD). Messages with a PD equal to RR are passed to the 5GRR entity of the own sublayer, all other messages are passed to the 5GMM sublayer at the service access point RR-SAP.

- For NAS over non-3GPP access:

- for initial registration, EAP-5G is used to transfer NAS messages between the peer entities of the 5GMM sublayers;

- after successful initial registration, IPSec transport mode and GRE will be used to encapsulate and un-encapsulate the NAS messages between the peer entities of the 5GMM sublayers.

- For 5GS services, the routing function of 5GS NAS passes standard L3 messages according to the protocol discriminator (PD) and, if applicable, the PDU session identity towards the 5GMM entity or towards the 5GSM entities of the various 5GS NAS SAP's.

The message (message header or other parts of the message) are neither changed nor removed by the RR routing function or non-3GPP access management or 5GMM routing function before passing it to the appropriate service access point.

## 6.4 Protocol architecture

The protocol architecture is visualized for each of the 5GS model:

- Figure 6.4.1 shows the protocol architecture for a MS supporting 5GS services over 3GPP access.

- Figure 6.4.2 shows the protocol architecture for a MS supporting 5GS services over non-3GPP access.



Figure 6.4.1: Protocol architecture of Non Access Stratum supporting MSs, MS‑side (over 3GPP access)



Figure 6.4.2: Protocol architecture of Non Access Stratum supporting MSs, MS‑side (over non-3GPP access)

Figure 6.4.1 defines three sublayers for 5GS services:

- the NRAS sublayer provides services to the 5GMM sublayer;

- the 5GMM sublayer provides services to the entities of the 5GCM sublayer. The 5GMM sublayer further includes one 5GMM entity;

- the 5GCM sublayer includes 5GSM entities;

- the 5GSM entity provides services to the QoS flow control (QFC) entity and uses services of the 5GMM sublayer;

- the QFC entity hides the concepts of radio resources that can be established/released while an 5GS context is active. If uplink data in the terminal is to be sent, and 5GS radio resources have been released, the QFC will trigger a service request procedure in 5GMM.

Figure 6.4.2 defines three sublayers for 5GS services:

- the Non-3GPP access stratum sublayer provides services to the 5GMM sublayer;

- the 5GMM sublayer provides services to the entities of the 5GCM sublayer. The 5GMM sublayer further includes one 5GMM entity;

- the 5GCM sublayer includes 5GSM entities;

- the 5GSM entity provides services to the QoS flow control (QFC) entity and uses services of the 5GMM sublayer;

- the QFC entity hides the concepts of non-3GPP access resources that can be established/released while a 5GS context is active. Whenever such resources are available, IPSec security associations will be established and maintained.

## 6.5 Standard L3 messages

Editor's note: 5GS NAS message IE applicability, 5GS NAS message standard L3 header, 5GS Protocol discriminator values, Possible new 5GS identities for routing and 5GS message type should be captured in this subclause.

## 6.6 General message format and information elements coding

Editor's note: The content of this sub-clause has been moved to 3GPP TS 24.501 [17], and therefore this sub-clause is no longer maintained.

### 6.6.1 Overview

Within the protocols defined in the present document, every 5GS NAS message is a standard L3 message as defined in 3GPP TS 24.007 [11]. This means that the message consists of the following parts:

Editor's note: The required updates on a standard L3 message definition in 3GPP TS 24.007 [11] are FFS.

1) if the message is a plain 5GS NAS message:

a) extended protocol discriminator;

b) security header type or PDU session identity;

c) procedure transaction identity;

d) message type;

e) other information elements, as required.

2) if the message is a security protected 5GS NAS message:

Editor's note: The message parts of a security protected 5GS NAS message are FFS.

The organization of a plain 5GS NAS message is illustrated in the example shown in figure 6.6.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Extended protocol discriminator | | | | | | | | octet 1 |
| Security header type associated with a spare half octet; or  PDU session identity | | | | | | | | octet 2 |
| Procedure transaction identity | | | | | | | | octet 3 |
| Message type | | | | | | | | octet 4 |
|  | | | | | | | | octet 5 |
| Other information elements as required | | | | | | | |  |
|  | | | | | | | | octet n |

Figure 6.6.1.1: General message organization example for a plain 5GS NAS message

Editor's note: The organization of a security protected 5GS NAS message is FFS.

Unless specified otherwise in the message descriptions of clause 8 and clause 9, a particular information element shall not be present more than once in a given message.

When a field extends over more than one octet, the order of bit values progressively decreases as the octet number increases. The least significant bit of the field is represented by the lowest numbered bit of the highest numbered octet of the field.

#### 6.6.2 Extended protocol discriminator

Bits 1 to 8 of the first octet of every 5GS NAS message contain the Extended protocol discriminator (EPD) IE. The EPD and its use are defined in 3GPP TS 24.007 [11]. Bits 1 to 4 of the EPD in the header of a plain 5GMM message is encoded as "1110".

Editor's note: The definition of the extended protocol discriminator in 3GPP TS 24.007 [11] is FFS.

#### 6.6.3 Security header type

Bits 1 to 4 of the second octet of every 5GMM message contain the Security header type IE. This IE includes control information related to the security protection of a 5GMM message. The total size of the Security header type IE is 4 bits.

Editor's note: The values of the Security header type are FFS.

#### 6.6.4 PDU session identity

Bits 1 to 8 of the second octet of every 5GSM message contain the PDU session identity IE. The PDU session identity and its use to identify a message flow are defined in 3GPP TS 24.007 [11]. See Annex E.

#### 6.6.5 Spare half octet

Bits 5 to 8 of the second octet of every 5GMM message contains the spare half octet which is filled with spare bits set to zero.

#### 6.6.6 Procedure transaction identity

Bits 1 to 8 of the third octet of every 5GSM message contain the procedure transaction identity. The procedure transaction identity and its use are defined in 3GPP TS 24.007 [11].

#### 6.6.7 Message type

The message type IE and its use are defined in 3GPP TS 24.007 [11].

Editor's note: The values of message type for 5GS NAS messages are FFS.

## 6.7 Handling of unknown, unforeseen, and erroneous protocol data

Editor's note: The content of this sub-clause has been moved to 3GPP TS 24.501 [17], and therefore this sub-clause is no longer maintained.

### 6.7.1 General

The procedures specified in the present document apply to those messages which pass the checks described in this subclause.

This subclause also specifies procedures for the handling of unknown, unforeseen, and erroneous protocol data by the receiving entity. These procedures are called "error handling procedures", but in addition to providing recovery mechanisms for error situations they define a compatibility mechanism for future extensions of the protocols.

Subclauses 6.7.1 to 6.7.7 shall be applied in order of precedence.

Detailed error handling procedures in the network are implementation dependent and may vary from PLMN to PLMN. However, when extensions of this protocol are developed, networks will be assumed to have the error handling that is indicated in this subclause as mandatory ("shall") and that is indicated as strongly recommended ("should").

Also, the error handling of the network is only considered as mandatory or strongly recommended when certain thresholds for errors are not reached during a dedicated connection.

For definition of semantical and syntactical errors see 3GPP TS 24.007 [11], subclause 11.4.2.

Editor's note: It is FFS to add more details and further alignment to align with 3GPP TS 24.301.

### 6.7.2 Message too short

When a message is received that is too short to contain a complete message type information element, that message shall be ignored, cf. 3GPP TS 24.007 [11].

### 6.7.3 Unknown or unforeseen procedure transaction identity or PDU Session identity

#### 6.7.3.1 Procedure transaction identity

Editor's note: It is FFS to add the content.

#### 6.7.3.2 PDU Session identity

Editor's note: It is FFS to add the content.

### 6.7.4 Unknown or unforeseen message type

If UE receives an 5GMM message or 5GSM message with message type not defined for the extended protocol discriminator (EPD) or not implemented by the receiver, it shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #97 "message type non-existent or not implemented".

If the network receives an 5GMM or 5GSM message with message type not defined for the EPD or not implemented by the receiver in a protocol state where reception of an unsolicited message with the given EPD from the UE is not foreseen in the protocol, the network actions are implementation dependent. Otherwise, if the network receives a message with message type not defined for the EPD or not implemented by the receiver, it shall ignore the message except that it should return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #97 "message type non-existent or not implemented".

NOTE: A message type not defined for the EPD in the given direction is regarded by the receiver as a message type not defined for the EPD, see 3GPP TS 24.007 [11].

If the UE receives a message not compatible with the protocol state, the UE shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #98 "message type not compatible with protocol state".

If the network receives a message not compatible with the protocol state, the network actions are implementation dependent.

### 6.7.5 Non-semantical mandatory information element errors

#### 6.7.5.1 Common procedures

When on receipt of a message,

- an "imperative message part" error; or

- a "missing mandatory IE" error

is diagnosed or when a message containing:

- a syntactically incorrect mandatory IE;

- an IE unknown in the message, but encoded as "comprehension required" (see 3GPP TS 24.007 [11]); or

- an out of sequence IE encoded as "comprehension required" (see 3GPP TS 24.007 [11]) is received,

the UE shall proceed as follows:

If the message is not one of the messages listed in subclause 6.7.5.3, item TBD, the UE shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #96 "invalid mandatory information"; and

Editor's note: Specific cases when the above is not applicable are FFS.

the network shall proceed as follows:

If the message is not one of the messages listed in subclause 6.7.5.3, item TBD, the network shall either:

- try to treat the message (the exact further actions are implementation dependent); or

- ignore the message except that it should return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #96 "invalid mandatory information".

Editor's note: Specific cases when the above is not applicable are FFS.

#### 6.7.5.2 5GS mobility management

Editor's note: It is FFS to add the content.

#### 6.7.5.3 5GS session management

Editor's note: It is FFS to add the content.

### 6.7.6 Unknown and unforeseen IEs in the non-imperative message part

#### 6.7.6.1 IEIs unknown in the message

The UE shall ignore all IEs unknown in a message which are not encoded as "comprehension required" (see 3GPP TS 24.007 [11]).

The network shall take the same approach.

#### 6.7.6.2 Out of sequence IEs

The UE shall ignore all out of sequence IEs in a message which are not encoded as "comprehension required" (see 3GPP TS 24.007 [11]).

The network should take the same approach.

#### 6.7.6.3 Repeated IEs

If an information element with format T, TV, TLV, or TLV-E is repeated in a message in which repetition of the information element is not specified in clause 8 and clause 9 of the present document, the UE shall handle only the contents of the information element appearing first and shall ignore all subsequent repetitions of the information element. When repetition of information elements is specified, the UE shall handle only the contents of specified repeated information elements. If the limit on repetition of information elements is exceeded, the UE shall handle the contents of information elements appearing first up to the limit of repetitions and shall ignore all subsequent repetitions of the information element.

The network should follow the same procedures.

### 6.7.7 Non-imperative message part errors

This category includes:

- syntactically incorrect optional IEs; and

- conditional IE errors.

#### 6.7.7.1 Syntactically incorrect optional IEs

The UE shall treat all optional IEs that are syntactically incorrect in a message as not present in the message.

The network shall take the same approach.

#### 6.7.7.2 Conditional IE errors

When upon receipt of a 5GMM or 5GSM message the UE diagnoses a "missing conditional IE" error or an "unexpected conditional IE" error, or when it receives a 5GMM or 5GSM message containing at least one syntactically incorrect conditional IE, the UE shall ignore the message and shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #100 "conditional IE error".

When the network receives a message and diagnoses a "missing conditional IE" error or an "unexpected conditional IE" error or when it receives a message containing at least one syntactically incorrect conditional IE, the network shall either:

- try to treat the message (the exact further actions are implementation dependent); or

- ignore the message except that it should return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #100 "conditional IE error".

### 6.7.8 Messages with semantically incorrect contents

When a message with semantically incorrect contents is received, the UE shall perform the foreseen reactions of the procedural part of the present document (i.e. of clauses 8, 9). If, however no such reactions are specified, the UE shall ignore the message except that it shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #95 "semantically incorrect message".

The network should follow the same procedure except that a status message is not normally transmitted.

# 7 Coordination between the protocols for 5GS mobility management and 5GS session management

Editor's note: The content of this sub-clause has been moved to 3GPP TS 24.501 [17], and therefore this sub-clause is no longer maintained.

A 5GS session management (5GSM) message is piggybacked in specific 5GS mobility management (5GMM) transport messages. To this purpose, the 5GSM messages can be transmitted in an information element in the 5GMM transport messages. In this case, the UE, the AMF and the SMF execute the 5GMM procedure and the 5GSM procedure in parallel. The success of the 5GMM procedure is not dependent on the success of the piggybacked 5GSM procedure.

The UE can only initiate the 5GSM procedure when there is a 5GMM context established at the UE and the AMF can only forward the 5GSM message for the 5GSM procedure initiated by the SMF when there is a 5GMM context established at the AMF.

Except for the 5GMM procedures piggybacking 5GSM messages, during 5GMM procedures the UE and the AMF shall suspend the transmission of 5GSM messages.

Editor's note: Which type of procedure will be included as 5GMM procedure is FFS.

# 8 5GS mobility management

Editor's note: The content of this sub-clause has been moved to 3GPP TS 24.501 [17], and therefore this sub-clause is no longer maintained.

## 8.1 Overview

### 8.1.1 General

The main function of the 5GS mobility management (5GMM) sublayer is to support the identification, security, mobility of a UE as well as generic message transport.

A further function of the 5GMM sublayer is to provide connection management services to the other sublayer(s).

Editor's note: Sublayer design can be revisited after the protocol framework is identified.

### 8.1.2 Domain selection

#### 8.1.2.1 UE’s usage setting

The UE’s usage setting defined in 3GPP TS 24.301 [15] applies to voice capable UEs in 5GS and indicates whether the UE has preference for voice services over data services or vice-versa, where:

- voice services include IMS voice; and

- data services include any kind of user data transfer without a voice media component.

The UE’s usage setting can be set to:

- "voice centric"; or

- "data centric".

If the UE is capable of S1 mode, there is a single UE’s usage setting at the UE which applies to both 5GS and EPS.

Editor's note: The definition of the UE’s usage setting in TS 24.301 needs to be updated to be applicable to 5GS.

#### 8.1.2.2 Domain selection for UE originating sessions / calls

The behaviour of the UE for domain selection is determined by:

- the UE usage setting;

- the availability of IMS voice; and

- whether the UE operates in single-registration mode or dual-registration mode (see 3GPP TS 23.501 [9]).

In the present document, "IMS voice not available" refers to one of the following conditions:

a) the UE does not support IMS voice;

b) the UE supports IMS voice, but the network indicates in the REGISTRATION ACCEPT message that IMS voice over PS sessions are not supported; or

c) the UE supports IMS voice, the network indicates in the REGISTRATION ACCEPT message that IMS voice over PS sessions are supported, but the upper layers:

- provide no indication that the UE is available for voice call in the IMS within a manufacturer determined period of time; or

- indicate that the UE is not available for voice calls in the IMS.

NOTE: If conditions a and b evaluate to false, the upper layers need time to attempt IMS registration. In the event an indication from the upper layers that the UE is available for voice calls in the IMS takes longer than the manufacturer determined period of time (e.g. due to delay when attempting IMS registration or due to delay in obtaining a QoS flow for SIP signalling), the NAS layer assumes the UE is not available for voice calls in the IMS.

Other conditions may exist but these are implementation specific.

In the present document, "IMS voice available" applies when "IMS voice not available" does not apply.

When IMS voice is not available, if the UE’s usage setting is "voice centric" and the UE operates in single-registration mode, the UE shall disable the N1 mode radio capabilities (see subclause 8.2.6), and attempt to select an E-UTRA cell connected to EPC. If such a cell is found, the UE shall then perform voice domain selection procedures as defined in 3GPP TS 24.301 [15].

When IMS voice is not available, if the UE’s usage setting is "voice centric" for 5GS and the UE operates in dual-registration mode, the UE may disable the N1 mode radio capabilities (see subclause 8.2.6), and attempt to select an E-UTRA cell connected to EPC. If such a cell is found, the UE shall then perform voice domain selection procedures as defined in 3GPP TS 24.301 [15].

#### 8.1.2.3 Change of UE’s usage setting

Whenever the UE's usage setting changes, the UE shall execute procedures according to table 8.1.2.3.1 and table 8.1.2.3.2:

a) The UE is in single registration mode

Table 8.1.2.3.1: Change of UE's usage setting for a UE in single registration mode

|  |  |
| --- | --- |
| UE's usage setting change | Procedure to execute |
| From "data centric" to "voice centric" and "IMS voice not available" | Disable the N1 mode radio capabilities (see subclause 8.2.6) |
| From "voice centric" to "data centric" and the N1 mode radio capabilities are disabled at the UE | Re-enable the N1 mode radio capabilities (see subclause 8.2.6) |

b) The UE is in dual registration mode

Table 8.1.2.3.2: Change of UE's usage setting for a UE in dual registration mode

|  |  |
| --- | --- |
| UE's usage setting change | Procedure to execute |
| From "data centric" to "voice centric" and "IMS voice not available" | Disable the N1 mode radio capabilities (see subclause 8.2.6) |
| From "voice centric" to "data centric" and the N1 mode radio capabilities are disabled at the UE | Re-enable the N1 mode radio capabilities (see subclause 8.2.6) |

#### 8.1.2.4 Change or determination of IMS voice availability

Whenever the IMS voice availability is determined or changes, the UE shall execute procedures according to table 8.1.2.4.1 and table 8.1.2.4.2:

a) The UE is in single registration mode

Table 8.1.2.4.1: Change of IMS voice availability for a UE in single registration mode

|  |  |
| --- | --- |
| Change of IMS voice available condition | Procedure to execute |
| IMS voice not available and the UE’s usage setting is "voice centric" | Disable the N1 mode radio capabilities (see subclause 8.2.6) |
| IMS voice available and the N1 mode radio capabilities are disabled at the UE | Re-enable the N1 mode radio capabilities (see subclause 8.2.6) |

b) The UE is in dual registration mode

Table 8.1.2.4.2: Change of IMS voice availability for a UE in dual mode

|  |  |
| --- | --- |
| **Change of IMS voice available condition** | **Procedure to execute** |
| IMS voice not available and the UE’s usage setting is "voice centric" | Disable the N1 mode radio capabilities (see subclause 8.2.6) |
| IMS voice available and the N1 mode radio capabilities are disabled at the UE | Re-enable the N1 mode radio capabilities (see subclause 8.2.6) |

### 8.1.3 Types of 5GMM procedures

Depending on how they can be initiated, three types of 5GMM procedures can be distinguished:

1) 5GMM common procedures

5GMM common procedure can always be initiated when the UE is in 5GMM-CONNECTED mode. The procedures belonging to this type are:

Initiated by the network:

- network-initiated NAS transport.

- primary authentication and key agreement procedure

- security mode control;

- generic UE configuration update

- identification

Initiated by the UE:

- UE-initiated NAS transport.

Initiated by the UE or the network and used to report certain error conditions detected upon receipt of 5GMM protocol data:

- 5GMM status.

2) 5GMM specific procedures:

At any time only one UE initiated 5GMM specific procedure can be running for each of the access network(s) that the UE is camping in. The procedures belonging to this type are:

Initiated by the UE and used e.g. to register to the network for 5GS services and establish a 5GMM context, to update the location/parameter(s) of the UE:

- registration.

Initiated by the UE or the network and used to deregister from the network for 5GS services and to release a 5GMM context:

- de-registration.

3) 5GMM connection management procedures:

Initiated by the UE and used to establish a secure connection to the network or to request the resource reservation for sending data, or both:

- service request.

The service request procedure can only be initiated if no UE initiated 5GMM specific procedure is ongoing for each of the access network(s) that the UE is camping in.

Initiated by the network and used to request the establishment of an N1 NAS signalling connection or to prompt the UE to perform re-registration if necessary as a result of a network failure; not applicable for the non-3GPP access network:

- paging.

Initiated by the network and used to request re-activation the PDU session(s) associated with non-3GPP access over 3GPP access when the UE is in 5GMM-CONNECTED mode over either 3GPP access or non 3GPP access:

- notification.

NOTE: The network can page the UE over 3GPP access for the re-activation of the PDU session(s) associated with non-3GPP access over 3GPP access.

### 8.1.4 5GMM sublayer states

#### 8.1.4.1 General

In the following subclauses, the 5GS mobility management (5GMM) sublayer of the UE and the network is described by means of different state machines. The 5GMM sublayer states is managed per access type independently, i.e. 3GPP access or non-3GPP access. In subclause 8.1.4.2, the states of the 5GMM sublayer are introduced.

#### 8.1.4.2 5GMM sublayer states

##### 8.1.4.2.1 General

In the following subclauses, the possible 5GMM sublayer states are described. In subclause 8.1.4.2.2, the states of the 5GMM sublayer in the UE are introduced. The behaviour of the UE depends on a 5GS update status that is described in subclause 8.1.4.2.3. The states for the network side are described in subclause 8.1.4.2.4.

##### 8.1.4.2.2 5GMM sublayer states in the UE

###### 8.1.4.2.2.1 General

In the following subclauses, the possible 5GMM sublayer states of the UE are described and shown in Figure 8.1.4.2.2.1.1.



NOTE: Not all possible transitions are shown in this figure.

Editor's note: The fatal causes and non-fatal causes used in the 5GMM procedures are FFS.

Figure 8.1.4.2.2.1.1: 5GMM main states in the UE

###### 8.1.4.2.2.2 Main states

8.1.4.2.2.2.1 5GMM-NULL

5GS services are disabled in the UE. No 5GS mobility management function shall be performed in this state.

8.1.4.2.2.2.2 5GMM-DEREGISTERED

In the state 5GMM-DEREGISTERED, no 5GMM context has been established and the UE location is unknown to the network and hence it is unreachable by a network. In order to establish a 5GMM context, the UE shall start the initial registration procedure.

8.1.4.2.2.2.3 5GMM-REGISTERED-INITIATED

A UE enters the state 5GMM-REGISTERED-INITIATED after it has started the initial registration procedure or the non-initial registration procedure, excluding the periodic regstriation update over non-3GPP access, and is waiting for a response from the network.

8.1.4.2.2.2.4 5GMM-REGISTERED

In the state 5GMM-REGISTERED, a 5GMM context has been established. Additionally, one or more PDU session context(s) may be activated at the UE. The UE may initiate the non-initial registration procedure (including the normal regstriation update and periodic registration update) and the service request procedure. The UE in the state 5GMM-REGISTERED over non-3GPP access shall not initiate the periodic registration update procedure.

8.1.4.2.2.2.5 5GMM-DEREGISTERED-INITIATED

A UE enters the state 5GMM-DEREGISTERED-INITIATED after it has requested release of the 5GMM context by starting the de-registration procedure and is waiting for a response from the network.

8.1.4.2.2.2.6 5GMM-SERVICE-REQUEST-INITIATED

A UE enters the state 5GMM-SERVICE-REQUEST-INITIATED after it has started the service request procedure and is waiting for a response from the network.

###### 8.1.4.2.2.3 Substates of state 5GMM-DEREGISTERED

8.1.4.2.2.3.1 General

The state 5GMM-DEREGISTERED is subdivided into a number of substates as described in this subclause. The following substates are not applicable to non-3GPP access:

- 5GMM-DEREGISTERED.LIMITED-SERVICE;

- 5GMM-DEREGISTERED.PLMN-SEARCH:

- 5GMM-DEREGISTERED.NO-SUPI;

- 5GMM-DEREGISTERED.NO-CELL-AVAILABLE; and

- 5GMM-DEREGISTERED.eCALL-INACTIVE.

Valid subscriber data are available for the UE before it enters the substates, except for the substate 5GMM-DEREGISTERED.NO-SUPI.

8.1.4.2.2.3.2 5GMM-DEREGISTERED.NORMAL-SERVICE

The substate 5GMM-DEREGISTERED.NORMAL-SERVICE is chosen in the UE when a suitable cell has been found and the PLMN or tracking area is not in the forbidden list.

8.1.4.2.2.3.3 5GMM-DEREGISTERED.LIMITED-SERVICE

The substate 5GMM-DEREGISTERED.LIMITED-SERVICE is chosen in the UE, when it is known that a selected cell is unable to provide normal service (e.g. the selected cell is in a forbidden PLMN or is in a forbidden tracking area).

This substate is not applicable to non-3GPP access.

8.1.4.2.2.3.4 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION

The substate 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION is chosen in the UE if the initial registration procedure failed due to a missing response from the network.

Editor's note: Other cases in which this substate is chosen are FFS.

8.1.4.2.2.3.5 5GMM-DEREGISTERED.PLMN-SEARCH

The substate 5GMM-DEREGISTERED.PLMN-SEARCH is chosen in the UE, if the UE is searching for PLMNs. This substate is left either when a cell has been selected (the new substate is NORMAL-SERVICE or LIMITED-SERVICE) or when it has been concluded that no cell is available at the moment (the new substate is NO-CELL-AVAILABLE).

This substate is not applicable to non-3GPP access.

8.1.4.2.2.3.6 5GMM-DEREGISTERED.NO-SUPI

The substate 5GMM-DEREGISTERED.NO-SUPI is chosen in the UE, if the UE has no valid subscriber data available (SIM/USIM not available, the SIM/USIM is considered invalid by the UE) and a cell has been selected.

This substate is not applicable to non-3GPP access.

8.1.4.2.2.3.7 5GMM-DEREGISTERED.NO-CELL-AVAILABLE

No 5G cell can be selected. This substate is entered after a first intensive search failed when in substate 5GMM-DEREGISTERED.PLMN-SEARCH. Cells are searched for at a low rhythm. No 5GS services are offered.

This substate is not applicable to non-3GPP access.

8.1.4.2.2.3.8 5GMM-DEREGISTERED.eCALL-INACTIVE

Editor's note: How the UE enters 5GMM-DEREGISTERED.eCALL-INACTIVE sutstate is FFS.

Editor's note: Other substates of state 5GMM-DEREGISTERED are FFS, e.g. 5GMM-DEREGISTERED.REGISTRATION-NEEDED.

This substate is not applicable to non-3GPP access.

###### 8.1.4.2.2.4 Substates of state 5GMM-REGISTERED

8.1.4.2.2.4.1 General

The state 5GMM-REGISTERED is subdivided into a number of substates as described in this subclause. The following substates are not applicable to non-3GPP access:

- 5GMM-REGISTERED.LIMITED-SERVICE;

- 5GMM-REGISTERED.PLMN-SEARCH:

- 5GMM-DEREGISTERED.NON-ALLOWED-SERVICE;

- 5GMM-REGISTERED.NO-CELL-AVAILABLE.

8.1.4.2.2.4.2 5GMM-REGISTERED.NORMAL-SERVICE

The substate 5GMM-REGISTERED.NORMAL-SERVICE is chosen by the UE as the primary substate when the UE enters the state 5GMM-REGISTERED and the cell the UE selected is known to be in an allowed area.

8.1.4.2.2.4.3 5GMM-REGISTERED.NON-ALLOWED-SERVICE

The substate 5GMM-REGISTERED.NON-ALLOWED-SERVICE is chosen in the UE, if the cell the UE selected is known to be in a non-allowed area.

This substate is not applicable to non-3GPP access.

8.1.4.2.2.4.4 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE

The substate 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE is chosen by the UE if the mobility and periodic registration update procedure failed due to a missing response from the network. No 5GMM procedure except:

- mobility and periodic registration update procedure over 3GPP access; and

- mobility registration procedure over non-3GPP access

shall be initiated by the UE in this substate. No data shall be sent or received.

NOTE: Mobility registration procedure over non-3GPP access can be trigger by e.g. the change of UE network capability or renegotiating some parameters.

Editor's note: Other cases in which this substate is chosed are FFS.

8.1.4.2.2.4.5 5GMM-REGISTERED.LIMITED-SERVICE

The substate 5GMM-REGISTERED.LIMITED-SERVICE is chosen in the UE, if the cell the UE selected is known not to be able to provide normal service.

This substate is not applicable to non-3GPP access.

8.1.4.2.2.4.6 5GMM-REGISTERED.PLMN-SEARCH

The substate 5GMM-REGISTERED.PLMN-SEARCH is chosen in the UE, while the UE is searching for PLMNs.

This substate is not applicable to non-3GPP access.

8.1.4.2.2.4.7 5GMM-REGISTERED.NO-CELL-AVAILABLE

5G coverage has been lost or MICO mode is active in the UE. If MICO mode is active, the UE can deactivate MICO mode at any time by activating the AS layer when the UE needs to send mobile originated signalling or user data. Otherwise, The UE shall not initiate any 5GMM procedure except for cell and PLMN reselection.

Editor's note: Other substates of state 5GMM-REGISTERED are FFS, e.g. 5GMM-REGISTERED.UPDATE-NEEDED.

This substate is not applicable to non-3GPP access.

##### 8.1.4.2.3 5GS update status

In order to describe the detailed UE behaviour, the 5GS update (5U) status pertaining to a specific subscriber is defined.

The 5GS update status is stored in a non-volatile memory in the USIM if the corresponding file is present in the USIM, else in the non-volatile memory in the ME.

The 5GS update status value is changed only after the execution of a registration, network-initiated de-registration, 5GS based primary authentication and key agreement, service request or paging procedure.

5U1: UPDATED

The last registration attempt was successful.

5U2: NOT UPDATED

The last registration attempt failed procedurally, e.g. no response or reject message was received from the AMF.

5U3: ROAMING NOT ALLOWED

The last registration, service request, or registration for mobility or periodic registration update attempt was correctly performed, but the answer from the AMF was negative (because of roaming or subscription restrictions).

##### 8.1.4.2.4 5GMM sublayer states in the network

###### 8.1.4.2.4.1 General

In the following subclauses, the possible 5GMM sublayer states of the network are described and shown in Figure 8.1.4.2.4.1.1.



NOTE: Not all possible transitions are shown in this figure.

Editor's note: The fatal causes and non-fatal causes used in the 5GMM procedures are FFS.

Figure 8.1.4.2.4.1.1: 5GMM main states in the network

###### 8.1.4.2.4.2 5GMM-DEREGISTERED

In the state 5GMM-DEREGISTERED, no 5GMM context has been established or the 5GMM context is marked as deregistered. The UE is deregistered. The network may answer to an initial registration procedure initiated by the UE. The network may also answer to a de-registration procedure initiated by the UE.

###### 8.1.4.2.4.3 5GMM-COMMON-PROCEDURE-INITIATED

The network enters the state 5GMM-COMMON-PROCEDURE-INITIATED, after it has started a common 5GMM procedure and is waiting for a response from the UE.

###### 8.1.4.2.4.4 5GMM-REGISTERED

In the state 5GMM-REGISTERED, a 5GMM context has been established. Additionally, one or more PDU session context(s) may be activated at the network.

###### 8.1.4.2.4.5 5GMM-DEREGISTERED-INITIATED

The network enters the state 5GMM-DEREGISTERED-INITIATED after it has started a de-registration procedure and is waiting for a response from the UE.

#### 8.1.4.3 Behaviour of the UE in state 5GMM-DEREGISTERED and state 5GMM-REGISTERED

##### 8.1.4.3.1 General

In this subclause, the detailed behaviour of the UE in the states 5GMM-DEREGISTERED and 5GMM-REGISTERED is described.

##### 8.1.4.3.2 UE behaviour in state 5GMM-DEREGISTERED

###### 8.1.4.3.2.1 General

The state 5GMM-DEREGISTERED is entered in the UE, when:

- the de-registration is performed either by the UE or by the network (see subclause 8.5.2.3);

- the registration request is rejected by the AMF (see subclause 8.5.2.2);

- the service request request is rejected by the MME (see subclause 8.5.3.1); or

- the UE is switched on.

In state 5GMM-DEREGISTERED, the UE shall behave according to the substate as explained in subclause 8.1.4.3.2.3.

Editor's note: Other cases in which the UE enters the state 5GMM-DEREGISTERED are FFS.

###### 8.1.4.3.2.2 Detailed description of UE behaviour in state 5GMM-DEREGISTERED

8.1.4.3.2.2.1 NORMAL-SERVICE

The UE shall initiate an initial registration procedure.

8.1.4.3.2.2.2 LIMITED-SERVICE

The UE shall initiate an initial registration procedure when entering a cell which provides normal service.

The UE may initiate initial registration for emergency services.

8.1.4.3.2.2.3 ATTEMPTING-REGISTRATION

The UE in 3GPP access:

- shall initiate an initial registration procedure on the expiry of timers T3502 or T3511 or T3346;

- may initiate an initial registration procedure for emergency services even if timer T3346 is running;

- shall initiate an initial registration procedure when entering a new PLMN, if timer T3346 is running and the new PLMN is not equivalent to the PLMN where the UE started timer T3346, the PLMN identity of the new cell is not in the forbidden PLMN lists and the tracking area is not in one of the lists of forbidden tracking areas; and

- shall initiate an initial registration procedure when the tracking area of the serving cell has changed, if timer T3346 is not running, the PLMN identity of the new cell is not in one of the forbidden PLMN lists and the tracking area of the new cell is not in one of the lists of forbidden tracking areas.

The UE in non-3GPP access:

- shall initiate an initial registration procedure on the expiry of timers T3502 or T3511.

8.1.4.3.2.2.4 PLMN-SEARCH

The UE shall perform PLMN selection. If a new PLMN is selected, the UE shall reset the registration attempt counter and initiate the initial registration procedure (see subclause 8.5.2.2.2).

If the selected cell is known not to be able to provide normal service, the UE may initiate registration for emergency services.

8.1.4.3.2.2.5 NO-SUPI

The UE shall perform cell selection.

The UE may initiate registration for emergency services.

8.1.4.3.2.2.6 NO-CELL-AVAILABLE

The UE shall perform cell selection and choose an appropriate substate when a cell is found.

8.1.4.3.2.2.7 eCALL-INACTIVE

Editor's note: The UE behaviour in this substate is FFS.

Editor's note: The other required UE behaviour in state 5GMM-DEREGISTERED is FFS, e.g. selection of the substate after power on, substate when back to state 5GMM-DEREGISTERED from another 5GMM state.

##### 8.1.4.3.3 UE behaviour in state 5GMM-REGISTERED

###### 8.1.4.3.3.1 General

The state 5GMM-REGISTERED is entered at the UE, when:

- the initial registration procedure is performed by the UE (see subclause 8.5.2.2.2).

In state 5GMM-REGISTERED, the UE shall behave according to the substate as explained in subclause 8.1.4.3.3.2.

###### 8.1.4.3.3.2 Detailed description of UE behaviour in state 5GMM-REGISTERED

8.1.4.3.3.2.1 NORMAL-SERVICE

The UE:

- shall initiate the mobility or the periodic registration update procedure (according to conditions given in subclause 8.5.2.2.3) , except that the periodic registration update procedure shall not be initiated over non-3GPP access;

- shall initiate the service request procedure (according to conditions given in subclause 8.5.3.1); and

- shall respond to paging.

NOTE: Paging is not supported over non-3GPP access.

8.1.4.3.3.2.2 NON-ALLOWED-SERVICE

The UE shall behave as specified in subclause 8.2.x.

8.1.4.3.3.2.3 ATTEMPTING-REGISTRATION-UPDATE

The UE in 3GPP access:

- shall not send any user data;

- shall initiate mobility registration update procedure on the expiry of timers T3502 or T3511 or T3346;

- shall initiate mobility registration update procedure when entering a new PLMN, if timer T3346 is running and the new PLMN is not equivalent to the PLMN where the UE started timer T3346, the PLMN identity of the new cell is not in the forbidden PLMN lists, and the tracking area is not in one of the lists of forbidden tracking areas;

- shall initiate mobility registration update procedure when the tracking area of the serving cell has changed, if timer T3346 is not running, the PLMN identity of the new cell is not in one of the forbidden PLMN lists and the tracking area is not in one of the lists of forbidden tracking areas;

- may initiate a mobility registration update procedure upon request of the upper layers to establish a PDU session for emergency services; and

- may perform de-registration locally and initiate an initial registration procedure for emergency services even if timer T3346 is running.

The UE in non-3GPP access:

- shall not send any user data; and

- shall initiate mobility registration update procedure on the expiry of timers T3502 or T3511.

8.1.4.3.3.2.4 LIMITED-SERVICE

The UE:

- shall perform cell selection/reselection; and

- may initiate registration for emergency services.

8.1.4.3.3.2.5 PLMN-SEARCH

The UE shall perform PLMN selection. If a new PLMN is selected, the UE shall reset the registration attempt counter and initiate the initial registration procedure (see subclause 8.5.2.1.2).

If the selected cell is known not to be able to provide normal service, the UE may initiate registration for emergency services.

8.1.4.3.3.2.6 NO-CELL-AVAILABLE

The UE shall perform cell selection and choose an appropriate substate when a cell is found.

### 8.1.5 Permanent identifiers

A globally unique permanent identity, the 5G subscription permanent identifier (SUPI), is allocated to each subscriber for 5GS-based services. In the current release, the IMSI and the network access identifier (NAI) are valid SUPI types. Though non-IMSI based SUPIs are possible by using NAI, the IMSI can be contained within the NAI for the SUPI. The structure of the SUPI and its derivatives will be specified in 3GPP TS 23.003 [5].

A UE supporting NG-RAN includes a SUPI when a valid 5G-GUTI is not available from the PLMN or equivalent PLMN to which the UE is attempting to register or if requested by the network, during the registration and generic UE configuration update procedures.

Each UE supporting NG-RAN contains a permanent equipment identifier (PEI) for accessing 5GS-based services. In the current release, the IMEI and the IMEISV are the only PEI format supported by 5GS.The structure of the PEI and its formats will be specified in 3GPP TS 23.003 [5].

A UE supporting NG-RAN includes a PEI:

- when neither SUPI nor valid 5G-GUTI is available to use for emergency services in the REGISTRATION REQUEST message with 5GS registration type IE set to "emergency registration"; and

- when the network requests the PEI by using the identification procedure, in the IDENTIFICATION RESPONSE message.

The AMF can request the PEI at any time by using the identification procedure.

### 8.1.6 Temporary identities

A globally unique temporary user identity for 5GS-based services, the 5G globally unique temporary identity (5G-GUTI), is used for identification within the signalling procedures. The 5G-GUTI is common to both 3GPP and non-3GPP access. In the paging and service request procedures, a shortened form of the 5G-GUTI, the 5G S-temporary mobile subscriber identity (5G-S-TMSI), is used to enable more efficient radio signalling. The purpose of the 5G-GUTI and 5G-S-TMSI is to provide identity confidentiality, i.e., to protect a user from being identified and located by an intruder. The structure of the 5G-GUTI and its derivatives is specified in 3GPP TS 23.003 [5]. The 5G-GUTI has two main components:

- the globally unique AMF id (GUAMI) that uniquely identifies the AMF that allocated the 5G-GUTI, and

- the 5G-TMSI that provides for an unambiguous identity of the UE within this AMF.

The 5G-S-TMSI has three main components:

- the AMF set ID that uniquely identifies the AMF set within the AMF region;

- the AMF pointer that uniquely identifies the AMF within the AMF set; and

- the 5G-TMSI.

A UE supporting N1 mode includes a valid 5G-GUTI, if any is available, in the REGISTRATION REQUEST and DEREGISTRATION REQUEST messages. In the SERVICE REQUEST message, the UE includes a valid 5G-S-TMSI as user identity. The AMF may assign a new 5G-GUTI for a particular UE at successful registration and generic UE configuration update procedures.

If a new 5G-GUTI is assigned by the AMF, the UE and the AMF handle the 5G-GUTI as follows:

- Upon receipt of a 5GMM message containing a new 5G-GUTI the UE considers the new 5G-GUTI as valid and the old 5G-GUTI as invalid.

- The AMF considers the old 5G-GUTI as invalid as soon as an acknowledgement for a registration or generic UE configuration update procedure is received.

### 8.1.7 Mobile initiated connection only mode

The UE can request the use of mobile initiated connection only (MICO) mode during the registration procedure (see 3GPP TS 23.501 [9] and 3GPP TS 23.502[10]).

If the UE requests the use of MICO, the network can accept the use of MICO mode by providing a MICO indication when accepting the registration procedure. The UE may use MICO mode only if the network has provided the MICO indication IE during the last registration procedure.

If the network accepts the use of MICO mode, the UE may deactivate the AS layer and activate MICO mode by entering the state 5GMM-REGISTERED.NO-CELL-AVAILABLE if:

a) the UE is in 5GMM-IDLE mode; and

b) in the 5GMM-REGISTERED.NORMAL-SERVICE state.

When MICO mode is activated all NAS timers are stopped and associated procedures aborted except for periodic registration update timer, any backoff timers, and the timer T controlling the periodic search for HPLMN or EHPLMN or higher prioritized PLMNs (see 3GPP TS 23.122 [7]).

The UE may deactivate MICO mode and activate the AS layer at any time. Upon deactivating MICO mode, the UE may initiate 5GMM procedures (e.g. for the transfer of mobile originated signalling or user data).

If the AMF accepts the use of MICO mode, the AMF starts the implicit de-registration timer when entering 5GMM-IDLE mode.

### 8.1.8 Handling of the periodic registration update timer and implicit de-registration timer

The registration procedure is used to periodically notify the availability of the UE to the network. The procedure is controlled in the UE by the periodic registration update timer, T3512.

Upon expiry of the implicit de-registration timer the network shall start the implicit detach timer. The value of the implicit detach timer is network dependent. If MICO is activated, the default value of the implicit detach timer is 4 minutes greater than timer Te. If the implicit detach timer expires before the UE contacts the network, the network shall implicitly detach the UE.

If the AMF provides T3346 value IE in the mobility management messages and T3346 value is greater than timer T3512, the AMF sets the periodic registration update timer and the implicit detach timer such that the sum of the timer values is greater than timer T3346 value.

Editor's note: Further details on timer handling are FFS (e.g. if T3512 expires while the UE is registered for emergency bearer services).

## 8.2 5GS mobility functions in IDLE and CONNECTED mode

### 8.2.1 Registration areas in the 5GS

#### 8.2.1.1 General

Within the 5GS, the registration area is managed independently per access type, i.e., 3GPP access or non-3GPP access. The AMF assigns a registration area to the UE during the registration procedure. A registration area is defined as a set of tracking areas and each of these tracking areas consists of one or more cells that cover a geographical area. Tracking areas cannot overlap each other. Within the 5GS, the concept of "registration to multiple tracking areas" applies:

- A tracking area is identified by a TAI which is broadcast in the cells of the tracking area. The TAI is constructed from a TAC and a PLMN identifier. In case of a shared network, one or more TAC and multiple PLMN identifiers are broadcast.

- In order to reduce the tracking area update signalling within the 5GS, the AMF can assign several tracking areas to the UE. These tracking areas construct a list of tracking areas which is identified by a TAI list. When generating the TAI list, the AMF shall include only TAIs that are applicable on the access where the TAI list is sent. The AMF shall be able to allocate a TAI List over different NG-RAN access technologies.

- The UE considers itself registered to a list of tracking areas and does not need to trigger mobility registration update procedure (i.e. registration procedure with registration type set to "mobility registration update") as long as the UE stays in one of the tracking areas of the list of tracking areas received from the AMF.

Editor's note: The maximum number of tracking areas which can be allocated per UE needs to be defined which can be as in EPS or different.

- The UE will consider the TAI list as valid, until it receives a new TAI list in the next mobility registration update or periodic registration update procedure, or the UE is commanded by the network to delete the TAI list by a reject message or it is detached from the 5GS. If the registration request is accepted or the TAI list is reallocated by the AMF, the AMF shall provide at least one entry in the TAI list. If the new and the old TAI list are identical, the AMF does not need to provide the new TAI list to the UE during mobility registration update or periodic registration update.

- The TAI list can be reallocated by the AMF.

- When the UE is detached from the 5GS, the TAI list in the UE is invalid.

- The AMF allocates one 5G-GUTI, which is common between 3GPP and non3GPP, to the UE.

- The UE includes the last visited registered TAI, if available, to the AMF.

#### 8.2.1.2 Open issues on registration areas in the 5GS

- CT1 need to study whether the periodic registration update timer for the periodic registration updating procedure and the periodic tracking area updating procedure in EPS can have different values, related values, or the same value.

- CT1 need to study the impacts on the periodic registration update timer when the mobile initiated connection only (MICO) mode (see 3GPP TS 23.501 [9]) is used.

### 8.2.2 Service area restrictions

The service area restrictions consist of either an allowed area, or a non-allowed area. The allowed area can be limited by a maximum allowed number of tracking areas or include all tracking areas in a PLMN. The non-allowed area can contain up to 16 tracking areas. The network conveys the service area restrictions to the UE by including either an allowed area, or a non-allowed area, but not both, in the Service area list IE of a REGISTRATION ACCEPT message or a CONFIGURATION UPDATE COMMAND message,

When the UE receives a Service area list IE with an allowed area indication during a registration procedure or a generic UE configuration update procedure:

- if the "Type of list" included in the Service area list IE does not indicate all TAIs belonging to the PLMN are allowed area, the UE shall delete the old list of "allowed tracking areas" and store the tracking areas in the allowed area as the list of "allowed tracking areas". If the UE has a stored list of "non-allowed tracking areas" for the registered PLMN, the UE shall delete that list; or

- if the "Type of list" included in the Service area list IE indicates all TAIs belonging to the PLMN are allowed area, the UE shall treat all tracking areas in the registered PLMN are allowed area and delete the stored list of "allowed tracking areas" or the stored list of "non-allowed tracking areas" for the registered PLMN.

When the UE receives a Service area list IE with a non-allowed area indication during a registration procedure or a generic UE configuration update procedure, the UE shall delete the old list of "non-allowed tracking areas" and store the tracking areas in the non-allowed area as the list of "non-allowed tracking areas". If the UE has a stored list of "allowed tracking areas" for the registered PLMN, the UE shall delete that list.

If the UE has a stored list of "allowed tracking areas":

- while camped on a cell whose TAI is in the list of "allowed tracking areas", the UE is allowed to initiate any 5GMM and 5GSM procedures; and

- while camped on a cell whose TAI is not in the list of "allowed tracking areas":

1) if the UE is in 5GMM-IDLE mode over 3GPP access, the UE:

i) shall not perform the mobility and periodic registration update procedure with uplink data status IE except for emergency services; and

ii) shall not initiate a service request procedure except for emergency services or for responding to core network paging; and

2) if the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication over 3GPP access, the UE:

i) shall not perform the mobility registration update procedure with uplink data status IE except for emergency services;

ii) shall not initiate a service request procedure except for emergency services; and

iii) shall not initiate a 5GSM procedure except for emergency services.

If the UE has a stored list of "non-allowed tracking areas":

- while camped on a cell whose TAI is not in the list of "non-allowed tracking areas", the UE is allowed to initiate any 5GMM and 5GSM procedures; and

- while camped on a cell whose TAI is in the list of "non-allowed tracking areas":

1) if the UE is in 5GMM-IDLE mode over 3GPP access, the UE:

i) shall not perform the mobility and periodic registration update procedure with uplink data status IE except for emergency services; and

ii) shall not initiate a service request procedure except for emergency services or for responding to core network paging; and

2) if the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication over 3GPP access, the UE:

i) shall not perform the mobility registration update procedure with uplink data status IE except for emergency services;

ii) shall not initiate a service request procedure except for emergency services; and

iii) shall not initiate a 5GSM procedure except for emergency services.

The list of "allowed tracking areas", as well as the list of "non-allowed tracking areas" shall be erased when:

- the UE is switched off;

- the UICC containing the USIM is removed; and

- periodically (with a period in the range 12 to 24 hours).

When the list of "allowed tracking areas" or the list of "non-allowed tracking areas" is erased, the UE performs cell selection procedure.

The UE shall evaluate the information in the list of "5GS forbidden tracking areas for roaming" and in the list of "5GS forbidden tracking areas for regional provision of service" before evaluating the information in the list of "allowed tracking areas" or the list of "non-allowed tracking areas".

### 8.2.3 UE NAS mobility functions in 5GMM-IDLE mode

In 5GMM-IDLE mode a UE with a valid USIM enabled will:

- when not registered to the 5GCN:

- perform registration procedure with registration type set to "initial registration" in order to receive services that require registration in the 5GS when not registered to the EPS;

- perform registration procedure with registration type set to "mobility registration update" when registered to the EPS;

- when registered to the 5GCN:

- perform registration procedure with registration type set to "mobility registration update" when:

- entering a tracking area not in the list of assigned tracking areas, in order to maintain the registration and enable the AMF to keep track of the UE; or

- the UE needs to update its capabilities towards the 5GCN; or

- the UE receives the CONFIGURATION UPDATE COMMAND and detects that registration update procedure is requested;

- answer to paging from the AMF by performing a service request procedure, unless the UE is in MICO mode;

- perform the service request procedure in order to establish a N1 NAS signalling connection to the network;

- perform de-registration procedure when the UE is switched off, the USIM is removed or disabled, or the 5GS capability of the UE is disabled.

In 5GMM-IDLE mode over 3GPP access, a UE with a valid USIM enabled will:

- perform cell selection/reselection procedure according to 3GPP TS 38.304 [27] and PLMN selection according to 3GPP TS 23.122 [7]; and

- when registered to the 5GCN:

- perform registration procedure with registration type set to "periodic registration update" to periodically notify the 5GS that the UE is available; and

- perform the service request procedure in order to request the establishment of radio bearers when uplink user data is to be sent.

In 5GMM-IDLE mode over 3GPP access a UE without valid USIM enabled will:

- perform cell selection/reselection according to 3GPP TS 38.304 [27], but not PLMN selection;

- perform registration procedure with 5GS registration type IE set to "emergency registration" if the UE needs to establish a PDU session for emergency services.

### 8.2.4 UE NAS mobility functions in 5GMM-CONNECTED mode

In 5GMM-CONNECTED mode a UE with a valid USIM enabled will:

- respond to identification requests from the AMF;

- perform authentication when requested by the AMF;

- initiate the ciphering and integrity protection for NAS signalling when requested by the AMF;

- not perform periodic registration update procedure (i.e. registration procedure with registration type set to "periodic registration update");

- perform mobility registration update procedure (i.e. registration procedure with registration type set to "mobility registration update") when after handover the UE detects that it has entered a tracking area not in the assigned list of tracking areas or when the UE receives the CONFIGURATION UPDATE COMMAND and detects that registration update procedure is requested; and

- perform de-registration procedure when the UE is switched off, the USIM is removed or disabled, the 5GS capability of the UE is disabled, or when requested by the AMF.

In 5GMM-CONNECTED mode over 3GPP access, a UE with a valid USIM enabled will:

- perform the service request procedure in order to request the establishment of the radio bearers when uplink user data is to be sent.

Editor's note: The case of the UE without a valid USIM registered to the 5GCN and using emergency services is FFS.

### 8.2.5 5GMM-CONNECTED mode with RRC inactive indication

This subclause is only applicable for UE's 5GMM mode over 3GPP access.

The UE is in 5GMM-CONNECTED mode with RRC inactive indication when the UE is in:

- 5GMM-CONNECTED mode over 3GPP access at the NAS layer; and

- RRC\_INACTIVE state at the AS layer (see 3GPP TS 38.300 [26]).

Unless stated otherwise, the UE behavior in 5GMM-CONNECTED mode with RRC inactive indication follows the UE behavior in 5GMM-CONNECTED over 3GPP access, except that:

- the UE shall apply the mobility restrictions; and

- the UE shall perform the PLMN selection procedures

as in 5GMM-IDLE mode over 3GPP access.

The UE shall transition from 5GMM-CONNECTED mode over 3GPP access to 5GMM-CONNECTED mode with RRC inactive indication upon indication from the lower layers that the UE has transitioned to RRC\_INACTIVE state.

The UE shall trigger a transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-CONNECTED mode over 3GPP access upon:

- uplink data transfer; or

- mobile originaiting signaling.

The UE shall transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-CONNECTED mode over 3GPP access upon receving from the lower layers indication that the UE has transitioned to RRC\_CONNECTED state (see 3GPP TS 38.300 [26]).

NOTE: The AMF can be aware of the transition between 5GMM-CONNECTED mode and 5GMM-CONNECTED mode with RRC inactive indication for a UE (see 3GPP TS 23.502 [10]).

The UE shall trigger a transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-IDLE mode upon selection of a PLMN that is not an equivalent PLMN to the registered PLMN.

The UE shall transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-IDLE mode over 3GPP access upon receving from the lower layers:

- indication that the transition from RRC\_INACTIVE state to RRC\_CONNECTED state has failed;

- indication of transition from RRC\_INACTIVE to RRC\_IDLE;

- AMF paging notification; or

- indication of cell selection to E-UTRAN.

The UE shall not trigger a transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-IDLE mode upon entering a new PLMN which is in the list of equivalent PLMNs.

### 8.2.6 Disabling and re-enabling of UE's N1 mode radio capabilities

When the UE supporting both N1 mode and S1 mode is disabling the N1 mode radio capabilities, it should proceed as follows:

a) select an E-UTRA cell connected to EPC of the registered PLMN or a PLMN from the list of equivalent PLMNs; or

b) if an E-UTRA cell connected to EPC of the registered PLMN or a PLMN from the list of equivalent PLMNs cannot be found, or the UE does not have a registered PLMN, then perform PLMN selection as specified in 3GPP TS 23.122 [7].

Editor's note: Instead of performing PLMN selection, whether the UE can select another RAT of the chosen PLMN is FFS.

Editor's note: If no other allowed PLMN for an E-UTRA cell connected to EPC are available, the UE’s behaviour is FFS.

When the UE supporting both N1 mode and S1 mode needs to stay in E-UTRA connected to EPC, in order to prevent unwanted handover or cell reselection from E-UTRA connected to EPC to E-UTRA connected to 5GCN or NR connected to 5GCN, the UE shall disable the N1 mode radio capabilities and:

- the UE NAS layer shall indicate the access stratum layer(s) of disabling of the N1 mode radio capabilities.

NOTE: The UE can only disable the N1 mode radio capabilities when in 5GMM-IDLE mode.

Editor's note: The N1 mode radio capabilities that the UE needs to disable in order to not reselect to NR or an E-UTRA cell connected to 5GC (i.e. avoid ping pong) need to be defined by RAN WGs.

Editor's note: To prevent unwanted handover from EPC to 5GCN, it is FFS how the UE indicates the disabling of the N1 mode radio capabilities to the network.

The UE shall re-enable the N1 mode radio capabilities when:

- the UE performs PLMN selection; and

- the UE powers off and powers on again or the USIM is removed.

Editor's note: When the N1 mode radio capabilities was re-enabled due to PLMN selection, whether the UE needs to memorize the identity of the PLMNs where N1 mode radio capabilities was disabled and use that stored information in subsequent PLMN selections, is FFS.

If the disabling of N1 mode radio capabilities was due to IMS voice is not available and the UE’s usage setting is "voice centric", the UE shall re-enable the N1 mode radio capabilities when the UE’s usage setting is changed from "voice centric" to "data centric".

Editor's note: Whether the UE starts an implementation specific timer for enabling N1 mode radio capabilities is FFS.

## 8.3 Establishment of the N1 NAS signalling connection

When the UE is in 5GMM-IDLE mode over 3GPP access and needs to transmit an initial NAS message, the UE shall request the lower layer to establish an RRC connection. Upon indication from the lower layers that the RRC connection has been established, the UE shall consider that the N1 NAS signalling connection over 3GPP access is established and enter 5GMM-CONNECTED mode over 3GPP access.

When the UE is in 5GMM-IDLE mode over non-3GPP access, and the UE receives an indication from the lower layers of access stratum connection establishment, the UE shall consider the N1 NAS signalling connection established, enter 5GMM-CONNECTED mode over non-3GPP access and send an initial NAS message.

Initial NAS messages are:

- REGISTRATION REQUEST;

- DEREGISTRATION REQUEST; and

- SERVICE REQUEST.

If the UE is capable of both N1 mode and S1 mode and lower layers provide an indication that the current E-UTRA cell is connected to both EPC and 5GCN, for the routing of the REGISTRATION REQUEST message during the initial registration procedure to the appropriate core network (EPC or 5GCN), the UE NAS provides the lower layers with the selected core network type information.

For the routing of the initial NAS message to the appropriate AMF, if the UE holds a valid 5G-GUTI, the UE NAS provides the lower layers with either the 5G-S-TMSI or the registered GUAMI that consists of the PLMN ID, the AMF region ID, the AMF set ID and the AMF pointer according to the following rules:

a) When the tracking area of the current cell is in theregistration area, the UE NAS shall provide the lower layers with the 5G-S-TMSI, but shall not provide the registered GUAMI to the lower layers;

b) When the tracking area of the current cell is not in theregistration area, the UE NAS shall provide the lower layers with the GUAMI (AMF identifier part of the valid 5G-GUTI);

c) When the REGISTRATION REQUEST message with the registration type set to "initial registration" is sent over 3GPP access in the same PLMN or equivalent PLMN to establish the NAS signalling connection, the UE NAS shall provide the lower layers with the GUAMI (AMF identifier part of the valid 5G-GUTI which is assigned over the non-3GPP access); or

d) When the REGISTRATION REQUEST message with the registration type set to "initial registration" is sent over non-3GPP access in the same PLMN or equivalent PLMN to establish the NAS signalling connection, the UE NAS shall provide the lower layers with the GUAMI (AMF identifier part of the valid 5G-GUTI which is assigned over the 3GPP access).

## 8.4 Release of the N1 NAS signalling connection

The signalling procedure for the release of the N1 NAS signalling connection is initiated by the network.

In N1 mode, upon indication from lower layers that the access stratum connection has been released, the UE shall enter 5GMM-IDLE mode and consider the N1 NAS signalling connection released.

To allow the network to release the N1 NAS signalling connection, the UE:

a) shall start the timer T3540 if the UE receives any of the 5GMM cause values #11, #12, #13 (not applicable to the service request procedure);

b) shall start the timer T3540 if:

- the UE receives a REGISTRATION ACCEPT message;

- the UE has not set the "follow-on request pending" indication in the REGISTRATION REQUEST message;

- the registration for mobility and periodic registration update procedure has been initiated in EMM-IDLE mode; and

- the user-plane radio resources for PDU sessions have not been set up;

c) shall start the timer T3540 if the UE receives a REGISTRATION REJECT message indicating:

- the 5GMM cause value #10.

d) shall start the timer T3540 if the UE receives a SERVICE REJECT message indicating:

- the 5GMM cause value #10.

Upon expiry of T3540,

- in cases a, and b, the UE shall locally release the established NAS signalling connection; or

- in cases c, and d the UE shall locally release the established N1 NAS signalling connection and the UE shall initiate the registration procedure as described in subclause 8.5.2.1.2.2 or 8.5.2.1.3.2.

In case b,

- upon an indication from the lower layers that the user-plane radio resources for PDU sessions are set up, the UE shall stop timer T3540 and may send uplink signalling via the existing N1 NAS signalling connection or user data via user plane; or

- upon receipt of a DEREGISTRATION REQUEST message, the UE shall stop timer T3540 and respond to the network-initiated de-registration request as specified in subclause 8.5.2.2.3.

In case c,

- upon an indication from the lower layers that the access stratum connection has been released, the UE shall stop timer T3540 and perform a new registration procedure as specified in subclause 8.5.2.1.2.2 or 8.5.2.1.3.2.

In cases d,

- upon an indication from the lower layers that the RRC connection has been released, the UE shall stop timer T3540 and perform a new registration procedure as specified in subclause 8.5.2.1.2.2 or 8.5.2.1.3.2.

Editor's note: The case of receiving a request from upper layers to establish a PDU session for emergency bearer services is FFS.

## 8.5 5GS mobility management procedures

### 8.5.1 5GMM common procedures

#### 8.5.1.1 Primary authentication and key agreement procedure

##### 8.5.1.1.1 General

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures, as specified in 3GPP TS 33.501 [24].

Two methods are defined:

- EAP based primary authentication and key agreement procedure.

- 5G AKA based primary authentication and key agreement procedure.

The UE and the AMF shall support the EAP based primary authentication and key agreement procedure and the 5G AKA based primary authentication and key agreement procedure.

##### 8.5.1.1.2 EAP based primary authentication and key agreement procedure

###### 8.5.1.1.2.1 General

Extensible authentication protocol (EAP) as specified in IETF RFC 3748 [30] enables authentication using various EAP methods.

EAP defines four types of EAP messages:

- an EAP-request message;

- an EAP-response message;

- an EAP-success message; and

- an EAP-failure message.

Several rounds of exchanges of an EAP-request message and a related EAP-response message can be required to achieve the authentication (see example in figure 8.5.1.1.2.1.1).

The EAP-request message is transported from the network to the UE using the AUTHENTICATION REQUEST message of the EAP message reliable transport procedure.

The EAP-response message is transported from the UE to the network using the AUTHENTICATION RESPONSE AUTHENTICATION RESPONSE message of the EAP message reliable transport procedure.

If the authentication of the UE completes successfully, the EAP-success message is transported from the network to the UE using the SECURITY MODE COMMAND message of the security mode command procedure.

Editor’s note: The security mode command procedure is not yet included in the TR, and EAP authentication procedure may need to be aligned when included.

If the authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE in a response of the initial 5GMM procedure as part of which the EAP based primary authentication and key agreement procedure is performed.

The AMF shall set the authenticator retransmission timer specified in IETF RFC 3748 [30] subclause 4.3 to infinite value.

NOTE: The EAP message reliable transport procedure provides a reliable transport of EAP messages and therefore retransmissions at the EAP layer do not occur.

The AUSF and the AMF support exchange of EAP messages using N12.

Editor’s note: The ngKSI handling at EAP authentication is FFS.



Figure 8.5.1.1.2.1.1: EAP based primary authentication and key agreement procedure

###### 8.5.1.1.2.2 EAP-AKA' related procedures

8.5.1.1.2.2.1 General

The UE shall support acting as EAP-AKA' peer as specified in IETF RFC 5448 [35]. The AUSF may support acting as EAP-AKA' server as specified in IETF RFC 5448 [35].

The EAP-AKA' enables mutual authentication of the UE and the network.

8.5.1.1.2.2.2 Initiation

In order to initiate the EAP based primary authentication and key agreement procedure using EAP-AKA', the AUSF shall send an EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [35]. The AUSF shall set the AT\_KDF\_INPUT attribute of the EAP-request/AKA'-challenge message to the SNN. The SNN is in format described in subclause 8.8.1. The AUSF may include AT\_RESULT\_IND attribute in the EAP-request/AKA'-challenge message.

Upon receiving an EAP-request/AKA'-challenge message, the UE checks whether the network name field of the AT\_KDF\_INPUT attribute is the SNN constructed according to subclause 8.y.1.

8.5.1.1.2.2.3 UE successfully authenticates network

If the SNN check is successful and procedures for handling of the EAP-request/AKA'-challenge message specified in IETF RFC 5448 [35] are successful, the UE shall generate KAUSF, KSEAF, and KAMF as described in 3GPP TS 33.501 [24] and shall send an EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [35].

If the EAP-request/AKA'-challenge message contains AT\_RESULT\_IND attribute, the UE may include AT\_RESULT\_IND attribute in the EAP-response/AKA'-challenge message.

8.5.1.1.2.2.4 Errors when handling EAP-request/AKA'-challenge message

If the SNN check fails or the UE does not accept AUTN during handling of the EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [35], the UE shall send an EAP-response/AKA'-authentication-reject message as specified in IETF RFC 5448 [35].

If the SNN check is successful but the UE detects that the sequence number in AUTN is not correct during handling of the EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [35], the UE shall send an EAP-response/AKA'-synchronization-failure message as specified in IETF RFC 5448 [35].

If the SNN check is successful, the sequence number in AUTN is correct and the UE detects another error during handling of the EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [35], the UE shall send an EAP-response/AKA'-client-error message as specified in IETF RFC 5448 [35].

8.5.1.1.2.2.5 Network successfully authenticates UE

Upon reception of the EAP-response/AKA'-challenge message, if procedures for handling an EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [35] are successful, the AUSF may generate KAUSF and shall generate KSEAF as described in 3GPP TS 33.501 [24] and checks whether the AT\_RESULT\_IND attribute is included in the EAP-response/AKA'-challenge message and:

- if the AT\_RESULT\_IND attribute is included in the EAP-response/AKA'-challenge message, the AUSF shall send an EAP-request/AKA'-notification message as specified in IETF RFC 5448 [35]; and

- if the AT\_RESULT\_IND attribute is not included in the EAP-response/AKA'-challenge message, the AUSF shall send an EAP-success message as specified in IETF RFC 5448 [35] along with the KSEAF and shall consider the procedure complete.

NOTE: SEAF generates KAMF based on the received KSEAF immediately following the primary authentication and key agreement procedure and provides KAMF to AMF.

8.5.1.1.2.2.6 UE handling EAP-AKA' notification

Upon receiving an EAP-request/AKA'-notification message, the UE shall send an EAP-response/AKA'-notification message as specified in IETF RFC 5448 [35].

8.5.1.1.2.2.7 Network sending EAP-success message

Upon reception of the EAP-response/AKA'-notification message, if earlier procedures for handling an EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [35] were successful, the AUSF shall send an EAP-success message as specified in IETF RFC 5448 [35] along with the KSEA and shall consider the procedure complete.

NOTE: SEAF generates KAMF based on the received KSEAF immediately following the primary authentication and key agreement procedure and provides KAMF to AMF.

8.5.1.1.2.2.8 UE handling EAP-success message

Upon receiving an EAP-success message, the UE shall consider the procedure complete.

8.5.1.1.2.2.9 Network not successfully authenticates UE

Upon reception of the EAP-response/AKA'-challenge message, if procedures for handling an EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [35] are not successful, the AUSF shall send an EAP-request/AKA'-notification message that implies failure as specified in IETF RFC 5448 [35].

8.5.1.1.2.2.10 Network sending EAP-failure message

Upon reception of the EAP-response/AKA'-notification message, if earlier procedures for handling an EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [35] were not successful, the AUSF shall send an EAP-failure message as specified in IETF RFC 5448 [35] and shall consider the procedure complete.

8.5.1.1.2.2.11 UE handling EAP-success

Upon receiving an EAP-failure message, the UE shall consider the procedure complete.

###### 8.5.1.1.2.3 EAP message reliable transport procedure

8.5.1.1.2.3.1 General

The purpose of the EAP message reliable transport procedure is to provide a reliable transport of an EAP-request message from the network to the UE and of an EAP-response message from the UE to the network.

The EAP message reliable transport procedure is initiated by an AUTHENTICATION REQUEST message with the EAP message IE.

8.5.1.1.2.3.2 EAP message reliable transport procedure initiation by the network

In order to initiate the EAP message reliable transport procedure, the AMF shall create an AUTHENTICATION REQUEST message.

The AMF shall set the EAP message IE of the AUTHENTICATION REQUEST message to the EAP-request message to be sent to the UE.

The AMF shall send the AUTHENTICATION REQUEST message to the UE, and the AMF shall start timer T3560 (see example in figure 8.5.1.1.2.3.2.1).



Figure 8.5.1.1.2.3.2.1: EAP message reliable transport procedure

Upon receipt of a AUTHENTICATION REQUEST message with the EAP message IE, the UE handles the EAP message received in the EAP message IE of the AUTHENTICATION REQUEST message.

8.5.1.1.2.3.3 EAP message reliable transport procedure accepted by the UE

The UE shall create a AUTHENTICATION RESPONSE message.

If the received EAP message is an EAP-request message, the UE shall set the EAP message IE of the AUTHENTICATION RESPONSE message to the EAP-response message responding to the received EAP-request message.

The UE shall send the AUTHENTICATION RESPONSE message to the AMF.

Upon receipt of a AUTHENTICATION RESPONSE message, the AMF shall stop timer T3560. If the EAP message IE is included in the AUTHENTICATION RESPONSE message, the AMF handles the EAP message received in the EAP message IE of the AUTHENTICATION RESPONSE message.

8.5.1.1.2.3.4 Abnormal cases on the network side

The following abnormal cases can be identified:

a) T3560 expired

Editor's note: Further abnormal cases are FFS

8.5.1.1.2.3.5 Abnormal cases in the UE

Editor's note: Abnormal cases are FFS

##### 8.5.1.1.3 5G AKA based primary authentication and key agreement procedure

###### 8.5.1.1.3.1 General

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on a key KAMF (see 3GPP TS 33.501 [24]). The cases when the 5G AKA based primary authentication and key agreement procedure is used are defined in 3GPP TS 33.501 [24].

The 5G AKA based primary authentication and key agreement procedure is always initiated and controlled by the network. However, the UE can reject the 5G authentication challenge sent by the network.

The UE shall proceed with an 5G authentication challenge only if a USIM is present.

A partial native 5GS security context is established in the UE and the network when an 5G authentication is successfully performed. During a successful 5G AKA based primary authentication and key agreement procedure, the CK and IK are computed by the USIM. CK and IK are then used by the ME as key material to compute a new key, KAMF. KAMF is stored in the 5GS security contexts (see 3GPP TS 33.501 [24]) of both the network and in the volatile memory of the ME while attached to the network, and is the root for the 5GS integrity protection and ciphering key hierarchy.

The 5G AKA based primary authentication and key agreement procedure is initiated by an AUTHENTICATION REQUEST message without the EAP message IE.

###### 8.5.1.1.3.2 Authentication initiation by the network

The network may initiate a 5G AKA based primary authentication and key agreement procedure for a UE in 5GMM-CONNECTED mode at any time. For restrictions applicable after handover or inter-system handover to N1 mode see subclause 8.5.1.1.2.3.

The network initiates the 5G AKA based primary authentication and key agreement procedure by sending an AUTHENTICATION REQUEST message to the UE and starting the timer T3560 (see example in figure 8.5.2.1.3.2.1). The AUTHENTICATION REQUEST message contains the parameters necessary to calculate the authentication response (see 3GPP TS 33.501 [24]).

If an ngKSI is contained in an initial NAS message during a 5GMM procedure, the network shall include a different ngKSI value in the AUTHENTICATION REQUEST message when it initiates a 5G AKA based primary authentication and key agreement procedure.



Figure 8.5.1.1.3.2.1: 5G AKA based primary authentication and key agreement procedure

###### 8.5.1.1.3.3 Authentication response by the UE

The UE shall respond to an AUTHENTICATION REQUEST message. With the exception of the cases described in subclause 8.5.1.1.3.6, the UE shall process the authentication challenge data and respond with an AUTHENTICATION RESPONSE message to the network.

Upon a successful 5G authentication challenge, the UE shall determine the PLMN identity to be used for the calculation of the new KAMF from the authentication challenge data according to the following rules:

a) When the UE moves from 5GMM-IDLE mode to 5GMM-CONNECTED mode, until the first handover, the UE shall use the PLMN identity of the selected PLMN; and

b) After handover or inter-system handover to N1 mode,

- if the target cell is not a shared network cell, the UE shall use the PLMN identity received as part of the broadcast system information;

- if the target cell is a shared network cell and the UE has a valid 5G-GUTI, the UE shall use the PLMN identity that is part of the 5G-GUTI; and

- if the target cell is a shared network cell and the UE has a valid 4G-GUTI and TAI, but not a valid 5G-GUTI, the UE shall use the PLMN identity that is part of the TAI.

Editor’s note: Security context coordination between EPS and 5GS is FFS.

Upon a successful 5G authentication challenge, the new KAMF calculated from the authentication challenge data shall be stored in a new 5GS security context in the volatile memory of the ME.

The USIM will compute the authentication response (RES) using the authentication challenge data received from the ME, and pass RES to the ME.

In order to avoid a synchronisation failure, when the UE receives an AUTHENTICATION REQUEST message, the UE shall store the received RAND together with the RES returned from the USIM in the volatile memory of the ME. When the UE receives a subsequent AUTHENTICATION REQUEST message, if the stored RAND value is equal to the new received value in the AUTHENTICATION REQUEST message, then the ME shall not pass the RAND to the USIM, but shall send the AUTHENTICATION RESPONSE message with the stored RES. If there is no valid stored RAND in the ME or the stored RAND is different from the new received value in the AUTHENTICATION REQUEST message, the ME shall pass the RAND to the USIM, shall override any previously stored RAND and RES with the new ones and start, or reset and restart timer T3516.

The RAND and RES values stored in the ME shall be deleted and timer T3516, if running, shall be stopped:

- upon receipt of a

- SECURITY MODE COMMAND,

- SERVICE REJECT,

- REGISTRATION REJECT,

- REGISTRATION ACCEPT, or

- AUTHENTICATION REJECT message;

- upon expiry of timer T3516;

- if the UE enters the 5GMM state 5GMM-DEREGISTERED or 5GMM-NULL; or

- if the UE enters 5GMM-IDLE mode.

###### 8.5.1.1.3.4 Authentication completion by the network

Upon receipt of an AUTHENTICATION RESPONSE message, the network stops the timer T3560 and checks the correctness of RES (see 3GPP TS 33.501 [24]).

If the 5G AKA based primary authentication and key agreement procedure has been completed successfully and the related ngKSI is stored in the 5GS security context of the network, the network shall include a different ngKSI value in the AUTHENTICATION REQUEST message when it initiates a new 5G AKA based primary authentication and key agreement procedure.

Upon receipt of an AUTHENTICATION FAILURE message, the network stops the timer T3560. In the case where the 5GMM cause #21 "synch failure" is received, the core network may renegotiate with the UDM/AUSF and provide the UE with new authentication parameters.

###### 8.5.1.1.3.5 Authentication not accepted by the network

Editor’s note: Authentication not accepted for normal services by the network is FFS.

Depending on local requirements or operator preference for emergency services, if the UE initiates a registration procedure with 5GS registration type IE set to "emergency registration" and the AMF is configured to allow emergency registration without user identity, the AMF needs not follow the procedures specified for the authentication failure in the present subclause. The AMF may continue a current 5GMM specific procedure.

###### 8.5.1.1.3.6 Authentication not accepted by the UE

Editor’s note: Authentication not accepted by the UE is FFS.

###### 8.5.1.1.3.7 Abnormal cases

Editor’s note: Abnormal cases are FFS. However the below message flow is expected to apply, .i.e. an authentication failure message is needed.



Figure 8.5.1.1.3.7.2: Authentication failure during 5G AKA based primary authentication and key agreement procedure

#### 8.5.1.2 Security mode control procedure

##### 8.5.1.2.1 General

The purpose of the NAS security mode control procedure is to take an 5GS security context into use, and initialise and start NAS signalling security between the UE and the AMF with the corresponding 5GS NAS keys and 5GS security algorithms.

Furthermore, the network may also initiate the security mode control procedure in the following cases:

- in order to change the NAS security algorithms for a current 5GS security context already in use; and

- in order to change the value of uplink NAS COUNT used in the latest SECURITY MODE COMPLETE message as described in 3GPP TS 33.501 [24], subclause 8.3.1.4.2.

For restrictions concerning the concurrent running of a security mode control procedure with other security related procedures in the AS or inside the core network see 3GPP TS 33.501 [24], subclause 6.5.3.6.

##### 8.5.1.2.2 NAS security mode control initiation by the network

The AMF initiates the NAS security mode control procedure by sending a SECURITY MODE COMMAND message to the UE and starting timer Tyx (see example in figure 8.5.1.2.1).

The AMF shall reset the downlink NAS COUNT counter and use it to integrity protect the initial SECURITY MODE COMMAND message if the security mode control procedure is initiated:

- to take into use the S security context created after a successful execution of the 5G AKA based primary authentication and key agreement procedure;

- upon receipt of REGISTRATION REQUEST message including an eKSI, if the AMF wishes to create a mapped 5GS security context (i.e. the type of security context flag is set to "mapped security context" in the NAS key set identifier IE included in the SECURITY MODE COMMAND message).

Editor's note: The name of NAS key set identifier used in 5GS is FFS.

The AMF shall send the SECURITY MODE COMMAND message unciphered, but shall integrity protect the message with the 5GS integrity key based on KAMF or mapped K'AMF indicated by the ngKSI included in the message. The AMF shall set the security header type of the message to "integrity protected with new 5GS security context".

Editor's note: Handling at emergency registration and emergency PDU sessions is FFS.

Upon receipt of a REGISTRATION REQUEST message including an eKSI, if the AMF does not have the valid current 5GS security context indicated by the UE, the AMF shall indicate the use of the new mapped 5GS security context to the UE by setting the type of security context flag in the NAS key set identifier IE to "mapped security context" and the KSI value related to the security context of the source system.

Editor's note: Handling at non-existing 5GS security context indicated by the UE when an emergency PDU session exists is FFS.

While having a current mapped 5GS security context with the UE, if the AMF wants to take the native 5GS security context into use, the AMF shall include the ngKSI that indicates the native 5GS security context in the SECURITY MODE COMMAND message.

The AMF shall include the replayed security capabilities of the UE (including the security capabilities with regard to NAS, RRC and UP (user plane) ciphering as well as NAS and RRC integrity, and other possible target network security capabilities, i.e. E-UTRAN if the UE included them in the message to network), the replayed nonceUE when creating a mapped 5GS security context and if the UE included it in the message to the network, the selected 5GS ciphering and integrity algorithms and the Key Set Identifier (ngKSI).

The AMF shall include both the nonceAMF and the nonceUE when creating a mapped 5GS security context during inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode.

The AMF may initiate a SECURITY MODE COMMAND in order to change the 5GS security algorithms for a current 5GS security context already in use. The AMF re-derives the 5GS NAS keys from KAMF with the new 5GS algorithm identities as input and provides the new 5GS algorithm identities within the SECURITY MODE COMMAND message. The AMF shall set the security header type of the message to "integrity protected with new 5GS security context".

If, during an ongoing registration procedure, the AMF is initiating a SECURITY MODE COMMAND (i.e. after receiving the REGISTRATION REQUEST message, but before sending a response to that message) and the REGISTRATION REQUEST message does not successfully pass the integrity check at the AMF, the AMF shall calculate the HASHAMF of the entire plain REGISTRATION REQUEST message as described in 3GPP TS 33.501 [24] and shall include the HASHAMF in the SECURITY MODE COMMAND message.

Additionally, the AMF may request the UE to include its IMEISV in the SECURITY MODE COMPLETE message.

NOTE 2: The AS and NAS security capabilities will be the same, i.e. if the UE supports one algorithm for NAS, the same algorithm is also supported for AS.



Figure 8.5.1.2.1: Security mode control procedure

##### 8.5.1.2.3 NAS security mode command accepted by the UE

Upon receipt of the SECURITY MODE COMMAND message, the UE shall check whether the security mode command can be accepted or not. This is done by performing the integrity check of the message and by checking that the received replayed UE security capabilities and the received nonceUE have not been altered compared to the latest values that the UE sent to the network. However, the UE is not required to perform the checking of the received nonceUE if the UE does not want to re-generate the K'AMF (i.e. the SECURITY MODE COMMAND message is to derive and take into use a mapped 5GS security context and the ngKSI matches the current 5GS security context, if it is a mapped 5GS security context).

Editor's note: Handling at emergency PDU sessions is FFS.

Editor's note: Handling of "null algorithms" is FFS.

If the type of security context flag included in the SECURITY MODE COMMAND message is set to "native security context" and if the KSI matches a valid non-current native 5GS security context held in the UE while the UE has a mapped 5GS security context as the current 5GS security context, the UE shall take the non-current native 5GS security context into use which then becomes the current native 5GS security context and delete the mapped 5GS security context.

If the SECURITY MODE COMMAND message can be accepted, the UE shall take the 5GS security context indicated in the message into use. The UE shall in addition reset the uplink NAS COUNT counter if:

- the SECURITY MODE COMMAND message is received in order to take a 5GS security context into use created after a successful execution of the 5G AKA based primary authentication and key agreement procedure;

- the SECURITY MODE COMMAND message received includes the type of security context flag set to "mapped security context" in the NAS key set identifier IE the ngKSI does not match the current 5GS security context, if it is a mapped 5GS security context.

If the SECURITY MODE COMMAND message can be accepted and a new 5GS security context is taken into use and SECURITY MODE COMMAND message does not indicate the "null integrity protection algorithm"5G-IA0 as the selected NAS integrity algorithm, the UE shall:

- if the SECURITY MODE COMMAND message has been successfully integrity checked using an estimated downlink NAS COUNT equal to 0, then the UE shall set the downlink NAS COUNT of this new 5GS security context to 0;

- otherwise the UE shall set the downlink NAS COUNT of this new 5GS security context to the downlink NAS COUNT that has been used for the successful integrity checking of the SECURITY MODE COMMAND message.

If the SECURITY MODE COMMAND message can be accepted, the UE shall send a SECURITY MODE COMPLETE message integrity protected with the selected 5GS integrity algorithm and the 5GS NAS integrity key based on the KAMF or mapped K'AMF if the type of security context flag is set to "mapped security context" indicated by the ngKSI. When the SECURITY MODE COMMAND message includes the type of security context flag set to "mapped security context" in the NAS key set identifier IE, the nonceAMF and the nonceUE, then the UE shall either:

- generate K'AMF from both the nonceAMF and the nonceUE as indicated in 3GPP TS 33.501 [24];or

- check whether the SECURITY MODE COMMAND message indicates the ngKSI of the current 5GS security context, if it is a mapped 5GS security context, in order not to re-generate the K'AMF.

Furthermore, if the SECURITY MODE COMMAND message can be accepted, the UE shall cipher the SECURITY MODE COMPLETE message with the selected 5GS ciphering algorithm and the 5GS NAS ciphering key based on the KAMF or mapped K'AMF indicated by the ngKSI. The UE shall set the security header type of the message to "integrity protected and ciphered with new 5GS security context".

From this time onward the UE shall cipher and integrity protect all NAS signalling messages with the selected 5GS integrity and ciphering algorithms.

If the AMF indicated in the SECURITY MODE COMMAND message that the IMEISV is requested, the UE shall include its IMEISV in the SECURITY MODE COMPLETE message.

If, during an ongoing registration procedure, the SECURITY MODE COMMAND message includes a HASHAMF, the UE shall compare HASHAMF with a hash value locally calculated as described in 3GPP TS 33.501 [24] from the entire plain REGISTRATION REQUEST message that the UE had sent to initiate the procedure. If HASHAMF and the locally calculated hash value are different, the UE shall include the complete REGISTRATION REQUEST message which the UE had previously sent in the Replayed NAS message container IE of the SECURITY MODE COMPLETE message.

If, prior to receiving the SECURITY MODE COMMAND message, the UE had sent an initial NAS message containing a limited set of IEs needed to establish security context, the UE shall include the complete initial message in the NAS SECURITY MODE COMPLETE message.

##### 8.5.1.2.4 NAS security mode control completion by the network

The AMF shall, upon receipt of the SECURITY MODE COMPLETE message, stop timer Tyx. From this time onward the AMF shall integrity protect and encipher all signalling messages with the selected 5GS integrity and ciphering algorithms.

If the SECURITY MODE COMPLETE message contains a Replayed NAS container message IE with an REGISTRATION REQUEST message, the AMF shall complete the ongoing registration procedure by considering the REGISTRATION REQUEST message contained in the Replayed NAS message container IE as the message that triggered the procedure.

##### 8.5.1.2.5 NAS security mode command not accepted by the UE

If the security mode command cannot be accepted, the UE shall send a SECURITY MODE REJECT message. The SECURITY MODE REJECT message contains an 5GMM cause that typically indicates one of the following cause values:

#23: UE security capabilities mismatch;

#24: security mode rejected, unspecified.

Upon receipt of the SECURITY MODE REJECT message, the AMF shall stop timer Tyx. The AMF shall also abort the ongoing procedure that triggered the initiation of the NAS security mode control procedure.

Both the UE and the AMF shall apply the 5GS security context in use before the initiation of the security mode control procedure, if any, to protect the SECURITY MODE REJECT message and any other subsequent messages according to the rules in subclause TBD.

Editor´s note: The NAS security subclause in the present document is FFS.

##### 8.5.1.2.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication from lower layers (if the security mode control procedure is triggered by a registration procedure)

The UE shall abort the security mode control procedure and re-initiate the registration procedure.

b) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication with TAI change from lower layers (if the security mode control procedure is triggered by a service request procedure)

If the current TAI is not in the TAI list, the security mode control procedure shall be aborted and a registration procedure shall be initiated.

If the current TAI is still part of the TAI list, the security mode control procedure shall be aborted and it is up to the UE implementation how to re-run the ongoing procedure that triggered the security mode control procedure.

c) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication without TAI change from lower layers (if the security mode control procedure is triggered by a service request procedure)

The security mode control procedure shall be aborted and it is up to the UE implementation how to re-run the ongoing procedure that triggered the security mode control procedure.

##### 8.5.1.2.7 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure before the SECURITY MODE COMPLETE or SECURITY MODE REJECT message is received

The network shall abort the security mode control procedure.

b) Expiry of timer Tyx

The network shall, on the first expiry of the timer Tyx, retransmit the SECURITY MODE COMMAND message and shall reset and start timer Tyx. This retransmission is repeated four times, i.e. on the fifth expiry of timer Tyx, the procedure shall be aborted.

NOTE: If the SECURITY MODE COMMAND message was sent to create a mapped 5GS security context during inter-system change from S1 mode to N1 mode, then the network does not generate new values for the nonceAMF and the nonceUE, but includes the same values in the SECURITY MODE COMMAND message (see the subclause 6.7.2 in 3GPP TS 33.501 [24]).

c) Collision between security mode control procedure and registration, service request or detach procedure not indicating switch off

The network shall abort the security mode control procedure and proceed with the UE initiated procedure.

d) Collision between security mode control procedure and other 5GMM procedures than in item c

The network shall progress both procedures.

e) Lower layers indication of non-delivered NAS PDU due to handover

If the SECURITY MODE COMMAND message could not be delivered due to an intra AMF handover and the target TA is included in the TAI list, then upon successful completion of the intra AMF handover the AMF shall retransmit the SECURITY MODE COMMAND message. If a failure of the handover procedure is reported by the lower layer and the N1 signalling connection exists, the AMF shall retransmit the SECURITY MODE COMMAND message.

#### 8.5.1.3 NAS transport procedures

##### 8.5.1.3.1 General

The purpose of the NAS transport procedures is to provide a transport of payload between the UE to the AMF. Two alternatives are described: subclause 8.5.1.3.2 describes Alternative 1 where there is a dedicated set of procedures for each of SM transport and non-SM transport; and subclause 8.5.1.3.3 describes Alternative 2 where there is a single set of procedures for both SM and non-SM transport.

Editor's note: It is FFS whether to extend the UL SM MESSAGE TRANSPORT message and the UL GENERIC TRANSPORT message (for alternative 1 for NAS transport) and the UL NAS TRANSPORT message (for alternative 2 for NAS transport) to enable their usage as initial 5GMM message.

##### 8.5.1.3.2 Alternative 1 for NAS transport

###### 8.5.1.3.2.1 SM transport procedures

8.5.1.3.2.1.1 UE-initiated SM message transport procedure

8.5.1.3.2.1.1.1 General

The purpose of the UE-initiated SM transport message procedure is to provide transport of:

- an SM message; and

- associated routing information (the PDU session ID, the S-NSSAI, the DNN, the request type);

from the UE to the AMF in the 5GMM message.

5GSM procedures specified in clause 9 describe conditions for inclusion of the S-NSSAI, and the DNN.

The request type is not provided along SM messages other than the PDU SESSION ESTABLISHMENT REQUEST message.

8.5.1.3.2.1.1.2 UE-initiated SM message transport initiation

The UE shall set the SM message container IE of the UL SM MESSAGE TRANSPORT message to the SM message.

The UE shall set the PDU session ID IE of the UL SM MESSAGE TRANSPORT message to the PDU session ID.

If an S-NSSAI is to be included, the UE shall set the S-NSSAI IE of the UL SM MESSAGE TRANSPORT message to the S-NSSAI.

If a DNN is to be included, the UE shall set the DNN IE of the UL SM MESSAGE TRANSPORT message to the DNN.

If a request type is to be included, the UE shall set the request type IE of the UL SM MESSAGE TRANSPORT message to the request type.

The UE shall send the UL SM MESSAGE TRANSPORT message to the AMF (see example in figure 8.5.1.3.2.1.1.2.1).



Figure 8.5.1.3.2.1.1.2.1: UE-initiated SM transport procedure

8.5.1.3.2.1.1.3 UE-initiated SM message transport of messages

Upon reception of an UL SM MESSAGE TRANSPORT message, the AMF looks up a PDU session routing context for the PDU session ID of the UL SM MESSAGE TRANSPORT message and the UE and:

a) if the AMF has a PDU session routing context for the PDU session ID and the UE, and the request type IE is not included in the UL SM MESSAGE TRANSPORT message, the AMF shall forward the SM message, and the PDU session ID of the UL S SM MESSAGE TRANSPORT message towards the SMF ID of the PDU session routing context;

b) if the AMF has a PDU session routing context for the PDU session ID and the UE, the PDU session routing context indicates that the PDU session is not an emergency PDU session, and the request type IE is included in the UL S SM MESSAGE TRANSPORT message and is set to "existing PDU session", the AMF shall forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the SMF ID of the PDU session routing context;

c) if the AMF has a PDU session routing context for the PDU session ID and the UE, the request type IE is included in the UL SM MESSAGE TRANSPORT message and is set to "initial request" and the AMF received a reallocation requested indication from the SMF indicating that the SMF is to be reused, the AMF shall forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the SMF ID of the PDU session routing context;

d) if the AMF has a PDU session routing context for the PDU session ID and the UE, the request type IE is included in the UL SM MESSAGE TRANSPORT message and is set to "initial request", the AMF received a reallocation requested indication from the SMF indicating that the SMF is to be reallocated and the PDU session routing context does not contain reallocated SMF ID:

1) the AMF shall select an SMF. If the DNN is not included in the UL SM MESSAGE TRANSPORT message, the AMF shall use the default DNN as the DNN. If the S-NSSAI is not included in the UL SM MESSAGE TRANSPORT message, the AMF may determine a default S-NSSAI according to the user's subscription context obtained from UDM and, if determined, the AMF may use the default S-NSSAI as the S-NSSAI; and

NOTE: SMF selection is out of scope of CT1.

2) if the SMF selection is successful:

A) the AMF shall set the reallocated SMF ID of the PDU session routing context to the SMF ID of the selected SMF; and

B) the AMF shall forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the reallocated SMF ID of the PDU session routing context; and

e) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, and the request type IE is included in the UL SM MESSAGE TRANSPORT message and is set to "initial request":

1) the AMF shall select an SMF. If the DNN is not included in the UL SM MESSAGE TRANSPORT message, the AMF shall use the default DNN as the DNN. If the S-NSSAI is not included in the UL SM MESSAGE TRANSPORT message and:

A) if the user’s subscription context from UDM contains one default S-NSSAI only, the AMF may use the default S-NSSAI as the S-NSSAI, and

B) if the user's subscription context obtained from UDM contains several default S-NSSAIs, the AMF may select one of the default S-NSSAIs based on the operator policy and use the selected S-NSSAI as the S-NSSAI; and

NOTE: SMF selection is out of scope of CT1.

2) if the SMF selection is successful:

A) the AMF shall store a PDU session routing context for the PDU session ID and the UE and shall set the SMF ID in the stored PDU session routing context to the SMF ID of the selected SMF; and

B) the AMF shall forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the SMF ID of the PDU session routing context; and

f) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the request type IE of the UL SM MESSAGE TRANSPORT message is included and is set to "existing PDU session", and the user’s subscription context obtained from the UDM contains an SMF ID corresponding to:

1) the DNN of the UL SM MESSAGE TRANSPORT message, if the DNN is included in the NAS SM MESSAGE TRANSPORT message; or

2) the default DNN, if the DNN is not included in the UL SM MESSAGE TRANSPORT message;

Editor's note: FFS how to obtain the correct SMF ID when the UE has several PDU sessions with a given DNN, each PDU session is provided by a different SMF, and the UE attempts to handover one of those PDU sessions.

then:

1) the AMF shall store a PDU session routing context for the PDU session ID and the UE, shall set the SMF ID in the stored PDU session routing context to the SMF ID corresponding to the DNN in the user’s subscription context obtained from the UDM; and

2) the AMF shall forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the SMF ID of with the PDU session routing context;

f) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the request type IE is included in the UL SM MESSAGE TRANSPORT message and is set to "initial emergency request", and the AMF does not have a PDU session routing context for another PDU session ID of the UE indicating that the PDU session is an emergency PDU session:

1) the AMF shall select an SMF. The AMF shall use the emergency DNN from the AMF emergency configuration data as the DNN, if configured. The AMF shall use the statically configured SMF from the AMF emergency configuration data, if configured; and

NOTE: SMF selection is out of scope of CT1.

2) if the SMF selection is successful:

A) the AMF shall store a PDU session routing context for the PDU session ID and the UE and shall set the SMF ID in the stored PDU session routing context to the SMF ID of the selected SMF and shall store an indication that the PDU session is an emergency PDU session in the stored PDU session routing context; and

B) the AMF shall forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the SMF ID of the PDU session routing context; and

g) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the request type IE is included in the UL SM MESSAGE TRANSPORT message and is set to "initial emergency request", and the AMF has a PDU session routing context indicating that the PDU session is an emergency PDU session for another PDU session ID of the UE:

1) the AMF shall store a PDU session routing context for the PDU session ID and the UE and shall set the SMF ID in the stored PDU session routing context to the SMF ID of the PDU session routing context for the other PDU session ID of the UE; and

2) the AMF shall forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the SMF ID of the PDU session routing context.

Editor's note: Handover between 3GPP access and non-3GPP access of emergency PDU session is FFS.

8.5.1.3.2.1.1.4 Abnormal cases on the network side

The following abnormal cases in AMF are identified:

a) the AMF does not have a PDU session routing context for the PDU session ID of the UL SM MESSAGE TRANSPORT message and the UE, the request type IE of the UL SM MESSAGE TRANSPORT message is set to "initial request", and the SMF selection fails.

Editor's note: Handling of this abnormal case is FFS

b) the AMF does not have a PDU session routing context for the PDU session ID of the UL SM MESSAGE TRANSPORT message and the UE, the request type IE of the UL SM MESSAGE TRANSPORT message is set to "existing PDU session", and the user’s subscription context obtained from the UDM does not contain an SMF ID corresponding to.

1) the DNN of the UL SM MESSAGE TRANSPORT message, if the DNN is included in the NAS SM MESSAGE TRANSPORT message; or

2) the default DNN, if the DNN is not included in the UL SM MESSAGE TRANSPORT message.

Editor's note: Handling of this abnormal case is FFS

c) if the AMF has a PDU session routing context for the PDU session ID of the UL SM MESSAGE TRANSPORT message and the UE, the request type IE of the UL SM MESSAGE TRANSPORT message is set to "initial request" and the AMF has not received a reallocation requested indication, the AMF should forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the SMF ID of the PDU session routing context.

d) if the AMF has a PDU session routing context for the PDU session ID of the UL SM MESSAGE TRANSPORT message and the UE, the PDU session routing context indicates that the PDU session is an emergency PDU session, the request type IE of the UL SM MESSAGE TRANSPORT message is set to "initial emergency request", the AMF should forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the SMF ID of the PDU session routing context.

e) if the AMF has a PDU session routing context for the PDU session ID of the UL SM MESSAGE TRANSPORT message and the UE, the request type IE of the UL SM MESSAGE TRANSPORT message is set to "initial request", the AMF has received a reallocation requested indication from the SMF indicating that the SMF is to be reallocated, and the PDU session routing context contains reallocated SMF ID, the AMF should forward the SM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type of the UL SM MESSAGE TRANSPORT message towards the reallocated SMF ID of the PDU session routing context.

8.5.1.3.2.1.3 Network-initiated SM message transport procedure

8.5.1.3.2.1.3.1 General

The purpose of the network-initiated SM message transport procedure is to provide transport of an SM message and a PDU session ID from the AMF to the UE in a 5GMM message.

8.5.1.3.2.1.3.2 Network-initiated SM message transport initiation

Upon:

a) reception of an SM message without an N1 SM delivery skip allowed indication for a UE served from an SMF; or

b) reception of an SM message, and an N1 SM delivery skip allowed indication for a served UE from an SMF and if the UE is in the 5GMM-CONNECTED state;

the AMF shall create a DL SM MESSAGE TRANSPORT message.

The AMF shall set the SM message container IE of the DL SM MESSAGE TRANSPORT message to the SM message from the SMF.

The AMF shall set the PDU session ID IE of the DL SM MESSAGE TRANSPORT message to the PDU session ID.

Editor's note: FFS how AMF determines the PDU session ID - (a) the AMF can receive the PDU session ID along the SM message in the N11 message from the SMF, or (b) if there is one N11 connection for each PDU session then the AMF can locally derive the PDU session ID from identifier of the N11 connection via which the N11 message is received.

The AMF shall send the DL SM MESSAGE TRANSPORT message to the UE (see example in figure 8.5.1.3.2.1.3.2.1).



Figure 8.5.1.3.2.1.3.2.1: UE-initiated SM transport procedure

8.5.1.3.2.1.3.3 Network-initiated SM message transport of messages

The SM message and the PDU session ID of a received DL SM MESSAGE TRANSPORT message is handled in the 5GSM procedures specified in clause 9.

###### 8.5.1.3.2.2 Non-SM message transport procedures

8.5.1.3.2.2.1 General

The purpose of the procedures is to provide a transport of non-SM messages between the UE and the AMF. The type of the non-SM message is identified by the message container type IE and corresponds to one of the followings:

- SMS; or

- LTE Positioning Protocol (LPP) message (see 3GPP TS 36.355 [25]).

Editor's note: Other types, such as location-services, are FFS.

8.5.1.3.2.2.2 UE-initiated non-SM message transport procedure

8.5.1.3.2.2.2.1 General

The purpose of the UE-initiated non-SM message transport procedure is to provide a transport of:

- SMS; or

- an LPP message

from the UE to the AMF in a 5GMM message.

8.5.1.3.2.2.2.2 UE-initiated non-SM message transport initiation

The UE shall set the message container IE of the UL GENERIC TRANSPORT message to the non-SM message.

The UE shall set the message container type IE of the UL GENERIC TRANSPORT message to the type of the non-SM message.

Editor's note: How the UE selects the access type to deliver the UL GENERIC TRANSPORT message with the message container type IE set to "SMS" is FFS.

If the message container type IE of the UL GENERIC TRANSPORT message is set to "LTE Positioning Protocol (LPP) message container", the UE shall set the Additional information IE of the UL GENERIC TRANSPORT message to the routing information provided by the upper layer location services application.

Editor's note: The encoding of the Additional information IE in the UL GENERIC TRANSPORT message is FFS.

The UE shall send the UL GENERIC TRANSPORT message to the AMF (see example in figure 8.5.1.3.2.2.2.2.1).



Figure 8.5.1.3.2.2.2.2.1: UE-initiated non-SM message transport procedure

8.5.1.3.2.2.2.3 UE-initiated non-SM message transport of messages

Upon reception of an UL GENERIC TRANSPORT message with the message container type IE set to "SMS", the AMF shall forward the SMS message of the UL GENERIC TRANSPORT message towards the SMSF associated with the UE.

Upon reception of an UL GENERIC TRANSPORT message with the message container type IE set to "LTE Positioning Protocol (LPP) message container":

a) the AMF shall forward the LPP message of the UL GENERIC TRANSPORT message to the Location Management Function (LMF) associated with the routing information included in the Additional information IE of the UL GENERIC TRANSPORT message:

8.5.1.3.2.2.3 Network-initiated non-SM message transport procedure

8.5.1.3.2.2.3.1 General

The purpose of the network-initiated non-SM message transport procedure is to provide a transport of:

- SMS; or

- an LPP message

from the AMF to the UE in a 5GMM message.

8.5.1.3.2.2.3.2 Network-initiated non-SM message transport initiation

Upon reception of a non-SM message for a UE from the other network function (e.g. SMSF), the AMF shall create a DL GENERIC TRANSPORT message.

The AMF shall set the message container IE of the DL GENERIC TRANSPORT message to the non-SM message from the other network function.

The AMF shall set the message container type IE of the DL GENERIC TRANSPORT message to the type of the non-SM message.

If the message container type IE of the DL GENERIC TRANSPORT message is set to "LTE Positioning Protocol (LPP) message container", the AMF shall set the Additional information IE of the UL GENERIC TRANSPORT message to the routing information associated with the LMF from which the LPP message was received.

Editor's note: The encoding of the Additional information IE in the DL GENERIC TRANSPORT message is FFS.

The AMF shall select the access network (either 3GPP or non-3GPP) through which the DL GENERIC TRANSPORT message is sent. If the AMF sets the message container type IE to "SMS" and the access type selection is required, the AMF shall select the acces type to deliver the DL GENERIC TRANSPORT message as follows:

- if the UE to receive the DL GENERIC TRANSPORT message is registered to the network via both 3GPP access and non-3GPP access, and the SMS allowed IE in the 5GMM context of the UE is set to "both 3GPP access and non-3GPP access", then the AMF selects either 3GPP access or non-3GPP access; and

- otherwise, the AMF selects 3GPP access.

NOTE: The AMF selects an access type between 3GPP access and non-3GPP access based on operator policy.

Editor's note: The cases when the access type selection is required for SMS deliver are FFS.

The AMF shall send the DL GENERIC TRANSPORT message to the UE (see example in figure 8.5.1.3.2.2.3.2.1).



Figure 8.5.1.3.2.2.3.2.1: Network-initiated non-SM message transport procedure

8.5.1.3.2.2.3.3 Network-initiated non-SM message transport of messages

Upon reception of a DL GENERIC TRANSPORT message, if the message container type IE is set to:

a) "SMS", the UE shall forward the content of the message container IE to the SMS entity; and

b) "LTE Positioning Protocol (LPP) message container", the UE shall forward the content of the message container IE and of the Additional information IE to the upper layer location services application.

##### 8.5.1.3.3 Alternative 2 for NAS transport

###### 8.5.1.3.3.1 General

The purpose of the NAS transport procedures is to provide a transport of payload between the UE to the AMF. The type of the payload is identified by the Payload container type IE and includes one of the following:

- a single 5GSM message;

- SMS; or

- an LPP message (see 3GPP TS 36.355 [25]).

Editor’s note: Other types of payload, such as generic application payload, are FFS.

Along with the payload, the NAS transport procedure may transport the associated information (e.g. PDU session information for 5GSM message payload).

###### 8.5.1.3.3.2 UE-initiated NAS transport procedure

8.5.1.3.3.2.1 General

The purpose of the UE-initiated NAS transport procedure is to provide a transport of:

a) a single 5GSM message;

b) SMS; or

c) an LPP message

and optional associated payload routing information from the UE to the AMF in a 5GMM message.

8.5.1.3.3.2.2 UE-initiated NAS transport procedure initiation

In the connected mode, the UE initiates the NAS transport procedure by sending the UL NAS TRANSPORT message, as shown in figure 8.5.1.3.3.2.2.1.

In case a) in subclause 8.5.1.3.3.2.1, the UE shall:

- include the PDU session information (PDU session ID, old PDU session ID, S-NSSAI, DNN, request type), if available:

- set the Payload container type IE to "N1 SM information"; and

- set the Payload container IE to the 5GSM message.

The UE shall set the PDU session ID IE to the PDU session ID. If an old PDU session ID is to be included, the UE shall set the Old PDU session ID IE to the old PDU session ID.

If an S-NSSAI is to be included, the UE shall set the S-NSSAI IE to the S-NSSAI. If a DNN is to be included, the UE shall set the DNN IE to the DNN. 5GSM procedures specified in clause 9 describe conditions for inclusion of the S-NSSAI and the DNN.

If a request type is to be included, the UE shall set the Request type IE to the request type. The request type is not provided along 5GSM messages other than the PDU SESSION ESTABLISHMENT REQUEST message.

The UE shall send the UL NAS TRANSPORT message to the AMF (see example in figure 8.5.1.3.3.2.2.1).

In case b) in subclause 8.5.1.3.3.2.1, the UE shall:

- set the Payload container type IE to "SMS"; and

- set the Payload container IE to the SMS payload.

Editor's note: How the UE selects the access type to deliver the UL NAS TRANSPORT message with the Payload container type IE set to "SMS" is FFS.

In case c) in subclause 8.5.1.3.3.2.1, the UE shall:

- set the Payload container type IE to "LTE Positioning Protocol (LPP) message container";

- set the Payload container IE to the LPP message payload; and

- set the Additional information IE to the routing information provided by the upper layer location services application.



Figure 8.5.1.3.3.2.2.1: UE-initiated NAS transport procedure

8.5.1.3.3.2.3 UE-initiated NAS transport of messages

Upon reception of an UL NAS TRANSPORT message, if the Payload container type IE is set to:

a) "N1 SM information", the AMF looks up a PDU session routing context for the UE and the PDU session ID IE or the Old PDU session ID IE, if included, and:

1) if the AMF has a PDU session routing context for the PDU session ID and the UE, and the Request type IE is not included, the AMF shall forward the 5GSM message, and the PDU session ID IE towards the SMF identified by the SMF ID of the PDU session routing context;

2) if the AMF has a PDU session routing context for the PDU session ID and the UE, the PDU session routing context indicates that the PDU session is not an emergency PDU session, and the Request type IE is included and is set to "existing PDU session", the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type towards the SMF identified by the SMF ID of the PDU session routing context;

3) if the old PDU session ID IE is included in the UL NAS TRANSPORT message, the AMF has a PDU session routing context for the old PDU session ID and the UE, the Request type IE is included and is set to "initial request", and the AMF received a reallocation requested indication from the SMF indicating that the SMF is to be reused, the AMF shall forward the 5GSM message, the PDU session ID, the old PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type towards the SMF identified by the SMF ID of the PDU session routing context;

4) if the old PDU session ID IE is included in the UL NAS TRANSPORT message, the AMF has a PDU session routing context for the old PDU session ID and the UE, the Request type IE is included and is set to "initial request", the AMF received a reallocation requested indication from the SMF indicating that the SMF is to be reallocated, and the PDU session routing context does not contain reallocated SMF ID:

i) the AMF shall select an SMF. If the DNN IE is not included, the AMF shall use the default DNN as the DNN. If the S-NSSAI IE is not included, the AMF may determine a default S-NSSAI according to the user's subscription context obtained from UDM and, if determined, the AMF may use the default S-NSSAI as the S-NSSAI; and

NOTE: SMF selection is out of scope of CT1.

ii) if the SMF selection is successful:

A) the AMF shall set the reallocated SMF ID of the PDU session routing context to the SMF ID of the selected SMF; and

B) the AMF shall forward the 5GSM message, the PDU session ID, the old PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type towards the SMF identified by the reallocated SMF ID of the PDU session routing context;

5) if the old PDU session ID IE is included in the UL NAS TRANSPORT message, the AMF does not have a PDU session routing context for the PDU session ID and the UE, and the Request type IE is included and is set to "initial request":

i) the AMF shall select an SMF. If the DNN IE is not included, the AMF shall use the default DNN as the DNN. If the S-NSSAI IE is not included, the AMF may determine a default S-NSSAI according to the user’s subscription context obtained from UDM and, if determined, the AMF may use the default S-NSSAI as the S-NSSAI; and

ii) if the SMF selection is successful:

A) the AMF shall set the reallocated SMF ID of the PDU session routing context to the SMF ID of the selected SMF; and

B) the AMF shall forward the PDU session ID, the 5GSM message in the Payload container IE, the S-NSSAI (if received), the DNN (if received), and the request type of the UL NAS TRANSPORT message towards the SMF associated with the PDU session ID;

6) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is included and is set to "existing PDU session", and the user’s subscription context obtained from the UDM contains an SMF ID corresponding to:

i) the DNN in the DNN IE, if the DNN IE is included; or

ii) the default DNN, if the DNN IE is not included;

Editor's note: FFS how to obtain the correct SMF ID when the UE has several PDU sessions with a given DNN, each PDU session is provided by a different SMF, and the UE attempts to handover one of those PDU sessions.

then:

i) the AMF shall store a PDU session routing context for the PDU session ID and the UE, shall set the SMF ID in the stored PDU session routing context to the SMF ID corresponding to the DNN in the user’s subscription context obtained from the UDM; and

ii) the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type towards the SMF identified by the SMF ID of the PDU session routing context;

7) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the R Request type IE is included and is set to "initial emergency request", and the AMF does not have a PDU session routing context for another PDU session ID of the UE indicating that the PDU session is an emergency PDU session:

i) the AMF shall select an SMF. The AMF shall use the emergency DNN or emergency S-NSSAI from the AMF emergency configuration data as the DNN or S-NSSAI, if configured. The AMF shall use the statically configured SMF from the AMF emergency configuration data, if configured; and

ii) if the SMF selection is successful:

A) the AMF shall store a PDU session routing context for the PDU session ID and the UE, shall set the SMF ID in the stored PDU session routing context to the SMF ID of the selected SMF, and shall store an indication that the PDU session is an emergency PDU session in the stored PDU session routing context; and

B) the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if configured), the DNN (if configured), and the request type towards the SMF identified by the SMF ID of the PDU session routing context; and

8) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is included and is set to "initial emergency request", and the AMF has a PDU session routing context indicating that the PDU session is an emergency PDU session for another PDU session ID of the UE:

i) the AMF shall store a PDU session routing context for the PDU session ID and the UE and shall set the SMF ID in the stored PDU session routing context to the SMF ID of the PDU session routing context for the other PDU session ID of the UE; and

ii) the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if configured), the DNN (if configured) and the request type towards the SMF identified by the SMF ID of the PDU session routing context;

Editor's note: Handover between 3GPP access and non-3GPP access of emergency PDU session is FFS.

b) "SMS", the AMF shall forward the content of the Payload container IE to the SMSF associated with the UE; and

c) "LTE Positioning Protocol (LPP) message container", the AMF shall forward the content of the Payload container IE to the LMF associated with the routing information included in the Additional information IE of the UL NAS TRANSPORT message.

Editor's note: What to do if the AMF cannot locate the LMF is FFS.

8.5.1.3.3.2.4 Abnormal cases on the network side

The following abnormal cases in AMF are identified:

a) the old PDU session ID IE is not included in the UL NAS TRANSPORT message, the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is set to "initial request", and the SMF selection fails.

Editor's note: Handling of this abnormal case is FFS

b) the old PDU session ID IE is included in the UL NAS TRANSPORT message, the AMF has a PDU session routing context for the old PDU session ID and the UE, the Request type IE is set to "initial request", the AMF received a reallocation requested indication from the SMF indicating that the SMF is to be reallocated, and the SMF selection fails.

Editor's note: Handling of this abnormal case is FFS

c) the old PDU session ID IE is not included in the UL NAS TRANSPORT message and the AMF has not received a reallocation requested indication from the SMF.

Editor's note: Handling of this abnormal case is FFS

d) the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is set to "existing PDU session", and the user’s subscription context obtained from the UDM does not contain an SMF ID corresponding to.

1) the DNN of the DNN IE, if the DNN IE is included; or

2) the default DNN, if the DNN IE is not included.

Editor's note: Handling of this abnormal case is FFS

e) if the old PDU session ID IE is included in the UL NAS TRANSPORT message, and the AMF has a PDU session routing context for the PDU session ID and the UE, the Request type IE is set to "initial request" and the AMF has not received a reallocation requested indication, the AMF should forward the 5GSM message, the PDU session ID, the old PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type towards the SMF ID of the PDU session routing context.

f) if the AMF has a PDU session routing context for the PDU session ID and the UE, the PDU session routing context indicates that the PDU session is an emergency PDU session, the Request type IE is set to "initial emergency request", the AMF should forward the 5GSM message, the PDU session ID, the S-NSSAI (if configured), the DNN (if configured) and the request type towards the SMF ID of the PDU session routing context.

g) if the old PDU session ID IE is included in the UL NAS TRANSPORT message, and the AMF has a PDU session routing context for the PDU session ID and the UE, the Request type IE is set to "initial request", the AMF has received a reallocation requested indication from the SMF indicating that the SMF is to be reallocated, and the old PDU session routing context contains reallocated SMF ID, the AMF should forward the 5GSM message, the PDU session ID, the old PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type towards the reallocated SMF ID of the PDU session routing context.

h) if the Request type IE is set to "initial emergency request" and the S-NSSAI or the DNN is received, the AMF ignores the received S-NSSAI or the DNN and uses the emergency DNN or emergency S-NSSAI from the AMF emergency configuration data, if any.

###### 8.5.1.3.3.3 Network-initiated NAS transport procedure

8.5.1.3.3.3.1 General

The purpose of the network-initiated NAS transport procedure is to provide a transport of:

a) a single 5GSM message;

b) SMS; or

c) an LPP message

from the AMF to the UE in a 5GMM message.

###### 8.5.1.3.3.3.2 Network-initiated NAS transport procedure initiation

In connected mode, the AMF initiaties the NAS transport procedure by sending the DL NAS TRANSPORT message, as shown in figure 8.5.1.3.3.3.2.1.

In case a) in subclause 8.5.1.3.3.3.1, i.e. upon reception from an SMF of a 5GSM message without an N1 SM delivery skip allowed indication for a UE or a 5GSM message with an N1 SM delivery skip allowed indication for a UE in the 5GMM-CONNECTED mode, the AMF shall:

- include the PDU session information (PDU session ID) in the PDU session ID IE;

- set the Payload container type IE to "N1 SM information"; and

- set the Payload container IE to the 5GSM message.

In case b) in subclause 8.5.1.3.3.3.1, i.e. upon reception from an SMSF of an SMS payload, the AMF shall:

- set the Payload container type IE to "SMS";

- set the Payload container IE to the SMS payload ; and

- select the access type to deliver the DL NAS TRANSPORT message as follows in case the access type selection is required:

i) if the UE to receive the DL NAS TRANSPORT message is registered to the network via both 3GPP access and non-3GPP access, and the SMS allowed IE in the 5GMM context of the UE is set to "both 3GPP access and non-3GPP access", then the AMF selects either 3GPP access or non-3GPP access; and

ii) otherwise, the AMF selects 3GPP access.

NOTE: The AMF selects an access type between 3GPP access and non-3GPP access based on operator policy.

Editor's note: The cases when the access type selection is required for SMS delivery are FFS.

In case c) in subclause 8.5.1.3.3.3.1 i.e. upon reception from an LMF of an LPP message payload,, the AMF shall:

- set the Payload container type IE to "LTE Positioning Protocol (LPP) message container";

- set the Payload container IE to the LPP message payload received from the LMF; and

- set the Additional information IE to the routing information associated with the LMF from which the LPP message was received.



Figure 8.5.1.3.3.3.2.1: Network-initiated NAS transport procedure

###### 8.5.1.3.3.3.3 Network-initiated NAS transport of messages

Upon reception of a DL NAS TRANSPORT message, if the Payload container type IE is set to:

a) "N1 SM information".the 5GSM message in the Payload container IE and the PDU session ID are handled in the 5GSM procedures specified in clause 9;

b) "SMS", the UE shall forward the content of the Payload container IE to the SMS stack entity ; and

c) "LTE Positioning Protocol (LPP) message container", the UE shall forward the content of the Payload container IE and the routing information included in the Additional information IE to the upper layer location services application.

##### 8.5.1.3.4 Criteria for evaluation of alternatives for NAS transport

The following criteria are considered:

- message size

- scalability

- specification and implementation impact

- extensibility (future proof)

The criteria are not prioritized.

##### 8.5.1.3.5 Evaluation of the alternatives for NAS transport

###### 8.5.1.3.5.1 Message size

Alternative 2 requires to indicate the type of payload/container type carried inside the NAS transport message. This could be a separate IE, which would take up two octets, or it could be a field in the payload information IE, which would take up one octet.

Alternative 1 does not require an indication of the payload/container type in the SM transport message. The additional code points for the SM transport message type for Alternative 1 do not have impact on the coded message size.

All other information, such as payload routing information etc., needs to be present in the messages for both alternatives.

Alternative 2 allows the option of including 5GSM payload and SMS payload in the same NAS message, which is more efficient. Alternaitve 1 does not allow for that option.

In conclusion, for transport of SM messages through the AMF, Alternative 1 allows to save one or two of octets in the coded messages, depending on the coding. Alternative 2 allows to combine 5GSM payload and SMS in the same message.

###### 8.5.1.3.5.2 Scalability

Alternative 1 assumes that the transport of SM messages through the AMF needs special consideration and therefore merits a separate procedure.

Alternative 2 uses a single procedure for all types of payload passed transparently through the AMF.

###### 8.5.1.3.5.3 Implementation and specification impact

Alternative 1 requires a separate SM transport procedure for the transport of SM payload vs. non-SM transport procedure for the transport of other kind of payload. If the NAS transport becomes an initial procedure, then Alternative 1 would create two initial procedures. Alternative 1 also requires maintaining separate subclauses for SM transport procedure vs. non-SM transport procedure. Separate procedure failure handling would need to be maintained as well.

Alternative 2 requires a single procedure. If the NAS transport becomes an initial procedure, then Alternative 2 would create one initial procedure.

Each additional procedure entails development and testing effort.

###### 8.5.1.3.5.4 Extensibility

In Alternative 1, the UE-initiated non-SM message transport procedure and the Network-initiated non-SM message transport procedure can be extended to carry the new payload by adding new payload type and conainer.

In Alternaitve 2, UL and DL NAS Transport procedure can be extended to carry new payload type and container.

##### 8.5.1.3.6 Selection of the NAS transport mechanism

Based on the evaluation of the two alternatives in the subsequent subclauses, both alternatives fulfil the objective of transporting the payload transparently through the AMF. Both alternatives are extensible to carry new payload types transparently thorugh the AMF as needed.

Advantages of the Alternative 1 include:

- smaller message size for SM message transport by one to two octets (the message size for non-SM message transport is the same for both alternatives)

Advantages of Alternative 2 include:

- ability to combine 5GSM and SMS payload in the same NAS message; and

- lower implementation and specification complexity.

Alternative 2 is selected as the way forward in the normative phase.

#### 8.5.1.4 Generic UE configuration update procedure

##### 8.5.1.4.1 General

The purpose of this procedure is to allow the AMF to update UE configuration by providing new parameter information with the command or request the UE to perform a new registration update with the network to update parameters.

The procedure may be initiated by the network and can only be used when the UE has an established 5GMM context, and the UE is in 5GMM-CONNECTED mode. The AMF may require a confirmation response in order to ensure that the parameter has been updated by the UE.

The following parameters are supported by the generic UE configuration update procedure without the need for triggering UE Registration Update procedure:

a) 5G-GUTI;

b) TAI list;

c) Service area list;

d) Allowed NSSAI;

e) Network Identity and Time Zone information (Full name for network, Short name for network, Local time zone, Universal time and local time zone, Network daylight saving time); and

f) LADN information;

Editor's note: It is FFS which configuration parameters are updated by this procedure (e.g. policy information).

Editor's note: It is FFS whether the case when configuration provided by a different NF than the AMF is covered by this or a different NAS procedure (e.g. UE route selection policies (URSP) provided by PCF).

The following parameters require triggering UE Registration Update procedure:

a) MICO.

Editor’s note: Other parameters requiring negotiation are FFS.



Figure 8.5.1.4.1.1: Generic UE configuration update procedure

##### 8.5.1.4.2 Generic UE configuration update procedure initiated by the network

The AMF shall initiate the generic UE configuration procedure by sending the CONFIGURATION UPDATE COMMAND message to the UE.

The AMF shall in the CONFIGURATION UPDATE COMMAND message either:

a) include one or more of 5G-GUTI, TAI list, allowed NSSAI, LADN information, service area list or NITZ;

b) indicate registration requested; or

c) a combination of both.

If an acknowledgement from the UE is requested, the AMF shall indicate acknowledgement requested in the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message and shall start timer T3555. Acknowledgement shall be requested for all parameters except when only NITZ is included.

To initiate parameter re-negotiation between the UE and network, the AMF shall indicate "registration requested" in the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message. In this case, the acknowledgement shall be requested.

If a new allowed NSSAI information or AMF re-configuration of supported S-NSSAIs requires an AMF relocation, the AMF shall indicate "registration requested" in the Configuration update indication IE and include the Allowed NSSAI IE in the CONFIGURATION UPDATE COMMAND message. In this case, the acknowledgement shall be requested.

During an established 5GMM context, the network may send none, one, or more CONFIGURATION UPDATE COMMAND messages to the UE. If more than one CONFIGURATION UPDATE COMMAND message is sent, the messages need not have the same content.

##### 8.5.1.4.3 Generic UE configuration update accepted by the UE

Upon receiving the CONFIGURATION UPDATE COMMAND message, the UE shall use the contents to update appropriate information stored within the UE.

If acknowledgement requested is indicated in the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message and:

- if all information elements included are successfully accepted by the UE; or

- if "registration requested" in the Configuration update indication IE is indicated;

the UE shall send a CONFIGURATION UPDATE COMPLETE message.

If the UE receives a new 5G-GUTI in the CONFIGURATION UPDATE COMMAND message, the UE considers the new 5G-GUTI as valid and the old 5G-GUTI as invalid; otherwise, the UE shall consider the old 5G-GUTI as valid.

If the UE receives a new TAI list in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new TAI list as valid and the old TAI list as invalid; otherwise, the UE shall consider the old TAI list as valid.

If the UE receives a new service area list in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new service area list as valid and the old mobility restrictions as invalid; otherwise, the UE shall consider the old service area list, if any, as valid.

If the UE receives a new Allowed NSSAI in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new Allowed NSSAI as valid, store the Allowed NSSAI as specified in subclause 13.2.2 and consider the old Allowed NSSAI as invalid; otherwise, the UE shall consider the old Allowed NSSAI as valid.

If the UE receives an indication for "registration requested" in the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message that lacks an Allowed NSSAI IE, the UE shall send a REGISTRATION REQUEST message immediately as specified in subclause 8.2.4 to re-negotiate MICO mode with the network.

If the UE receives a new LADN information in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new LADN information as valid and the old LADN information as invalid; otherwise, the UE shall consider the old LADN information as valid.

If the UE receives an allowed NSSAI in the CONFIGURATION UPDATE COMMAND message and the UE has one or more PDU session contexts associated with S-NSSAI(s) not included in the received allowed NSSAI, the UE shall locally release all such PDU session context(s).

If the CONFIGURATION UPDATE COMMAND indicates "registration requested" in the Configuration update indication IE and a new allowed NSSAI is included, the UE shall release the existing NAS signalling connection and:

a) deactivate the PDU session(s) context locally, if any; and

b) set the 5G-GUTI as invalid and initiate a mobility registration update procedure with a REGISTRATION REQUEST message using SUPI as specified in subclause 8.2.3; and

c) should re-establish any previous active PDU sessions(s).

Editor’s note: It is FFS if the UE must wait for AMF to release the N1 NAS signalling connection prior to the UE attempts to initiate a mobility update procedure with SUPI.

Editor's note: Further details on handling of specific IEs are FFS.

##### 8.5.1.4.4 Generic UE configuration update completion by the network

Upon receipt of the CONFIGURATION UPDATE COMPLETE message, the AMF shall stop the timer T3555.

If a new 5G-GUTI was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the new 5G-GUTI as valid and the old 5G-GUTI as invalid.

If a new TAI list was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the new TAI list as valid and the old TAI list as invalid.

If a new service area list was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the new service area list as valid and the old service area list as invalid.

If new allowed NSSAI information was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the new Allowed NSSAI information as valid and the old allowed NSSAI information as invalid.

If a new LADN information was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the new LADN information as valid and the old LADN information as invalid.

Editor's note: Further details on handling of specific IEs are FFS.

##### 8.5.1.4.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of the CONFIGURATION UPDATE COMPLETE message.

Editor's note: Further abnormal cases in the UE are FFS.

##### 8.5.1.4.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3555.

The network shall, on the first expiry of the timer T3555, retransmit the CONFIGURATION UPDATE COMMAND message and shall reset and start timer T3555. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3555, the procedure shall be aborted.

b) Lower layer failure

If a lower layer failure is detected before the CONFIGURATION UPDATE COMMAND message is received, the old and the new 5G-GUTI shall be considered as valid until the old 5G-GUTI can be considered as invalid by the AMF. If a new TAI list was provided in the CONFIGURATION UPDATE COMMAND message, the old and new TAI list shall also be considered as valid until the old TAI list can be considered as invalid by the AMF.

During this period the AMF:

- may first use the old 5G-S-TMSI from the old 5G-GUTI for paging within the area defined by the old TAI list for an implementation dependent number of paging attempts for network originated transactions. If a new TAI list was provided with old 5G-GUTI in the CONFIGURATION UPDATE COMMAND message, the new TAI list should also be used for paging. Upon response from the UE, the AMF may re-initiate the CONFIGURATION UPDATE COMMAND. If the response is received from a tracking area within the old and new TAI list, the network shall re-initiate the CONFIGURATION UPDATE COMMAND. If no response is received to the paging attempts, the network may use the new 5G-S-TMSI from the new 5G-GUTI for paging for an implementation dependent number of paging attempts. In this case, if a new TAI list was provided with new 5G-GUTI in the CONFIGURATION UPDATE COMMAND message, the new TAI list shall be used instead of the old TAI list. Upon response from the UE the AMF shall consider the new 5G-GUTI as valid and the old 5G-GUTI as invalid. If no response is received to the paging attempts, the AMF may use the IMSI for paging for an implementation dependent number of paging attempts;

- shall consider the new 5G-GUTI as valid if it is used by the UE and, additionally, the new TAI list as valid if it was provided with this 5G-GUTI in the CONFIGURATION UPDATE COMMAND message; and

- may use the identification procedure followed by a new generic UE configuration update procedure if the UE uses the old 5G-GUTI.

Editor's note: Further abnormal cases in the network are FFS.

#### 8.5.1.5 Identification procedure

##### 8.5.1.5.1 General

The purpose of this procedure is to to request a particular UE to provide specific identification parameters, e.g. the SUPI or the PEI. SUPI and PEI definition and structure are specified in 3GPP TS 23.003 [5].

##### 8.5.1.5.2 Identification initiation by the network

The AMF initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and starting timer T3570 (see example in figure 8.5.1.5.2.1). The IDENTITY REQUEST message specifies the requested identification parameters in the Identity type information element.



Figure 8.5.1.5.2.1: Identification procedure

##### 8.5.1.5.3 Identification response by the UE

A UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in 5GMM-CONNECTED mode.

Upon receipt of the IDENTITY REQUEST message the UE shall send an IDENTITY RESPONSE message to the network. The IDENTITY RESPONSE message shall contain the identification parameters as requested by the network.

##### 8.5.1.5.4 Identification completion by the network

Upon receipt of the IDENTITY RESPONSE the network shall stop the timer Tf.

##### 8.5.1.5.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of the IDENTIFY RESPONSE message (if the identification procedure is triggered by a registration procedure).

Editor's note: Further abnormal cases in the UE are FFS.

##### 8.5.1.5.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3570

The network shall, on the first expiry of the timer T3570, retransmit the IDENTITY REQUEST message and reset and restart the timer T3570. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3570, the network shall abort the identification procedure and any ongoing 5GMM procedure.

Editor's note: Further abnormal cases in the network are FFS.

#### 8.5.1.6 5GMM status procedure

##### 8.5.1.6.1 General

The purpose of the 5GMM STATUS procedure is to report at any time in the 5GMM STATUS message certain error conditions detected upon receipt of 5GMM protocol data in the UE. The 5GMM STATUS message can be sent by both the AMF and the UE (see example in figure 8.5.1.6.1).



Figure 8.5.1.6.1: 5GMM status procedure

##### 8.5.1.6.2 5GMM status received in the UE

On receipt of a 5GMM STATUS message, no state transition and no specific action shall be taken as seen from the radio interface, i.e. local actions are possible. The local actions to be taken by UE on receipt of an 5GMM STATUS message are implementation dependent.

##### 8.5.1.6.3 5GMM status received in the network

On receipt of a 5GMM STATUS message in the AMF, no state transition and no specific action shall be taken as seen from the radio interface, i.e. local actions are possible. The local actions to be taken by the AMF on receipt of an 5GMM STATUS message are implementation dependent.

### 8.5.2 5GMM specific procedures

#### 8.5.2.1 Registration procedure

##### 8.5.2.1.1 General

The registration procedure is always initiated by the UE and can be used for the following purposes:

- initial registration for 5GS services;

- mobility registration updating to update the registration of the actual tracking area of a UE in the network;

- periodic registration updating to periodically notify the availability of the UE to the network;

- initial registration for emergency services;

- initial registration for SMS over NAS service, change in the requirements to use SMS over NAS service, and de-registration from SMS over NAS service.

Editor's note: Further purposes are FFS.

##### 8.5.2.1.2 Registration procedure for initial registration

###### 8.5.2.1.2.1 General

This procedure can be used by a UE for initial registration for 5GS services.

When the UE initiates the registration procedure for initial registration, the UE shall indicate "initial registration" in the 5GS registration type IE. When the UE initiates the registration procedure for emergency services, the UE shall indicate "emergency registration" in the 5GS registration type IE.

###### 8.5.2.1.2.2 Initial registration initiation

The UE initiates the registration procedure for initial registration by sending a REGISTRATION REQUEST message to the AMF, starting timer T3510. If timer T3502 is currently running, the UE shall stop timer T3502. If timer T3511 is currently running, the UE shall stop timer T3511.

If the UE holds a valid 5G-GUTI, the UE shall indicate the 5G-GUTI in the 5GS mobile identity IE. If the UE does not hold a valid 5G-GUTI, the UE shall include the SUPI in the 5GS mobile identity IE.

If the UE operating in the single-registration mode holds a valid 4G-GUTI only, the UE shall include the 5G-GUTI IE mapped from the 4G-GUTI as specified in 3GPP TS 23.003 [5] in the 5GS mobile identity IE of the REGISTRATION REQUEST message. If the UE operating in the single-registration mode holds a valid 4G-GUTI and a valid 5G-GUTI, it shall include in the 5GS mobile identity IE of the REGISTRATION REQUEST message either 5G-GUTI mapped from 4G-GUTI or 5G-GUTI according to the system (i.e. either EPS or 5GS), where the last successful EPS attach, tracking area updating or registration procedure was performed.

If the UE is operating in the dual-registration mode, the UE shall include the UE status IE with the EMM registration status set to "UE is in EMM-REGISTERED state". If the UE has a valid 5G-GUTI, the UE shall include the 5G-GUTI in the REGISTRATION REQUEST message. The UE operating in the dual-registration mode shall not use 4G-GUTI even if the UE has a valid 4G-GUTI.

If the last visited registered TAI is available, the UE shall include the last visited registered TAI in the REGISTRATION REQUEST message.

If the UE supports network slicing, the UE shall include the requested NSSAI containing the S-NSSAI(s) corresponding to the slice(s) to which the UE wishes to register in the REGISTRATION REQUEST. If the UE has allowed NSSAI or configured NSSAI for the current PLMN, the requested NSSAI shall be either:

- the configured NSSAI for the current PLMN, or a subset thereof as described below, if the UE has no allowed NSSAI for the current PLMN; or

- the allowed NSSAI for the current PLMN, or a subset thereof as described below, if the UE has an allowed NSSAI for the current PLMN; or

- the allowed NSSAI for the current PLMN, or a subset thereof as described below, plus one or more S-NSSAIs from the configured NSSAI for which no corresponding S-NSSAI is present in the allowed NSSAI and those are neither in the temporarily rejected NSSAI for the current registration are nor in the permanently rejected NSSAI for the current registration area.

Otherwise if the UE has neither allowed NSSAI nor configured NSSAI for the current PLMN, the UE shall not include a requested NSSAI in the REGISTRATION REQUEST message.

The subset of configured NSSAI provided in the requested NSSAI consists of one or more S-NSSAIs in the configured NSSAI applicable to the current PLMN, if:

- the S-NSSAI is neither in the temporarily rejected NSSAI for the current registration area nor in the permanently rejected NSSAI for the current registration area; or

- the S-NSSAI was not previously added by the UE in a requested NSSAI.

The subset of allowed NSSAI provided in the requested NSSAI consists of one or more S-NSSAIs in the allowed NSSAI for the current PLMN.

NOTE 1: How the UE selects the subset of configured NSSAI or allowed NSSAI to be provided in the requested NSSAI is implementation.

NOTE 2: The number of S-NSSAI(s) included in the requested NSSAI cannot exceed eight.

If the UE wishes to prolong the established NAS signalling connection after the completion of the initial registration procedure, it shall set the "follow-on request pending" indication to 1.

If the UE supports S1 mode, the UE shall set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message.



Figure 8.5.2.1.2.2.1: Registration procedure for initial registration

###### 8.5.2.1.2.3 5GMM common procedure initiation

The network may initiate 5GMM common procedures, e.g. the identification, authentication and security procedures during the registration procedure, depending on the information received in the REGISTRATION REQUEST message.

During a registration procedure with 5GS registration type IE set to "emergency registration", if the AMF is configured to support emergency registration for unauthenticated SUPIs, the AMF may choose to skip the authentication procedure even if no 5GS security context is available and proceed directly to the execution of the security mode control procedure.

###### 8.5.2.1.2.4 Initial registration accepted by the network

During a registration procedure with 5GS registration type IE set to "emergency registration", the AMF shall not check for mobility and access restrictions, regional restrictions or subscription restrictions, when processing the REGISTRATION REQUEST message.

If the initial registration request is accepted by the network, the AMF shall send a REGISTRATION ACCEPT message to the UE and start timer T3550.

The AMF shall assign and include a TAI list as a registration area the UE is registered to in the REGISTRATION ACCEPT message. The UE, upon receiving a REGISTRATION ACCEPT message, shall delete its old TAI list and store the received TAI list.

The 5G-GUTI reallocation may be part of the initial registration procedure. When the REGISTRATION REQUEST message includes the SUPI or PEI, or the AMF considers the 5G-GUTI provided by the UE is invalid, or the 5G-GUTI provided by the UE was assigned by another AMF, the AMF shall allocate a new 5G-GUTI to the UE. The AMF shall include in the REGISTRATION ACCEPT message the new assigned 5G-GUTI together with the assigned TAI list. In this case the AMF shall shall start timer T3550 and enter state 5GMM-COMMON-PROCEDURE-INITIATED as described in subclause 8.1.4.2.3.3.

If the REGISTRATION ACCEPT message contained a 5G-GUTI, the UE shall return a REGISTRATION COMPLETE message to the AMF to acknowledge the received 5G-GUTI.

Upon receiving a REGISTRATION COMPLETE message, the AMF shall stop timer T3550 and change to state 5GMM-REGISTERED. The 5G-GUTI, if sent in the REGISTRATION ACCEPT message, shall be considered as valid.

The AMF shall include the allowed NSSAI in the REGISTRATION ACCEPT if the UE included the requested NSSAI in the REGISTRATION REQUEST message and the AMF allows one or more S-NSSAIs in the requested NSSAI. The AMF may also include rejected NSSAI in the REGISTRATION ACCEPT message. Rejected NSSAI contains S-NSSAI(s) which was included in the Request NSSAI but rejected by the network associated with rejection cause(s).

The UE receiving the rejected NSSAI in the REGISTRATION ACCEPT message takes the following actions based on the rejection cause in the rejected NSSAI:

"S-NSSAI not available in the current PLMN"

The UE shall add the rejected S-NSSAI(s) in the permanently rejected NSSAI for the current PLMN as specified in subclause 13.2.2 and not attempt to use this S-NSSAI in the current PLMN until switching off the UE or the UICC containing the USIM is removed.

"S-NSSAI temporarily not available in the current PLMN"

The UE shall add the rejected S-NSSAI(s) in the temporarily rejected NSSAI for the current PLMN as specified in subclause 13.2.2 and consider this S-NSSAI is temporarily not available in the current PLMN.

Editor's note: It is FFS whether the rejection cause "S-NSSAI temporarily not available in this PLMN" is needed.

"S-NSSAI not available in the current registration area"

The UE shall add the rejected S-NSSAI(s) with the registration area(s) in the permanently rejected NSSAI for this PLMN as specified in subclause 13.2.2 and not attempt to use this S-NSSAI in the present registration area until switching off the UE, the UE moving out of the current registration area or the UICC containing the USIM is removed.

"S-NSSAI temporarily not available in the current registration area"

The UE shall add the rejected S-NSSAI(s) in the tempararily rejected NSSAI for the current PLMN and registration area combination as specified in subclause 13.2.2 and consider the S-NSSAI is temporarily not available in this current registration area.

Editor's note: Further UE action is FFS when the rejection cause is "S-NSSAI temporarily not available in the registration area".

The AMF may include in the allowed NSSAI one or more new S-NSSAIs each of which is associated with an S-NSSAI contained in the requested NSSAI.

If the UE did not include the requested NSSAI in the REGISTRATION REQUEST message and one or more subscribed S-NSSAIs (containing one or more S-NSSAIs each of which may be associated with a new S-NSSAI) marked as default are available, the AMF shall put the subscribed S-NSSAI(s) marked as default in the allowed NSSAI of the REGISTRAION ACCEPT message.

If the REGISTRATION ACCEPT contains the allowed NSSAI, then the UE shall store the included allowed NSSAI together with the PLMN identity of the registered PLMN and the registration area as specified in subclause 13.2.2.

If the UE included S1 mode supported indication in the REGISTRATION REQUEST message, the AMF supporting intersystem change with EPS shall set the dual-registration supported IE to either:

- "dual-registration not supported" if the AMF supports interworking procedures with N26 interface; or

- "dual-registration supported" if the AMF supports interworking procedures without N26 interface.

The UE shall operate in the mode for intersystem change with EPS as follows:

1) if the dual-registration supported IE is set to "dual-registration not supported", the UE shall operate in single-registration mode;

2) if the dual-registration support IE is set to "dual-registration supported" and the UE supports dual-registration mode,, the UE shall operate in dual-registration mode; or

3) if the dual-registration support IE is set to "dual-registration supported" and the UE only supports single-registration mode, the UE shall operate in single-registration mode,

The UE shall treat the received dual-registration supported IE for intersystem change with EPS as valid in the entire PLMN.

The network informs the UE about the support of specific features, such as IMS voice over PS session or emergency services, in the 5G network feature support information element. In a UE with IMS voice over PS session capability, the IMS voice over PS session indicator shall be provided to the upper layers. The upper layers take the IMS voice over PS session indicator into account when selecting the access domain for voice sessions or calls. When initiating an emergency call, the upper layers also take both the IMS voice over PS session indicator and the emergency service support indicator into account for the access domain selection.

Editor's note: Further details on initial registration accepted by the network are FFS.

If the UE has indicated "follow-on request pending" in REGISTRATION REQUEST message, the AMF shall not immediately release the NAS signalling connection after the completion of the registration procedure.

###### 8.5.2.1.2.5 Initial registration not accepted by the network

If the initial registration request cannot be accepted by the network, the AMF shall send a REGISTRATION REJECT message to the UE including an appropriate 5GMM cause value.

If the initial registration request request is rejected due to general NAS level mobility management congestion control, the network shall set the 5GMM cause value to #22 "congestion" and assign a back-off timer T3346.

The UE shall take the following actions depending on the 5GMM cause value received in the REGISTRATION REJECT message.

#xx (N1 mode not allowed);

The UE capable of S1 mode shall disable the N1 mode radio capabilities (see subclause 8.2.6).

#3 (Illegal UE);

#6 (Illegal ME);

#8 (5GS services not allowed); or

#22 (Congestion);

If the T3346 value IE is present in the REGISTRATION REJECT message and the value indicates that this timer is neither zero nor deactivated, the UE shall proceed as described below; otherwise it shall be considered as an abnormal case and the behaviour of the UE for this case is specified in subclause 8.5.2.1.2.7.

The UE shall abort the initial registration procedure, set the 5GS update status to 5U2 NOT UPDATED and enter state 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION.

The UE shall stop timer T3346 if it is running.

If the REGISTRATION REJECT message is integrity protected, the UE shall start timer T3346 with the value provided in the T3346 value IE.

If the REGISTRATION REJECT message is not integrity protected, the UE shall start timer T3346 with a random value from the default range specified in 3GPP TS 24.008 [12].

The UE stays in the current serving cell and applies the normal cell reselection process. The initial registration procedure is started if still needed when timer T3346 expires or is stopped.

Editor's note: Further details on initial registration not accepted by the network are FFS.

###### 8.5.2.1.2.6 Initial registration for emergency services not accepted by the network

Upon receiving the REGISTRATION REJECT message including 5GMM cause #5 "PEI not accepted", the UE shall enter the state 5GMM-DEREGISTERED.NO-SUPI.

Upon receiving the REGISTRATION REJECT message including 5GMM cause value which is not #5 "PEI not accepted", the UE shall perform the actions as described in subclause 8.5.2.1.2.5 with the following addition: the UE shall inform the upper layers of the failure of the procedure.

NOTE 1: This can result in the upper layers requesting implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 can result in the emergency call being attempted to another IP-CAN.

If the initial registration request for emergency services fails due to abnormal cases, the UE shall perform the actions as described in subclause 8.5.2.1.2.7 and inform the upper layers of the failure to access the network or the failure of the procedure.

NOTE 2: This can result in the upper layers requesting other implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 can result in the emergency call being attempted to another IP-CAN.

In a shared network, upon receiving the REGISTRATION REJECT message, the UE shall perform the actions as described in subclause 8.5.2.1.2.5, and shall:

a) inform the upper layers of the failure of the procedure; or

NOTE 1: The upper layers may request implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [13] that can result in the emergency call being attempted to another IP-CAN.

b) attempt to perform a PLMN selection in the shared network and initiate an initial registration for emergency services to the selected PLMN.

In a shared network, if the initial registration request for emergency services fails due to abnormal cases, the UE shall perform the actions as described in subclause 8.5.2.1.2.7 and shall:

a) inform the upper layers of the failure of the procedure; or

NOTE 2: The upper layers may request implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [13] that can result in the emergency call being attempted to another IP-CAN.

b) attempt the initial registration for emergency services to another PLMN in the shared network.

###### 8.5.2.1.2.7 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Timer T3346 is running

The UE shall not start the initial registration procedure unless:

- the UE is a UE configured to use AC11 – 15 in selected PLMN; or

- the UE needs to initial registration for emergency services

The UE stays in the current serving cell and applies the normal cell reselection process.

NOTE 1: It is considered an abnormal case if the UE needs to initiate an initial registration procedure while timer T3346 is running independent on whether timer T3346 was started due to an abnormal case or a non successful case.

###### 8.5.2.1.2.8 Abnormal cases on the network side

Editor's note: Abnormal cases in the network are FFS.

##### 8.5.2.1.3 Registration procedure for mobility and periodic registration update

###### 8.5.2.1.3.1 General

This procedure can be used by a UE for mobility and periodic registration update for 5GS services.

When the UE initiates the registration procedure for mobility and periodic registration update, the UE shall indicate "mobility registration update" or "periodic registration update" respectively in the 5GS registration type IE.

The periodic registration updating procedure is controlled in the UE by timer T3512. When timer T3512 expires, the periodic registration area updating procedure is started. Start and reset of timer T3512 is described in subclause 8.9.

###### 8.5.2.1.3.2 Mobility and periodic registration update initiation

The UE in state 5GMM-REGISTERED shall initiate the mobility and periodic registration updating procedure by sending a REGISTRATION REQUEST message to the AMF,

a) when the UE detects entering a tracking area that is not in the list of tracking areas that the UE previously registered in the AMF; or

b) when the periodic registration updating timer Te expires; or

c) when requested by CONFIGURATION UPDATE COMMAND.

Editor's note: Further cases for initiation of mobility and periodic registration update are FFS.

After sending the REGISTRATION REQUEST message to the AMF the UE shall start timer T3510. If timer T3502 is currently running, the UE shall stop timer T3502. If timer T3511 is currently running, the UE shall stop timer T3511.

If the last visited registered TAI is available, the UE shall include the last visited registered TAI in the REGISTRATION REQUEST message.

If the UE holds a valid 5G-GUTI, the UE shall indicate the 5G-GUTI in the 5GS mobile identity IE.

If the UE is initiating the mobility registration update procedure, the UE may include the uplink data status IE to indicate which PDU session(s) have pending user data to be sent. If the UE is located outside the LADN service area, the UE shall not include the PDU session for LADN in the uplink data status IE.

When the registration procedure is initiated in 5GMM-IDLE mode, the UE may include a PDU session status IE in the REGISTRATION REQUEST message, indicating which PDU session contexts are active in the UE.

If the UE operating in the single-registration mode performs mobility from S1 mode to N1 mode, the UE shall indicate "mobility registration update" in the 5GS registration type IE and shall include the UE status IE with the EMM registration status set to "UE is in EMM-REGISTERED state" in the REGISTRATION REQUEST message. In this case, if the UE holds a valid 4G-GUTI, the UE shall include the 5G-GUTI IE mapped from the 4G-GUTI as specified in 3GPP TS 23.003 [5] in the 5GS mobility identity IE of the REGISTRATION REQUEST message. The UE may include the PDU session status IE in the REGISTRATION REQUEST message indicating the status of the PDU session(s) mapped during the intersystem change from S1 mode to N1 mode from the PDN connection(s) for which the EPS indicated that interworking to 5GS is supported, if any (see subclause 11.2.4).

If the UE is operating in the dual-registration mode and the UE has a valid 5G-GUTI, the UE shall include the 5G-GUTI in the REGISTRATION REQUEST message. The UE operating in the dual-registration mode shall not use 4G-GUTI even if the UE has a valid 4G-GUTI.

If the UE supports network slicing, the UE shall include the requested NSSAI containing the S-NSSAIs corresponding to the slices to which the UE wishes to register in the REGISTRATION REQUEST. If the UE has allowed NSSAI or configured NSSAI for the current PLMN, the requested NSSAI shall be either:

- the configured NSSAI for the current PLMN, or a subset thereof as described below, if the UE has no allowed NSSAI for the current PLMN; or

- the allowed NSSAI for the current PLMN, or a subset thereof as described below, if the UE has an allowed NSSAI for the current PLMN; or

- the allowed NSSAI for the current PLMN, or a subset thereof as described below, plus one or more S-NSSAIs from the configured NSSAI for which no corresponding S-NSSAI is present in the allowed NSSAI and that were not previously rejected with "S-NSSAI not available in this PLMN" or "S-NSSAI not available in this registration area"(see subclause 8.5.2.1.2.4 and subclause 8.5.2.1.3.4) by the network for the present registration area.

Otherwise if the UE has neither allowed NSSAI nor configured NSSAI for the current PLMN, the UE shall not include a requested NSSAI in the REGISTRATION REQUEST message.

The subset of configured NSSAI provided in the requested NSSAI consists of one or more S-NSSAIs in the configured NSSAI applicable to this PLMN, if:

- the S-NSSAI was not previously rejected with "S-NSSAI not available in this PLMN" (see subclause 8.5.2.1.2.4 and subclause 8.5.2.1.3.4) by the network for the present registration area; or

- the S-NSSAI was not previously added by the UE in a requested NSSAI.

The subset of allowed NSSAI provided in the requested NSSAI consists of one or more S-NSSAIs in the allowed NSSAI for this PLMN.

NOTE 1: How the UE selects the subset of configured NSSAI or allowed NSSAI to be provided in the requested NSSAI is implementation.

NOTE 2: The number of S-NSSAI(s) included in the requested NSSAI cannot exceed eight.

If the UE wishes to prolong the established NAS signalling connection after the completion of the mobility and periodic registration updating registration procedure, it shall set the "follow-on request pending" indication to 1.



Figure 8.5.2.1.3.2.1: Registration procedure for mobility and periodic registration update

###### 8.5.2.1.3.3 5GMM common procedure initiation

The network may initiate 5GMM common procedures, e.g. the identification, authentication and security procedures during the registration procedure, depending on the information received in the REGISTRATION REQUEST message.

###### 8.5.2.1.3.4 Mobility and periodic registration update accepted by the network

If the registration update request has been accepted by the network, the AMF shall send a REGISTRATION ACCEPT message to the UE. If the AMF assigns a new 5G-GUTI for the UE, a 5G-GUTI shall be included in the REGISTRATION ACCEPT message. In this case, the AMF shall start timer T3550.

The AMF may include a new TAI list for the UE in the REGISTRATION ACCEPT message. The UE, upon receiving a REGISTRATION ACCEPT message, shall delete its old TAI list and store the received TAI list. If there is no TAI list received, the UE shall consider the old TAI list as valid.

If the AMF assigns a new 5G-GUTI for the UE, a 5G-GUTI shall be included in the REGISTRATION ACCEPT message. In this case the AMF shall start timer T3550 and enter state 5GMM-COMMON-PROCEDURE-INITIATED as described in subclause 8.1.4.2.3.3.

If the REGISTRATION ACCEPT message contained a 5G-GUTI, the UE shall return a REGISTRATION COMPLETE message to the AMF to acknowledge the received 5G-GUTI.

Upon receiving a REGISTRATION COMPLETE message, the AMF shall stop timer T3550 and change to state 5GMM-REGISTERED. The 5G-GUTI, if sent in the REGISTRATION ACCEPT message, shall be considered as valid.

The AMF shall include the allowed NSSAI in the REGISTRATION ACCEPT if the UE included the requested NSSAI in the REGISTRATION REQUEST message and the AMF allows one or more S-NSSAIs in the requested NSSAI. The AMF may also include rejected NSSAI in the REGISTRATION ACCEPT message. Rejected NSSAI contains S-NSSAI(s) which was included in the Request NSSAI but rejected by the network associated with rejection cause(s).

The UE receiving the rejected NSSAI in the REGISTRATION ACCEPT message takes the following actions based on the rejection cause in the rejected NSSAI:

"S-NSSAI not available in the current PLMN"

The UE shall add the rejected S-NSSAI(s) in the permanently rejected NSSAI for the current PLMN as specified in subclause 13.2.2 and not attempt to use this S-NSSAI in the current PLMN until switching off the UE or the UICC containing the USIM is removed.

"S-NSSAI temporarily not available in the current PLMN"

The UE shall add the rejected S-NSSAI(s) in the temporarily rejected NSSAI for the current PLMN as specified in subclause 13.2.2 and consider this S-NSSAI is temporarily not available in the current PLMN.

Editor's note: It is FFS whether the rejection cause "S-NSSAI temporarily not available in this PLMN" is needed.

"S-NSSAI not available in the current registration area"

The UE shall add the rejected S-NSSAI(s) in the permanently rejected NSSAI for the current PLMN and registration area combination as specified in subclause 13.2.2 and not attempt to use this S-NSSAI in the current registration area until switching off the UE, the UE moving out of the current registration area or the UICC containing the USIM is removed.

"S-NSSAI temporarily not available in the current registration area"

The UE shall add the rejected S-NSSAI(s) in the tempararily rejected NSSAI for the current PLMN and registration area combination as specified in subclause 13.2.2 and consider this S-NSSAI(s) is(are) temporarily not available in the current registration area.

Editor's note: Further UE action is FFS when the rejection cause is"S-NSSAI temporarily not available in the registration area".

If the UE did not include the requested NSSAI in the REGISTRATION REQUEST message and one or more subscribed S-NSSAIs marked as default are available, the AMF shall put the subscribed S-NSSAI(s) marked as default in the allowed NSSAI of the REGISTRATION ACCEPT message.

If the REGISTRATION ACCEPT contains the allowed NSSAI, then the UE shall store the included allowed NSSAI together with the PLMN identity of the registered PLMN and the registration area as specified in subclause 13.2.2. If the UE has one or more PDU session contexts associated with S-NSSAI(s) not included in the received allowed NSSAI, the UE shall locally release all such PDU session context(s).

The AMF may include in the allowed NSSAI one or more new S-NSSAIs each of which is associated with an S-NSSAI contained in the requested NSSAI.

If the uplink data status IE is included in the REGISTRATION REQUEST message, the AMF shall:

- indicate the SMF to re-activate the user plane for the corresponding PDU session; and

- include PDU session reactivation result IE in the REGISTRATION ACCEPT message to indicate the user plane reactivation result of the PDU sessions the UE requested to re-activate.

If the uplink data status IE is not included in the REGISTRATION REQUEST message, the AMF may indicate the SMF to re-activate the user plane for the PDU sessions.

If a PDU session status IE is included in the REGISTRATION REQUEST message, the AMF shall:

- release all those PDU session locally (without peer-to-peer signalling between the network and the UE) which are in 5GSM state PDU SESSION ACTIVE on the AMF side, but are indicated by the UE as being in 5GSM state PDU SESSION INACTIVE; and

- include a PDU session status IE in the REGISTRATION ACCEPT message to indicate which PDU sessions are active in the AMF.

If the AMF needs to initiate PDU session status synchronization the AMF shall include a PDU session status IE in the REGISTRATION ACCEPT message to indicate the UE which PDU sessions are active in the AMF.

The AMF may include the LADN information in the REGISTRATION ACCEPT message as described in subclause 8.5.2.1.2.4.

If the AMF does not include the LADN information in the REGISTATION ACCEPT message during mobility registration update procedure, the UE shall delete its old LADN information.

If the PDU session status IE is included in the REGISTRATION ACCEPT message, the UE shall release all those PDU sessions locally (without peer-to-peer signalling between the network and the UE) which are in 5GSM state PDU SESSION ACTIVE on the UE side, but are indicated by the AMF as being in 5GSM state PDU SESSION INACTIVE.

The network informs the UE about the support of specific features, such as IMS voice over PS session, in the 5G network feature support information element. In a UE with IMS voice over PS session capability, the IMS voice over PS session indicator shall be provided to the upper layers. The upper layers take the IMS voice over PS session indicator into account when selecting the access domain for voice sessions or calls.

Editor's note: Further details on mobility and periodic registration update accepted by the network are FFS.

If the UE has indicated "follow-on request pending" in REGISTRATION REQUEST message, the AMF shall not immediately release the NAS signalling connection after the completion of the registration procedure.

If the UE included in the REGISTRATION REQUEST message the UE status information IE with the EMM registration status set to "UE in EMM-REGISTERED state" and the AMF does not support N26 interface, the AMF shall operate as described in subclause 8.5.2.1.2.4.

###### 8.5.2.1.3.5 Mobility and periodic registration update not accepted by the network

If the mobility and periodic registration update request cannot be accepted by the network, the AMF shall send a REGISTRATION REJECT message to the UE including an appropriate 5GMM cause value.

The UE shall take the following actions depending on the 5GMM cause value received in the REGISTRATION REJECT message.

#xx (N1 mode not allowed);

The UE capable of S1 mode shall disable the N1 mode radio capabilities (see subclause 8.2.6).

#3 (Illegal UE);

#6 (Illegal ME); or

#8 (5GS services not allowed) or

#22 (Congestion);

If the T3346 value IE is present in the REGISTRATION REJECT message and the value indicates that this timer is neither zero nor deactivated, the UE shall proceed as described below, otherwise it shall be considered as an abnormal case and the behaviour of the UE for this case is specified in subclause 8.5.2.1.3.6.

The UE shall abort the mobility and periodic registration update procedure. If the rejected request was not for initiating a PDU session for emergency services, the UE shall set the 5GS update status to 5U2 NOT UPDATED and change to state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE.

The UE shall stop timer T3346 if it is running.

If the REGISTRATION REJECT message is integrity protected, the UE shall start timer T3346 with the value provided in the T3346 value IE.

If the REGISTRATION REJECT message is not integrity protected, the UE shall start timer T3346 with a random value from the default range specified in 3GPP TS 24.008 [12].

The UE stays in the current serving cell and applies the normal cell reselection process. The mobility and periodic registration update procedure is started, if still necessary, when timer T3346 expires or is stopped.

Editor's note: Further details on mobility and periodic registration update not accepted by the network are FFS.

###### 8.5.2.1.3.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Timer T3346 is running

The UE shall not start the mobility and periodic registration update procedure unless:

- the UE is in 5GMM-CONNECTED mode;

- the UE received a paging;

- the UE receives a NOTIFICATION message over non-3GPP access when the UE is in 5GMM-CONNECTED mode over non-3GPP access and in 5GMM-IDLE mode over 3GPP access;

- the UE is a UE configured to use AC11 – 15 in selected PLMN; or

- the UE has a PDU session for emergency services established or is establishing a PDU session for emergency services

The UE stays in the current serving cell and applies the normal cell reselection process.

NOTE 1: It is considered an abnormal case if the UE needs to initiate a mobility and periodic registration update procedure while timer T3346 is running independent on whether timer T3346 was started due to an abnormal case or a non successful case.

###### 8.5.2.1.3.7 Abnormal cases on the network side

Editor's note: Abnormal cases in the network are FFS.

#### 8.5.2.2 De-registration procedure

##### 8.5.2.2.1 General

The de-registration procedure is used:

- by the UE to de-register for 5GS services over 3GPP access when the UE is registered over 3GPP access;;

- by the UE to de-register for 5GS services over 3GPP access, non-3GPP access, or both when the UE is registered in the same PLMN over both accesses;

- by the network to inform the UE that it is deregistered for 5GS services over 3GPP access when the UE is registered over 3GPP access;

- by the network to inform the UE that it is deregistered for 5GS services over 3GPP access, non-3GPP access, or both when the UE is registered in the same PLMN over both accesses; and

- by the network to inform the UE to re-register to the network.

The de-registration procedure with appropriate de-registration type shall be invoked by the UE:

- if the UE is switched off.

The de-registration procedure with appropriate de-registration type shall be invoked by the network:

- if the network informs whether the UE should re-register to the network.

The de-registration procedure with appropriate access type shall be invoked by the UE:

- if the UE wishes to de-register for 5GS services over 3GPP access when the UE is registered over 3GPP access; or

- the UE wishes to de-register for 5GS services over 3GPP access, non-3GPP access, or both when the UE is registered in the same PLMN over both accesses.

If the de-registration procedure is triggered due to USIM removal, the UE shall indicate "switch off" in the de-registration type IE.

If the de-registration procedure is requested by the UDM for a UE that has PDU sessions for emergency services, the AMF shall not send a DEREGISTRATION REQUEST message to the UE.

If the de-registration procedure for 5GS services is performed, the PDU sessions, if any, for this particular UE are released locally without peer-to-peer signalling between the UE and the network.

The UE is allowed to initiate the de-registration procedure even if the timer T3346 is running.

##### 8.5.2.2.2 UE-initiated de-registration procedure

###### 8.5.2.2.2.1 UE-initiated de-registration procedure initiation

The de-registration procedure is initiated by the UE by sending a DEREGISTRATION REQUEST message (see example in figure 8.5.2.2.2.1.1). The De-registration type IE included in the message indicates whether the de-registration procedure is due to a "switch off" or not. The access type included in the message indicates whether the de-registration procedure is:

for 5GS services over 3GPP access, or

for 5GS services over both 3GPP access and non-3GPP access when the UE is registered in the same PLMN over both accesses.

If the UE has a valid 5G-GUTI, the UE shall populate the mobile identity IE with the valid 5G-GUTI. If the UE does not have a valid 5G-GUTI, the UE shall populate the mobile identity IE with its SUPI.

If the UE does not have a valid 5G-GUTI and it does not have a valid SUPI, then the UE shall populate the mobile identity IE with its PEI.

If the de-registration request is not due to switch off and the UE is in the state 5GMM-REGISTERED or 5GMM-REGISTERED-INITIATED, timer Txa shall be started in the UE after the DEREGISTRATION REQUEST message has been sent. The UE shall enter the state 5GMM-DEREGISTERED-INITIATED.

If the UE is to be switched off, the UE shall try for a period of 5 seconds to send the DEREGISTRATION REQUEST message. During this period, the UE may be switched off as soon as the DEREGISTRATION REQUEST message has been sent.



Figure 8.5.2.2.2.1.1: UE-initiated de-registration procedure

###### 8.5.2.2.2.2 UE-initiated de-registration procedure completion for 5GS services over 3GPP access

When the DEREGISTRATION REQUEST message is received by the AMF, the AMF shall send a DEREGISTRATION ACCEPT message to the UE, if the De-registration type IE does not indicate "switch off". Otherwise, the procedure is completed when the AMF receives the DEREGISTRATION REQUEST message.

If the access type in the DEREGISTRATION REQUEST indicates that the de-registration procedure is for 3GPP access, the AMF shall trigger the SMF to release the PDU session context(s) established over 3GPP access, if any, locally for this UE without peer-to-peer signalling between the UE and the SMF. The UE shall release the PDU session context(s) established over 3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE is marked as inactive in the AMF for 5GS services for 3GPP access. The AMF shall enter the state 5GMM-DEREGISTERED for 3GPP access.

The UE, when receiving the DEREGISTRATION ACCEPT message, shall stop timer Txa. Furthermore, if the UE supports N1 mode only then:

- If the de-registration procedure was performed due to disabling of 5GS services, then the UE shall enter the 5GMM-NULL state for 3GPP access.

- Otherwise, the UE shall enter the 5GMM-DEREGISTERED state for 3GPP access.

###### 8.5.2.2.2.3 UE-initiated de-registration procedure completion for 5GS services over both 3GPP access and non-3GPP access

The description for UE-initiated de-registration procedure completion for 5GS services over 3GPP access as specified in subclause 8.5.2.2.2.2 shall be followed. In addition, the following description for de-registration over non-3GPP access applies.

If the access type in the DEREGISTRATION REQUEST indicates that the de-registration procedure is for both 3GPP access and non-3GPP access when the UE is registered in the same PLMN over both accesses, the AMF shall trigger SMF to release the PDU session context(s) established over non-3GPP access, if any, locally for this UE without peer-to-peer signalling between the UE and the SMF. The UE shall release the PDU session context(s) established over non-3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE is marked as inactive in the AMF for 5GS services for non-3GPP access. The AMF shall enter the state 5GMM-DEREGISTERED over non-3GPP access.

If the UE supports N1 mode only then:

- If the de-registration procedure was performed due to disabling of 5GS services, then the UE shall enter the 5GMM-NULL state for non-3GPP access.

- Otherwise, the UE shall enter the 5GMM-DEREGISTERED state for non-3GPP access.

###### 8.5.2.2.2.4 Abnormal cases in the UE

Editor's note: Abnormal cases in the UE are FFS.

###### 8.5.2.2.2.5 Abnormal cases in the network side

Editor's note: Abnormal cases in the network are FFS.

##### 8.5.2.2.3 Network-initiated de-registration procedure

###### 8.5.2.2.3.1 Network-initiated de-registration procedure initiation

The network initiates the de-registration procedure by sending a DEREGISTRATION REQUEST message to the UE (see example in figure 8.5.2.2.3.1.1).

NOTE: If the AMF performs a local de-registration, it will inform the UE with a 5GMM messages (e.g. SERVICE REJECT or REGISTRATION REJECT) with 5GMM cause #10 "implicitly de-registered" only when the UE initiates a 5GMM procedure.

The network may include a 5GMM cause IE to specify the reason for the DEREGISTRATION REQUEST message. The network shall start timer T3522. The network shall indicate whether re-registration is needed or not in the De-registration type IE. The network shall also indicate via the access type whether the de-registration procedure is for 3GPP access, or for both 3GPP access and non-3GPP access when the UE is registered in the same PLMN for both accesses. The network shall release the PDU session context(s) over the indicated access(es), if any, for the UE locally and enter state 5GMM-DEREGISTERED-INITIATED.

Figure 8.5.2.2.3.1.1: Network-initiated de-registration procedure

###### 8.5.2.2.3.2 Network-initiated de-registration procedure completion by the UE

Upon receiving the DEREGISTRATION REQUEST message, and the DEREGISTRATION REQUEST message indicates "re-registration required" and the de-registration request is for 3GPP access, the UE shall release the PDU sessions over 3GPP access, if any, locally without peer-to-peer signalling between the UE and the network. The UE shall stop the timer(s) T3346, if it is running, T35ab, if it is running, T35cd, if it is running.The UE shall ignore the 5GMM cause IE if received. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for 3GPP access. The UE shall delete the temporarily rejected NSSAI(s) and permanently rejected NSSAI(s) for the current PLMN. Furthermore, the UE shall, after the completion of the de-registration procedure, and the release of the existing NAS signalling connection, initiate an initial registration. The UE should also re-establish any previously established PDU sessions.

Editor's note: it is FFS to use which timer for T35ab.

Editor's note: it is FFS to use which timer for T35cd.

Upon receiving the DEREGISTRATION REQUEST message and the DEREGISTRATION REQUEST message indicates "re-registration required" and the de-registration request is for both 3GPP access and non-3GPP access when the UE is registered in the same PLMN for both accesses, the UE shall release the PDU sessions over both 3GPP access and non-3GPP access, if any, locally without peer-to-peer signalling between the UE and the network. The UE shall stop the timer(s) T3346, if it is running, T35ab, if it is running, T35cd, if it is running.The UE shall ignore the 5GMM cause IE if received. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for both 3GPP access and non-3GPP access. Furthermore, the UE shall, after the completion of the de-registration procedure, and the release of the existing NAS signalling connection, initiate an initial registration. The UE should also re-establish any previously established PDU sessions.

NOTE 1: When the de-registration type indicates "re-registration required", user interaction is necessary in some cases when the UE cannot re-activate the PDU session (s), if any, automatically.

Upon receiving the DEREGISTRATION REQUEST message and the DEREGISTRATION REQUEST message indicates "re-registration not required" and the de-registration request is for 3GPP access, the UE shall release the PDU sessions over 3GPP access, if any, locally without peer-to-peer signalling between the UE and the network. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for 3GPP access.

Upon receiving the DEREGISTRATION REQUEST message and the DEREGISTRATION REQUEST message indicates "re-registration not required" and the de-registration request is for both 3GPP access and non-3GPP access when the UE is registered in the same PLMN for both accesses, the UE shall release the PDU sessions over both 3GPP access and non-3GPP access, if any, locally without peer-to-peer signalling between the UE and the network. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for both 3GPP access and non-3GPP access.

If the de-registration type indicates "re-registration required", then the UE shall ignore the 5GMM cause IE if received.

If the de-registration type indicates "re-registration not required", the UE shall take the actions depending on the received 5GMM cause value:

#xx (N1 mode not allowed);

The UE capable of S1 mode shall attempt to select an E-UTRA cell connected to EPC and disable the N1 mode radio capabilities (see subclause 8.2.6).

###### 8.5.2.2.3.3 Network-initiated de-registration procedure completion by the network

The network shall stop timer T3522 upon receipt of the DEREGISTRATION ACCEPT message. The network shall enter state 5GMM-DEREGISTERED for 3GPP access if the de-registration request is for 3GPP access. The network shall enter state 5GMM-DEREGISTERED for both 3GPP access and non-3GPP access if the de-registration request is for both 3GPP access and non-3GPP access.

###### 8.5.2.2.3.4 Abnormal cases in the UE

Editor's note: Abnormal cases in the UE are FFS.

###### 8.5.2.2.3.5 Abnormal cases in the network side

Editor's note: Abnormal cases in the network are FFS.

### 8.5.3 5GMM connection management procedures

#### 8.5.3.1 Service request procedure

##### 8.5.3.1.1 General

The purpose of the service request procedure is to change the 5GMM mode from 5GMM-IDLE to 5GMM-CONNECTED mode, and/or to request establishment of user-plane radio resources for PDU sessions which are activated without radio resources. In latter case, the 5GMM mode can be the 5GMM-IDLE mode or the 5GMM-CONNECTED mode over 3GPP access if the UE requires radio resources. This procedure is used when:

- the network has downlink signalling pending over 3GPP access and the UE is in 5GMM-IDLE mode over 3GPP access;

- the network has downlink signalling pending over non-3GPP access, the UE is in 5GMM-IDLE mode over non-3GPP access and in 5GMM-IDLE or 5GMM-CONNECTED mode over 3GPP access;

- the UE has uplink signalling pending over 3GPP access and the UE is in 5GMM-IDLE mode over 3GPP access;

- the network has downlink user data pending over 3GPP access and the UE is in 5GMM-IDLE mode over 3GPP access;

- the network has downlink user data pending over non-3GPP access, the UE is in 5GMM-IDLE mode over 3GPP access and in 5GMM-IDLE or 5GMM-CONNECTED mode over 3GPP access;

- the UE has user data pending over 3GPP access and the UE is in 5GMM-IDLE or 5GMM-CONNECTED mode over 3GPP access; or

- the UE in 5GMM-IDLE mode over non-3GPP access, receives an indication from the lower layers of non-3GPP access, that the access stratum connection is established between UE and network.

This procedure shall not be used for initiating user data transfer or PDU session related signalling related to a PDU session for LADN when the UE is located outside the LADN service area.

The service request procedure is initiated by the UE, however, it can be triggered by the network by means of:

- the paging procedure (see subclause 8.5.3.2) for the transfer of downlink signalling or user data pending over 3GPP access to a UE in 5GMM-IDLE mode over 3GPP access;

- the paging procedure (see subclause 8.5.3.2) for the transfer of downlink signalling or user data pending over non-3GPP access to a UE in 5GMM-IDLE mode over 3GPP access and in 5GMM-IDLE mode over non-3GPP access;

- the notification procedure (see subclause 8.5.3.3) for the transfer of downlink signalling or user data pending over non-3GPP access to a UE in 5GMM-CONNECTED mode over3GPP access and in 5GMM-IDLE mode over non-3GPP access; or

- the notification procedure (see subclause 8.5.3.3) for the transfer of downlink signalling or user data pending over 3GPP access to a UE in 5GMM-IDLE mode over 3GPP access and in 5GMM-CONNECTED mode over non-3GPP access.

NOTE: In case the UE is in 5GMM-IDLE mode over 3GPP access and in 5GMM-CONNECTED mode over non-3GPP access and downlink signalling or user data pending over 3GPP access needs to be transferred, the AMF can trigger either the notification procedure or the paging procedure based on implementation.

The UE shall invoke the service request procedure when:

a) the UE, in 5GMM-IDLE mode over 3GPP access, receives a paging request from the network;

b) the UE, in 5GMM-CONNECTED mode over 3GPP access, receives a notification from the network;

c) the UE, in 5GMM-IDLE mode over 3GPP access, has uplink signalling pending;

d) the UE, in 5GMM-IDLE mode over 3GPP access, has uplink user data pending;

e) the UE, in 5GMM-CONNECTED mode over 3GPP access, has user data pending due to no user-plane radio resources established for PDU session(s) used for user data transport;

f) the UE in 5GMM-IDLE mode over non-3GPP access, receives an indication from the lower layers of non-3GPP access, that the access stratum connection is established between UE and network; or

g) the UE, in 5GMM-IDLE mode over 3GPP access, receives a notification from the network when the UE is in 5GMM-CONNECTED mode over non-3GPP access.



Figure 8.5.3.1.1.1: Service Request procedure

##### 8.5.3.1.2 Service request procedure initiation

The UE initiates the service request procedure by sending a SERVICE REQUEST message to the AMF and starts timer T3517.

For case a in subclause 8.5.3.1.1:

- if the paging request includes an indication for non-3GPP access type, the Allowed PDU session status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) that the UE allows to be re-activate over 3GPP access;

- if the UE has uplink user data pending to be sent, the Uplink data status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) the UE has pending user data to be sent; or

- otherwise, the Uplink data status IE shall not be included in the SERVICE REQUEST message.

For case b in subclause 8.5.3.1.1, the Allowed PDU session status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) that the UE allows to re-activate over 3GPP access.

For case c and f in subclause 8.5.3.1.1, the Uplink data status IE shall not be included in the SERVICE REQUEST message.

For cases d and e in subclause 8.5.3.1.1, the Uplink data status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) the UE has pending user data to be sent.

For case g in subclause 8.5.3.1.1, if the UE has uplink user data pending to be sent, the Uplink data status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) the UE has pending user data to be sent.

The PDU session status information element may be included in the SERVICE REQUEST message to indicate the PDU session(s) available in the UE. If the PDU session status information element is included in the SERVICE REQUEST message, then the AMF shall release all those PDU session contexts locally (without peer-to-peer signalling between the UE and the network) which are in active on the AMF side, but are indicated by the UE as being inactive.

##### 8.5.3.1.3 Common procedure initiation

Upon receipt of the SERVICE REQUEST message, the AMF may initiate the common procedures e.g. the 5G AKA based primary authentication and key agreement procedure or the EAP based primary authentication and key agreement procedure.

##### 8.5.3.1.4 Service request procedure accepted by the network

For cases a, b, c, d, e and g in subclause 8.5.3.1.1, the UE shall treat the reception of the SERVICE ACCEPT message as successful completion of the procedure and stop timer T3517 and enter the state 5GMM-REGISTERED.

Editor's note: For cases a, b, d, e and g in subclause 8.5.3.1.1, whether the indication from the lower layers that the user-plane radio resources are set up needs to be considered as a successful completion of the procedure is FFS.

If the AMF needs to initiate PDU session status synchronization or a PDU session status IE was included in the SERVICE REQUEST message, the AMF shall include a PDU session status IE in the SERVICE ACCEPT message to indicate which PDU sessions are active in the AMF. If the PDU session status information element is included in the SERVICE ACCEPT message, then the UE shall release all those PDU sessions locally (without peer-to-peer signalling between the network and the UE) which are in active on the UE side, but are indicated by the AMF as being inactive.

The AMF may include the rejection cause in the SERVICE ACCEPT message if the UE initiated the service request procedure for a PDU Session corresponding to a LADN when the UE is located outside the LADN service area. The rejection cause indicates the PDU session is not activated due to LADN not available in the PDU session reactivation result IE.

If the Uplink data status IE is included in the SERVICE REQUEST message, the AMF shall:

- indicate the SMF to re-activate the user plane for the corresponding PDU session contexts; and

- include the PDU session reactivation result IE in the SERVICE ACCEPT message to indicate the user plane reactivation result of the PDU sessions the UE requested to re-activate.

If the Allowed PDU session status IE is included in the SERVICE REQUEST message, the AMF shall:

- indicate the SMF to re-activate the user plane for the corresponding PDU session contexts allowed to be re-activated over 3GPP access and have indicated pending downlink data; and

- notify the SMF that have indicated pending downlink data, that reactivation of the corresponding PDU Session contexts user plane cannot be performed if not allowed to be re-activated over 3GPP access; and

- include the PDU session reactivation result IE in the SERVICE ACCEPT message to indicate the successfully reactivated PDU session contexts.

##### 8.5.3.1.5 Service request procedure not accepted by the network

If the service request cannot be accepted, the network shall return a SERVICE REJECT message to the UE including an appropriate 5GMM cause value and stop timer T3517.

If the AMF needs to initiate PDU session status synchronisation or a PDU session status IE was included in the SERVICE REQUEST message, the AMF shall include a PDU session status IE in the SERVICE REJECT message to indicate which PDU sessions are active in the AMF. If the PDU session status IE is included in the SERVICE REJECT message, then the UE shall deactivate all those PDU sessions locally (without peer-to-peer signalling between the network and the UE) which are active on the UE side, but are indicated by the AMF as being inactive.

On receipt of the SERVICE REJECT message, if the message is integrity protected, the UE shall stop timer Tx if running. If the SERVICE REJECT message was received without integrity protection, then the UE shall discard the message.

If the service request for mobile originated services is rejected due to general NAS level mobility management congestion control, the network shall set the 5GMM cause value to #22 "congestion" and assign a value for back-off timer T3346.

The UE shall take the following actions depending on the 5GMM cause value received in the SERVICE REJECT message.

#xx (N1 mode not allowed);

The UE capable of S1 mode shall disable the N1 mode radio capabilities and attempt to select an E-UTRA cell connected to EPC. The UE shall re-enable the N1 mode radio capabilities when:

- the UE performs PLMN selection; and

- the UE powers off and powers on again or the USIM is removed.

#xy (Restricted service area):

The UE shall perform the mobility registration update procedure.

Editor's note: Whether the existing cause value(s) can be used for this purpose is FFS.

#3 (Illegal UE);

#6 (Illegal ME); or

#8 (5GS services not allowed).

Editor's note: Further details on UE actions upon receipt of the 5GMM cause value are FFS.

#10 (Implicitly de-registered).

Editor's note: Further details on UE actions upon receipt of the 5GMM cause value are FFS.

#22 (Congestion);

If the T3346 value IE is present in the SERVICE REJECT message and the value indicates that this timer is neither zero nor deactivated, the UE shall proceed as described below, otherwise it shall be considered as an abnormal case and the behaviour of the UE for this case is specified in subclause 8.5.3.1.6.

If the rejected request was not for initiating a PDU session for emergency services, the UE shall abort the service request procedure and enter state 5GMM-REGISTERED, and stop timer T3517 if still running.

The UE shall stop timer T3346 if it is running.

If the SERVICE REJECT message is integrity protected, the UE shall start timer T3346 with the value provided in the T3346 value IE.

If the SERVICE REJECT message is not integrity protected, the UE shall start timer T3346 with a random value from the default range specified in 3GPP TS 24.008 [12].

For all other cases the UE stays in the current serving cell and applies normal cell reselection process. The service request procedure is started, if still necessary, when timer T3346 expires or is stopped.

##### 8.5.3.1.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Timer T3346 is running

The UE shall not start the service request procedure unless:

- the UE receives a paging;

- the UE receives a NOTIFICATION message over non-3GPP access when the UE is in 5GMM-CONNECTED mode over non-3GPP access and in 5GMM-IDLE mode over 3GPP access;

- the UE is a UE configured to use AC11–15 in selected PLMN;

- the UE has a PDU session for emergency services established or is establishing a PDU session for emergency services;

If the UE is in 5GMM-IDLE mode, the UE stays in the current serving cell and applies normal cell reselection process. The service request procedure is started, if still necessary, when timer T3346 expires or is stopped.

##### 8.5.3.1.7 Abnormal cases on the network side

Editor's note: Abnormal cases on the network side are FFS.

#### 8.5.3.2 Paging procedure

##### 8.5.3.2.1 General

The paging procedure is used by the network to request the establishment of an NAS signalling connection to the UE. The paging procedure is also used by the network to request the UE to re-activate the user plane radio resources of PDU sessions for downlink user data transport. Another purpose of the paging procedure is to request the UE to re-activate the PDU session(s) associated with non-3GPP access over 3GPP access.

Additionally, the network can use the paging procedure to initiate the mobile terminating SMS.

##### 8.5.3.2.2 Paging for 5GS services

###### 8.5.3.2.2.1 General

The network shall initiate the paging procedure for 5GS services when NAS signalling messages or user data is pending to be sent to the UE in 5GMM-IDLE mode (see example in figure 8.5.3.2.2.1).



Figure 8.5.3.2.2.1.1: Paging procedure

To initiate the procedure the 5GMM entity in the AMF requests the lower layer to start paging and shall start timer T3513. Upon reception of a paging indication, the UE shall initiate a service request procedure to respond to the paging (see 3GPP TS 23.502 [10]).

Editor's note: It is FFS how the paging procedure is performed depending on different UE Identity of the paging message.

If downlink signalling or user data is pending to be sent over non-3GPP access, the 5GMM entity in the AMF shall indicate the lower layer that the paging is due to signalling or user data associated to non-3GPP access.

Upon reception of a paging indication, the UE shall stop the timer T3346, if running, and shall initiate the service request procedure over 3GPP access as specified in subclauses 8.5.3.1.

The network shall stop timer T3513 for the paging procedure when an integrity-protected response is received from the UE and successfully integrity checked by the network. If the response received is not integrity protected, or the integrity check is unsuccessful, timer T3513 for the paging procedure shall be kept running.

Upon expiry of timer T3513, the network may reinitiate paging.

If the network, while waiting for a response to the paging sent without paging priority, receives downlink signalling or downlink data associated with priority user-plane radio resources for PDU sessions, the network shall stop the timer for the paging procedure (i.e. either timer T3413), and then initiate the paging procedure with paging priority.

###### 8.5.3.2.2.2 Abnormal cases on the network side

Editor's note: Abnormal cases on the network side are FFS.

###### 8.5.3.2.2.3 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Paging message received with access type set to non-3GPP access while the UE is in 5GMM-CONNECTED mode overnon-3GPP access.

- The UE shall not respond to paging message.

Editor's note: Abnormal cases on the UE side are FFS.

#### 8.5.3.3 Notification procedure

##### 8.5.3.3.1 General

The notification procedure is used by the network:

a) to request the UE, by sending the NOTIFICATION message over 3GPP access, to re-activate the PDU session(s) associated with non-3GPP access over 3GPP access when the UE is in 5GMM-IDLE mode over non-3GPP access and in 5GMM-CONNECTED mode over 3GPP access; or

b) to request the UE, by sending the NOTIFICATION message over non-3GPP access, to re-activate the PDU session(s) associated with 3GPP access over 3GPP access when the UE is in 5GMM-CONNECTED mode over non-3GPP access and in 5GMM-IDLE mode over 3GPP access.

##### 8.5.3.3.2 Notification procedure initiation

The network shall initiate the notification procedure by sending the NOTIFICATION message to the UE and start timer Tx (see example in figure 8.5.3.3.2.1).

For a) in subclause 8.5.3.3.1, the NOTIFICATION message is sent from the network to the UE via 3GPP access.

For b) in subclause 8.5.3.3.1, the NOTIFICATION message is sent from the network to the UE via non-3GPP access.



Figure 8.5.3.3.2.1: Notification procedure

Upon reception of NOTIFICATION message, the UE may initiate a service request procedure over 3GPP access as specified in subclauses 8.5.3.1.

Upon reception of NOTIFICATION message:

- For case a) in subclause 8.5.3.3.1, if the UE decides not to initiate a service request procedure over 3GPP access based on UE policy;

- For case b) in subclause 8.5.3.3.1, if the UE is in 5GMM-REGISTERED.NO-CELL-AVAILABLE state or 5GMM-REGISTERED.PLMN-SEARCH state; or

then the UE shall respond with NOTIFICATION RESPONSE message indicating failure to re-activate the user plane radio resources of PDU sessions.

Editor's note: Message coding for NOTIFICATION RESPONSE message is FFS.

For case b) in subclause 8.5.3.3.1, upon reception of NOTIFICATION message, the UE shall stop the timer T3346, if running.

##### 8.5.3.3.3 Notification procedure completion

Upon reception of SERVICE REQUEST message, the network shall stop T3565 and trigger service request procedure as specified in subclauses 8.5.3.1.

Upon reception of NOTIFICATION RESPONSE message:

- For case a) in subclause 8.5.3.3.1, the AMF should notify the SMF that the UE was reachable but did not accept to re-activate the user plane radio resources of PDU sessions.

- For case b) in subclause 8.5.3.3.1, the AMF should notify the SMF that the UE is unreachable.

##### 8.5.3.3.4 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3565:

The network shall, on the first expiry of the timer T3565, retransmit the NOTIFICATION message and shall reset and start timer T3565. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3565, the procedure shall be aborted. In addition, upon the fifth expiry of timer T3565:

For case a) in subclause 8.5.3.3.1, the AMF should notify the SMF that the UE is unreachable. The AMF may enter 5GMM\_IDLE mode over 3GPP access.

For case b) in subclause 8.5.3.3.1, the AMF may either:

- perform the paging procedure over the 3GPP access; or

- notify the SMF that the UE is unreachable.

NOTE: Whether the AMF performs the paging procedure or notifies the SMF is up to operator’s policies.

Editor's note: Further abnormal cases on the network side are FFS.

## 8.6 5GS mobility management message coding

### 8.6.1 Authentication failure

#### 8.6.1.1 Message definition

This message is sent by the UE to the network to indicate that authentication of the network has failed. See table 8.6.1.1.

Message type: AUTHENTICATION FAILURE

Significance: dual

Direction: UE to network

Table 8.6.1.1: AUTHENTICATION FAILURE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Authentication failure message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  8.7.1 | M | V | 1 |

Editor's note: The further contents of the Authentication failure message is FFS. At least the following is needed: authentication failure parameter (optional).

### 8.6.2 Authentication reject

#### 8.6.2.1 Message definition

This message is sent by the network to the UE to indicate that the authentication procedure has failed and that the UE shall abort all activities. See table 8.6.2.1.

Message type: AUTHENTICATION REJECT

Significance: dual

Direction: network to UE

Table 8.6.2.1: AUTHENTICATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Authentication reject message identity | Message type  6.6.6.7 | M | V | 1 |

Editor's note: The content of the Authentication reject message is FFS.

### 8.6.3 Authentication request

#### 8.6.3.1 Message definition

This message is sent by the network to the UE to initiate authentication of the UE identity. See table 8.6.3.1.

Message type: AUTHENTICATION REQUEST

Significance: dual

Direction: network to UE

Table 8.6.3.1: AUTHENTICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Authentication request message identity | Message type  6.6.6.7 | M | V | 1 |
|  | ngKSI | NAS key set identifier  8.7.2 | M | V | 1/2 |
|  | Authentication parameter RAND (5G authentication challenge) | Authentication parameter RAND  8.7.3 | O | TV | 16 |
|  | Authentication parameter AUTN (5G authentication challenge) | Authentication parameter AUTN  8.7.4 | O | TLV | 17 |
| x | EAP message | EAP message  8.7.30 | O | TLV-E | 7-1503 |

Editor's note: The content of the Authentication request message is FFS.

#### 8.6.3.2 EAP message

EAP message IE is included if the AUTHENTICATION REQUEST message is used in an EAP authentication procedure.

### 8.6.4 Authentication response

#### 8.6.4.1 Message definition

This message is sent by the UE to the network to deliver a calculated authentication response to the network. See table 8.6.4.1.

Message type: AUTHENTICATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.6.4.1: AUTHENTICATION RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Authentication response message identity | Message type  6.6.6.7 | M | V | 1 |
| x | EAP message | EAP message  8.7.30 | O | TLV-E | 7-1503 |

Editor's note: The content of the Authentication response message is FFS. At least the following is needed: authentication response parameter (mandatory).

#### 8.6.4.2 EAP message

EAP message IE is included if the EAP message received in a related AUTHENTICATION REQUEST message was an EAP-request.

### 8.6.5 Registration request

#### 8.6.5.1 Message definition

The REGISTRATION REQUEST message is sent by the UE to the network.

Message type: REGISTRATION REQUEST

Significance: dual

Direction: UE to network

Table 8.6.5.1: REGISTRATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended Protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Registration request message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GS registration type | 5GS registration type  8.7.37 | M | V | TBD |
|  | ngKSI | NAS key set identifier  8.7.2 | M | V | 1 |
|  | Mobile identity | 5G mobile identity  8.7.16 | M | LV | TBD |
|  | NonceUE | Nonce  8.7.46 | O | TV | 5 |
|  | 5GMM capability | 5GMM capability  8.7.31 | O | TLV | 4-15 |
|  | UE security capability | UE security capability  8.7.47 | O | TLV | 4-6 |
|  | Requested NSSAI | NSSAI  8.7.29 | O | TBD | TBD |
|  | Last visited registered TAI | Tracking area identity  8.7.38 | O | TV | 6 |
|  | S1 UE network capability | S1 UE network capability  8.7.39 | O | TV | 6-13 |
|  | Uplink data status | Uplink data status  8.7.26 | O | TLV | 4 |
|  | PDU session status | PDU session status  8.7.27 | O | TLV | 4 |

Editor's note: The content of the REGISTRATION REQUEST message when a limited set of IEs including those needed to establish security in the initial message when it has no NAS security context is FFS.

#### 8.6.5.2 NonceUE

Editor's note: Inclusion criteria for NonceUE are FFS.

#### 8.6.5.3 5GMM capability

Editor's note: Inclusion criteria for 5GMM capability are FFS.

#### 8.6.5.4 UE security capability

Editor's note: Inclusion criteria for UE security capability are FFS.

#### 8.6.5.5 Requested NSSAI

Editor's note: Inclusion criteria for Requested NSSAI are FFS.

#### 8.6.5.6 Last visited registered TAI

Editor's note: Inclusion criteria for Last visited registered TAI are FFS.

#### 8.6.5.7 S1 UE network capability

Editor's note: Inclusion criteria for S1 UE network capability are FFS.

#### 8.6.5.8 Uplink data status

This IE shall be included if the UE has uplink user data pending to be sent.

#### 8.6.5.9 PDU session status

This IE shall be included if the UE wants to indicate the PDU session that are active within the UE.

### 8.6.6 Registration accept

#### 8.6.6.1 Message definition

The REGISTRATION ACCEPT message is sent by the network to the UE.

Message type: REGISTRATION ACCEPT

Significance: dual

Direction: network to UE

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Registration accept message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GS registration result | Registration result  8.7.40 | M | V | TBD |
|  | TAI list | Tracking area identity list  8.7.17 | O | TLV | 8-98 |
|  | 5G-GUTI | 5G mobile identity  8.7.16 | O | TLV | TBD |
|  | Equivalent PLMNs | PLMN list  8.7.41 | O | TLV | 5-47 |
|  | Allowed NSSAI | NSSAI  8.7.29 | O | TLV | TBD |
|  | Rejected NSSAI | NSSAI  8.7.29 | O | TLV | TBD |
|  | Dual registration supported | Dual registration supported  8.7.x9 | O | TBD | TBD |
|  | 5GMM network feature support | 5GMM network feature support  8.7.42 | O | TBD | TBD |
|  | PDU session status | PDU session status  8.7.27 | O | TLV | 4 |
|  | PDU session reactivation result | PDU session reactivation result  8.7.35 | O | TBD | TBD |
|  | LADN information | LADN information  8.7.32 | O | TBD | TBD |

#### 8.6.6.2 5G-GUTI

Editor's note: Inclusion criteria for 5G-GUTI are FFS.

#### 8.6.6.3 Equivalent PLMNs

Editor's note: Inclusion criteria for Equivalent PLMNs are FFS.

#### 8.6.6.4 TAI list

Editor's note: Inclusion criteria for TAI list are FFS.

#### 8.6.6.5 Allowed NSSAI

Editor's note: Inclusion criteria for Allowed NSSAI are FFS.

#### 8.6.6.6 Rejected NSSAI

Editor's note: Inclusion criteria for Rejected NSSAI are FFS.

#### 8.6.6.7 Dual registration supported

Editor's note: Inclusion criteria for Dual registration supported are FFS.

#### 8.6.6.8 5GMM network feature support

Editor's note: Inclusion criteria for 5GMM network feature support are FFS.

#### 8.6.6.8 PDU session status

This IE shall be included if the network wants to indicate the PDU session contexts that are active in the network.

#### 8.6.6.8 PDU session reactivation result

Editor's note: Inclusion criteria for PDU session reactivation result are FFS.

#### 8.6.6.8 LADN information

Editor's note: Inclusion criteria for LADN information are FFS.

### 8.6.7 Registration complete

#### 8.6.7.1 Message definition

The REGISTRATION COMPLETE message is sent by the UE to the network.

Message type: REGISTRATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.6.7.1: REGISTRATION COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1/2 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.65 | M | V | 1/2 |
|  | Registration complete message identity | Message type  6.6.6.6 | M | V | 1 |

### 8.6.8 Registration reject

#### 8.6.8.1 Message definition

The REGISTRATION REJECT message is sent by the network to the UE.

Message type: REGISTRATION REJECT

Significance: dual

Direction: network to UE

Table 8.6.8.1: REGISTRATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1/2 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Registration reject message identity | Message type  6.6.6.6 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  8.7.1 | M | V | 1 |
|  | T3346 value | GPRS timer 2  8.7.35 | O | TLV | 3 |

#### 8.6.8.2 T3346 value

The AMF may include this IE when the general NAS level mobility management congestion control is active

### 8.6.9 UL SM message transport for Alternative 1

#### 8.6.9.1 Message definition

The UL SM MESSAGE TRANSPORT message conveys an SM message and associated information from the UE to the network.

Message type: UL SM MESSAGE TRANSPORT

Significance: dual

Direction: UE to network

Table 8.6.9.1.1: UL SM MESSAGE TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | UL SM MESSAGE TRANSPORT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | SM message container | SM message container  8.7.5 | M | LV-E | 3-65537 |
| A | Request type | Request type  8.7.6 | O | TV | 1 |
| B | S-NSSAI | S-NSSAI  8.7.7 | O | TLV | 3 or 6 |
| C | DNN | DNN  8.7.8 | O | TLV | 3-TBD |

### 8.6.10 DL SM message transport for Alternative 1

#### 8.6.10.1 Message definition

DL SM MESSAGE TRANSPORT message conveys an SM message and associated information from the network to the UE.

Message type: DL SM MESSAGE TRANSPORT

Significance: dual

Direction: network to UE

Table 8.6.10.1.1: DL SM MESSAGE TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | DL SM MESSAGE TRANSPORT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | SM message container | SM message container  8.7.5 | M | LV-E | 3-65537 |

### 8.6.11 UL generic transport for Alternative 1

#### 8.6.11.1 Message definition

The UL GENERIC TRANSPORT message transports a non-SM message and associated information from the UE to the network.

Message type: UL GENERIC TRANSPORT

Significance: dual

Direction: UE to network

Table 8.6.11.1.1: UL GENERIC TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | UL GENERIC TRANSPORT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | Message container type | Message container type  8.7.9 | M | V | 1 |
|  | Message container | Message container  8.7.10 | M | LV-E | 2-65537 |

### 8.6.12 UL NAS transport for Alternative 2

#### 8.6.12.1 Message definition

The UL NAS TRANSPORT message transports message payload and associated information to the network.

Message type: UL NAS TRANSPORT

Significance: dual

Direction: UE to AMF

Table 8.6.12.1.1: UL NAS TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | UL NAS TRANSPORT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | Payload container type | Payload container type  8.7.11 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Payload container | Payload container  8.7.12 | M | LV-E | 3-65537 |
| R | PDU session ID | PDU session identity  6.6.6.4 | C | V | 1 |
| TBD | Old PDU session ID | Old PDU session identity  8.7.34 | O | TV | 2 |
| A | Request type | Request type  8.7.6 | O | TV | 1 |
| B | S-NSSAI | S-NSSAI  8.7.7 | O | TLV | 3-6 |
| C | DNN | DNN  8.7.8 | O | TLV | 3-102 |
| S | Additional information | Additional information  8.7.14 | O | TLV | 3-n |

#### 8.6.12.2 PDU session ID

The UE shall include this IE when the Payload container type IE is set to "N1 SM information".

#### 8.6.12.3 Old PDU session ID

The UE shall include this IE if the UL NAS TRANSPORT message transports a PDU SESSION ESTABLISHMENT REQUEST message upon receiving the PDU SESSION MODIFICATION COMMAND message with the 5GSM cause IE set to #39 "reactivation requested".

#### 8.6.12.4 Request type

The UE may include this IE when the PDU session ID IE is included.

#### 8.6.12.5 S-NSSAI

The UE may include this IE when the Request type IE is set to "initial request".

#### 8.6.12.6 DNN

The UE may include this IE when the Request type IE is set to "initial request".

#### 8.6.12.7 Additional information

The UE may include this IE when the Payload container type IE is set to "LTE Positioning Protocol (LPP) message container".

### 8.6.13 DL generic transport for Alternative 1

#### 8.6.13.1 Message definition

The DL GENERIC TRANSPORT message transports a non-SM message and associated information from the network to the UE.

Message type: DL GENERIC TRANSPORT

Significance: dual

Direction: Network to UE

Table 8.6.13.1.1: DL GENERIC TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | DL GENERIC TRANSPORT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | Message container type | Message container type  8.7.9 | M | V | 1 |
|  | Message container | Message container  8.7.10 | M | LV-E | 2-65537 |

### 8.6.14 DL NAS transport for Alternative 2

#### 8.6.14.1 Message definition

The DL NAS TRANSPORT message transports message payload and associated information to the UE.

Message type: DL NAS TRANSPORT

Significance: dual

Direction: AMF to UE

Table 8.6.14.1.1: DL NAS TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IEI** | **Information Element** | **Type/Reference** | **Presence** | **Format** | **Length** |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | DL NAS TRANSPORT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | Payload container type | Payload container type  8.7.11 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Payload container | Payload container  8.7.12 | M | LV-E | 3-65537 |
| r | PDU session ID | PDU session idenitty  6.6.6.4 | C | V | 1 |
| s | Additional information | Additional information  8.7.14 | O | TLV | 3-n |

#### 8.6.14.2 PDU session ID

The AMF shall include this IE when the Payload container type IE is set to "N1 SM information".

#### 8.6.14.3 Additional information

The AMF may include this IE when the Payload container type IE is set to "LTE Positioning Protocol (LPP) message container".

### 8.6.15 De-registration request (UE originating de-registration)

#### 8.6.15.1 Message definition

The DEREGISTRATION REQUEST message is sent by the UE to the network.

Message type: DEREGISTRATION REQUEST

Significance: dual

Direction: UE to network

Table 8.6.15.1.1: DEREGISTRATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | De-registration request message identity | Message type  6.6.6.7 | M | V | 1 |
|  | De-registration type | De-registration type  8.7.28 | M | V | 1 |
|  | 5GS mobile identity | 5GS mobile identity  8.7.16 | M | TLV | TBD |

### 8.6.16 De-registration accept (UE originating de-registration)

#### 8.6.16.1 Message definition

The DEREGISTRATION ACCEPT message is sent by the network to the UE.

Message type: DEREGISTRATION ACCEPT

Significance: dual

Direction: network to UE

Table 8.6.16.1.1: DEREGISTRATION ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | De-registration accept message identity | Message type  6.6.6.7 | M | V | 1 |

### 8.6.17 De-registration request (UE terminated de-registration)

#### 8.6.17.1 Message definition

The DEREGISTRATION REQUEST message is sent by the UE to the network.

Message type: DEREGISTRATION REQUEST

Significance: dual

Direction: network to UE

Table 8.6.17.1.1: DEREGISTRATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | De-registration request message identity | Message type  6.6.6.7 | M | V | 1 |
|  | De-registration type | De-registration type  8.7.28 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  8.7.1 | O | TV | 2 |
| TBD | T3346 value | GPRS timer 2  8.7.35 | O | TLV | 3 |

#### 8.6.17.2 5GMM cause

This information element is included if a 5GMM cause is provided.

#### 8.6.17.3 T3346 value

The AMF may include this IE when the general NAS level mobility management congestion control is active.

### 8.6.18 De-registration accept (UE terminated de-registration)

#### 8.6.18.1 Message definition

The DEREGISTRATION ACCEPT message is sent by the network to the UE.

Message type: DEREGISTRATION ACCEPT

Significance: dual

Direction: UE to network

Table 8.6.18.1.1: DEREGISTRATION ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | De-registration accept message identity | Message type  6.6.6.7 | M | V | 1 |

### 8.6.19 Service request

#### 8.6.19.1 Message definition

The SERVICE REQUEST message is sent by the UE to the network in order to request the establishment of an N1 NAS signalling connection and/or to request establishment of user-plane radio resources for PDU sessions which are activated without radio resources.

Message type: SERVICE REQUEST

Significance: dual

Direction: UE to network

Table 8.6.19.1: SERVICE REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Service request message identity | Message type  6.6.6.7 | M | V | 1 |
|  | ngKSI | NAS key set identifier  8.7.2 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.4 | M | V | 1/2 |
|  | Sequence number | Sequence number  8.7.24 | M | V | 1 |
|  | Message authentication code | Message authentication code  8.7.25 | M | V | 4 |
| TBD | Uplink data status | Uplink data status  8.7.26 | O | TLV | 4 |
| TBD | PDU session status | PDU session status  8.7.27 | O | TLV | 4 |
| TBD | Allowed PDU session status | Allowed PDU session status  8.7.36 | O | TLV | 4-34 |

#### 8.6.19.2 Uplink data status

This IE shall be included if the UE has uplink user data pending to be sent.

#### 8.6.19.3 PDU session status

This IE shall be included if the UE wants to indicate the PDU sessions that are active within the UE.

#### 8.6.19.4 Allowed PDU session status

This IE shall be included if the SERVICE REQUEST message is sent as a response to paging or notification via 3GPP access for PDU session(s) associated with non-3GPP access and the UE wants to indicate the non-3GPP PDU session(s) allowed to be re-activated over 3GPP access.

### 8.6.20 Service accept

#### 8.6.21.1 Message definition

The SERVICE ACCEPT message is sent by the network to the UE in order to accept the service request procedure.

Message type: SERVICE ACCEPT

Significance: dual

Direction: network to UE

Table 8.6.21.1: SERVICE ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Service accept message identity | Message type  6.6.6.7 | M | V | 1 |
| TBD | PDU session status | PDU session status  8.7.27 | O | TLV | 4 |
| TBD | PDU session reactivation result | PDU session reactivation result  8.7.33 | O | TLV | 4 |

#### 8.6.21.2 PDU session status

This IE shall be included if the network wants to indicate the PDU sessions that are active within the network.

#### 8.6.21.3 PDU session reactivation result

This IE shall be included if the uplink data status IE is included in the SERVICE REQUEST message.

### 8.6.22 Service reject

#### 8.6.22.1 Message definition

The SERVICE REJECT message is sent by the network to the UE in order to reject the service request procedure.

Message type: SERVICE REJECT

Significance: dual

Direction: network to UE

Table 8.6.22.1: SERVICE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Protocol discriminator | Protocol discriminator  9.2 | M | V | 1/2 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Service reject message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  8.7.1 | M | V | 1 |
| TBD | PDU session status | PDU session status  8.7.27 | O | TLV | 4 |
| TBD | T3346 value | GPRS timer 2  8.7.35 | O | TLV | 3 |

#### 8.6.22.2 PDU session status

This IE shall be included if the network wants to indicate the PDU sessions that are active within the network.

#### 8.6.22.3 T3346 value

The AMF may include this IE when the general NAS level mobility management congestion control is active.

### 8.6.23 Configuration update command

#### 8.6.23.1 Message definition

The CONFIGURATION UPDATE COMMAND message is sent by the network to the UE.

Message type: CONFIGURATION UPDATE COMMAND

Significance: dual

Direction: network to UE

Table 8.6.23.1.1: CONFIGURATION UPDATE COMMAND message content

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IEI | Information Element | | Type/Reference | | Presence | | Format | | Length | |
|  | Extended protocol discriminator | | Extended protocol discriminator  6.6.6.2 | | M | | V | | 1 | |
|  | Security header type | | Security header type  6.6.6.3 | | M | | V | | 1/2 | |
|  | Spare half octet | | Spare half octet  6.6.6.5 | | M | | V | | 1/2 | |
|  | Configuration update command message identity | | Message type  6.6.6.7 | | M | | V | | 1 | |
|  | Configuration update indication | | Configuration update indication  8.7.15 | | M | | V | | 1/2 | |
|  | Spare half octet | | Spare half octet  6.6.6.5 | | M | | V | | 1/2 | |
| A | 5G-GUTI | | 5GS mobile identity  87.16 | | O | | TLV | | TBD | |
| B | TAI list | | Tracking area identity list  8.7.17 | | O | | TLV | | 8-98 | |
|  | | Allowed NSSAI | | NSSAI  8.7.28 | | O | | TLV | | 4-82 |
| C | Service area list | | Service area list  8.7.18 | | O | | TLV | | 6-194 | |
| D | Full name for network | | Network name  8.7.19 | | O | | TLV | | 3-n | |
| E | Short name for network | | Network name  8.7.19 | | O | | TLV | | 3-n | |
| F | Local time zone | | Time zone  8.7.20 | | O | | TV | | 2 | |
| G | Universal time and local time zone | | Time zone and time  8.7.21 | | O | | TV | | 8 | |
| H | Network daylight saving time | | Daylight saving time  8.7.22 | | O | | TLV | | 3 | |
| I | LADN information | | LADN information  8.7.32 | | O | | TLV-E | | 13-1602 | |

Editor's note: The further contents of the CONFIGURATION UPDATE COMMAND message is FFS.

### 8.6.24 Configuration update complete

#### 8.6.24.1 Message definition

The CONFIGURATION UPDATE COMPLETE message is sent by the UE to the network.

Message type: CONFIGURATION UPDATE COMPLETE

Significance: dual

Direction: UE to network

Table 8.6.24.1.1: CONFIGURATION UPDATE COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | ½ |
|  | Configuration update complete message identity | Message type  6.6.6.7 | M | V | 1 |

Editor's note: The further contents of the CONFIGURATION UPDATE COMPLETE message is FFS.

### 8.6.25 Identity request

#### 8.6.25.1 Message definition

The IDENTITY REQUEST message is sent by the network to the UE to request the UE to provide specified identity.

Message type: IDENTITY REQUEST

Significance: dual

Direction: AMF to UE

Table 8.6.25.1: IDENTITY REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Identity request message identity | Message type  6.6.6.7 | M | V | 1 |
|  | Identity type | Identity type  FFS | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |

Editor’s note: The reference to "identity type" information element is FFS as certain identities will need to be defined.

### 8.6.26 Identity response

#### 8.6.26.1 Message definition

The IDENTITY RESPONSE message is sent by the UE to the AMF to provide the requested identity.

Message type: IDENTITY RESPONSE

Significance: dual

Direction: UE to AMF

Table 8.6.26.1: IDENTITY RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | Identity response message identity | Message type  6.6.6.7 | M | V | 1 |
|  | Mobile identity | 5GS mobile identity  8.7.16 | M | LV | TBD |

### 8.6.27 Notification

#### 8.6.27.1 Message definition

This message is sent by the network to the UE to notify the UE to initiate a service request procedure. See table 8.6.27.1.

Message type: NOTIFICATION

Significance: dual

Direction: network to UE

Table 8.6.27.1: NOTIFICATION message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | ½ |
|  | Notification message identity | Message type  6.6.6.7 | M | V | 1 |

Editor's note: The further contents of the NOTIFICATION message is FFS.

### 8.6.28 5GMM status

#### 8.6.28.1 Message definition

This message is sent by the UE or by the network at any time to report certain error conditions. See table 8.6.28.1.

Message type: 5GMM STATUS

Significance: local

Direction: both

Table 8.6.28.1: 5GMM STATUS message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.5 | M | V | 1/2 |
|  | 5GMM STATUS message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  8.7.1 | M | V | 2 |

### 8.6.29 Security mode command

#### 8.6.29.1 Message definition

This message is sent by the network to the UE to establish NAS signalling security. See table 8.6.29.1.1.

Message type: SECURITY MODE COMMAND

Significance: dual

Direction: network to UE

Table 8.6.29.1.1: SECURITY MODE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.4 | M | V | 1/2 |
|  | Security mode command message identity | Message type  6.6.6.7 | M | V | 1 |
|  | Selected NAS security algorithms | NAS security algorithms  8.7.45 | M | V | 1 |
|  | NAS key set identifier | NAS key set identifier  8.7.2 | M | V | 1 |
|  | Replayed UE security capabilities | UE security capability  8.7.47 | M | LV | 3-5 |
| xa | Allowed NSSAI | NSSAI  8.7.28 | O | TBD | TBD |
| xb | IMEISV request | IMEISV request  8.7.44 | O | TV | 1 |
| xc | Replayed nonceUE | Nonce  8.7.46 | O | TV | 5 |
| xd | NonceAMF | Nonce  8.7.46 | O | TV | 5 |
| xe | HashAMF | HashAMF  8.7.48 | O | TV | 9 |
| xf | EAP message | EAP message  8.7.30 | O | TLV-E | 7 |

#### 8.6.29.2 Allowed NSSAI

The AMF may include this information element to indicate Allowed NSSAI.

Editor’s note: In 3GPP TS 33.501 [24] v0.4.0 inclusion of the Allowed NSSAI is indicated to be mandatory in the SECURITY MODE COMMAND message. Whether this is correct or if inclusion is optional is FFS.

#### 8.6.29.3 IMEISV request

The AMF may include this information element to request the UE to send its IMEISV with the corresponding SECURITY MODE COMPLETE message.

#### 8.6.29.4 Replayed nonceUE

The AMF may include this information element to indicate to the UE to use the replayed nonceUE.

#### 8.6.29.5 NonceAMF

The AMF may include this information element to indicate to the UE to use the nonceAMF.

#### 8.6.29.6 HashAMF

The AMF shall include this information element when the AMF is initiating a SECURITY MODE COMMAND during a registration procedure and the REGISTRATION REQUEST message did not successfully pass the integrity check at the AMF.

8.6.29.7 EAP message

This IE is included when the EAP Success message is sent as part of the EAP-based primary authentication and key agreement procedure, as specified in subclause 8.5.1.1.2.

### 8.6.30 Security mode complete

#### 8.6.30.1 Message definition

This message is sent by the UE to the network in response to a SECURITY MODE COMMAND message. See table 8.6.30.1.1.

Message type: SECURITY MODE COMPLETE

Significance: dual

Direction: UE to network

Table 8.6.30.1.1: SECURITY MODE COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.4 | M | V | 1/2 |
|  | Security mode complete message identity | Message type  6.6.6.7 | M | V | 1 |
|  | Allowed NSSAI | NSSAI  8.7.28 | M | TBD | TBD |
| xa | IMEISV | Mobile identity  8.7.16 | O | TLV | TBD |
| xb | NAS message container | NAS message container  8.7.49 | O | TLV-E | 3-n |

#### 8.6.30.2 IMEISV

The UE shall include this information element, if the IMEISV was requested within the corresponding SECURITY MODE COMMAND message.

#### 8.6.30.3 NAS message container

The UE shall include this information element:

a) if during an ongoing registration procedure, the AMF included HASHAMF in the SECURITY MODE COMMAND message and HASHAMF has a different value from the hash value locally calculated at the UE as described in 3GPP TS 33.501 [24]; and

b) when the UE has sent an initial NAS message with a limited set of IEs before the SECURITY MODE COMMAND message was received and the UE needs to include the complete initial NAS message in the SECURITY MODE COMPLETE message, as described in 3GPP TS 33.501 [24].8.6.31 Security mode reject

#### 8.6.31.1 Message definition

This message is sent by the UE to the network to indicate that the corresponding security mode command has been rejected. See table 8.6.31.1.1.

Message type: SECURITY MODE REJECT

Significance: dual

Direction: UE to network

Table 8.6.31.1.1: SECURITY MODE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | Security header type | Security header type  6.6.6.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  6.6.6.4 | M | V | 1/2 |
|  | Security mode reject message identity | Message type  6.6.6.7 | M | V | 1 |
|  | EMM cause | 5GMM cause  8.7.1 | M | V | 1 |

## 8.7 5GMM information elements

### 8.7.1 5GMM cause

The purpose of the 5GMM cause information element is to indicate the reason why a 5GMM request from the UE is rejected by the network.

The 5GMM cause information element is coded as shown in figure 8.9.3.9.1 and table 8.9.3.9.1.

The 5GMM cause is a type 3 information element with 2 octets length.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GMM cause IEI | | | | | | | | octet 1 |
| Cause value | | | | | | | | octet 2 |

Figure 8.7.1.1: 5GMM cause information element

Table 8.7.1.1: 5GMM cause information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cause value (octet 2) | | | | | | | | | |
|  | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |  | Illegal UE |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |  | PEI not accepted |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |  | Illegal ME |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |  | 5GS services not allowed |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |  | Implicitly deregistered |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |  | PLMN not allowed |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |  | Tracking area not allowed |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |  | Roaming not allowed in this tracking area |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |  | Synch failure |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |  | Semantically incorrect message |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |  | Invalid mandatory information |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |  | Message type non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |  | Message type not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |  | Information element non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |  | Conditional IE error |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |  | Message not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |  | Protocol error, unspecified |
|  |  |  |  |  |  |  |  |  |  |
| Any other value received by the mobile station shall be treated as 0110 1111, "protocol error, unspecified". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified". | | | | | | | | | |
|  | | | | | | | | | |

### 8.7.2 NAS key set identifier

The NAS key set identifier is allocated by the network.

The NAS key set identifier information element is coded as shown in figure 8.7.2.1 and table 8.7.2.1.

The NAS key set identifier is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NAS key set identifier IEI | | | | TSC | NAS key set identifier | | | octet 1 |

Figure 8.7.2.1: NAS key set identifier information element

Table 8.7.2.1: NAS key set identifier information element

|  |  |  |  |
| --- | --- | --- | --- |
| Type of security context flag (TSC) (octet 1) | | | |
|  | | | |
| Bit | | | |
| 4 |  |  |  |
| 0 |  |  | native security context (for KSIAMF) |
| 1 |  |  | mapped security context (for ngKSI) |
|  | | | |
| TSC does not apply for NAS key set identifier value "111". | | | |
|  | | | |
| NAS key set identifier (octet 1) | | | |
|  | | | |
| Bits | | | |
| 3 | 2 | 1 |  |
|  |  |  |  |
| 0 | 0 | 0 |  |
| through | | | possible values for the NAS key set identifier |
| 1 | 1 | 0 |  |
|  |  |  |  |
| 1 | 1 | 1 | no key is available (UE to network); |
|  |  |  | reserved (network to UE) |

### 8.7.3 Authentication parameter RAND

See subclause 10.5.3.1 in 3GPP TS 24.008 [12].

Editor's note: The format of the Authentication parameter RAND IE in 3GPP TS 24.008 is TV with a length of 17 octets.

### 8.7.4 Authentication parameter AUTN

See subclause 10.5.3.1.1 in 3GPP TS 24.008 [12].

Editor's note: The format of the Authentication parameter AUTN IE in 3GPP TS 24.008 is TLV with a length of 18 octets.

### 8.7.5 SM message container (for alternative 1)

The purpose of the SM message container information element is to transport an 5GSM message within an 5GMM message.

The SM message container information element is coded as shown in figure 8.7.5.1 and table 8.7.5.1.

The SM message container is a type 6 information element with a minimum length of 4 octets and a maximum length of 65538 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| SM message container IEI | | | | | | | | octet 1 |
| Length of SM message container contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
|  | | | | | | | | octet 4 |
| SM message container contents | | | | | | | |  |
|  | | | | | | | | octet n |

Figure 8.7.5.1: SM message container information element

Table 8.7.5.1: SM message container information element

|  |
| --- |
| SM message container contents (octet 4 to octet n); Max value of 65535 octets |
|  |
| This IE can contain any 5GSM PDU as defined in subclause 9.6. |
|  |

### 8.7.6 Request type

The purpose of the request type information element is to indicate type of the PDU session establishment.

The request type information element is coded as shown in figure 8.7.6.1 and table 8.7.6.1.

The request type is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Request type IEI | | | | Request type value | | | | Octet 1 |

Figure 8.7.6.1: Request type information element

Table 8.7.6.1: Request type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Request type value (octet 1, bit 1 to bit 4) | | | | |
|  | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 1 | initial request |
| 0 | 0 | 1 | 0 | existing PDU session |
| All other values are reserved. | | | | |

### 8.7.7 S-NSSAI

The purpose of the S-NSSAI information element is to identify a network slice.

The S-NSSAI information element is coded as shown in figure 8.7.7.1 and table 8.7.7.1.

The S-NSSAI is a type 4 information element with 3 octets length or with 6 octets length. If octet 4 is included, then also octet 5 and 6 shall be included.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| S-NSSAI IEI | | | | | | | | octet 1 |
| Length of S-NSSAI contents | | | | | | | | octet 2 |
| SST | | | | | | | | octet 3 |
| SD | | | | | | | | octet 4\*  octet 6\* |

Figure 8.7.7.1: S-NSSAI information element

Table 8.7.7.1: S-NSSAI information element

|  |
| --- |
| Slice/service type (SST) (octet 3) |
|  |
| Slice differentiator (SD) (octet 4 to octet 6) |
|  |

### 8.7.8 DNN

The purpose of the DNN information element is to identify the data network.

The DNN information element is coded as shown in figure 8.7.8.1.

The DNN is a type 4 information element with a minimum length of 3 octets and a maximum length of 102 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| DNN IEI | | | | | | | | octet 1 |
| Length of DNN contents | | | | | | | | octet 2 |
| DNN value | | | | | | | | octet 3  octet n |

Figure 8.7.8.1: DNN information element

A DNN value field contains an APN as defined in 3GPP TS 23.003 [5].

### 8.7.9 Message container type (for alternative 1)

The purpose of the message container type information element is to indicate type of payload in the message container.

The message container type information element is coded as shown in figure 8.7.9.1 and table 8.7.9.1.

The message container type is a type 3 information element with 2 octet length.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Message container type IEI | | | | | | | | Octet 1 |
| Message container type | | | | | | | | Octet 2 |

Figure 8.7.9.1: Message container type information element

Table 8.7.9.1: Message container type information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Message container type (octet 2) | | | | | | | | | |
|  | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |  | SMS |
| All other values are reserved. | | | | | | | | | |

### 8.7.10 Message container (for alternative 1)

The purpose of the message container information element is to transport a payload indicated by the message container type information element.

The message container information element is coded as shown in figure 8.7.10.1 and table 8.7.10.1.

The message container is a type 6 information element with a minimum length of 3 octets and a maximum length of 65538 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Message container IEI | | | | | | | | octet 1 |
| Length of message container contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
|  | | | | | | | | octet 4 |
| Message container contents | | | | | | | |  |
|  | | | | | | | | octet n |

Figure 8.7.10.1: Message container information element

Table 8.7.10.1: Message container information element

|  |
| --- |
| Message container contents (octet 4 to octet n); Max value of 65535 octets |
|  |

8.7.11 Payload container type (for alternative 2)

The payload container type information element indicates type of payload included in the payload container information element.

The payload container information element is coded as shown in figure 8.7.11.1 and table 8.7.11.1.

The payload container is a type 1 information element with a length of half octet.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| - | - | - | - | Payload container type value | | | | octet 1 |

Figure 8.7.11.1: Payload container information element

**Table 8.7.11**.1: Payload container information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Payload container type value (octet 1, bit 1 to bit 4) | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 1 | N1 SM information |
| 0 | 0 | 1 | 0 | SMS |
| 0 | 0 | 1 | 1 | LTE Positioning Protocol (LPP) message container |
| All other values are reserved. | | | | |

8.7.12 Payload container (for alternative 2)

The purpose of the payload container information element is to transport a payload.

The payload container information element is coded as shown in figure 8.7.12.1 and table 8.7.12.1.

The payload container is a type 6 information element with a minimum length of 3 octets and a maximum length of 65537 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Length of payload container contents | | | | | | | | octet 1 |
|  | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
| Payload container contents | | | | | | | |  |
|  | | | | | | | | octet n |

Figure 8.7.12.1: Payload container information element

**Table 8.7.12.1: Payload container inform**ation element

|  |
| --- |
| Payload container contents (octet 3 to octet n); max value of 65535 octets |

### 8.7.14 Additional information (for alternative 2)

The purpose of the additional information information element is to provide additional information to upper layers in relation to the NAS transport mechanism.

The additional information information element is coded as shown in figure 8.7.14.1 and table 8.7.14.1.

The additional information is a type 4 information element with a minimum length of 3 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Additional information IEI | | | | | | | | octet 1 |
| Additional information length | | | | | | | | octet 2 |
| Additional information value | | | | | | | | octets 3-n |

Figure 8.7.14.1: Additional information information element

Table 8.7.14.1: Additional information information element

|  |
| --- |
| Additional information value (octet 3 to octet n) |
|  |
| The coding of the additional information value is dependent on the LCS application. |

### 8.7.15 Configuration update indication

The purpose of the Configuration update indication information element is to indicate the additional information associated with the generic UE configuration update procedure.

The Configuration update indication information element is coded as shown in figure 8.7.15.1 and table 8.7.15.1.

The Configuration update indication is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Configuration update indication IEI | | | | 0  Spare | 0  Spare | RED | ACK | octet 1 |

Figure 8.7.15.1: Configuration update indication

Table 8.7.15.1: Configuration update indication

|  |  |
| --- | --- |
| Acknowledgement (ACK) value (octet 1, bit 1) | |
|  | |
| Bits | |
| 1 |  |
| 0 | acknowledgement not requested |
| 1 | acknowledgement requested |
|  |  |
| Registration requested (RED) value (octet 1, bit 2) | |
|  |  |
| Bits | |
| 1 |  |
| 0 | registration not requested |
| 1 | registration requested |
|  | |

### 8.7.16 5GS mobile identity

The purpose of the 5GS mobile identity information element is to provide either the IMSI, the 5G-GUTI or the IMEI.

The 5GS mobile identity information element is coded as shown in figures 8.7.16.1 and 8.7.16.2 and table 8.7.16.1.

The 5GS mobile identity is a type 4 information element with a minimum length of 3 octets and a maximum length of xx2 octets.

Editor's note: The definition of 5G-GUTI is FFS, and will be added when defined by CT4.

Figure 8.7.16.1: 5GS mobile identity information element for type of identity "5G-GUTI"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2 |
| Identity digit 1 | | | | odd/  even  indic | Type of identity | | | octet 3 |
| Identity digit p+1 | | | | Identity digit p | | | | octet 4\* |

Figure 8.7.16.2: 5GS mobile identity information element for type of identity "IMSI" or "IMEI"

Table 8.7.16.1: 5GS mobile identity information element

|  |  |  |  |
| --- | --- | --- | --- |
| Type of identity (octet 3)  Bits | | | |
| 3 | 2 | 1 |  |
| 0 | 0 | 1 | IMSI |
| 1 | 1 | 0 | 5G-GUTI |
| 0 | 1 | 1 | IMEI |
| All other values are reserved. | | | |
|  | | | |
| Odd/even indication (octet 3)  Bit | | | |
| 4 |  |  |  |
| 0 |  |  | even number of identity digits |
| 1 |  |  | odd number of identity digits |
|  | | | |
| Identity digits (octet 4 etc)  For the IMSI, this field is coded using BCD coding. If the number of identity digits is even then bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". | | | |
|  | | | |
| For the IMEI, this field is coded using BCD coding. The format of the IMEI is described in 3GPP TS 23.003 [5]. | | | |
|  | | | |

### 8.7.17 Tracking area identity list

See subclause 9.9.3.33 in 3GPP TS 24.301 [15].

### 8.7.18 Service area list

The purpose of the Service area list information element is to transfer a list of allowed tracking areas for an allowed area or a list of non-allowed tracking areas for a non-allowed area from the network to the UE.

The coding of the information element allows combining different types of lists. The lists of type "00" and "01" allow a more compact encoding, when the different TAIs are sharing the PLMN identity. The lists of type "11" indicates all TAIs in the PLMN are allowed area.

The Service area list information element is coded as shown in figure 8.7.18.1, figure 8.7.18.2, figure 8.7.18.3, figure 8.7.18.4, figure 8.7.18.5 and table 8.7.18.1.

The Service area list is a type 4 information element with a minimum length of 6 octets and a maximum length of 98 octets. The list can contain a maximum of 16 different tracking area identities.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Service area list IEI | | | | | | | | octet 1 |
| Length of service area list contents | | | | | | | | octet 2 |
| Partial service area list 1 | | | | | | | | octet 3  octet i |
| Partial service area list 2 | | | | | | | | octet i+1\*  octet l\* |
| … | | | | | | | | octet l+1\*  octet m\* |
| Partial service area list p | | | | | | | | octet m+1\*  octet n\* |

Figure 8.7.18.1: Service area list information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed type | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC 1 | | | | | | | | octet 5 |
| TAC 1 (continued) | | | | | | | | octet 6 |
| … | | | | | | | | … |
| … | | | | | | | | … |
| TAC k | | | | | | | | octet 2k+3\* |
| TAC k (continued) | | | | | | | | octet 2k+4\* |

Figure 8.7.18.2: Partial service area list – type of list = "00"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed type | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC 1 | | | | | | | | octet 5 |
| TAC 1 (continued) | | | | | | | | octet 6 |

Figure 8.7.18.3: Partial service area list – type of list = "01"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed type | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC 1 | | | | | | | | octet 5 |
| TAC 1 (continued) | | | | | | | | octet 6 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 7\* |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 8\* |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 9\* |
| TAC 2 | | | | | | | | octet 10\* |
| TAC 2 (continued) | | | | | | | | octet 11\* |
| … | | | | | | | |  |
| … | | | | | | | |  |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 5k-3\* |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 5k-2\* |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 5k-1\* |
| TAC k | | | | | | | | octet 5k\* |
| TAC k (continued) | | | | | | | | octet 5k+1\* |

Figure 8.7.18.4: Partial service area list – type of list = "10"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed type | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |

Figure 8.7.18.5: Partial service area list – type of list = "11"

Table 8.7.18.1: Service area list information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Value part of the Service area list information element (octet 3 to n) | | | | | |
|  | | | | | |
| The value part of the Service area list information element consists of one or several partial service area lists. The length of each partial service area list can be determined from the 'type of list' field and the 'number of elements' field in the first octet of the partial service area list. | | | | | |
| For allowed type "0", TAIs contained in all partial service area lists are allowed area. For allowed type "1", TAIs contained in all partial service area lists are non-allowed area.  The UE shall store the complete list received. If more than 16 TAIs are included in this information element, the UE shall store the first 16 TAIs and ignore the remaining octets of the information element. | | | | | |
|  | | | | | |
|  | | | | | |
| Partial service area list: | | | | | |
|  | | | | | |
| Allowed type (octet 1) | | | | | |
| Bits | | | | | |
| 8 |  |  | | | |
| 0 |  | list of TAIs are allowed area | | | |
| 1 |  | list of TAIs are non-allowed area | | | |
|  | | | | | |
| Type of list (octet 1) | | | | | |
| Bits | | | | | |
| 7 | 6 |  | | | |
| 0 | 0 | list of TACs belonging to one PLMN, with non-consecutive TAC values | | | |
| 0 | 1 | list of TACs belonging to one PLMN, with consecutive TAC values | | | |
| 1 | 0 | list of TAIs belonging to different PLMNs (see NOTE) | | | |
| 1 | 1 | All TAIs belonging to the PLMN are allowed area | | | |
|  | | | | | |
| Number of elements (octet 1) | | | | | |
| Bits | | | | | |
| 5 | 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | 0 | 1 element |
| 0 | 0 | 0 | 0 | 1 | 2 elements |
| 0 | 0 | 0 | 1 | 0 | 3 elements |
| … | | | | |  |
| 0 | 1 | 1 | 0 | 1 | 14 elements |
| 0 | 1 | 1 | 1 | 0 | 15 elements |
| 0 | 1 | 1 | 1 | 1 | 16 elements |
|  | | | | | |
| All other values are unused and shall be interpreted as 16, if received by the UE. | | | | | |
|  | | | | | |
| For type of list = "00" and number of elements = k: | | | | | |
|  | | | | | |
| octet 2 to 4 contain the MCC+MNC, and | | | | | |
| for j = 1, k: | | | | | |
| octet 2j+3 and 2j+4 contain the TAC of the j-th TAI belonging to the partial list, | | | | | |
|  | | | | | |
| For type of list = "01" and number of elements = k: | | | | | |
|  | | | | | |
| octet 2 to 4 contain the MCC+MNC, and | | | | | |
| octet 5 and 6 contain the TAC of the first TAI belonging to the partial list. | | | | | |
| The TAC values of the other k-1 TAIs are TAC+1, TAC+2, …, TAC+k-1. | | | | | |
|  | | | | | |
| For type of list = "10" and number of elements = k: | | | | | |
|  | | | | | |
| for j = 1, k. | | | | | |
| octet 5j-3 to 5j-1 contain the MCC+MNC, and | | | | | |
| octet 5j and 5j+1 contain the TAC of the j-th TAI belonging to the partial list. | | | | | |
|  | | | | | |
| For type of list = "11": | | | | | |
|  | | | | | |
| Allowed type shall be coded as "0" and number of elements shall be ignored, and | | | | | |
| octet 2 to 4 contain the MCC+MNC.  If allowed type is coded as "1", it shall be interpreted as "0". | | | | | |
|  | | | | | |
|  | | | | | |
| MNC, Mobile network code | | | | | |
|  | | | | | |
| The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111". | | | | | |
|  | | | | | |
| TAC, Tracking area code | | | | | |
|  | | | | | |
| In the TAC field bit 8 of the first octet is the most significant bit and bit 1 of second octet the least significant bit. | | | | | |
| The coding of the tracking area code is the responsibility of each administration. Coding using full hexadecimal representation may be used. The tracking area code consists of 2 octets. | | | | | |
|  | | | | | |
| NOTE: If the "list of TAIs belonging to different PLMNs" is used, the PLMNs included in the list need to be present in the list of "equivalent PLMNs". | | | | | |

### 8.7.19 Network name

See subclause 10.5.3.5a in 3GPP TS 24.008 [12].

### 8.7.20 Time zone

See subclause 10.5.3.8 in 3GPP TS 24.008 [12].

### 8.7.21 Time zone and time

See subclause 10.5.3.9 in 3GPP TS 24.008 [12].

### 8.7.22 Daylight saving time

See subclause 10.5.3.12 in 3GPP TS 24.008 [12].

### 8.7.23 Identity type 2

See subclause 10.5.5.9 in 3GPP TS 24.008 [12].

### 8.7.24 Sequence number

This IE includes the NAS message sequence number (SN).

Editor’s note: Further description of the SN would be aligned with 3GPP TS 33.501 [24]. The usage of SN is FFS.

### 8.7.25 Message authentication code

The message authentication code (MAC) information element contains the integrity protection information for the message. The MAC IE shall be included in the security protected NAS message if a valid 5GS security context exists and security functions are started.

Editor’s note: The usage of MAC is FFS.

### 8.7.26 Uplink data status

The purpose of the Uplink data status information element is to indicate to the network which preserved PDU session contexts have uplink data pending.

The Uplink data status information element is coded as shown in figure 8.7.26.1 and table 8.7.26.1.

The uplink data status information element is a type 4 information element with minimum length of 4 octets a maximum length of 34 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Uplink data status IEI | | | | | | | | octet 1 |
| Length of uplink data status contents | | | | | | | | octet 2 |
| PSI  (7) | PSI  (6) | PSI  (5) | PSI  (4) | PSI  (3) | PSI  (2) | PSI  (1) | PSI  (0) | octet 3 |
| PSI  (15) | PSI  (14) | PSI  (13) | PSI  (12) | PSI  (11) | PSI  (10) | PSI  (9) | PSI  (8) | octet 4 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  |
| spare | | | | | | | | octet 5\* -34\* |

Figure 8.7.26.1: Upllink data status information element

Table 8.7.26.1: Uplink data status information element

|  |
| --- |
| PSI(x) shall be coded as follows:  PSI(0) - PSI(4):  Bits 1 to 5 of octet 3 are spare and shall be coded as zero.  PSI(5) – PSI(15):  0 indicates that no uplink data are pending for the corresponding PDU session identity.  1 indicates that uplink data are pending for the corresponding PDU session identity.  All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element. |

### 8.7.27 PDU session status

The purpose of the PDU session status information element is to indicate the state of each PDU session that can be identified by a PDU session identity.

The PDU session status information element is coded as shown in figure 8.7.27.1 and table 8.7.27.1.

The PDU session status information element is a type 4 information element with minimum length of 4 octets and a maximum length of 34 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PDU session status IEI | | | | | | | | octet 1 |
| Length of PDU session status contents | | | | | | | | octet 2 |
| PSI  (7) | PSI  (6) | PSI  (5) | PSI  (4) | PSI  (3) | PSI  (2) | PSI  (1) | PSI  (0) | octet 3 |
| PSI  (15) | PSI  (14) | PSI  (13) | PSI  (12) | PSI  (11) | PSI  (10) | PSI  (9) | PSI  (8) | octet 4 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | octet 5\*- |
| spare | | | | | | | | 34\* |

Figure 8.7.27.1: PDU session status information element

Table 8.7.27.1: PDU sesssion status information element

|  |
| --- |
| PSI(x) shall be coded as follows:  PSI(0) - PSI(4):  Bits 1 to 5 of octet 3 are spare and shall be coded as zero.  PSI(5) – PSI(15):  0 indicates that the 5GSM state of the corresponding PDU session is PDU SESSION INACTIVE.  1 indicates that the 5GSM state of the corresponding PDU session is not PDU SESSION INACTIVE  All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element. |

### 8.7.28 De-registration type

The purpose of the de-registration type information element is to indicate the type of de-registration.

The de-registration type information element is coded as shown in figure 8.7.28.1 and table 8.7.28.1.

The de-registration type is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| De-registration type  IEI | | | | Switch  off | Re-registration required | Access type | | octet 1 |

Figure 8.7.28.1: Deregistration type information element

Table 8.7.28.1: Deregistration type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Switch off (octet 1, bit 4) | | | | |
| In the UE to network direction: | | | | |
| Bit | | | | |
| 4 |  |  |  |  |
| 0 |  |  |  | Normal detach |
| 1 |  |  |  | Switch off |
|  | | | | |
| In the network to UE direction bit 4 is spare. The network shall set this bit to zero. | | | | |
|  | | | | |
| Re-registration required (octet 1, bit 3) | | | | |
|  | | | | |
| In the network to UE direction: | | | | |
| Bit | | | | |
| 3 |  |  |  |  |
| 0 |  |  |  | re-registration not required |
| 1 |  |  |  | re-registration required |
|  | | | | |
| In the UE to network direction bit 3 is spare. The UE shall set this bit to zero. | | | | |
|  | | | | |
| Access type (octet 1,bit 2, bit 1) | | | | |
| Bit | | | | |
| 2 | 1 |  |  |  |
| 0 | 1 |  |  | 3GPP access |
| 1 | 0 |  |  | Non-3GPP access |
| 1 | 1 |  |  | 3GPP access and non-3GPP access |
|  | | | | |
| All other values are reserved. | | | | |
|  | | | | |

### 8.7.29 NSSAI

The purpose of the NSSAI information element is to identify a collection of S-NSSAIs

The NSSAI information element is coded as shown in figure 8.7.29.1 and table 8.7.29.1.

The S-NSSAI is a type 4 information element with a minimum length of 4 octets and a maximum length of 82 octets.

NOTE: The number of S-NSSAI(s) cannot exceed eight.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NSSAI IEI | | | | | | | | octet 1 |
| Length of NSSAI contents | | | | | | | | octet 2 |
| S-NSSAI 1 | | | | | | | | octet 3  octet m |
| S-NSSAI 2 | | | | | | | | octet m+1\*  octet n\* |
| … | | | | | | | | octet n+1\*  octet u\* |
| S-NSSAI n | | | | | | | | octet u+1\*  octet v\* |

Figure 8.7.29.1: NSSAI information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| S-NSSAI Identifier | | | | | | | | octet m+1 |
| Length of S-NSSAI contents | | | | | | | | octet m+2 |
| SST | | | | | | | | octet m+3 |
| SD | | | | | | | | octet m+4\*  octet m+6\* |
| mapped subscribed SST | | | | | | | | octet m+7\* |
| mapped subscribed SD | | | | | | | | octet m+8\*  octet m+10\* |

Figure 8.7.29.2: S-NSSAI information element

Editor's note: It is FFS how the permanent or the temporarily rejected S-NSSAI is coded in the NSSAI.

Table 8.7.29.1: S-NSSAI information element

|  |
| --- |
| S-NSSAI identifier (octet m+1)  The S-NSSAI identifier field is used to identify the S-NSSAI.  Slice/service type (SST) (octet m+3) |
|  |
| Slice differentiator (SD) (octet m+4 to octet m+6) |
| NOTE 1: If the octet m+4 is included, then octet m+5 and octet m+6 shall be included.  NOTE 2: If the octet m+8 is included, then octet m+9 and octet m+10 shall be included. |

### 8.7.30 EAP message

The EAP message information element transport an EAP message as specified in IETF RFC 3748 [30].

The EAP message information element is coded as shown in figure 8.7.30.1 and table 8.7.30.1.

The EAP message is a type 6 information element with minimum length of 7 octets and maximum length of 1503 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| EAP message IEI | | | | | | | | octet 1 |
| Length of EAP message contents | | | | | | | | octet 2  octet 3 |
| EAP message | | | | | | | | octet 4  octet x |

Figure 8.7.30.1: EAP message information element

Table 8.7.30.1: EAP message information element

|  |
| --- |
| EAP message (octet 4 to x) |
| An EAP message as specified in IETF RFC 3748 [30]. |
|  |

### 8.7.31 5GMM capability

The purpose of the 5GMM capability information element is to provide the network with information concerning aspects of the UE related to the 5GCN or interworking with the EPS. The contents might affect the manner in which the network handles the operation of the UE.

The 5GMM capability information element is coded as shown in figure 8.7.31.1 and table 8.7.31.2.

The 5GMM capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| 5GMM capability IEI | | | | | | | | | | | | | | | | octet 1 |
| Length of 5GMM capability contents | | | | | | | | | | | | | | | | octet 2 |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | S1 mode | | octet 3 |
| 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | octet 4\* -15\* |
| Spare | | | | | | | | | | | | | | | |

Figure 8.7.31.1: 5GMM capability information element

Table 8.7.31.2: 5GMM capability information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| EPC NAS supported (S1 mode) (octet 3, bit 1) | | | | |
| 0 |  |  |  | S1 mode not supported |
| 1 |  |  |  | S1 mode supported |
|  | | | | |
|  | | | | |
| All other bits in octet 3 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | |
|  | | | | |

### 8.7.32 LADN information

The purpose of the LADN information IE is to provide the UE the LADN service area for each available LADN in the current registration area.

The LADN information IE is coded as shown in figure 8.7.32.1, figure 8.7.32.2 and table 8.7.32.1.

The LADN information IE is a type 6 information element with a minimum length of 13 octets and a maximum length of 15602 octets.

The LADN information IE can contain a maximum of 8 different LADNs each including a DNN and a tracking area identity lists. If more than 8 LADNs are included in this information element, the UE shall store the first 8 and ignore the remaining octets of the information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| LADN information IEI | | | | | | | | octet 1 |
| Length of LADN information contents | | | | | | | | octet 2  octet 3 |
| LADN 1 | | | | | | | | octet 4  octet a |
| LADN 2 | | | | | | | | octet a+1\*  octet b\* |
| … | | | | | | | | octet b+1\*  octet g\* |
| LADN n | | | | | | | | octet g+1\*  octet h\* |

Figure 8.7.32.1: LADN information IE

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| LADN Identifier | | | | | | | | octet 1 |
| Length of LADN contents | | | | | | | | octet 2 |
| Length of DNN value | | | | | | | | octet 3 |
| DNN value | | | | | | | | octet 4  octet a |
| Length of tracking area identity list contents | | | | | | | | octet a+1 |
| Tracking area identity list contents | | | | | | | | octet a+2  octet b |

Figure 8.7.32.2: LADN IE

Table 8.7.32.1: LADN IE

|  |
| --- |
| LADN identifier (octet 1)  The LADN identifier field is used to identify a LADN.  The DNN value is coded as specified in subclause 8.7.8. |
|  |
| The tracking area identity list contents is coded as specified in subclause 8.7.17 starting with the third octet |

### 8.7.33 PDU session reactivation result

The purpose of the PDU session reactivation result information element is to indicate the result of PDU sessions activation requested by UE in Uplink data status IE of SERVICE REQUEST message.

The PDU session reactivation result information element is coded as shown in figure 8.7.33.1 and table 8.7.33.1.

The PDU session reactivation result information element is a type 4 information element with minimum length of 4 octets and maximum length of 34 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PDU session reactivation result IEI | | | | | | | | octet 1 |
| Length of PDU session reactivation result | | | | | | | | octet 2 |
| PSI  (7) | PSI  (6) | PSI  (5) | PSI  (4) | PSI  (3) | PSI  (2) | PSI  (1) | PSI  (0) | octet 3 |
| PSI  (15) | PSI  (14) | PSI  (13) | PSI  (12) | PSI  (11) | PSI  (10) | PSI  (9) | PSI  (8) | octet 4 |
| |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | spare | | | | | | | | | | | | | | | | octet 5\* -34\* |

Figure 8.7.33.1: PDU session reactivation result information element

Table 8.7.33.1: PDU session reactivation result information element

|  |
| --- |
| PSI(x) shall be coded as follows:  PSI(0) - PSI(4):  Bits 0 to 4 of octet 3 are spare and shall be coded as zero.  PSI(5) – PSI(15):  0 indicates PDU session reactivation was not requested in Uplink data status IE or User plane reactivation is successful.  1 indicates PDU session reactivation was requested in Uplink data status IE but User plane reactivation is not successful.  All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element. |

Editor's note: Coding of the reject cause value for the case of user plane reactivation failure of corresponding PDU session ID is FFS.

### 8.7.34 Old PDU session identity

The purpose of the old PDU session identity information element is to indicate the PDU session identity associated with the PDU SESSION MODIFICATION COMMAND message with the 5GSM cause IE set to #39 "reactivation requested".

The old PDU session identity information element is coded as shown in figure 8.7.34.1 and table 8.7.34.1.

The old PDU session identity is a type 3 information element with 2 octet length.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Old PDU session identity IEI | | | | | | | | octet 1 |
| Old PDU session identity value | | | | | | | | octet 2 |

Figure 8.7.34.1: Old PDU session identity information element

Table 8.7.34.1: Old PDU session identity information element

|  |
| --- |
| Old PDU session identity value (octet 2) |
| The coding of the old PDU session identity value is identical to the coding of the PDU session identity value (see annex E.1). |

### 8.7.35 GPRS timer 2

See subclause 10.5.7.4 in 3GPP TS 24.008 [12].

### 8.7.36 Allowed PDU session status

The purpose of the Allowed PDU session status information element is to indicate to the network which PDU sessions that can be re-activated over 3GPP access.

The Allowed PDU session status information element is coded as shown in figure 8.7.36.1 and table 8.7.36.1.

The Allowed PDU session status information element is a type 4 information element with minimum length of 4 octets and maximum length of 34 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed PDU session status IEI | | | | | | | | octet 1 |
| Length of Allowed PDU session status contents | | | | | | | | octet 2 |
| PSI  (7) | PSI  (6) | PSI  (5) | PSI  (4) | PSI  (3) | PSI  (2) | PSI  (1) | PSI  (0) | octet 3 |
| PSI  (15) | PSI  (14) | PSI  (13) | PSI  (12) | PSI  (11) | PSI  (10) | PSI  (9) | PSI  (8) | octet 4 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  |
| spare | | | | | | | | octet 5\* -34\* |

Figure 8.7.36.1: Allowed PDU session status information element

Table 8.7.36.1: Allowed PDU session status information element

|  |
| --- |
| PSI(x) shall be coded as follows:  PSI(0) - PSI(4):  Bits 1 to 5 of octet 3 are spare and shall be coded as zero.  PSI(5) – PSI(15):  0 indicates that the corresponding PDU session is not allowed to be re-activated over 3GPP access.  1 indicates that the corresponding PDU session can be re-activated over 3GPP access.  All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element. |

### 8.7.37 5GS registration type

Editor's note: The definition of 5GS registration type is FFS. If 5GS registration type includes a follow-on request indication is FFS.

### 8.7.38 Tracking area identity

See subclause 9.9.3.32 in 3GPP TS 24.301 [15].

### 8.7.39 S1 UE network capability

See subclause 9.9.3.34 in 3GPP TS 24.301 [15].

### 8.7.40 Registration result

Editor's note: The definition of Registration result is FFS.

### 8.7.41 PLMN list

See subclause 10.5.1.13 in 3GPP TS 24.008 [12].

### 8.7.42 5GS network feature support

Editor's note: The definition of 5GS network feature support is FFS, but should include a dual registration supported indication.

### 8.7.43 UE status

The purpose of the UE status information element is to provide the network with information concerning aspects of the current UE registration status which is used for interworking with EPS.

The UE context status information element is coded as shown in figure 8.7.43.1 and table 8.7.43.1.

The UE context status is a type 4 information element with a length of 3 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| UE status IEI | | | | | | | | | | | | | | | | octet 1 |
| Length of UE status contents | | | | | | | | | | | | | | | | octet 2 |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | S1 mode reg | | octet 3 |

Figure 8.7.43.1: UE status information element

Table 8.7.43.1: UE status information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| EMM registration status (S1 mode reg) (octet 3, bit 1) | | | | |
| 0 |  |  |  | UE is not in EMM-REGISTERED state |
| 1 |  |  |  | UE is in EMM-REGISTERED state |
|  | | | | |
| All other bits in octet are spare and shall be coded as zero, | | | | |

### 8.7.44 IMEISV request

The purpose of the IMEISV request information element is to indicate that the IMEISV shall be included by the UE in the security mode complete message.

The IMEISV request is a type 1 information element.

The IMEISV request information element is coded as shown in figure 8.7.44.1 and table 8.7.44.1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | | 2 | 1 |  |
| IMEISV request  IEI | | | | 0  spare | | | IMEISV request  value | | | octet 1 |

Figure 8.7.44.1: **IMEISV request** information element

Table 8.7.44.1: IMEISV request information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IMEISV request value (octet 1) | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 0 |  | IMEISV not requested |
| 0 | 0 | 1 |  | IMEISV requested |
|  | | | | |
| All other values are interpreted as IMEISV not requested by this version of the protocol. | | | | |

### 8.7.45 NAS security algorithms

The purpose of the NAS security algorithms information element is to indicate the algorithms to be used for ciphering and integrity protection.

The NAS security algorithms information element is coded as shown in figure 8.7.45.1 and table 8.7.45.1.

The NAS security algorithms is a type 3 information element with a length of 2 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NAS security algorithms IEI | | | | | | | | octet 1 |
| 0  spare | Type of ciphering algorithm | | | 0  spare | Type of integrity protection algorithm | | | octet 2 |

Figure 8.7.45.1: NAS security algorithms information element

Table 8.7.45.1: NAS security algorithms information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of integrity protection algorithm (octet 2, bit 1 to 3) | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 0 |  | 5GS integrity algorithm 5G-IA0 (null integrity protection algorithm) |
| 0 | 0 | 1 |  | 5GS integrity algorithm 128-5G-IA1 |
| 0 | 1 | 0 |  | 5GS integrity algorithm 128-5G-IA2 |
| 0 | 1 | 1 |  | 5GS integrity algorithm 128-5G-IA3 |
| 1 | 0 | 0 |  | 5GS integrity algorithm 5G-IA4 |
| 1 | 0 | 1 |  | 5GS integrity algorithm 5G-IA5 |
| 1 | 1 | 0 |  | 5GS integrity algorithm 5G-IA6 |
| 1 | 1 | 1 |  | 5GS integrity algorithm 5G-IA7 |
|  | | | | |
| Type of ciphering algorithm (octet 2, bit 5 to 7) | | | | |
| Bits | | | | |
| 7 | 6 | 5 |  |  |
| 0 | 0 | 0 |  | 5GS encryption algorithm 5G-EA0 (null ciphering algorithm) |
| 0 | 0 | 1 |  | 5GS encryption algorithm 128-5G-EA1 |
| 0 | 1 | 0 |  | 5GS encryption algorithm 128-5G-EA2 |
| 0 | 1 | 1 |  | 5GS encryption algorithm 128-5G-EA3 |
| 1 | 0 | 0 |  | 5GS encryption algorithm 5G-EA4 |
| 1 | 0 | 1 |  | 5GS encryption algorithm 5G-EA5 |
| 1 | 1 | 0 |  | 5GS encryption algorithm 5G-EA6 |
| 1 | 1 | 1 |  | 5GS encryption algorithm 5G-EA7 |
|  | | | | |
| Bit 4 and 8 of octet 2 are spare and shall be coded as zero. | | | | |

### 8.7.46 Nonce

See subclause 9.9.3.25 in 3GPP TS 24.301 [13].

### 8.7.47 UE security capability

The UE security capability information element is used by the network to indicate which security algorithms are supported by the UE in N1 mode and S1 mode. Security algorithms supported in N1 mode are supported both for NAS and for AS security.

The UE security capability information element is coded as shown in figure 8.7.47.1 and table 8.7.47.1.

The UE security capability is a type 4 information element with a minimum length of 4 octets and a maximum length of 6 octets.

Octets 5 and 6 are optional. If octet 5 is included, then also octet 6 shall be included.

If the UE did not indicate support of any security algorithm for S1 mode octets 5 and 6 shall not be included.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| UE security capability IEI | | | | | | | | | | | | | | | | octet 1 |
| Length of UE security capability contents | | | | | | | | | | | | | | | | octet 2 |
| 5G-EA0 | | 128-  5G-EA1 | | 128-  5G-EA2 | | 128-  5G-EA3 | | 5G-EA4 | | 5G-EA5 | | 5G-EA6 | | 5G-EA7 | | octet 3 |
| 5G-IA0 | | 128-  5G-IA1 | | 128-  5G-IA2 | | 128-  5G-IA3 | | 5G-IA4 | | 5G-IA5 | | 5G-IA6 | | 5G-IA7 | | octet 4 |
| EEA0 | | 128-  EEA1 | | 128-  EEA2 | | 128-  EEA3 | | EEA4 | | EEA5 | | EEA6 | | EEA7 | | octet 5\* |
| EIA0 | | 128-  EIA1 | | 128-  EIA2 | | 128-  EIA3 | | EIA4 | | EIA5 | | EIA6 | | EIA7 | | octet 6\* |

Figure 8.7.47.1: UE security capability information element

Table 8.7.47.1: UE security capability information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5GS encryption algorithms supported (octet 3) | | | | |
|  | | | | |
| 5GS encryption algorithm 5G-EA0 supported (octet 3, bit 8) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA0 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA0 supported |
|  | | | | |
| 5GS encryption algorithm 128-5G-EA1 supported (octet 3, bit 7) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 128-5G-EA1 not supported |
| 1 |  |  |  | 5GS encryption algorithm 128-5G-EA1 supported |
|  | | | | |
| 5GS encryption algorithm 128-5G-EA2 supported (octet 3, bit 6) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 128-5G-EA2 not supported |
| 1 |  |  |  | 5GS encryption algorithm 128-5G-EA2 supported |
|  | | | | |
| 5GS encryption algorithm 128-5G-EA3 supported (octet 3, bit 5) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 128-5G-EA31 not supported |
| 1 |  |  |  | 5GS encryption algorithm 128-5G-EA3 supported |
|  | | | | |
| 5GS encryption algorithm 5G-EA4 supported (octet 3, bit 4) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA4 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA4 supported |
|  | | | | |
| 5GS encryption algorithm 5G-EA5 supported (octet 3, bit 3) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA5 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA5 supported |
|  | | | | |
| 5GS encryption algorithm 5G-EA6 supported (octet 3, bit 2) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA6 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA6 supported |
|  | | | | |
| 5GS encryption algorithm 5G-EA7 supported (octet 3, bit 1) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA7 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA7 supported |
|  | | | | |
| EPS integrity algorithms supported (octet 4) | | | | |
|  | | | | |
| 5GS integrity algorithm 5G-IA0 supported (octet 4, bit 8) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA0 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA0 supported |
|  | | | | |
| 5GS integrity algorithm 128-5G-IA1 supported (octet 4, bit 7) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 128-5G-IA1 not supported |
| 1 |  |  |  | 5GS integrity algorithm 128-5G-IA1 supported |
|  | | | | |
| 5GS integrity algorithm 128-5G-IA2 supported (octet 4, bit 6) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 128-5G-IA2 not supported |
| 1 |  |  |  | 5GS integrity algorithm 128-5G-IA2 supported |
|  | | | | |
| 5GS integrity algorithm 128-5G-IA3 supported (octet 4, bit 5) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 128-5G-IA3 not supported |
| 1 |  |  |  | 5GS integrity algorithm 128-5G-IA3 supported |
|  | | | | |
| 5GS integrity algorithm 5G-IA4 supported (octet 4, bit 4) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA4 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA4 supported |
|  | | | | |
| 5GS integrity algorithm 5G-IA5 supported (octet 4, bit 3) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA5 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA5 supported |
|  | | | | |
| 5GS integrity algorithm 5G-IA6supported (octet 4, bit 2) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA6 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA6 supported |
|  | | | | |
| 5GS integrity algorithm 5G-IA7 supported (octet 4, bit 1) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA7 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA7 supported |
|  | | | | |
| EPS encryption algorithms supported (octet 5) | | | | |
|  | | | | |
| EPS encryption algorithm EEA0 supported (octet 5, bit 8) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA0 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA0 supported |
|  | | | | |
| EPS encryption algorithm 128-EEA1 supported (octet 5, bit 7) | | | | |
| 0 |  |  |  | EPS encryption algorithm 128-EEA1 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA1 supported |
|  | | | | |
| EPS encryption algorithm 128-EEA2 supported (octet 5, bit 6) | | | | |
| 0 |  |  |  | EPS encryption algorithm 128-EEA2 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA2 supported |
|  | | | | |
| EPS encryption algorithm 128-EEA3 supported (octet 5, bit 5) | | | | |
| 0 |  |  |  | EPS encryption algorithm 128-EEA3 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA3 supported |
|  | | | | |
| EPS encryption algorithm EEA4 supported (octet 5, bit 4) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA4 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA4 supported |
|  | | | | |
| EPS encryption algorithm EEA5 supported (octet 5, bit 3) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA5 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA5 supported |
|  | | | | |
| EPS encryption algorithm EEA6 supported (octet 5, bit 2) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA6 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA6 supported |
|  | | | | |
| EPS encryption algorithm EEA7 supported (octet 5, bit 1) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA7 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA7 supported |
|  | | | | |
| EPS integrity algorithms supported (octet 6) | | | | |
|  | | | | |
| EPS integrity algorithm EIA0 supported (octet 6, bit 8) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA0 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA0 supported |
|  | | | | |
| EPS integrity algorithm 128-EIA1 supported (octet 6, bit 7) | | | | |
| 0 |  |  |  | EPS integrity algorithm 128-EIA1 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA1 supported |
|  | | | | |
| EPS integrity algorithm 128-EIA2 supported (octet 6, bit 6) | | | | |
| 0 |  |  |  | EPS integrity algorithm 128-EIA2 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA2 supported |
|  | | | | |
| EPS integrity algorithm 128-EIA3 supported (octet 6, bit 5) | | | | |
| 0 |  |  |  | EPS integrity algorithm 128-EIA3 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA3 supported |
|  | | | | |
| EPS integrity algorithm EIA4 supported (octet 6, bit 4) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA4 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA4 supported |
|  | | | | |
| EPS integrity algorithm EIA5 supported (octet 6, bit 3) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA5 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA5 supported |
|  | | | | |
| EPS integrity algorithm EIA6 supported (octet 6, bit 2) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA6 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA6 supported |
|  | | | | |
| EPS integrity algorithm EIA7 supported (octet 6, bit 1) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA7 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA7 supported |
|  | | | | |

### 8.7.48 HashAMF

The purpose of the HashAMF information element is to transfer a 64-bit hash value to the UE so the UE can check the AMF calculated value against the value locally calculated by the UE to determine whether the REGISTRATION REQUEST message sent by the UE has been modified.

The HashAMF information element is coded as shown in figure 8.7.48.1 and table 8.7.48.1.

The HashAMF is a type 3 information element with a length of 9 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| HashAMF IEI | | | | | | | | octet 1 |
| HashAMF value | | | | | | | | octet 2  octet 9 |

Figure 8.7.48.1: HashAMF information element

Table 8.7.48.1: HashAMF information element

|  |
| --- |
| HashAMF value (octet 2 to 9) |
|  |
| This field contains the binary representation of the HashAMF. Bit 8 of octet 2 represents the most significant bit of the HashAMF and bit 1 of octet 9 the least significant bit. |

### 8.7.49 NAS message container

The purpose of the NAS message container IE is to encapsulate a NAS message without NAS security header.

The NAS message container information element is coded as shown in figure 8.7.49.1 and table 8.7.49.1.

The NAS message container is a type 6 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NAS message container IEI | | | | | | | | octet 1 |
| Length of NAS message container contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
|  | | | | | | | | octet 4 |
| NAS message container contents | | | | | | | |  |
|  | | | | | | | | octet n |

Figure 8.7.49.1: NAS message container information element

Table 8.7.49.1: NAS message container information element

|  |
| --- |
| NAS message container contents (octet 4 to octet n); Max value of 65535 octets |
|  |
| This IE can contain a REGISTRATION REQUEST message as defined in subclause 8.6.5, or a SERVICE REQUEST message as defined in subclause 8.6.19. |

## 8.8 3GPP specific coding information defined within present document

### 8.8.1 Serving network name (SNN)

The serving network name (SNN) is used in the network name field of the AT\_KDF\_INPUT attribute defined in IETF RFC 5448 [35].

SNN shall take the generic format of an octet string without terminating null characters.

SNN is of maximum length of 1020 octets.

SNN consists of SNN-prefix and SNN-value, delimited by a colon.

SNN-value identifies the serving PLMN.

MCC and MNC in the SNN-PLMN-ID are MCC and MNC of the serving PLMN. If the MNC of the serving PLMN has two digits, then a zero is added at the beginning.

ABNF syntax of SNN is specified in table 8.8.1.1

Table 8.8.1.1: ABNF syntax of SNN

SNN = SNN-prefix ":" SNN-value

SNN-prefix = %x35.47 ; "5G"

SNN-value = SNN-PLMN-ID

SNN-PLMN-ID = SNN-mnc-string SNN-mnc-digits "." SNN-mcc-string SNN-mcc-digits "." SNN-3gppnetwork-string "." SNN-org-string

SNN-mnc-digits = DIGIT DIGIT DIGIT ; MNC of the PLMN ID

SNN-mcc-digits = DIGIT DIGIT DIGIT ; MCC of the PLMN ID

SNN-mnc-string = %x6d.6e.63 ; "mnc" in lower case

SNN-mcc-string = %x6d.63.63 ; "mcc" in lower case

SNN-3gppnetwork-string = %x33.67.70.70.6e.65.74.77.6f.72.6b ; "3gppnetwork" in lower case

SNN-org-string = %x6f.72.67 ; "org" in lower case

NOTE: SNN-prefix allows for distinguishing of ANID specified in 3GPP TS 24.302 [16] and SNN as either of SNN or ANID can be carried in the AT\_KDF\_INPUT attribute.

EXAMPLE: If PLMN ID contains MCC = 234 and MNC = 15, SNN is 5G:mnc015.mcc234.3gppnetwork.org.

Editors' note: 3GPP TS 24.302 [16] needs to be extended so that ANID-prefix "5G" points to the SNN.

## 8.9 Timers of 5GS mobility management

Timers of 5GS mobility management are shown in table 8.9.1 and table 8.9.2

Table 8.9.1: Timers of 5GS mobility management – UE side

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  EXPIRY |
| --- | --- | --- | --- | --- | --- |
| T3510 | TBD | TBD | Transmission of REGISTRATION REQUEST message | REGISTRATION ACCEPT message received or REGISTRATION REJECT message received | Retransmission of REGISTRATION REQUEST message |
| T3502 | TBD | TBD | At registration failure and the attempt counter is equal to 5 | Transmission of REGISTRATION REQUEST message | Initiation of the registration procedure, if still required |
| T3511 | TBD | TBD | At registration failure due to lower layer failure, T3510 timeout or registration rejected with other 5GMM cause values than those treated in subclause 8.5.2.1.2.5 for initial registration or subclause 8.5.2.1.3.5 for mobility and periodic registration | Transmission of REGISTRATION REQUEST message | Retransmission of the REGISTRATION REQUEST, if still required |
| T3512 | TBD | TBD | In 5MM-REGISTERED, when 5MM-CONNECTED mode is left | When entering state 5MM-DEREGISTERED or when entering 5MM-CONNECTED mode | Initiation of the periodic registration procedure |
| T3517 | TBD | TBD | Transmission of SERVICE REQUEST message | SERVICE ACCEPT message received, or  SERVICE REJECT message received | Abort the procedure |
| T3521 | TBD | TBD | Transmission of DEREGISTRATION REQUEST message when de-registration procedure is not due to a "switch off" | DEREGISTRATION ACCEPT message received | Retransmission of DEREGISTRATION REQUEST message |
| T3540 | TBD | TBD | REGISTRATION REJECT, DEREGISTRATION REQUEST, with any of the 5GMM cause #8, #11, #12 or #13  SERVICE REJECT received with any of the 5GMM cause #8, #11, #12 or #13 | N1 NAS signalling connection released  Bearers have been set up | Release the NAS signalling connection for the cases a) and b) as described in subclause 8.4 |
|  |  | TBD | REGISTRATION REJECT, SERVICE REJECT with the 5GMM cause #10 | N1 NAS signalling connection released | Release the NAS signalling connection for the cases c) as described in subclause  8.4 and initiation of the registration procedure as specified in subclause 8.5.2.1.2.2 or 8.5.2.1.3.2 |

Table 8.9.2: Timers of 5GS mobility management – AMF side

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  EXPIRY |
| --- | --- | --- | --- | --- | --- |
| T3550 | TBD | TBD | Transmission of REGISTRATION ACCEPT message at initial registration  Transmission of REGISTRATION ACCEPT message with 5G-GUTI at mobility or periodic registration | REGISTRATION COMPLETE message received | Retransmission of REGISTRATION ACCEPT message |
| T3560 | TBD | 5GMM-COMMON-PROCEDURE-INITIATED | AUTHENTICATION REQUEST message sent  SECURITY MODE COMMAND message sent | AUTHENTICATION RESPONSE message received  AUTHENTICATION FAILURE message received  SECURITY MODE COMPLETE received  SECURITY MODE REJECT received | Retransmission of AUTHENTICATION REQUEST message or SECURITY MODE COMMAND |
| T3570 | TBD | TBD | Transmission of IDENTITY REQUEST message | IDENTITY RESPONSE message received | Retransmission of IDENTITY REQUEST message |
| T3513 | TBD | TBD | Paging procedure initiated | Paging procedure completed as specified in subclause 8.5.3.2.2.1 | Network dependent |
| T3522 | TBD | TBD | Transmission of DEREGISTRATION REQUEST message | DEREGISTRATION ACCEPT message received | Retransmission of DEREGISTRATION REQUEST message |
| T3555 | TBD | TBD | Transmission of CONFIGURATION UPDATE COMMAND message with Acknowledgement requested flag IE | CONFIGURATION UPDATE COMPLETE message received | Retransmission of CONFIGURATION UPDATE COMMAND message |
| T3565 | TBD | TBD | Transmission of NOTIFICATION message | SERVICE REQUEST message received | Trigger of service request procedure |
| Implicit de-registration timer | NOTE 1 | All except 5GMM-DEREGISTERED | Entering 5GMM-IDLE mode | N1 NAS signalling connection established | Network dependent, but typically paging is halted on 1st expiry if the UE is not registered for emergency bearer services.  Implicitly detach the UE which is registered for emergency bearer services.  Start implicit detach timer |
| Implicit detach timer | NOTE 2 | All except 5GMM-DEREGISTERED | The implicit de-registration timer expires while the network is in 5GMM-IDLE mode | N1 NAS signalling connection established | Implicitly detach the UE on 1st expiry |
| NOTE 1: The default value of this timer is 4 minutes greater than T3512. If the UE is attached for emergency bearer services, the value of this timer is set equal to T3512.  NOTE 2: The value of this timer is network dependent. . If MICO is activated, the default value of this timer is 4 minutes greater than Te. | | | | | |

## 8.10 Cause values for 5GS mobility management

### 8.10.1 Causes related to UE identification

Cause #3 – Illegal UE

This 5GMM cause is sent to the UE when the network refuses service to the UE either because an identity of the UE is not acceptable to the network or because the UE does not pass the authentication check..

Cause #6 – Illegal ME

This 5GMM cause is sent to the UE if the ME used is not acceptable to the network, e.g. blacklisted.

Cause #10 – Implicitly de-registered

This 5GMM cause is sent to the UE either if the network has implicitly de-registered the UE, e.g. after the implicit de-registration timer has expired, or if the 5GMM context data related to the subscription does not exist in the AMF e.g. because of a AMF restart, or because of a registration request for mobility or registration update is routed to a new AMF.

### 8.10.2 Cause related to subscription options

Cause #8 – 5GS services not allowed

This 5GMM cause is sent to the UE when it is not allowed to operate 5GS services.

Cause #11 – PLMN not allowed

This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate.

Cause #12 – Tracking area not allowed

This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a tracking area where the HPLMN determines that the UE, by subscription, is not allowed to operate.

NOTE 1: If 5GMM cause #12 is sent to a roaming subscriber the subscriber is denied service even if other PLMNs are available on which registration was possible.

Cause #13 – Roaming not allowed in this tracking area

This 5GMM cause is sent to an UE which requests service, or if the network initiates a de.registration request, in a tracking area of a PLMN which by subscription offers roaming to that UE but not in that tracking area.

Cause #5 – PEI not accepted

This cause is sent to the UE if the network does not accept an initial registration procedure for emergency services using a PEI.

Cause #xx – N1 mode not allowed

This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a PLMN where the UE by subscription, is not allowed to operate in N1 mode.

### 8.10.3 Causes related to PLMN specific network failures and congestion/authentication failures

Cause #21 – Synch failure

This 5GMM cause is sent to the network if the USIM detects that the SQN in the AUTHENTICATION REQUEST message is out of range.

Cause #22 – Congestion

This 5GMM cause is sent to the UE because of congestion in the network (e.g. no channel, facility busy/congested etc.).

Cause #23 – UE security capabilities mismatch

This 5GMM cause is sent to the network if the UE detects that the UE security capability does not match the one sent back by the network.

Cause #24 – Security mode rejected, unspecified

This 5GMM cause is sent to the network if the security mode command is rejected by the UE if the UE detects that the nonceUE does not match the one sent back by the network or for unspecified reasons.

Cause #xy – Restricted service area

This 5GMM cause is sent to the UE if it requests service in a tracking area which is a part of the UE’s non-allowed area or is not a part of the UE’s allowed area.

### 8.10.4 Causes related to invalid messages

Cause value #95 – Semantically incorrect message.

This 5GMM cause is used to report receipt of a message with semantically incorrect contents.

Cause value #96 – Invalid mandatory information.

This cause 5GMM indicates that the equipment sending this 5GMM cause has received a message with a non-semantical mandatory IE error.

Cause value #97 – Message type non-existent or not implemented.

This 5GMM cause indicates that the equipment sending this 5GMM cause has received a message with a message type it does not recognize either because this is a message not defined, or defined but not implemented by the equipment sending this 5GMM cause.

Cause value #98 – Message type not compatible with protocol state.

This 5GMM cause indicates that the equipment sending this 5GMM cause has received a message not compatible with the protocol state.

Cause value #99 – Information element non-existent or not implemented.

This 5GMM cause indicates that the equipment sending this 5GMM cause has received a message which includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the 5GMM cause. However, the information element is not required to be present in the message in order for the equipment sending the 5GMM cause to process the message.

Cause value #100 – Conditional IE error.

This 5GMM cause indicates that the equipment sending this cause has received a message with conditional IE errors.

Cause value #101 – Message not compatible with protocol state.

This 5GMM cause indicates that a message has been received which is incompatible with the protocol state.

Cause value #111 – Protocol error, unspecified.

This 5GMM cause is used to report a protocol error event only when no other 5GMM cause in the protocol error class applies.

# 9 5GS session management

Editor's note: The content of this sub-clause has been moved to 3GPP TS 24.501 [17], and therefore this sub-clause is no longer maintained.

## 9.1 General

The 5GS architecture reference model defined in 3GPP TS 23.501 [9] shows that the N11 reference point is used to connect the core access and mobility management function (AMF) and the session management function (SMF). The SMF handles the session management part of the NAS signalling exchanged with the UE. 3GPP TS 23.502 [10] specifies that session management procedures (e.g., PDU session establishment) are not performed between the AMF and the SMF but the UE and the SMF.

CT1 will specify the control-plane 5G session management (5GSM) towards the UE and the SMF. This includes the procedures, messages, information elements and the necessary error handling for the session management part of the NAS signalling.

## 9.2 Overview

### 9.2.1 PDU session types

The following PDU Session types are supported:

- IPv4;

- IPv6;

- Ethernet (EtherType as defined in IEEE 802.3); and

- Unstructured.

IP Address Allocation for IPv4 and IPv6 PDU session types is described in subclause 9.3.

Neither a MAC nor an IP address is allocated by the 5GC to the UE for Ethernet PDU session type.

### 9.2.2 PDU session management

The SMF is responsible for the session management functions to provide the PDU connectivity service to the UE via the SM signalling between UE and SMF. The session management procedures includes:

a) the UE-requested PDU session establishment procedure;

b) the PDU session establishment authentication and authorization procedure;

c) the UE-requested PDU session modification procedure;

d) the network-requested PDU session modification procedure; and

e) the UE-requested PDU session release procedure; and

f) the network-requested PDU session release procedure.

A UE may establish multiple PDU sessions, to the same data network or to different data networks, via 3GPP and via and Non-3GPP access networks at the same time.

The session management messages between UE and SMF are transferred via AMF as specified in subclause 9.6.

### 9.2.3 Local area data network

The UE can receive the Local area data network (LADN) information consisting of LADN DNNs and LADN service area (a set of tracking areas that belong to the current registration area) information based on the UE location during the registration procedure or the generic UE configuration update procedure (see 3GPP TS 23.501 [9] and 3GPP TS 23.502 [10]).

The UE may request a PDU session establishment and modification or initiate the service request to re-active the PDU session for an available LADN when the UE is located in the LADN service area. If the UE has moved out of the LADN service area, the PDU session for LADN may be released by the SMF, or the user-plane resources for the PDU session may be deactivated by the SMF. If the UE has returned to the LADN service area, and the network has downlink user data pending, the network re-activates the user-plane resources for the PDU session for LADN.

NOTE: In this release, LADNs apply only to 3GPP accesses.

### 9.3.4 Types of 5GSM procedures

Three types of 5GSM procedures can be distinguished:

1) Procedures related to PDU sessions:

These procedures are initiated by the network and are used for authentication and authorization or manipulation of PDU sessions:

- PDU session establishment authentication and authorization;

- network-initiated PDU session modification;

- network-initiated PDU session release.

This procedure is initiated by the UE and to request for establishment of PDU sessions or to perform handover of an existing PDU session between 3GPP access and non-3GPP access, or to transfer an existing PDN connection in the EPS to the 5GS:

- UE-requested PDU session establishment.

2) Transaction related procedures:

These procedures are initiated by the UE to request for handling of PDU sessions, i.e. to modify a PDU session, or to release a PDU session:

- UE-requested PDU session modification;

- UE-requested PDU session release.

A successful transaction related procedure initiated by the UE triggers the network to execute one of the following procedures related to PDU session; network-initiated PDU session modification procedure or network-initiated PDU session release procedure. The UE treats the start of the procedure related to the PDU session as completion of the transaction related procedure.

3) Common procedure:

The following 5GSM procedure can be related to a PDU session or to a procedure transaction:

- 5GSM status procedure.

## 9.3 5GSM sublayer states

### 9.3.1 General

In the following subclauses, the possible states of a 5G PDU session context in the UE and the network side are described.

Editor's note: The procedure transaction states for 5GSM are FFS.

### 9.3.2 5GSM sublayer states in the UE

#### 9.3.2.1 Overview

In the following subclauses, the possible 5GSM sublayer states of the UE are described and shown in figure 9.3.2.1.1.



NOTE: Not all possible transitions are shown in this figure.

Editor's note: The fatal causes and non-fatal causes used in the 5GSM procedure are FFS.

Editor's note: Whether the PDU session establishment authentication and authorization procedure impacts the state transition is FFS.

Figure 9.3.2.1.1: The 5GSM sublayer states for PDU session handling in the UE (overview)

#### 9.3.2.2 PDU SESSION INACTIVE

No PDU session context exists.

#### 9.3.2.3 PDU SESSION ACTIVE PENDING

The UE has initiated a PDU session establishment procedure towards the network and is waiting for a response from the network.

#### 9.3.2.4 PDU SESSION ACTIVE

The PDU session context is active in the UE.

#### 9.3.2.5 PDU SESSION INACTIVE PENDING

The UE has initiated a PDU session release procedure towards the network and is waiting for a response from the network.

#### 9.3.2.6 PDU SESSION MODIFICATION PENDING

The UE has initiated a PDU session modification procedure towards the network and is waiting for a response from the network.

#### 9.3.2.7 PDU SESSION ACTIVE PENDING

The UE has initiated a PDU session establishment procedure towards the network and is waiting for a response from the network.

#### 9.3.2.8 PDU SESSION ACTIVE

The PDU session context is active in the UE.

#### 9.3.2.9 PDU SESSION INACTIVE PENDING

The UE has initiated a PDU session release procedure towards the network and is waiting for a response from the network.

#### 9.3.2.10 PDU SESSION MODIFICATION PENDING

The UE has initiated a PDU session modification procedure towards the network and is waiting for a response from the network.

#### 9.3.2.11 PROCEDURE TRANSACTION INACTIVE

No procedure transaction exists.

#### 9.3.2.12 PROCEDURE TRANSACTION PENDING

The UE has initiated a procedure transaction towards the network.



Figure 9.3.2.12.1: The procedure transaction states in the UE (overview)

### 9.3.3 5GSM sublayer states in the network

#### 9.3.3.1 Overview

In the following subclauses, the possible 5GSM sublayer states of the network are described and shown in Figure 9.3.3.1.1.



NOTE: Not all possible transitions are shown in this figure.

Editor's note: The fatal causes and non-fatal causes used in the 5GSM procedure are FFS.

Editor's note: Whether the PDU session establishment authentication and authorization procedure impacts the state transition is FFS.

Figure 9.3.3.1.1: The 5GSM sublayer states for PDU session handling in the network (overview)

#### 9.3.3.2 PDU SESSION INACTIVE

No PDU session context exists.

#### 9.3.3.3 PDU SESSION ACTIVE

The PDU session context is active in the network.

#### 9.3.3.4 PDU SESSION INACTIVE PENDING

The network has initiated a PDU session release procedure towards the UE and is waiting for a response from the UE.

#### 9.3.3.5 PDU SESSION MODIFICATION PENDING

The network has initiated a PDU session modification procedure towards the UE and is waiting for a response from the UE.

#### 9.3.3.6 PROCEDURE TRANSACTION INACTIVE

No procedure transaction exists.

#### 9.3.3.7 PROCEDURE TRANSACTION PENDING

The network has initiated a procedure transaction towards the UE.



Figure 9.3.3.7.1: The procedure transaction states in the network (overview)

## 9.4 IP address allocation

### 9.4.1 General

This clause specifies IP address allocation for the PDU session.

In this release of specification, PDU sessions initiated with the PDU session type IP shall support only one IP version, i.e. IPv4 PDU session type or IPv6 PDU session type.

IP address allocation to the UE shall be performed by SMF based on the selected IP version and operator policies. If IPv4 PDU session type is selected, an IPv4 address is allocated to the UE. If IPv6 PDU session type is selected, an IPv6 prefix and an interface identifier for the IPv6 link local address are allocated to the UE.

For IPv4 PDU session type, the UE:

1) shall obtain an IPv4 address via:

A) NAS signalling as specified in subclause 9.4.2; or

B) DHCPv4; and

2) may obtain IPv4 configuration parameters (e.g. DNS server address) via DHCPv4.

For IPv6 PDU session type, the UE:

- shall obtain /64 IPv6 prefix via IPv6 stateless address autoconfiguration as specified in 3GPP TS 23.501 [9] and IETF RFC 4862 [33]; and

- may obtain IPv6 configuration parameters via stateless DHCPv6 as specified in IETF RFC 3736 [29]. The UE shall build an IPv6 link local address based on the allocated interface identifier for the IPv6 link local address.

The UE capable of IPv6 shall support acting as a type C host as specified in IETF RFC 4191 [31].

### 9.4.2 IP address allocation via NAS signalling

The UE shall set the PDU session type IE in the PDU SESSION ESTABLISHMENT REQUEST message, based on its IP stack capabilities if the UE requests IP connectivity as follows:

a) A UE:

- which is IPv6 and IPv4 capable, shall set the PDU session type IE to IP.

- which is only IPv6 capable, shall set the PDU session type IE to IPv6.

- which is only IPv4 capable, shall set the PDN type IE to IPv4.

b) When the IP version capability of the UE is unknown in the UE (as in the case when the MT and TE are separated and the capability of the TE is not known in the MT), the UE shall set the PDU session type IE to IP.

If the UE wants to use DHCPv4 for IPv4 address assignment, it shall indicate that to the network within the extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT REQUEST.

On receipt of the PDU SESSION ESTABLISHMENT REQUEST message sent by the UE, the network when allocating an IP address shall take into account the PDU session type IE, the operator's policies of the network, and the user's subscription data and:

- if the UE requests the PDU session type IP, but the subscription or SMF configuration is limited to IPv4 only or IPv6 only for the requested DNN, the network shall set the PDU session type IE to either "IPv4" or "IPv6" and the 5GSM cause value to #50 "PDU session type IPv4 only allowed", or #51 "PDU session type IPv6 only allowed" in the PDU SESSION ESTABLISHMENT ACCEPT message, respectively. The UE shall not subsequently initiate another UE requested PDU session establishment procedure to the same DNN to obtain a PDU session type different from the one allowed by the network;

- if the network sets the PDU session type IE to IPv4, the network shall include an IPv4 address in the PDU address IE; and

- if the network sets the PDU session type IE to IPv6, the network shall include an interface identifier for the IPv6 link local address in the PDU address IE.

## 9.5 5GS session management procedures

### 9.5.1 General

#### 9.5.1.1 Principles of PTI handling for 5GSM procedures

When the UE or the network initiates a transaction related procedure (i.e. a procedure consisting of more than one message and the messages are related), it shall include a valid PTI value in the message header of the request message or of the command message.

If a response message is sent as result of a received request message or a received command message, the sending entity shall include in the response message the PTI value received within the request message or within the command message (see examples in figure 9.5.1.1.1, figure 9.5.1.1.2, figure 9.5.1.1.3, and figure 9.5.1.1.4).

If a command message is sent as result of a received request message, the sending entity shall include in the command message the PTI value received with the request message (see examples in figure 9.5.1.1.3).

If a command message is not sent as result of a received request message, the sending entity shall include in the command message the PTI value set to "no procedure transaction identity assigned" (see examples in figure 9.5.1.1.3).



Figure 9.5.1.1.1: UE-requested transaction related procedure accepted by the network



Figure 9.5.1.1.2: UE-requested transaction related procedure rejected by the network



Figure 9.5.1.1.3: UE-requested transaction related procedure triggering a network-requested transaction related procedure



Figure 9.5.1.1.4: network-requested transaction related procedure not triggered by a UE-requested transaction related procedure

### 9.5.2 Local PDU session release without NAS signalling

The UE shall release PDU sessions locally without peer-to-peer 5GSM signalling in the following cases:

1) during the mobility and periodic registration update procedure or service request procedure, for PDU sessions which are in 5GSM state PDU SESSION ACTIVE on the UE side, but are indicated by the network as being in 5GSM state PDU SESSION INACTIVE in the PDU session status IE; or

2) during the mobility and periodic registration update procedure or generic UE configuration update procedure, if the UE has one or more PDU sessions associated with S-NSSAI(s) not included in the received allowed NSSAI.

Editor's note: Further cases are FFS.

The SMF shall release PDU sessions locally without peer-to-peer 5GSM signalling in the following cases:

1) during the mobility and periodic registration update procedure, de-registration procedure or service request procedure, if the SMF is triggered by the AMF to locally release the indicated PDU sessions;

2) during the mobility and periodic registration update procedure or service request procedure, if the UE has moved out of the LADN service area and the SMF decides to release the PDU session for LADN;

3) during the network-requested PDU session release procedure, if the UE is in 5GMM-IDLE mode and the N1 SM delivery skip allowed indication is sent by the SMF to the AMF; or

4) during the network-requested PDU session release procedure, it the SMF has been notified by the AMF that the UE is unreachable.

NOTE: The synchronisation of the PDU session status is achieved in the next mobility and periodic registration update procedure or service request procedure.

Editor's note: Further cases are FFS.

### 9.5.3 UE-requested PDU session establishment procedure

#### 9.5.3.1 General

The purpose of the UE-requested PDU session establishment procedure is to establish a new PDU session with a DN or to perform handover of an existing PDU session between 3GPP access and non-3GPP access or to transfer an existing PDN connection in the EPS to the 5GS. If accepted by the network, the PDU session enables exchange of PDUs between the UE and the DN. The UE shall not request a PDU session establishment for an LADN when the UE is located outside the LADN service area.

#### 9.5.3.2 UE-requested PDU session establishment procedure initiation

In order to initiate the UE-requested PDU session establishment procedure, the UE shall create a PDU SESSION ESTABLISHMENT REQUEST message.

The UE shall allocate a PTI value currently not used and shall set the PTI IE of the PDU SESSION ESTABLISHMENT REQUEST message to the allocated PTI value.

If the UE requests to establish a new non-emergency PDU session with a DN and requests a PDU session type, the UE shall set the PDU session type IE of the PDU SESSION ESTABLISHMENT REQUEST message to one of the following values: the IP version capability as specified in subclause 9.4.2, "Ethernet" or "Unstructured".

NOTE: When the UE initiates the UE-requested PDU session establishment procedure to transfer an existing non-IP PDN connection in the EPS to the 5GS, the UE can use locally available information associated with the PDN connection to select the PDU session type between "Ethernet" and "Unstructured".

If the UE requests to establish a new non-emergency PDU session with a DN and the UE requests an SSC mode, the UE shall set the SSC mode IE of the PDU SESSION ESTABLISHMENT REQUEST message to the SSC mode.

If the UE requests to establish a new PDU session with a DN, the UE may include the SM PDU DN request container with a DN-specific identity of the UE complying with network access identifier (NAI) format as specified in IETF RFC 4282 [32].

If the UE requests to establish a new PDU session of "IP", "IPv4", "IPv6" or "Ethernet" PDU session type and the UE supports reflective QoS, the UE shall set the RQoS bit to "Reflective QoS supported" in the UE SM capability IE of the PDU SESSION ESTABLISHMENT REQUEST message.

If the UE has an emergency PDU session, the UE shall not perform the UE-requested PDU session establishment procedure to establish another emergency PDU session.

The UE shall transport:

a) the PDU SESSION ESTABLISHMENT REQUEST message;

b) the PDU session ID of the PDU session being established;

c) the S-NSSAI, if the request type is not set to "initial emergency request" and the UE requests a S-NSSAI other than default S-NSSAI;

d) and the requested DNN, if the request type is not set to "initial emergency request" and the UE requests a connectivity to a DNN other than the default DNN; and

e) the request type set:

1) to "initial request", if the UE requests to establish a new non-emergency PDU session;

2) to "existing PDU session", if the UE requests:

i) handover of an existing non-emergency PDU session between 3GPP access and non-3GPP access; or

ii) transfer of an existing PDN connection in the EPS to the 5GS;

3) to "initial emergency request", if the UE requests to establish a new emergency PDU session; and

f) the old PDU session ID which is the PDU session ID of the existing PDU session, if the UE initiates the UE-requested PDU session establishment procedure upon receiving the PDU SESSION MODIFICATION COMMAND messages with the 5GSM cause IE set to #39 "reactivation requested";

using the NAS transport procedure as specified in subclause 8.5.1.1, and the UE shall start timer T3580 (see example in figure 9.5.3.2.1).



Figure 9.5.3.2.1: UE-requested PDU session establishment procedure

Upon receipt of a PDU SESSION ESTABLISHMENT REQUEST message, a PDU session ID, optionally a S-NSSAI, optionally a DNN, the request type, and optionally an old PDU session ID, the SMF checks whether connectivity with the requested DN can be established. If the requested DNN is not included, the SMF shall use the default DNN. If the S-NSSAI is not included, the SMF may determine a default S-NSSAI according to the subscription context from UDM and, if determined, the SMF may use the default S-NSSAI as the S-NSSAI.

If the PDU session being established is a non-emergency PDU session and the PDU session authentication and authorization by the external DN is required due to local policy, the SMF shall check whether the PDU SESSION ESTABLISHMENT REQUEST message includes the PDU DN request container.

If the PDU session being established is a non-emergency PDU session, the PDU DN request container is included in the PDU SESSION ESTABLISHMENT REQUEST message and the PDU session authentication and authorization by the external DN is required due to local policy and user's subscription data, the SMF shall:

- if the information for the PDU session authentication and authorization by the external DN in PDU DN request container is compliant with the local policy and user's subscription data, proceed with the EAP Authentication procedure specified in 3GPP TS 33.501 [24] and refrain from accepting or rejecting the PDU SESSION ESTABLISHMENT REQUEST message until the EAP Authentication procedure finalizes; and

- if the information for the PDU session authentication and authorization by the external DN in PDU DN request container is not compliant with the local policy, reject the PDU session establishment request including the 5GSM cause #xx "DN authentication failed", in the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU session being established is a non-emergency PDU session, the PDU DN request container is not included in the PDU SESSION ESTABLISHMENT REQUEST message and the PDU session authentication and authorization by the external DN is required due to local policy and user's subscription data, the SMF shall proceed with the EAP Authentication procedure specified in 3GPP TS 33.501 [24] and refrain from accepting or rejecting the PDU SESSION ESTABLISHMENT REQUEST message until the EAP Authentication procedure finalizes.

If the SMF receives the old PDU session ID from the AMF and a PDU session exists for the old PDU session ID, the SMF shall consider that the request for the relocation of SSC mode 3 PDU session anchor with multiple PDU sessions as specified in 3GPP TS 23.502 [10] is accepted by the UE.

#### 9.5.3.3 UE-requested PDU session establishment procedure accepted by the network

If the connectivity with the requested DN is accepted by the network, the SMF shall create a PDU SESSION ESTABLISHMENT ACCEPT message.

The SMF shall set the authorized QoS rules IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the authorized QoS rules of the PDU session. If the received request type is "initial emergency request", the SMF shall set the authorized QoS rules IE according to the initial QoS parameters used for establishing emergency services configured in the SMF Emergency Configuration Data.

The SMF shall set the selected SSC mode IE of the PDU SESSION ESTABLISHMENT ACCEPT message to:.

- either the received SSC mode or the SSC mode modified from the received SSC mode based on the subscription, the SMF configuration, or both if the request type IE is set to "initial request", and the SSC mode IE is included in the PDU SESSION ESTABLISHMENT REQUEST message;

- otherwise, either the default SSC mode for the data network listed in the subscription or the SSC mode associated with the SMF configuration.

If the PDU session is an emergency PDU session, the SMF shall set the selected SSC mode IE of the PDU SESSION ESTABLISHMENT ACCEPT message to "SSC mode 1".

The SMF shall set the selected S-NSSAI IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the selected S-NSSAI of the PDU session.

The SMF shall set the selected PDU session type IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the selected PDU session type of the PDU session.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IP", the SMF shall select either "IPv4" or "IPv6" as the selected PDU session type IE of the PDU session. If the subscription, the SMF configuration, or both, are limited to IPv4 only or IPv6 only for the requested DNN, the SMF shall include the 5GSM cause value #50 "PDU session type IPv4 only allowed", or #51 "PDU session type IPv6 only allowed", respectively, in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT ACCEPT message.

If the selected PDU session type is "IPv4", the SMF shall include the PDU address IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the PDU address IE to an IPv4 address is allocated to the UE in the PDU session.

If the selected PDU session type is "IPv6", the SMF shall include the PDU address IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the PDU address IE to an interface identifier for the IPv6 link local address.

The SMF shall set the selected DNN IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the selected DNN of the PDU session.

The SMF shall set the selected Session-AMBR IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the Session-AMBR of the PDU session.

If the selected PDU session type is "IPv4", "IPv6" or "Ethernet" and if the PDU SESSION ESTABLISHMENT REQUEST message includes a UE SM capability IE with the RQoS bit set to "Reflective QoS supported", the SMF shall consider that reflective QoS is supported for QoS flows belonging to this PDU session and include the RQ timer IE set to an RQ timer value.

NOTE: If the 5G core network determines that reflective QoS is to be used for a QoS flow, the SMF sends reflective QoS indication (RQI) to UPF to activate reflective QoS. If the QoS flow is established over 3GPP access, the SMF also includes reflective QoS Attribute (RQA) in QoS profile of the QoS flow during QoS flow establishment.

If the DN authentication of the UE was performed and completed successfully, the SMF shall set the EAP message IE of the PDU SESSION ESTABLISHMENT ACCEPT message to an EAP-success message as specified in IETF RFC 3748 [30], provided by the DN.

The SMF shall send the PDU SESSION ESTABLISHMENT ACCEPT message.

Upon receipt of a PDU SESSION ESTABLISHMENT ACCEPT message and a PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.1, the UE shall stop timer T3580, shall release the allocated PTI value and shall consider that the PDU session was established.

If the UE requests the PDU session type "IP" and:

a) the UE receives the selected PDU session type set to "IPv4" and does not receive the 5GSM cause value #50 "PDU session type IPv4 only allowed"; or

b) the UE receives the selected PDU session type set to "IPv6" and does not receive the 5GSM cause value #51 "PDU session type IPv6 only allowed";

the UE may subsequently request another PDU session for the other IP version using the UE-requested PDU session establishment procedure to the same DNN with a single address PDN type (IPv4 or IPv6) other than the one already activated.

If the UE requests the PDU session type "IP", receives the selected PDU session type set to "IPv4" and the 5GSM cause value #50 "PDU session type IPv4 only allowed", the UE shall not subsequently request another PDU session for "IPv6" using the UE-requested PDU session establishment procedure to the same DNN and the PDU session type "IPv6" until the PDU session is released.

If the UE requests the PDU session type "IP", receives the selected PDU session type set to "IPv6" and the 5GSM cause value #51 "PDU session type IPv6 only allowed", the UE shall not subsequently request another PDU session for "IPv4" using the UE-requested PDU session establishment procedure to the same DNN and the PDU session type "IPv4" until the PDU session is released.

#### 9.5.3.4 UE requested PDU session establishment procedure not accepted by the network

##### 9.5.3.4.1 General

If the connectivity with the requested DN is rejected by the network, the SMF shall create a SM PDU SESSION ESTABLISHMENT REJECT message.

If the UE requests a PDU session establishment for an LADN when the UE is located outside the LADN service area, the SMF shall reject the request.

The SMF shall set the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message to indicate the reason for rejecting the PDU session establishment.

The 5GSM cause IE typically indicates one of the following SM cause values:

#26: insufficient resources;

#27: missing or unknown DNN;

#31: request rejected, unspecified;

#50 PDU session type IPv4 only allowed;

#51 PDU session type IPv6 only allowed; or

#ss insufficient resources for specific slice and DNN;

#xx: DN authentication failed.

Editor's note: Further 5GSM causes are FFS.

Editor's note: Further contents of the PDU SESSION ESTABLISHMENT REJECT are FFS.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IPv6", and the subscription, the SMF configuration, or both, are limited to IPv4 only for the requested DNN, the SMF shall include the 5GSM cause value #50 "PDU session type IPv4 only allowed" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IPv4", and the subscription, the SMF configuration, or both, are limited to IPv6 only for the requested DNN, the SMF shall include the 5GSM cause value #51 "PDU session type IPv6 only allowed" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message.

The SMF may include a Back-off timer value IE in the PDU SESSION ESTABLISHMENT REJECT message when the 5GSM cause value #26"insufficient resources" is included in the PDU SESSION ESTABLISHMENT REJECT message. If the 5GSM cause value is #26"insufficient resources" and the PDU SESSION ESTABLISHMENT REQUEST message was received from a UE configured to use AC11–15 in selected PLMN or the request type in the PDU SESSION ESTABLISHMENT REQUEST message was set to "initial emergency request", the network shall not include a Back-off timer value IE.

Editor's note It is FFS whether both 5GSM cause value #26 and 5GSM cause values #ss are used or whether 5GSM cause value #26 together with an indication should be used instead.

The SMF may include a Back-off timer value IE in the PDU SESSION ESTABLISHMENT REJECT message when the 5GSM cause cause #ss "insufficient resources for specific slice and DNN" is included in the PDU SESSION ESTABLISHMENT REJECT message. If the 5GSM cause value is #ss "insufficient resources for specific slice and DNN" and the PDU SESSION ESTABLISHMENT REQUEST message was received from a UE configured to use AC11–15 in selected PLMN or the request type is "initial emergency request" in the PDU SESSION ESTABLISHMENT REQUEST message, the network shall not include a Back-off timer value IE.

Editor's note: It is FFS whether both 5GSM cause value #26 and 5GSM cause values #ss are used or whether 5GSM cause value #26 together with an indication should be used instead.

The SMF shall send the SM PDU SESSION ESTABLISHMENT REJECT message.

Upon receipt of a PDU SESSION ESTABLISHMENT REJECT message and a PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3, the UE shall stop timer T3580 shall release the allocated PTI value and shall consider that the PDU session was not established.

If the DN authentication of the UE was performed and completed unsuccessfully, the SMF shall include the 5GSM cause value #xx "DN authentication failed" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message and shall set the EAP message IE of the PDU SESSION ESTABLISHMENT REJECT message to an EAP-failure message as specified in IETF RFC 3748 [30], provided by the DN.

If the 5GSM cause value is #26 "insufficient resources" and the Back-off timer value IE is included, the UE shall take different actions depending on the timer value received for timer T35ab in the Back-off timer value:

1) If the timer value indicates neither zero nor deactivated and a DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message, the UE shall stop timer T35ab associated with the corresponding DNN, if it is running. If the timer value indicates neither zero nor deactivated and no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request", the UE shall stop timer T35ab associated with no DNN if it is running. The UE shall then start timer T35ab with the value provided in the Back-off timer value IE and:

- shall not send another PDU SESSION ESTABLISHMENT REQUEST,or PDU SESSION MODIFICATION REQUEST message for the same DNN that was sent by the UE, until timer T35ab expires or timer T35ab is stopped; and

- shall not send another PDU SESSION ESTABLISHMENT REQUEST message without an DNN and with request type different from "initial emergency request", or another PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an DNN provided by the UE, if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request", until timer T35ab expires or timer T35ab is stopped.

The UE shall not stop timer T35ab upon a PLMN change or inter-system change;

2) if the timer value indicates that this timer is deactivated and a DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message, the UE shall stop timer T35ab associated with the corresponding DNN, if it is running. If the timer value indicates that this timer is deactivated and no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request", the UE shall stop timer T35ab associated with no DNN if it is running. The UE:

- shall not send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST for the same DNN until the UE is switched off or the USIM is removed, or the UE receives an PDU SESSION MODIFICATION REQUEST message for the same DNN from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same DNN from the network; and

- shall not send another PDU SESSION ESTABLISHMENT REQUEST message without an DNN and with request type different from "initial emergency request", or another PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an DNN provided by the UE, if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request", until the UE is switched off or the USIM is removed, or the UE receives an PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an DNN provided by the UE, or a PDU SESSION RELEASE COMMAND messages including 5GSM cause IE set to 5GSM cause #39 "reactivation requested" for a non-emergency PDU session established without an DNN provided by the UE.

The timer T35ab remains deactivated upon a PLMN change or inter-system change; and

3) if the timer value indicates zero, the UE:

- shall stop timer T35ab associated with the corresponding DNN, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same DNN; and

- if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request ", the UE shall stop timer T35ab associated with no DNN, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST message without a DNN, or another PDU SESSION MODIFICATION REQUEST message without an DNN provided by the UE.

If the Back-off timer value IE is not included, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same DNN or without a DNN.

When the timer T35ab is running or the timer is deactivated, the UE is allowed to initiate a PDU session establishment procedure for emergency services.

If the timer T35ab is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T35ab is kept running until it expires or it is stopped.

If the UE is switched off when the timer T35ab is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

- let t1 be the time remaining for T35ab timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

If the 5GSM cause value is #ss "insufficient resources for specific slice and DNN" and the Back-off timer value IE is included, the UE shall take different actions depending on the timer value received for timer T35cd in the Back-off timer value:

1) If the timer value indicates neither zero nor deactivated, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is established, if it is running. The UE shall then start timer T35cd with the value provided in the Back-off timer value IE. The UE shall not send another PDU SESSION ESTABLISHMENT REQUEST with request type different from "initial emergency request", or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination that was sent by the UE, until timer T35cd expires or timer T35cd is stopped;

The UE shall not stop timer T35cd upon a PLMN change or inter-system change;

2) if the timer value indicates that this timer is deactivated, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is established, if it is running. The UE shall not send another PDU SESSION ESTABLISHMENT REQUEST with request type different from "initial emergency request", or PDU SESSION MODIFICATION REQUEST for the same [S-NSSAI, DNN] combination that was sent by the UE, until the UE is switched off or the USIM is removed, or the UE receives an PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same [S-NSSAI, DNN] combination from the network; and

The timer T35cd remains deactivated upon a PLMN change or inter-system change; and

3) if the timer value indicates zero, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination that was sent by the UE, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

If the Back-off timer value IE is not included, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

When the timer T35cd is running or the timer is deactivated, the UE is allowed to initiate a PDU session establishment procedure for emergency services.

If the timer T35cd is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T35cd is kept running until it expires or it is stopped.

If the UE is switched off when the timer T35cd is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

- let t1 be the time remaining for T35cd timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

##### 9.5.3.4.2 Handling of network rejection due to 5GSM cause #26

Editor's note: Handling of network rejection due to 5GSM cause #26 is FFS.

##### 9.5.3.4.3 Handling of network rejection due to 5GSM cause other than 5GSM cause #26

If the 5GSM cause value is #27 "missing or unknown DNN", the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message in the PLMN for the same DNN that was sent by the UE, until the UE is switched off, the USIM is removed, or the network updates the LADN information during the registration procedure or the generic UE configuration update procedure.

Editor's note: Handling of network rejection due to 5GSM cause other than 5GSM cause #27 "missing or unknown DNN" is FFS.

#### 9.5.3.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) T3580 expired

The UE shall, on the first expiry of the timer T3580, retransmit the PDU SESSION ESTABLISHMENT REQUEST message and shall reset and start timer T3580. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3580, the UE shall abort the procedure.

Editor's note: Further abnormal cases in the UE are FFS.

#### 9.5.3.6 Abnormal cases on the network side

Editor's note: Further abnormal cases in the network side are FFS.

The following abnormal cases can be identified:

a) If the received request type is "initial emergency request" and there is already another emergency PDU session for the UE, the SMF shall reject the PDU SESSION ESTABLISHMENT REQUEST message with ESM cause #31 "request rejected, unspecified" or release the existing emergency PDU session locally without notification to the UE and proceed the new PDU SESSION ESTABLISHMENT REQUEST message.

b) The information for the PDU session authentication and authorization by the external DN in PDU DN request container is not compliant with local policy and user's subscription data

If the PDU session being established is a non-emergency PDU session, the PDU session authentication and authorization by the external DN is required due to local policy and user's subscription data and the information for the PDU session authentication and authorization by the external DN in PDU DN request container is not compliant with local policy and user's subscription data, the SMF shall reject the PDU session establishment request including the 5GSM cause #xx "DN authentication failed", in the PDU SESSION ESTABLISHMENT REJECT message.

### 9.5.4 PDU session establishment authentication and authorization procedure

#### 9.5.4.1 General

The purpose of the PDU session establishment authentication and authorization procedure is to enable the DN:

1) to authenticate the upper layers of the UE, when establishing the PDU session;

2) to authorize the upper layers of the UE, when establishing the PDU session; or

3) both of the above.

The PDU session establishment authentication and authorization procedure can be performed only during the UE-requested PDU session establishment procedure establishing a non-emergency PDU session. The PDU session establishment authentication and authorization procedure shall not be performed during the UE-requested PDU session establishment procedure establishing an emergency PDU session.

The network authenticates the UE using the Extensible Authentication Protocol (EAP) as specified in IETF RFC 3748 [30].

EAP has defined four types of EAP messages:

- an EAP-request message;

- an EAP-response message;

- an EAP-success message; and

- an EAP-failure message.

The EAP-request message is transported from the network to the UE using the PDU SESSION AUTHENTICATION REQUEST message.

The EAP-response message to the EAP-request message is transported from the UE to the network using the PDU SESSION AUTHENTICATION ACCEPT message.

If the DN authentication of the UE completes successfully, the EAP-success message is transported from the network to the UE as part of the UE-requested PDU session establishment procedure in the PDU SESSION ESTABLISHMENT ACCEPT message.

If the DN authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE as part of the UE-requested PDU session establishment procedure in the PDU SESSION ESTABLISHMENT REJECT message.

There can be several rounds of exchange of an EAP-request message and a related EAP-response message for the DN to complete the authentication and authorization of the request for a PDU session (see example in figure 9.5.4.1.1).

The SMF shall set the authenticator retransmission timer specified in IETF RFC 3748 [30] subclause 4.3 to infinite value.

NOTE 2: The PDU session establishment authentication and authorization procedure provides a reliable transport of EAP messages and therefore retransmissions at the EAP layer of the SMF do not occur.



Figure 9.5.4.1.1: PDU session establishment authentication and authorization procedure

#### 9.5.4.2 PDU session establishment authentication and authorization procedure initiation

In order to initiate the PDU session establishment authentication and authorization procedure, the SMF shall create a PDU SESSION AUTHENTICATION REQUEST message.

The SMF shall set the PTI IE of the PDU SESSION AUTHENTICATION REQUEST message to "No procedure transaction identity assigned".

The SMF shall set the EAP message IE of the PDU SESSION AUTHENTICATION REQUEST message to the EAP-request message provided by the DN or generated locally.

The SMF shall send the PDU SESSION AUTHENTICATION REQUEST message, and the SMF shall start timer T3590 (see example in figure 9.5.4.1.1).

Upon receipt of a PDU SESSION AUTHENTICATION REQUEST message and a PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3, the UE passes to the upper layers the EAP message received in the EAP message IE of the PDU SESSION AUTHENTICATION REQUEST message. Apart from this action, the authentication and authorization procedure initiated by the DN is transparent to the 5GSM layer of the UE.

#### 9.5.4.3 PDU session establishment authentication and authorization procedure accepted

When the upper layers provide an EAP-response message responding to the received EAP-request message, the UE shall create a PDU SESSION AUTHENTICATION ACCEPT message.

The UE shall set the EAP message IE of the PDU SESSION AUTHENTICATION ACCEPT message to the EAP-response message.

The UE shall transport the PDU SESSION AUTHENTICATION ACCEPT message and the PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3. Apart from this action, the authentication and authorization procedure initiated by the DN is transparent to the 5GSM layer of the UE.

Upon receipt of a PDU SESSION AUTHENTICATION ACCEPT message, the SMF shall stop timer T3590 and provides the EAP message received in the EAP message IE of the PDU SESSION AUTHENTICATION ACCEPT message to the DN or handles it locally.

#### 9.5.4.4 Abnormal cases on the network side

The following abnormal cases can be identified:

a) T3590 expired

The SMF shall, on the first expiry of the timer T3590, retransmit the PDU SESSION AUTHENTICATION REQUEST message and shall reset and start timer T3590. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3590, the SMF shall abort the procedure.

Editor's note: Further abnormal cases are FFS

#### 9.5.4.5 Abnormal cases in the UE

Editor's note: Abnormal cases are FFS

### 9.5.5 UE-requested PDU session modification procedure

#### 9.5.5.1 General

The purpose of the UE-requested PDU session modification procedure is to enable the UE to request modification of a PDU session. The UE shall not request a PDU session modification for an LADN when the UE is located outside the LADN service area. If the UE supports Reflective QoS, the UE shall initiate this procedure to indicate the support of Reflective QoS after an inter-system change from S1 mode to N1 mode.

#### 9.5.5.2 UE-requested PDU session modification procedure initiation

In order to initiate the UE-requested PDU session modification procedure, the UE shall create a PDU SESSION MODIFICATION REQUEST message.

The UE shall allocate a PTI value currently not used and shall set the PTI IE of the PDU SESSION MODIFICATION REQUEST message to the allocated PTI value.

The UE shall not perform the UE-requested PDU session modification procedure for an emergency PDU session.

If the UE requests a specific QoS handling, the UE shall include the requested QoS rules IE indicating requested QoS rules for the specific QoS handling.

The UE shall transport the PDU SESSION MODIFICATION REQUEST message and the PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3, and the UE shall start timer T3581 (see example in figure 9.5.5.2.1).



Figure 9.5.5.2.1: UE-requested PDU session modification procedure

#### 9.5.5.3 UE-requested PDU session modification procedure accepted by the network

Upon receipt of a PDU SESSION MODIFICATION REQUEST message, if the SMF accepts the request to modify the PDU session, the SMF shall perform the network-requested PDU session modification procedure as specified in subclause 9.5.6.

#### 9.5.5.4 UE-requested PDU session modification procedure not accepted by the network

Upon receipt of a PDU SESSION MODIFICATION REQUEST message, if the SMF does not accepts the request to modify the PDU session, the SMF shall create a PDU SESSION MODIFICATION REJECT message.

If the UE requests a PDU session modification for an LADN when the UE is located outside the LADN service area, the SMF shall reject the request.

The SMF shall set the 5GSM cause IE of the PDU SESSION MODIFICATION REJECT message to indicate the reason for rejecting the PDU session modification.

The 5GSM cause IE typically indicates one of the following SM cause values:

#26: insufficient resources;

#31: request rejected, unspecified; or

#ss insufficient resources for specific slice and DNN;

Editor's note: Further 5GSM causes are FFS.

The SMF may include a Back-off timer value IE in the PDU SESSION MODIFICATION REJECT message. If the 5GSM cause value is #26 "insufficient resources" and the PDU SESSION MODIFICATION REQUEST message was received from a UE configured to use AC11–15 in selected PLMN or the request type was set to "initial emergency request" for the establishment of the PDU session, the network shall not include a Back-off timer value IE.

Editor's note: It is FFS whether both 5GSM cause value #26 and 5GSM cause values #ss are used or whether 5GSM cause value #26 together with an indication should be used instead.

The SMF may include a Back-off timer value IE in the PDU SESSION MODIFICATION REJECT message when the 5GSM cause cause #ss "insufficient resources for specific slice and DNN" is included in the PDU SESSION MODIFICATION REJECT message. If the 5GSM cause value is #ss "insufficient resources for specific slice and DNN" and the PDU SESSION MODIFICATION REQUEST message was received from a UE configured to use AC11–15 in selected PLMN or the request type is set to "initial emergency request" for the establisment of the PDU session, the network shall not include a Back-off timer value IE.

Editor's note: It is FFS whether both 5GSM cause value #26 and 5GSM cause values #ss are used or whether 5GSM cause value #26 together with an indication should be used instead.

The SMF shall send the PDU SESSION MODIFICATION REJECT message.

Upon receipt of a PDU SESSION MODIFICATION REJECT message and a PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3, the UE shall stop timer T3581, shall release the allocated PTI value and shall consider that the PDU session is not modified.

If the 5GSM cause value is #26 "insufficient resources" and the Back-off timer value IE is included, the UE shall take different actions depending on the timer value received for timer T35ab in the Back-off timer value:

1) If the timer value indicates neither zero nor deactivated, the UE shall stop timer T35ab associated with the corresponding DNN, if it is running. The UE shall then start timer T35ab with the value provided in the Back-off timer value IE and shall not send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same DNN that was sent by the UE, until timer T35ab expires or timer T35ab is stopped.

If the UE did not provide a DNN for the establishment of the PDU session and the request type was different from "initial emergency request", the UE shall stop the timer T35ab associated with no DNN if it is running. The UE shall start timer T35ab with the received value and not send another PDU SESSION ESTABLISHMENT REQUEST message without an DNN and with request type different from "initial emergency request", or another PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an DNN provided by the UE, until timer T35ab expires or timer T35ab is stopped.

The UE shall not stop timer T35ab upon a PLMN change or inter-system change.

2) if the timer value indicates that this timer is deactivated, the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same DNN until the UE is switched off or the USIM is removed, or the UE receives an PDU SESSION MODIFICATION REQUEST message for the same DNN from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same DNN from the network.

If the UE did not provide an DNN for the establishment of the PDU session and the request type was different from "initial emergency request", the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message without an DNN and with request type different from "initial emergency request", or another PDU SESSION MODIFICATION REQUEST for a non-emergency PDU session established without DNN provided by the UE, until the UE is switched off or the USIM is removed, or the UE receives an PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an DNN provided by the UE, or the UE receives a PDU SESSION RELEASE COMMAND messages including 5GSM cause IE set to 5GSM cause #39 "reactivation requested" for a non-emergency PDU session established without an DNN provided by the UE.

The timer T35ab remains deactivated upon a PLMN change or inter-system change.

3) if the timer value indicates zero, the UE shall stop timer T35ab associated with the corresponding DNN, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same DNN.

if the UE did not provide an DNN for the establishment of the PDU session and the request type was different from " initial emergency request ", the UE shall stop timer T35ab associated with no DNN, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST message without an DNN, or another PDU SESSION MODIFICATION REQUEST message established without an DNN provided by the UE.

If the Back-off timer value IE is not included, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same DNN or without DNN.

If the timer T35ab is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T35ab is kept running until it expires or it is stopped.

If the UE is switched off when the timer T35ab is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

- let t1 be the time remaining for T35ab timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

If the 5GSM cause value is #ss "insufficient resources for specific slice and DNN" and the Back-off timer value IE is included, the UE shall take different actions depending on the timer value received for timer T35cd in the Back-off timer value:

1) If the timer value indicates neither zero nor deactivated, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is establishe, if it is running. The UE shall then start timer T35cd with the value provided in the Back-off timer value IE and shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination that was sent by the UE, until timer T35cd expires or timer Tsm1 is stopped.

The UE shall not stop timer Tsm1 upon a PLMN change or inter-system change.

2) if the timer value indicates that this timer is deactivated, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is established, if it is running. the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST for the same [S-NSSAI, DNN] combination until the UE is switched off or the USIM is removed, or the UE receives an PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same [S-NSSAI, DNN] combination from the network

The timer T35cd remains deactivated upon a PLMN change or inter-system change.

3) if the timer value indicates zero, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

If the Back-off timer value IE is not included, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

When the timer T35cd is running or the timer is deactivated, the UE is allowed to initiate a PDU session establishment procedure for emergency services.

If the timer T35cd is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T35cd is kept running until it expires or it is stopped.

If the UE is switched off when the timer T35cd is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

- let t1 be the time remaining for T35cd timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

#### 9.5.5.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) T3581 expired

The UE shall, on the first expiry of the timer T3581, retransmit the PDU SESSION MODIFICATION REQUEST message and shall reset and start timer T3581. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3581, the UE shall abort the procedure and shall release the allocated PTI.

Editor's note: Further abnormal cases are FFS.

#### 9.5.5.6 Abnormal cases on the network side

Editor's note: Further abnormal cases are FFS.

The following abnormal cases can be identified:

a) If the PDU session is an emergency PDU session, the SMF shall reject the PDU SESSION MODIFICATION REQUEST message with ESM cause #31 "request rejected, unspecified".

### 9.5.6 Network-requested PDU session modification procedure

#### 9.5.6.1 General

The purpose of the network-requested PDU session modification procedure is to enable the network to modify a PDU session.

Editor's note: The solution for situation when the UE is in 5GMM-IDLE mode and the AMF decides to invoke asynchronous type communication is FFS.

Editor's note: It is FFS whether there are cases where the UE can validly reject the PDU SESSION MODIFICATION COMMAND message.

#### 9.5.6.2 Network-requested PDU session modification procedure initiation

In order to initiate the network-requested PDU session modification procedure, the SMF shall create a PDU SESSION MODIFICATION COMMAND message.

If the authorized QoS rules of the PDU session is modified, the SMF shall set the authorized QoS rules IE of the PDU SESSION MODIFICATION COMMAND message to the authorized QoS rules of the PDU session.

If the session-AMBR of the PDU session is modified, the SMF shall set the selected Session-AMBR IE of the PDU SESSION MODIFICATION COMMAND message to the session-AMBR of the PDU session.

If the network-requested PDU session modification procedure is triggered by a UE-requested PDU session modification procedure, the SMF shall set the PTI IE of the PDU SESSION MODIFICATION COMMAND message to the PTI of the PDU SESSION MODIFICATION REQUEST message received as part of the UE-requested PDU session modification procedure.

If the network-requested PDU session modification procedure is not triggered by a UE-requested PDU session modification procedure, the SMF shall set the PTI IE of the PDU SESSION MODIFICATION COMMAND message to "No procedure transaction identity assigned".

If the selected SSC mode of the PDU session is "SSC mode 3" and the SMF requests the relocation of SSC mode 3 PDU session anchor with multiple PDU sessions as specified in 3GPP TS 23.502 [10], the SMF shall include 5GSM cause #39 "reactivation requested" , in the PDU SESSION MODIFICATION COMMAND message.

The SMF shall send the PDU SESSION MODIFICATION COMMAND message, and the SMF shall start timer T3591 (see example in figure 9.5.6.2.1).

NOTE: If the SMF requests the relocation of SSC mode 3 PDU session anchor with multiple PDU sessions as specified in 3GPP TS 23.502 [10], the reallocation requested indication indicating whether the SMF is to be reallocated or the SMF is to be reused is provided to the AMF.



Figure 9.5.6.2.1: Network-requested PDU session modification procedure

#### 9.5.6.3 Network-requested PDU session modification procedure accepted by the UE

Upon receipt of the PDU SESSION MODIFICATION COMMAND message, if the UE provided a DNN for the establishment of the PDU session, the UE shall stop timer T35ab, if it is running for the DNN provided by the UE. If the UE did not provide a DNN for the establishment of the PDU session and the request type was different from "initial emergency request", the UE shall stop the timer T35ab associated with no DNN if it is running. If the MODIFY EPS BEARER CONTEXT REQUEST message was received for an emergency PDU session, the UE shall not stop the timer T35ab associated with no DNN if it is running.

Upon receipt of the PDU SESSION MODIFICATION COMMAND message, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is establishe, if it is running.

Upon receipt of a PDU SESSION MODIFICATION COMMAND message and a PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3, if the UE accepts the PDU SESSION MODIFICATION COMMAND message, the UE considers the PDU session as modified and the UE shall create a PDU SESSION MODIFICATION COMPLETE message.

If the PDU SESSION MODIFICATION COMMAND message contains the PTI value allocated in the UE-requested PDU session modification procedure, the UE shall release the PTI value indicated by the PTI IE and shall stop the timer T3581.

If the selected SSC mode of the PDU session is "SSC mode 3" and the PDU SESSION MODIFICATION COMMAND messages includes 5GSM cause #39 "reactivation requested", the UE may re-initiate the UE-requested PDU session establishment procedure as specified in subclause 9.5.3 for the PDU session type, the SSC mode, the DNN, and the S-NSSAI as provided in the UE-requested PDU session establishment procedure of the present PDU session, after the complete of the network-requested PDU session modification procedure.

The UE shall transport the PDU SESSION MODIFICATION COMPLETE message and the PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3.

Upon receipt of a PDU SESSION MODIFICATION COMPLETE message, the SMF shall stop timer T3591 and shall consider the PDU session as modified.

#### 9.5.6.4 Network-requested PDU session modification procedure not accepted by the UE

Editor's note: FFS whether to change message name of PDU SESSION MODIFICATION COMMAND because of the possibility of the rejections from the UE

Upon receipt of a PDU SESSION MODIFICATION COMMAND message and a PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3, if the UE rejects the PDU SESSION MODIFICATION COMMAND message, the UE considers the PDU session as not modified and the UE shall create a PDU SESSION MODIFICATION COMMAND REJECT message.

If the PDU SESSION MODIFICATION COMMAND message contains the PTI value allocated in the UE-requested PDU session modification procedure, the UE shall release the PTI indicated by the PTI IE and shall stop the timer T3581.

The UE shall set the 5GSM cause IE of the PDU SESSION MODIFICATION COMMAND REJECT message to indicate the reason for rejecting the PDU session modification.

If the selected SSC mode of the PDU session is "SSC mode 3" and the PDU SESSION MODIFICATION COMMAND messages includes 5GSM cause #39 "reactivation requested", while the UE does not have sufficient resources for initiating the PDU session establishment procedure as specified in subclause 9.5.3 then the UE shall set cause IE to #26 "insufficient resources".

The 5GSM cause IE typically indicates one of the following 5GSM cause values:

#26: "insufficient resources".

Editor's note: Other 5GSM causes are FFS.

The UE shall transport the PDU SESSION MODIFICATION COMMAND REJECT message and the PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3.

Upon receipt of a PDU SESSION MODIFICATION COMMAND REJECT message, the SMF shall stop timer T3591 and shall consider the PDU session as not modified.

#### 9.5.6.5 Abnormal cases on the network side

The following abnormal cases can be identified:

a) T3591 expired

On the first expiry of the timer T3591:

the SMF shall resend the PDU SESSION MODIFICATION COMMAND message and shall reset and restart timer T3591. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3591 depending on the 5GSM value included in the PDU SESSION MODIFICATION COMMAND message:

#39; the SMF shall initiate the network-requested PDU session release procedure procedure indicating the PDU session identity of the old PDU session.

otherwise, the SMF shall abort the procedure and enter the state PDU SESSION ACTIVE.

if the PDU SESSION MODIFICATION COMMAND message did not contain 5GSM value #39, the SMF may continue to use the previous configuration of the PDU session or initiate the network-requested PDU session release procedure.

Editor's note: Further abnormal cases are FFS.

#### 9.5.6.6 Abnormal cases in the UE

Editor's note: Abnormal cases are FFS.

### 9.5.7 UE-requested PDU session release procedure

#### 9.5.7.1 General

The purpose of the UE-requested PDU session release procedure is to enable by the UE to request a release of a PDU session.

The UE is allowed to initiate the PDU session release procedure even if the timer T35ab is running.

The UE is allowed to initiate the PDU session release procedure even if the timer T35cd is running.

#### 9.5.7.2 UE-requested PDU session release procedure initiation

In order to initiate the UE-requested PDU session release procedure, the UE shall create an PDU SESSION RELEASE REQUEST message.

The UE shall allocate a PTI value currently not used and shall set the PTI IE of the PDU SESSION RELEASE REQUEST message to the allocated PTI value.

The UE shall transport the PDU SESSION RELEASE REQUEST message and the PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3, and the UE shall start timer T3582 (see example in figure 9.5.7.2.1).



Figure 9.5.7.2.1: UE-requested PDU session release procedure

#### 9.5.7.3 UE-requested PDU session release procedure accepted by the network

Upon receipt of a PDU SESSION RELEASE REQUEST message and an PDU session ID, if the SMF accepts the request to release the PDU session, and shall perform the network-requested PDU session release procedure as specified in subclause 9.5.8.

#### 9.5.7.4 UE-requested PDU session release procedure rejected by the network

Upon receipt of an PDU SESSION RELEASE REQUEST message, if the SMF does not accept the request to release the PDU session, the SMF shall create an PDU SESSION RELEASE REJECT message.

The SMF shall set the 5GSM cause IE of the PDU SESSION RELEASE REJECT message to indicate the reason for rejecting the PDU session release.

The 5GSM cause IE typically indicates one of the following SM cause values:

Editor's note: 5GSM causes are FFS.

The SMF shall send the PDU SESSION RELEASE REJECT message.

Upon receipt of an PDU SESSION RELEASE REJECT message and a PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3, the UE shall stop timer T3582, shall release the allocated PTI value, and shall consider that the PDU session is not released.

#### 9.5.7.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) T3582 expired

The UE shall, on the first expiry of the timer T3582, retransmit the PDU SESSION RELEASE REQUEST message and shall reset and start timer T3582. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3582, the UE shall abort the procedure, shall release the allocated PTI, and shall perform the registration procedure for mobility and periodic registration update with a REGISTRATION REQUEST message including the PDU session status IE.

Editors' note: Further abnormal cases are FFS.

#### 9.5.7.6 Abnormal cases on the network side

Editors' note: Abnormal cases are FFS.

### 9.5.8 Network-requested PDU session release procedure

#### 9.5.8.1 General

The purpose of the network-requested PDU session release procedure is to enable the network to release a PDU session.

#### 9.5.8.2 Network-requested PDU session release procedure initiation

In order to initiate the network-requested PDU session release procedure, the SMF shall create an PDU SESSION RELEASE COMMAND message.

The SMF shall set the SM cause IE of the PDU SESSION RELEASE COMMAND message to indicate the reason for releasing the PDU session.

The SM cause IE typically indicates one of the following SM cause values:

#36: regular deactivation; or

#39: reactivation requested.

Editor's note: Further 5GSM causes are FFS.

If the selected SSC mode of the PDU session is "SSC mode 2" and the SMF requests the relocation of SSC mode 2 PDU session anchor with different PDU sessions as specified in 3GPP TS 23.502 [10], the SMF shall include 5GSM cause #39 "reactivation requested".

If the network-requested PDU session release procedure is triggered by a UE-requested PDU session release procedure, the SMF shall set the PTI IE of the PDU SESSION RELEASE COMMAND message to the PTI of the PDU SESSION RELEASE REQUEST message received as part of the UE-requested PDU session release procedure.

If the network-requested PDU session release procedure is not triggered by a UE-requested PDU session release procedure, the SMF shall set the PTI IE of the PDU SESSION RELEASE COMMAND message to "No procedure transaction identity assigned".

The SMF shall send:

a) the PDU SESSION RELEASE COMMAND message; and

b) if the SMF allows the AMF to skip sending of the N1 SM container to the UE and the 5GSM cause IE is not set to #39 "reactivation requested", the N1 SM delivery skip allowed indication;

towards the AMF, and the SMF shall start timer T3592 (see example in figure 9.5.8.2.1).



Figure 9.5.8.2.1: Network-requested PDU session release procedure

#### 9.5.8.3 Network-requested PDU session release procedure accepted by the UE

Upon receipt of an PDU SESSION RELEASE COMMAND message and a PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3, the UE considers the PDU session as released and the UE shall create an PDU SESSION RELEASE COMPLETE message.

If the PDU SESSION RELEASE COMMAND message contains the PTI value allocated in the UE-requested PDU session release procedure, the UE shall release the PTI value indicated by the PTI IE and shall stop the timer T3582.

If the PDU SESSION RELEASE COMMAND messages includes 5GSM cause #39 "reactivation requested", the UE should re-initiate the UE-requested PDU session establishment procedure as specified in subclause 9.5.3 for the PDU session type, the SSC mode, the DNN, and the S-NSSAI as provided in the UE-requested PDU session establishment procedure of the released PDU session, after completion of the network-requested PDU session release procedure.

If the PDU SESSION RELEASE COMMAND includes 5GSM cause #39 "reactivation requested" and the UE provided a DNN for the establishment of the PDU session, the UE shall stop timer T35ab if it is running for the DNN provided by the UE. The UE should then re-initiate the UE requested PDU session establishment procedure for the same DNN. If the UE did not provide a DNN for the establishment of the PDU session and the request type was different from "initial emergency request", the UE shall stop the timer T35ab associated with no DNN if it is running, and should re-initiate the UE requested PDU session establishment procedure without including a DNN. If the PDU SESSION RELEASE COMMAND message was received for an emergency PDU session, the UE shall not stop the timer T35ab associated with no DNN if it is running.

If the PDU SESSION RELEASE COMMAND includes 5GSM cause #39 "reactivation requested", the UE shall stop timer T35cd if it is running for the same [S-NSSAI, DNN] combination provided by the UE. The UE should then re-initiate the UE requested PDU session establishment procedure for the same [S-NSSAI, DNN] combination.

NOTE: User interaction is necessary in some cases when the UE cannot re-initiate the UE-requested PDU session establishment procedure automatically.

Editor's note: When the UE re-initiates the UE-requested PDU session establishment procedure, it is FFS how to ensure routing to the SMF serving the released PDU session and whether the PDU session ID is reused.

The UE shall transport the PDU SESSION RELEASE COMPLETE message and the PDU session ID, using the NAS transport procedure as specified in subclause 8.5.1.3.

Upon receipt of a PDU SESSION RELEASE COMPLETE message, the SMF shall stop timer T3592 and shall consider the PDU session as released.

#### 9.5.8.4 N1 SM delivery skipped

If the PDU SESSION RELEASE COMMAND message was sent along the N1 SM delivery skip allowed indication towards AMF, then upon receipt of an indication that N1 SM delivery was skipped, the SMF shall stop timer T3592 and shall consider the PDU session as released.

#### 9.5.8.5 Abnormal cases on the network side

The following abnormal cases can be identified:

a) T3592 expired

The SMF shall, on the first expiry of the timer T3592, retransmit the PDU SESSION RELEASE COMMAND message and shall reset and start timer T3592. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3592, the SMF shall abort the procedure.

Editors' note: Further abnormal cases are FFS.

#### 9.5.8.6 Abnormal cases in the UE

Editors' note: Abnormal cases are FFS.

### 9.5.9 5GSM status procedure

#### 9.5.9.1 General

The purpose of the sending of the 5GSM STATUS message is to report at any time certain error conditions detected upon receipt of 5GSM protocol data. The 5GSM STATUS message can be sent by both the network and the UE (see example in figure 9.5.9.1).



Figure 9.5.9.1: 5GSM status procedure

#### 9.5.9.2 5GSM status received in the UE

If the 5GSM entity of the UE receives an 5GSM STATUS message the UE shall take different actions depending on the received 5GSM cause value:

#97 (Message type non-existent or not implemented);

The UE shall abort any ongoing 5GSM procedure related to the PTI or PDU session Id and stop any related timer.

Editor’s note: Additional cause values and actions is FFS.

On receipt of an 5GSM STATUS message with any other 5GSM cause value no state transition and no specific action shall be taken as seen from the radio interface, i.e. local actions are possible.

#### 9.5.9.3 5GSM status received in the SMF

If the SMF receives an 5GSM STATUS message the SMF shall take different actions depending on the received 5GSM cause value:

#97 (Message type non-existent or not implemented);

The SMF shall abort any ongoing 5GSM procedure related to the PTI or PDU session Id and stop any related timer.

Editor’s note: Additional cause values and actions is FFS.

The local actions to be taken by the SMF on receipt of an 5GSM STATUS message with any other 5GSM cause value are implementation dependent.

## 9.6 5GS session management coding

### 9.6.1 PDU session establishment request

#### 9.6.1.1 Message definition

The PDU SESSION ESTABLISHMENT REQUEST message is sent by the UE to the network to initiate establishment of a PDU session.

Message type: PDU SESSION ESTABLISHMENT REQUEST

Significance: dual

Direction: UE to network

Table 9.6.1.1.1: PDU SESSION ESTABLISHMENT REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION ESTABLISHMENT REQUEST message identity | Message type  6.6.6.7 | M | V | 1 |
| a- | PDU session type | PDU session type  9.7.1 | O | TV | 1 |
| b- | SSC mode | SSC mode  9.7.2 | O | TV | 1 |
| xx | UE SM capability | UE SM capability  9.7.8 | O | TLV | 3-15 |
| d | SM PDU DN request container | SM PDU DN request container  9.7.4 | O | TBD | TBD |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.1.2 PDU session type

This IE is included in the message when the UE requests to establish a new PDU session with a DN and requests a PDU session type.

#### 9.6.1.3 SSC mode

This IE is included in the message when the UE requests to establish a new PDU session with a DN and requests an SSC mode.

#### 9.6.1.4 UE SM capability

This IE is included in the message when the UE requests to establish a new PDU session of "IP", "IPv4", "IPv6" or "Ethernet" PDU session type and the UE supports Reflective QoS.

#### 9.6.1.5 SM PDU DN request container

This IE is included in the message when the UE requests to establish a new PDU session with a DN and needs to provide information for the PDU session authentication and authorization by the external DN.

#### 9.6.1.6 Extended protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

### 9.6.2 PDU session establishment accept

#### 9.6.2.1 Message definition

The PDU SESSION ESTABLISHMENT ACCEPT message is sent by the network to the UE in response to PDU SESSION ESTABLISHMENT REQUEST message and indicates successful establishment of a PDU session.

Message type: PDU SESSION ESTABLISHMENT ACCEPT

Significance: dual

Direction: network to UE

Table 9.6.2.1.1: PDU SESSION ESTABLISHMENT ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION ESTABLISHMENT ACCEPT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | Selected PDU session type | PDU session type  9.7.1 | M | V | 1/2 |
|  | Selected SSC mode | SSC mode  9.7.2 | M | V | 1/2 |
|  | Selected S-NSSAI | S-NSSAI  8.7.7 | M | LV | 2 or 5 |
|  | Selected DNN | DNN  8.7.8 | M | LV | 2-TBD |
|  | Authorized QoS rules | QoS rules  12.4.2.1 | M | LV-E | 2-65537 |
|  | Session AMBR | Session-AMBR  12.4.2.2 | M | LV | TBD |
| a | 5GSM cause | 5GSM cause  9.7.6 | O | TV | 2 |
| b | PDU address | PDU address  9.7.5 | O | TLV | 7 |
| c | EAP message | EAP message  8.7.30 | O | TLV-E | 7-1503 |
| d | RQ timer value | GPRS timer  9.7.7 | O | TV | 2 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.2.2 5GSM cause

This IE is included when the selected PDU session type which is different from the PDU session type requested by the UE.

#### 9.6.2.3 PDU address

This IE is included when the selected PDU session type is "IPv4" or "IPv6".

#### 9.6.2.4 EAP message

This IE is included when the external DN successfully performed authentication and authorization of the UE using EAP.

#### 9.6.2.5 RQ timer value

This IE is included when the network wants to provide the RQ timer value.

#### 9.6.2.6 Extended protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

### 9.6.3 PDU session establishment reject

#### 9.6.3.1 Message definition

The PDU SESSION ESTABLISHMENT REJECT message is sent by the network to the UE in response to PDU SESSION ESTABLISHMENT REQUEST message and indicates unsuccessful establishment of a PDU session.

Message type: PDU SESSION ESTABLISHMENT REJECT

Significance: dual

Direction: network to UE

Table 9.6.3.1.1: PDU SESSION ESTABLISHMENT REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION ESTABLISHMENT REJECT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.7.6 | M | V | 1 |
| X | EAP message | EAP message  8.7.30 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.3.2 Extended protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

#### 9.6.3.3 EAP message

This IE is included when the external DN unsuccessfully performed authentication and authorization of the UE using EAP.

### 9.6.4 PDU session authentication request

#### 9.6.4.1 Message definition

The PDU SESSION AUTHENTICATION REQUEST message is sent by the network to the UE for authentication of the UE establishing the PDU session.

Message type: PDU SESSION AUTHENTICATION REQUEST

Significance: dual

Direction: network to UE

Table 9.6.4.1.1: PDU SESSION AUTHENTICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION AUTHENTICATION REQUEST message identity | Message type  6.6.6.7 | M | V | 1 |
| X | EAP message | EAP message  8.7.30 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.4.2 EAP message

This IE is included when the external DN performs authentication and authorization of the UE using EAP.

#### 9.6.4.3 Extended protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

### 9.6.5 PDU session authentication accept

#### 9.6.5.1 Message definition

The PDU SESSION AUTHENTICATION ACCEPT message is sent by the UE to the network in response to the PDU SESSION AUTHENTICATION REQUEST message and indicates acceptance of the PDU SESSION AUTHENTICATION REQUEST message.

Message type: PDU SESSION AUTHENTICATION ACCEPT

Significance: dual

Direction: UE to network

Table 9.6.5.1.1: PDU SESSION AUTHENTICATION ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION AUTHENTICATION ACCEPT message identity | Message type  6.6.6.7 | M | V | 1 |
| x | EAP message | EAP message  8.7.30 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.5.2 EAP message

This IE is included when the external DN performs authentication and authorization of the UE using EAP.

#### 9.6.5.3 Extended protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

### 9.6.7 PDU session modification request

#### 9.6.7.1 Message definition

The PDU SESSION MODIFICATION REQUEST message is sent by the UE to the network to request a modification of a PDU session.

Message type: PDU SESSION MODIFICATION REQUEST

Significance: dual

Direction: UE to network

Table 9.6.7.1.1: PDU SESSION MODIFICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION REQUEST message identity | Message type  6.6.6.7 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |
| b | Requested QoS rules | QoS rules  12.4.2.1 | O | TLV-E | 3-65538 |

#### 9.6.7.2 Extended protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

#### 9.6.7.3 Requested QoS rules

This IE is included in the message when the UE requests a specific QoS handling.

### 9.6.8 PDU session modification reject

#### 9.6.8.1 Message definition

The PDU SESSION MODIFICATION REJECT message is sent by the network to the UE to indicate rejection of the PDU SESSION MODIFICATION REQUEST.

Message type: PDU SESSION MODIFICATION REJECT

Significance: dual

Direction: network to UE

Table 9.6.8.1.1: PDU SESSION MODIFICATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION REJECT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.7.6 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.8.2 Extended protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

### 9.6.9 PDU session modification command

#### 9.6.9.1 Message definition

The PDU SESSION MODIFICATION COMMAND message is sent by the network to the UE to indicate a modification of a PDU session.

Message type: PDU SESSION MODIFICATION COMMAND

Significance: dual

Direction: network to UE

Table 9.6.9.1.1: PDU SESSION MODIFICATION COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION COMMAND message identity | Message type  6.6.6.7 | M | V | 1 |
| a | 5GSM cause | 5GSM cause  9.7.6 | O | TV | 2 |
| b | Authorized QoS rules | QoS rules  12.4.2.1 | O | TLV-E | 3-65538 |
| c | Session AMBR | Session-AMBR  12.4.2.2 | O | TLV | TBD |
| d | PDU session release time | GPRS timer  9.7.7 | O | TV | 2 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.9.2 5GSM cause

This IE is included when the network performs the PDU session anchor relocation for SSC mode 3.

#### 9.6.9.3 Authorized QoS rules

This IE is included when the authorized QoS rules of the PDU session are modified.

#### 9.6.9.4 Session-AMBR

This IE is included when the session-AMBR of the PDU session is modified.

#### 9.6.9.5 PDU session release time

This IE is included when the network performs the PDU session anchor relocation for SSC mode 3.

#### 9.6.9.6 Extended protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

### 9.6.10 PDU session modification accept

#### 9.6.10.1 Message definition

The PDU SESSION MODIFICATION ACCEPT message is sent by the UE to the network in response to the PDU SESSION MODIFICATION COMMAND message and indicates an acceptance of the PDU SESSION MODIFICATION COMMAND message.

Message type: PDU SESSION MODIFICATION ACCEPT

Significance: dual

Direction: UE to network

Table 9.6.10.1.1: PDU SESSION MODIFICATION ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION ACCEPT message identity | Message type  6.6.6.7 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.10.2 Extended protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

### 9.6.11 PDU session modification command reject

#### 9.6.11.1 Message definition

The PDU SESSION MODIFICATION COMMAND REJECT message is sent by the UE to the network to indicate rejection of the PDU SESSION MODIFICATION COMMAND message.

Message type: PDU SESSION MODIFICATION COMMAND REJECT

Significance: dual

Direction: UE to network

Table 9.5.11.1.1: PDU SESSION MODIFICATION COMMAND REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION COMMAND REJECT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.7.6 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.11.2 Extended protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

### 9.6.12 PDU session release request

#### 9.6.12.1 Message definition

The PDU SESSION RELEASE REQUEST message is sent by the UE to the network to request a release of a PDU session.

Message type: PDU SESSION RELEASE REQUEST

Significance: dual

Direction: UE to network

Table 9.6.12.1.1: PDU SESSION RELEASE REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION RELEASE REQUEST message identity | Message type  6.6.6.7 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.12.2 Extended protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

### 9.6.13 PDU session release reject

#### 9.6.13.1 Message definition

The PDU SESSION RELEASE REJECT message is sent by the network to the UE to indicate rejection of request a release of a PDU session.

Message type: PDU SESSION RELEASE REJECT

Significance: dual

Direction: network to UE

Table 9.6.13.1.1: PDU SESSION RELEASE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU RELEASE RELEASE REJECT message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.7.6 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.13.2 Extended protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

### 9.6.14 PDU session release command

#### 9.6.14.1 Message definition

The PDU SESSION RELEASE COMMAND message is sent by the network to the UE to indicate a release of a PDU session.

Message type: PDU SESSION RELEASE COMMAND

Significance: dual

Direction: network to UE

Table 9.6.14.1.1: PDU SESSION RELEASE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION RELEASE COMMAND message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.7.6 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.1.2 Extended protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

### 9.6.15 PDU session release accept

#### 9.6.15.1 Message definition

The PDU SESSION RELEASE ACCEPT message is sent by the UE to the network in response to the PDU SESSION RELEASE COMMAND message and indicates an acceptance of a release of the PDU session.

Message type: PDU SESSION RELEASE ACCEPT

Significance: dual

Direction: UE to network

Table 9.6.15.1.1: PDU SESSION RELEASE ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | PDU SESSION RELEASE ACCEPT message identity | Message type  6.6.6.7 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.7.3 | O | TLV-E | 4-65538 |

#### 9.6.15.2 Extended protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

### 9.6.16 5GSM status

#### 9.6.16.1 Message definition

This message is sent by the network or the UE to pass information on the status of the indicated PDU session and report certain error conditions. See table 9.6.16.1.

Message type: 5GSM STATUS

Significance: dual

Direction: both

Table 9.6.16.1: 5GSM STATUS message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  6.6.6.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  6.6.6.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  6.6.6.6 | M | V | 1 |
|  | 5GSM STATUS message identity | Message type  6.6.6.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.7.6 | M | V | 1 |

## 9.7 5GSM information elements

### 9.7.1 PDU session type

The purpose of the PDU session type information element is to indicate type of the PDU session.

The PDU session type information element is coded as shown in figure 9.7.1.1 and table 9.7.1.1.

The PDU session type is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PDU session type IEI | | | | PDU session type value | | | | Octet 1 |

Figure 9.7.1.1: PDU session type information element

Table 9.7.1.1: PDU session type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PDU session type value (octet 1, bit 1 to bit 4) | | | | |
|  | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 1 | IP |
| 0 | 0 | 1 | 0 | IPv4 |
| 0 | 0 | 1 | 1 | IPv6 |
| 0 | 1 | 0 | 0 | Unstructured |
| 0 | 1 | 0 | 1 | Ethernet |
| All other values are reserved. | | | | |

### 9.7.2 SSC mode

The purpose of the SSC mode information element is to indicate SSC mode.

The SSC mode information element is coded as shown in figure 9.7.2.1 and table 9.7.2.1.

The SSC mode is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| SSC mode IEI | | | | SSC mode value | | | | Octet 1 |

Figure 9.7.2.1: SSC mode information element

Table 9.7.2.1: SSC mode information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SSC mode value (octet 1, bit 1 to bit 4) | | | | |
|  | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 1 | SSC mode 1 |
| 0 | 0 | 1 | 0 | SSC mode 2 |
| 0 | 0 | 1 | 1 | SSC mode 3 |
| All other values are reserved. | | | | |

### 9.7.3 Extended protocol configuration options

See subclause 10.5.6.3A in 3GPP TS 24.008 [12].

### 9.7.4 SM PDU DN request container

The SM PDU DN request container contains a DN-specific identity of the UE in the network access identifier (NAI) format.

### 9.7.5 PDU address

The PDU address information element can assign to the UE an IPv4 address associated with a PDU session and can provide the UE with an interface identifier for the IPv6 link local address associated with a PDU session.

The PDU address information element is coded as shown in figure 9.7.5.1 and table 9.7.5.1.

The PDN address is a type 4 information element with length of 7 or 11 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PDU address IEI | | | | | | | | octet 1 |
| Length of PDU address contents | | | | | | | | octet 2 |
| 0  Spare | 0  Spare | 0  Spare | 0  Spare | PDU session type value | | | | octet 3 |
| PDU address information | | | | | | | | octet 4  octet x |

Figure 9.7.5.1: PDU address information element

Table 9.7.5.1: PDU address information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PDU session type value (octet 3) | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 1 | 0 | IPv4 |
| 0 | 0 | 1 | 1 | IPv6 |
|  | | | | |
| All other values are reserved. | | | | |
|  | | | | |
| PDU address information (octet 4 to x) | | | | |
|  | | | | |
| If the PDU session type value indicates IPv4, the PDU address information in octet 4 to octet 7 contains an IPv4 address. | | | | |
|  | | | | |
| If the PDU session type value indicates IPv6, the PDU address information in octet 4 to octet 11 contains an interface identifier for the IPv6 link local address. | | | | |

### 9.7.6 5GSM cause

The purpose of the 5GSM cause information element is to indicate the reason why a 5GSM request is rejected.

The 5GSM cause information element is coded as shown in figure 9.7.6.1 and table 9.7.6.1.

The 5GSM cause is a type 3 information element with 2 octets length.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GSM cause IEI | | | | | | | | octet 1 |
| Cause value | | | | | | | | octet 2 |

Figure 9.7.6.1: 5GSM cause information element

Table 9.7.6.1: 5GSM cause information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cause value (octet 2) | | | | | | | | | |
|  | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |  | User authentication failed |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |  | Request rejected, unspecified |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |  | Service option temporarily out of order |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |  | Regular deactivation |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |  | Reactivation requested |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |  | PDU session type IPv4 only allowed |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |  | PDU session type IPv6 only allowed |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |  | Semantically incorrect message |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |  | Invalid mandatory information |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |  | Message type non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |  | Message type not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |  | Information element non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |  | Conditional IE error |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |  | Message not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |  | Protocol error, unspecified |
|  |  |  |  |  |  |  |  |  |  |
| Any other value received by the UE shall be treated as 0010 0010, "service option temporarily out of order". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified". | | | | | | | | | |
|  | | | | | | | | | |

### 9.7.7 GPRS timer

See subclause 10.5.7.3 in 3GPP TS 24.008 [12].

### 9.7.8 UE SM capability

The purpose of the UE SM capability information element is to indicate UE capability related to the PDU session management.

The UE SM capability information element is coded as shown in figure 9.7.8.1 and table 9.7.8.1.

The UE SM capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| UE SM capability IEI | | | | | | | | | | | | | | | | octet 1 |
| Length of UE SM capability contents | | | | | | | | | | | | | | | | octet 2 |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | RQoS | | octet 3 |
| 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | octet 4\* -15\* |
| Spare | | | | | | | | | | | | | | | |

Figure 9.7.8.1: UE SM capability information element

Table 9.7.8.1: UE SM capability information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| UE SM capability value | | | | |
|  | | | | |
| RQoS(octet 3, bit 1)  This bit indicates the UE capability to support reflective QoS. | | | | |
| 0 |  |  |  | Reflective QoS not supported |
| 1 |  |  |  | Reflective QoS supported |
|  | | | | |
| All other bits in octet 3 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | |
|  | | | | |

## 9.8 Timers of 5GS session management

Timers of 5GS session management are shown in table 9.8.1 and table 9.8.2.

Table 9.8.1: Timers of 5GS session management – UE side

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  THE 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1) |
| --- | --- | --- | --- | --- | --- |
| T3580 | TBD | TBD | Transmission of PDU SESSION ESTABLISHMENT REQUEST message | PDU SESSION ESTABLISHMENT ACCEPT message received or  PDU SESSION ESTABLISHMENT REJECT message received | Retransmission of PDU SESSION ESTABLISHMENT REQUEST message |
| T3581 | TBD | TBD | Transmission of PDU SESSION MODIFICATION REQUEST message | PDU SESSION MODIFICATION COMMAND message with the same PTI is received or PDU SESSION MODIFICATION REJECT message received | Retransmission of PDU SESSION MODIFICATION REQUEST message |
| T3582 | TBD | TBD | Transmission of PDU SESSION RELEASE REQUEST message | PDU SESSION RELEASE COMMAND message with the same PTI is received or PDU SESSION RELEASE REJECT message received | Retransmission of PDU SESSION RELEASE REQUEST message |
| NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description. | | | | | |

Table 9.8.2: Timers of 5GS session management – SMF side

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  THE 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1) |
| --- | --- | --- | --- | --- | --- |
| T3590 | TBD | TBD | Transmission of PDU SESSION AUTHENTICATION REQUEST message | PDU SESSION AUTHENTICATION ACCEPT message received or PDU SESSION AUTHENTICATION REJECT message received | TBD |
| T3591 | TBD | TBD | Transmission of PDU SESSION MODIFICATION COMMAND message with any 5GSM cause but #39 | PDU SESSION MODIFICATION ACCEPT message received or PDU SESSION MODIFICATION REJECT message received | Retransmission of PDU SESSION MODIFICATION COMMAND message |
| Transmission of PDU SESSION MODIFICATION COMMAND message with 5GSM cause #39. | PDU SESSION RELEASE REQUEST message is received. | Retransmission of PDU SESSION MODIFICATION COMMAND message |
| T3591 | TBD | TBD | Transmission of PDU SESSION RELEASE COMMAND message | PDU SESSION RELEASE ACCEPT message received or  N1 SM delivery skipped indication received | Retransmission of PDU SESSION RELEASE COMMAND message |
| NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description. | | | | | |

## 9.9 Cause values for 5GS session management

### 9.9.1 Causes related to nature of request

Cause #26 – Insufficient resources

This 5GSM cause is used by the UE or by the network to indicate that the requested service cannot be provided due to insufficient resources.

Editor's note: Semantic of 5GSM cause value #26 includes semantic of 5GSM cause value #ss. If both 5GSM cause values are needed, semantics of 5GSM cause values have to be different.

Cause #27 – Missing or unknown DNN

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN because the DNN was not included although required or if the DNN could not be resolved.

Cause #29 – User authentication failed

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN due to a failed user authentication.

Cause #31 – Request rejected, unspecified

This 5GSM cause is used by the network or by the UE to indicate that the requested service or operation or the request for a resource was rejected due to unspecified reasons.

Cause #36 – Regular deactivation

This 5GSM cause is used to indicate a regular UE or network initiated release of PDU session resources.

Cause #39 – Reactivation requested

This 5GSM cause is used by the network to request a PDU session reactivation.

Cause #50 – PDU session type IPv4 only allowed

This 5GSM cause is used by the network to indicate that only PDU session type IPv4 is allowed for the requested IP connectivity.

Cause #51 – PDU session type IPv6 only allowed

This 5GSM cause is used by the network to indicate that only PDU session type IPv6 is allowed for the requested IP connectivity.

Cause #ss –Insufficient resources for specific slice and DNN;

This 5GSM cause is by the network to indicate that the requested service cannot be provided due to insufficient resources for specific slice and DNN.

Editor's note: Semantic of 5GSM cause value #26 includes semantic of 5GSM cause value #ss. If both 5GSM cause values are needed, semantics of 5GSM cause values have to be different.

### 9.9.2 Protocol errors (e.g., unknown message)

Cause #95 – Semantically incorrect message

This 5GSM cause is used to report receipt of a message with semantically incorrect contents.

Cause #96 – Invalid mandatory information

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message with a non-semantical mandatory IE error.

Cause #97 – Message type non-existent or not implemented

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message with a message type it does not recognize either because this is a message not defined, or defined but not implemented by the equipment sending this 5GSM cause.

Cause #98 – Message type not compatible with protocol state

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message not compatible with the protocol state.

Cause #99 – Information element non-existent or not implemented

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message which includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the 5GSM cause. However, the information element is not required to be present in the message in order for the equipment sending the 5GSM cause to process the message.

Cause #100 – Conditional IE error

This 5GSM cause indicates that the equipment sending this cause has received a message with conditional IE errors.

Cause #101 – Message not compatible with protocol state

This 5GSM cause indicates that a message has been received which is incompatible with the protocol state.

Cause #111 – Protocol error, unspecified

This 5GSM cause is used to report a protocol error event only when no other 5GSM cause in the protocol error class applies.

# 10 Access to the 5G core network via non-3GPP access networks

## 10.1 General

In this release, the 5GS supports untrusted non-3GPP accesses and does not support trusted non-3GPP accesses (see 3GPP TS 23.501 [9]).

Access to the 5GCN via non-3GPP access networks shall be supported by the non-3GPP interworking function (N3IWF). Between the UE and the N3IWF, an IPsec SA shall be established. During the IPsec SA establishment, the UE shall be authenticated by and registered to the 5G core network. The N3IWF interfaces to 5G core network via N2 and N3 reference points.

Editor's note: How to transmit a registration request message is FFS.

If the UE is authenticated by the 5G core network, secure NAS message exchange between the UE and the 5G core network shall be supported using the N1 reference point over the N3IWF.

When a UE isin 5GMM-CONNECTED mode over 3GPP access and in 5GMM-CONNECTED mode over non-3GPP access, two N1 NAS signalling connections shall exist for the UE.

A UE simultaneously registered to a single PLMN over 3GPP access and non-3GPP access, shall be served by a single AMF. In this case, when a UE is in 5GMM-CONNECTED mode over 3GPP access and in 5GMM-CONNECTED mode over non-3GPP access, two N1 NAS signalling connections shall exist for the AMF. Otherwise a UE registered to two different PLMNs over 3GPP and non-3GPP access networks, shall be served by two AMFs in two different PLMNs. In this case, when a UE is in 5GMM-CONNECTED mode over 3GPP access and in 5GMM-CONNECTED mode over non-3GPP access, single N1 NAS signalling connections shall exist for each of the AMFs.

During the IPsec SA establishment between the UE and the N3IWF, the N3IWF retrieves the NAI of the UE and the NAI is used to identify the UE in the 5G core network.

## 10.2 Protocol stack

### 10.2.1 Control plane protocol stacks



**Legend:**

- NG Application Protocol (NGAP): Application Layer Protocol between the N3IWF and the AMF.

Figure 10.2.1-1: Control plane protocol stack during signalling IPsec SA establishment

Editor's note: The definition of EAP-5G protocol is FFS.



**Legend:**

- NG Application Protocol (NGAP): Application Layer Protocol between the N3IWF and the AMF.

Figure 10.2.1-2: Control plane protocol stack when signalling IPSec child SA is established



**Legend:**

- NG Application Protocol (NGAP): Application Layer Protocol between the N3IWF and the AMF.

- IKEv2 is used to establish or delete the Child SA between UE and N3IWF for each PDU Session.

Figure 10.2.1-3: Control plane protocol stack for user plane establishment via N3IWF

### 10.2.2 User plane protocol stacks



**Legend:**

- PDU Layer: This layer corresponds to the PDU carried between the UE and the DN over the PDU Session. E.g. when the PDU Session type is IPV6, it corresponds to IPv6 packets; When the PDU Session Type is Ethernet, it corresponds to Ethernet frames.

- **GPRS Tunnelling Protocol for the user plane (GTP-U):** This protocol supports multiplexing traffic of different PDU Sessions (possibly corresponding to different PDU Session Types) by tunnelling user data over N3 (i.e. between N3IWF and the UPF) in the backbone network.

- The N3IWF relays the user data between per PDU Session IPsec tunnel over NWu and corresponding N3 tunnel.

Figure 10.2.2-1: User plane protocol stack via N3IWF

Editor's note: The value of protocol type in GRE header for unstructured PDU session type packets encapsulation is FFS.

## 10.3 NAS over non-3GPP access

### 10.3.1 General

From the UE's NAS perspective, the N1 interface is indistiguishable over the 3GPP access or the non-3GPP access in so much as the peer-to-peer signalling procedures and messages defined for UE NAS to 5GCN NAS over 3GPP access will be used for same purposes for UE NAS to 5GCN NAS over non-3GPP access. The 5GS NAS state machines of both 3GPP access or non-3GPP access should likewise have minimum differences. Maximum reuse should be the objective with any deviations or exceptions adopted if without such deviations or exceptions, signalling procedures and intended services will fail or malfunction, or service or archtitectural (or both) requirments cannot be met.

### 10.3.2 Mobility management over non-3GPP access

The mobility management procedures defined for N1 over 3GPP access will be re-used for N1 over non-3GPP access with the following exceptions:

- the status of the UE's non-3GPP 5GMM instance and the status of the UE's 3GPP 5GMM instance are independent and can be different.

- single registration mode and dual registration mode do not apply for 5GMM over non-3GPP access.

- there will be one instance of 5GMM for 3GPP access and one instance of 5GMM for non-3GPP access. The RPLMN over non-3GPP access can be different from the RPLMN over 3GPP access. The MCC of the RPLMN over 3GPP access and the MCC of the RPLMN over the non-3GPP access can also be different.

- as over non-3GPP access the 5GS operates one common registration area for an entire PLMN, list management of registration areas and resultant registration updating due to registration area change with the registered PLMN is not required. Periodic registration over a non-3GPP access shall not be applied. Registration updating at change of PLMN is still required.

- the 5GMM over non-3GPP access considers that the N1 NAS signalling connection is established when the lower layers indicate that the access stratum connection is established succcessfully.

Editor's note: Further exceptions are possible and are FFS.

- UE-initiated service request procedure via non-3GPP access is supported. Upon indication from the lower layers of non-3GPP access, that the access stratum conncetion is established between UE and network, the UE in 5GMM-REGISTERED state and in 5GMM-IDLE mode over non-3GPP access shall initiate the service request procedure via non-3GPP access to re-activate user plane connections for all PDU sessions associated with non-3GPP access, but not PDU sessions associated with 3GPP access.

- There is no network initiated service request procedure via non-3GPP Access.

### 10.3.3 Session management over non-3GPP access

The session management procedures defined for N1 over 3GPP access will be re-used for N1 over non-3GPP access.

Editor's note: Further exceptions are possible and are FFS.

## 10.4 Registration over non-3GPP access

### 10.4.1 General

The UE registers separately for 3GPP access and non-3GPP access, respectively.

An access stratum connection must exist before the UE can perform the registration procedure.

The UE shall not perform periodic registration update over a non-3GPP access.

The UE cannot be paged over a non-3GPP access.

### 10.4.2 Registration over non-3GPP access

Upon successful establishment of the N1 NAS signalling connection over non-3GPP access, the NAS performs the registration over non-3GPP access, to the selected PLMN by follow the registration procedure for initial registration given in subclause 8.5.2.1.2, except for the following:-

- the UE shall not request use of MICO mode.

When the UE is registered with a PLMN over a non-3GPP access, the AMF and the UE maintain:

- Registration state and state machine over non-3GPP access;

- Security context;

- 5G-GUTI;

- Registration area for non-3GPP access, which is associated with a fixed well-known N3GPP TAI; and

- Non-3GPP de-registration timer in the UE and non-3GPP implicit de-registration timer in the AMF.

Editor’s note: What information the N3IWF maintains for a registered UE is FFS.

### 10.4.3 Registration over non-3GPP access and 3GPP access

When the UE is registered with a PLMN over a non-3GPP access and over a 3GPP access, the AMF and the UE maintain:

- Separate registration states and separate instances of state machines over 3GPP access and non-3GPP access, respectively;

Editor’s note: The state machine over non-3GPP access is FFS.

- Separate registration areas; and

- Same security context and5G-GUTI, only if the UE is registered with the same PLMN over both accesses. Otherwise, the security contexts and the 5G-GUTI shall be separate.

Editor’s note: To what extent the security context is the same when the UE is registered with the same PLMN over both accesses is FFS.

When the UE initiates registration over a non-3GPP access to a PLMN for which it has a valid 5G-GUTI, the UE shall use this 5G-GUTI during the registration. When the UE is currently registered with the same PLMN over a 3GPP access, the 5G-GUTI is considered as valid.

When the UE wishes to initiate registration over both 3GPP access and non-3GPP access in the same PLMN (e.g. the 3GPP access and the selected N3IWF are located in the same PLMN), the UE:

- in 5GMM-REGISTERED-INITIATED over 3GPP access shall not initiate registration over non-3GPP access; or

- in 5GMM-REGISTERED-INITIATED over non-3GPP access shall not initiate registration over 3GPP access.

NOTE: To which access (i.e. 3GPP access or non-3GPP access) the UE initiates registration first is up to UE implementation).

### 10.4.4 De-registration over non-3GPP access

The UE and the AMF may initiate de-registration for a non-3GPP access by:

- Initiating a de-registration request over a non-3GPP access when the UE is registered over non-3GPP access;

- Initiating a de-registration request over a 3GPP access when the UE is registered in the same PLMN over both accesses; or

- Initiating a de-registration request over a 3GPP access or non-3GPP access with an indication that it applies to all accesses when the UE is registered in the same PLMN over both accesses.

When the UE has no PDU sessions over non-3GPP access, or the UE moves all the PDU sessions over a non-3GPP access to a 3GPP access, the UE and the AMF need not initiate de-registration over the non-3GPP access.

The AMF shall provide the UE with a non-3GPP de-registration timer Tx.

Once the UE enters the 5GMM-IDLE over non-3GPP access, the UE starts a non-3GPP de-registraion timer Tx. When the timer Tx expires, the UE shall perform de-registration for non-3GPP access and enter the state 5GMM-DEREGISTERED over non-3GPP access.

Once the AMF enters the 5GMM-IDLE, the AMF starts a non-3GPP implicit de-registration timer Ty. When the timer Ty expires, the AMF shall perform de-registration for non-3GPP access and enter the state 5GMM-DEREGISTERED over non-3GPP access.

The non-3GPP implicit de-registration timer Ty shall be longer than the non-3GPP de-registration timer Tx.

Editor’s note: The non-3GPP de-registration timer Tx and the non-3GPP implicit de-registration timer Ty are FFS.

## 10.5 Selection of N3IWF

The ePDG selection procedure specified in the 3GPP TS 24.302 [16] is reused as mechanism for N3IWF selection except for the following differences:

1) The UE performs N3IWF selection based on the information configured by the HPLMN in the UE and based on the UE's knowledge of the PLMN it is attached to.

Editor's note: The format and contents of N3IWF configuration information are FFS.

2) The input to the DNS query to retrive IP address(es) of the N3IWF is a N3IWF FQDN (N3IWF fully qualified domain name). A N3IWF FQDN is either provisioned by the home operator or constructed by UE in either the operator identifier FQDN format or the tracking area identity FQDN format. Location area identity FQDN format is not used.

Editor's note: The detailed format of the N3IWF FQDN format is FFS and is to be specified in 3GPP TS 23.003 [5].

## 10.6 Procedures between UE and N3IWF

Editor's note: This subclause specifies the IKEv2 procedures between the UE and N3IWF due to UE registration/de-registration, PDU session setup, PDU session modification and PDU session release.

### 10.7.1 IKE SA creation procedure for UE registration via untrusted non-3GPP access

#### 10.7.1.1 General

The purpose of this procedure is to establish a secure connection between the UE and N3IWF, which is used to securely exchange NAS signalling messages between the UE and AMF, via N3IWF.

The IKE SA and first child SA are created between the UE and N3IWF after the IKE initial exchanges are completed, i.e. after the IKE\_SA\_INIT exchange and after the IKE\_AUTH exchange (see IETF RFC 7296 [36]).

During UE registration the first child SA established is used to transfer NAS signalling traffic. The child SA that is used to convey NAS signalling traffic is termed as the signalling IPsec SA. Additional child SAs (user plane IPsec SAs) can be established between the UE and N3IWF to transfer user-plane traffic (see subclause 10.7.2A).

The signalling IPsec SA and IKE SA are established between the UE and N3IWF by executing the procedure in subclause 10.7.1.2. A vendor-specific EAP method (EAP-5G) is used to encapsulate NAS messages between the UE and the N3IWF. The EAP-5G packets utilize the "Expanded" EAP type and the existing 3GPP Vendor-Id registered with IANA under the SMI Private Enterprise Code registry (i.e. 10415). The EAP-5G method is utilized only for encapsulating NAS messages (not for authentication). The EAP-5G procedure is described in subclause 10.7.1.3.

#### 10.7.1.2 IKE SA and signalling IPsec SA establishment procedure

When the UE is required to initiate UE registration via a non-3GPP access and has selected an N3IWF (see 3GPP TS 23.502 [10]) the UE starts to establish an IKE SA and first child SA (signalling IPsec SA). The UE shall initiate an IKE\_SA\_INIT exchange followed by an IKE\_AUTH exchange as specified in IETF RFC 7296 [36]. The UE shall indicate the intention to use EAP by not including the AUTH payload in the initial IKE\_AUTH request as specified in IETF RFC 7296 [36].

Upon reception of the IKE\_AUTH request without AUTH payload, the N3IWF shall respond with an IKE\_AUTH response with an indication to start an EAP-5G session in order to convery the initial NAS messages. The EAP-5G procedure is described in subclause 10.7.1.3.

When the EAP-5G session is completed the UE receives from the N3IWF an IKE\_AUTH response with an EAP-Success packet. The UE completes the IKE SA and signalling IPsec SA (first child SA) establishment procedure by initiating an IKE\_AUTH exchange including an AUTH payload computed based on the N3IWF key as described in 3GPP TS 33.501 [24].

This completes the establishment of the IKE SA and signalling IPsec SA between the UE and N3IWF. The UE and N3IWF shall send further NAS messages within the signalling IPsec SA (first child SA) (see example in figure 10.7.1.2.1).

Editor’s note: It is FFS how the signalling IPsec SA is handled in case of rekeying of the IKE SA.



Figure 10.7.1.2.1: IKE SA and first child SA establishment procedure for UE registration over non-3GPP access

#### 10.7.1.3 EAP-5G procedure for registration over non-3GPP access

The UE and the N3IWF exchange EAP-5G messages within IKE\_AUTH request and IKE\_AUTH response messages.The N3IWF on reception of an IKE\_AUTH request with no AUTH payload shall start an EAP-5G session by sending an EAP-Request/5G-Start message.

The UE acknowledges start of the EAP-5G session by sending an EAP-Response/5G-NAS message. The 5G-NAS packet shall include:

- a NAS-PDU attribute that contains a NAS Registration Request message; and

- an AN-params attribute that contains access network parameters, such as S-NSSAI, 5G-GUTI, etc. (see 3GPP TS 23.502 [10]).Further NAS messages between the UE and the AMF, via the N3IWF, that are required to complete the registration procedure shall be inserted in NAS-PDU attribute of an 5G-NAS packet within EAP-Request/EAP-Response messages. If the authentication of the UE completes successfully the UE receives the SECURITY MODE COMMAND request from the AMF as described in subclause 8.5.1.1.2.1. The UE creates a NAS security context and an N3IWF key as described in 3GPP TS 33.501 [24] and request the completion of the EAP-5G session. The UE terminates the EAP-5G session by sending an EAP-Request/5G-Complete message.

Editor’s note: The message format of the EAP-Request/5G-Start, EAP-Request/5G-NAS, EAP-Response/5G-NAS and EAP-Request/5G-Complete messages is FFS.

When the N3IWF receives the EAP-Request/5G-Complete message and the N3IWF key from AMF, the N3IWF shall respond with an EAP-Success packet. The UE and N3IWF proceed to establish an IKE SA and signalling IPsec SA as described in subclause 10.7.1.2.

An example of an EAP-5G session is shown in figure 10.7.1.3.1.



Figure 10.7.1.3.1: EAP-5G session for UE registration over non-3GPP access

#### 10.7.1.4 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE for this specific procedure (not specified in IETF RFC 7296 [36]) are FFS.

#### 10.7.1.5 Abnormal cases in the N3IWF

Editor's note: The abnormal cases in the N3IWF for this specific procedure (not specified in IETF RFC 7296 [36]) are FFS.

### 10.7.2 User plane Ipse SA creation procedure for UE-requested PDU session establishment

Editor's note: This subclause specifies user plane IPsec (additional child SA) creation procedure for PDU session setup via untrusted non-3GPP access.

#### 10.7.2.1 General

The purpose of the Child SA creation procedure during the UE-requested PDU session establishment is to establish a Child SA associating to the QoS profiles of the PDU session. This procedure shall be initiated by the N3IWF.

One Child SA can be accoiated with one or more QoS profiles of the PDU session. The N3IWF will determine the number of Child SAs to establish and the QoS profiles associated with each Child SA based on local policies, configuration and the QoS profiles received from the network.

#### 10.7.2.2 Child SA creation procedure initiation

The N3IWF shall initiate the Child SA creation procedure by sending a CREATE\_CHILD\_SA request message to the UE as specified in IETF RFC 7296 [36].

The CREATE\_CHILD\_SA request message shall include:

- USE\_TRANSPORT\_MODE notification; and

- 5G\_QOS\_INFO Notify payload which contains:

- QoS profile(s); and

- PDU session ID.

The CREATE\_CHILD\_SA request message may also include:

- a DSCP value.

Editor's note: The definition of 5G\_QOS\_INFO Notify payload is FFS.

Editor's note: Whether 5G\_QOS\_INFO Notify can contain QFI instead of QoS profile need to be FFS.

Editor's note: How to handle the packet in transport mode is FFS.

#### 10.7.2.3 Child SA creation procedure accepted by the UE

If the UE accepts the CREATE\_CHILD\_SA request, the UE shall send the CREATE\_CHILD\_SA response as specified in IETF RFC 7296 [36].

The CREATE\_CHILD\_SA request message shall include:

- USE\_TRANSPORT\_MODE notification.

Any IKEv2 Notify payload indicating an error shall not be included in the CREATE\_CHILD\_SA response.

#### 10.7.2.4 Child SA creation procedure not accepted by the UE

If the UE does not accept the Child SA creation, the UE shall send a send the CREATE\_CHILD\_SA response message with the corresponding Notify payload of error type as specified in IETF RFC 7296 [36].

Editor's note: Whether 5G specific private Notify Message - Error Types needs to be defined is FFS.

Editor's note: The behaviour of N3IWF is FFS upon receipt of the the CREATE\_CHILD\_SA response message indicating failure of the procedure.

#### 10.7.2.5 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE for this specific procedure (not specified in IETF RFC 7296 [36]) are FFS.

#### 10.7.2.6 Abnormal cases in the N3IWF

Editor's note: The abnormal cases in the N3IWF for this specific procedure (not specified in IETF RFC 7296 [36]) are FFS.

### 10.7.3 Child SA change procedure for PDU session modification

Editor's note: This subclause specifies child SA change procedure for PDU session modification via untrusted non-3GPP access.

### 10.7.4 Child SA deletion procedure for PDU session release

Editor's note: This subclause specifies child SA deletion procedure for PDU session release via untrusted non-3GPP access.

#### 10.7.4.1 General

The purpose of the Child SA deletion procedure for PDU session release is to delete all the Child SAs associated with the PDU session. This procedure shall be initiated by the N3IWF.

#### 10.7.4.2 Child SA deletion procedure initiation

The N3IWF shall initiate the Child SA deletion procedure by sending an INFORMATIONAL request message including a Delete payload to the UE as specified in IETF RFC 7296 [36]. The Delete payload shall include:

- the Protocol ID set to "3" for ESP; and

- all the N3IWF's ESP Security Parameter Indexe(s) associated to the released PDU session.

#### 10.7.4.3 Child SA deletion procedure accepted by the UE

If the UE accepts the INFORMATIONAL request message for deletion of the Child SAs, the UE shall send the INFORMATIONAL response to the N3IWF including the Delete payload received in the corresponding INFORMATIONAL request message as specified in IETF RFC 7296 [36].

Any IKEv2 Notify payload indicating an error shall not be included in the INFORMATIONAL response.

Editor's note: The possible Notify messages for status type in the INFORMATIONAL response are FFS.

#### 10.7.4.5 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE for this specific procedure (not specified in IETF RFC 7296 [36]) are FFS.

#### 10.7.4.6 Abnormal cases in the N3IWF

Editor's note: The abnormal cases in the N3IWF for this specific procedure (not specified in IETF RFC 7296 [36]) are FFS.

### 10.7.5 IKE SA deletion for de-registration via untrusted non-3GPP access

Editor's note: This subclause specifies IKE SA deletion procedure for de-registration via untrusted non-3GPP access.

#### 10.7.5.1 General

The purpose of the IKE SA deletion procedure for de-registration via untrusted non-3GPP access is to delete the IKE SA of the UE. This procedure shall be initiated by the N3IWF.

#### 10.7.5.2 IKE SA deletion procedure initiation

The N3IWF shall initiate the IKE SA deletion procedure by sending an INFORMATIONAL request message including a Delete payload to the UE as specified in IETF RFC 7296 [36].

The Protocol ID shall be set to "1" and no subsequent SPI in the Delete payload. This indicates that the IKE security association, and all IPsec ESP security associations that were negotiated within it between N3IWF and UE shall be deleted.

#### 10.7.5.3 IKE SA deletion procedure accepted by the UE

If the UE accepts the INFORMATIONAL request message for deletion of the IKE SA, the UE shall send an empty INFORMATIONAL response to the N3IWF as specified in IETF RFC 7296 [36].

#### 10.7.5.5 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE for this specific procedure (not specified in IETF RFC 7296 [36]) are FFS.

#### 10.7.5.6 Abnormal cases in the N3IWF

Editor's note: The abnormal cases in the N3IWF for this specific procedure (not specified in IETF RFC 7296 [36]) are FFS.

## 10.8 IKEv2 payload extensions

Editor's note: This subclause defines the coding of IKEv2 payload for untrusted non-3GPP access to 5GCN.

# 11 Interworking with E-UTRAN connected to EPC

## 11.1 General

In order to interwork with E-UTRAN connected to EPC, the UE supporting both S1 mode and N1 mode can operate in single-registration mode or dual-registration mode (see 3GPP TS 23.501 [9]). Support of single-registration mode is mandatory for UEs supporting both S1 mode and N1 mode.

During the attach procedure or initial registration procedure, the mode for intersystem change is selected if the UE supports both S1 mode and N1 mode, and the network supports intersystem change. See 3GPP TS 24.301 [15] and subclause 8.4.2.1 for further details.

## 11.2 Single-registration mode

### 11.2.1 General

If both 5GMM and EMM are enabled, a UE, which is capable of N1 mode and S1 mode in the single-registration mode, shall maintain one common registration for 5GMM and EMM.

### 11.2.2 Coordination between 5GMM and EMM with N26 interface

A UE that is not registered shall be in state EMM-DEREGISTERED and in state 5GMM-DEREGISTERED.

In N1 mode, upon successful registration procedure, the UE operating in the single-registration mode shall enter substates 5GMM-REGISTERED.NORMAL-SERVICE and EMM-REGISTERED.NO-CELL-AVAILABLE.

At intersystem change from S1 mode to N1 mode in 5GMM-IDLE mode, the UE shall stay in state 5GMM-REGISTERED.NORMAL-SERVICE and state EMM-REGISTERED.NO-CELL-AVAILABLE and initiate a mobility registration update procedure.

In S1 mode, upon successful attach or tracking area updating procedure, the UE operating in the single-registration mode shall enter substates 5GMM-REGISTERED.NO-CELL-AVAILABLE and EMM-REGISTERED.NOMRAL-SERVICE.

At intersystem change from N1 mode to S1 modein EMM-IDLE mode when no PDU session context for which interworking to EPS is supported (specified in subclause 11.2.4) is active, EMM-REGISTERED without PDN connection is not supported by the UE or the MME, the UE shall move to state 5GMM-DEREGISTERED and state EMM-DEREGISTERED and then initiate the attach procedure. If EMM-REGISTERED without PDN connection is supported by the UE and the MME, the UE shall move to state EMM-REGISTERED.NORMAL-SERVICE and state 5GMM-REGISTERED.NO-CELL-AVAILABLE and initiate a tracking area updating procedure.

At intersystem change from N1 mode to S1 mode in EMM-IDLE mode when at least one PDU session context for which interworking to EPS is supported (specified in subclause 11.2.4) is active, the UE shall move to state EMM-REGISTERED.NORMAL-SERVICE and state 5GMM-REGISTERED.NO-CELL-AVAILABLE and initiate a tracking area updating procedure.

Editor's note: It is FFS whether and how the intersystem change for UEs operating in the single-registration mode in a network supporting N26 interface is impacted due to PDU session context for which interworking to EPS is not supported.

### 11.2.3 Coordination between 5GMM and EMM without N26 interface

A UE that is not registered shall be in state EMM-DEREGISTERED and in state 5GMM-DEREGISTERED.

In N1 mode, upon successful registration procedure, the UE operating in the single-registration mode shall enter substates 5GMM-REGISTERED.NORMAL-SERVICE and EMM-REGISTERED.NO-CELL-AVAILABLE.

In S1 mode, upon successful attach or tracking area updating procedure, the UE operating in the single-registration mode shall enter substates 5GMM-REGISTERED.NO-CELL-AVAILABLE and EMM-REGISTERED.NOMRAL-SERVICE.

At intersystem change from N1 mode to S1 mode in EMM-IDLE mode when at least one PDU session context is active, the UE shall stay in state EMM-REGISTERED.NORMAL-SERVICE and state 5GMM-REGISTERED.NO-CELL-AVAILABLE and then initiate the attach procedure with request type set to "handover" in the PDN CONNECTIVITY REQUEST message if the UE supports the attach procedure with request type set to "handover". After succesfully attached in S1 mode, the UE shall transfer all other active PDU sessions from N1 mode to S1 mode by initiating the PDN connectivity procedure with request type set to "handover" in the PDN CONNECTIVITY REQUEST message

Editor's note: If the UE does not support the attach procedure with request type set to "handover", the UE behaviour is FFS.

Editor's note: The paragraph above only implements one option (the first bullet, i.e. the attach procedure) for mobility from 5GC to EPC as specified in subclause 5.17.2.3.2 of 3GPP TS 23.501 [9]. This implies neither that implementing the other option (the second bullet, i.e. the TAU procedure) is prohibited, nor that the implemented option is preferred by CT1. Zero, one, or two of the two options can be implemented for the normative work.

Editor’s note: If there is no PDU session context active in N1 mode, the UE behaviour is FFS.

At intersystem change from S1 mode to N1 mode in 5GMM-IDLE mode, the UE shall stay in state EMM-REGISTERED.NO-CELL-AVAILABLE and state 5GMM- REGISTERED.NORMAL-SERVICE and then initiate the mobility registration update procedure. After succesfully registered in N1 mode and if the handover PDU session from EPC is supported by the AMF, the UE shall transfer all active PDN connections from S1 mode to N1 mode by initiating the PDU session establishment procedure with request type set to "existing PDU session". If the handover PDU session from EPC is not supported by the AMF, the UE shall re-establish PDU sessions corresponding to all active PDN connections by initiating the PDU session establishment procedure with request type set to "initial request".

### 11.2.4 Coordination between 5GSM and ESM

Interworking to EPS is supported for a PDU session context, if the context includes one or more QoS rules each of which contains associated EPS bearer identity, mapped EPS QoS parameters, mapped extended EPS QoS parameters, and optionally a mapped traffic flow template. The QoS rule for the default QoS flow does not need to contain a mapped traffic flow template. See coding of the QoS rules in subclause 12.4.2.1.

Upon inter-system change from N1 mode to S1 mode in EMM-IDLE mode, the UE uses the parameters from each PDU session context for which interworking to EPS is supported to create corresponding default EPS bearer context and optinally dedicated EPS bearer context(s) as follows:

- the PDU session type of the PDU session context shall be mapped to the PDN type of the default EPS bearer context as follows:

1) the PDN type shall be set to "non-IP" if the PDU session type is "Ethernet" or "Unstructured";

2) the PDN type shall be set to "IPv4" if the PDU session type is "IPv4"; and

3) the PDN type shall be set to "IPv6" if the PDU session type is "IPv6";

- the PDU address of the PDU session context shall be mapped to the PDN address of the default EPS bearer context;

- the DNN of the PDU session shall be mapped to the APN of the default EPS bearer context;

- for each PDU session context of a PDU session in state PDU SESSION ACTIVE or PDU SESSION MODIFICATION PENDING the UE shall set the state of the mapped default EPS bearer context to BEARER CONTEXT ACTIVE; and

- for any other PDU session context of a PDU session the UE shall set the state of the mapped default EPS bearer context to BEARER CONTEXT INACTIVE.

Additionally, the UE shall set for each QoS flow in the PDU session context:

1) the EPS bearer identity to the EPS bearer identity received in the parameters of a QoS rule for the QoS flow;

2) the EPS QoS parameters to the mapped EPS QoS parameters received in the parameters of a QoS rule for the QoS flow;

3) the extended EPS QoS parameters to the mapped extended EPS QoS parameters received in the parameters of a QoS rule for the QoS flow; and

4) the traffic flow template to the mapped traffic flow template received in the parameters of a QoS rule for the QoS flow.

Interworking to 5GS is supported for a PDN connection, if the corresponding default EPS bearer context includes a PDU session identity, session AMBR and one or more QoS rules (see annex D.1).

Upon inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode, the UE uses the parameters from the default EPS bearer context of each PDN connection for which interworking to 5GS is supported to create a corresponding PDU session context as follows:

- the PDN type of the default EPS bearer context optionally associated with locally available information associated with the PDN connection (either "Ethernet" or "Unstructured") shall be mapped to the PDU session type of the PDU session context as follows:

1) if the PDN type is "non-IP", the PDU session type is set to the locally available information associated with the PDN connection (either "Ethernet" or "Unstructured"), if available;

2) if the PDN type is "IPv4" the PDU session type is set to "IPv4"; and

3) if the PDN type is "IPv6", the PDU session type is set to "IPv6";

- the PDN address of the default EPS bearer context shall be mapped to PDU address of the PDU session context;

- the APN of the default EPS bearer context shall be mapped to the DNN of the PDU session context;

- for each default EPS bearer context in state BEARER CONTEXT ACTIVE or BEARER CONTEXT MODIFY PENDING the UE shall set the state of the mapped PDU session context to PDU SESSION ACTIVE; and

- for any other default EPS bearer context the UE shall set the state of the mapped PDU session context to PDU SESSION INACTIVE.

Additionally, the UE shall set:

- the PDU session identity of the PDU session context to the PDU session identity included by the UE in the protocol configuration options IE or extended protocol configuration options IE in the PDN CONNECTIVITY REQUEST message; and

- the session-AMBR of the PDU session context to the session-AMBR included by the network in the protocol configuration options IE or extended protrocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER REQUEST message; and

for each EPS bearer context of the PDN connection, the UE shall create QoS flow(s) each of which is associated with the QoS rule(s) received in the protocol configuration options IE or extended protrocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER REQUEST message, ACTIVATE DEDICATED EPS BEARER REQUEST message, and/or MODIFY EPS BEARER REQUEST message.

## 11.3 Dual-registration mode

If both 5GMM and EMM are enabled, a UE, which is capable of N1 mode and S1 mode in the dual-registration mode, shall maintain independent registrations for 5GMM and EMM independently and coordination between 5GMM and EMM is not needed. A UE operating in the dual-registration mode may register to N1 mode only, S1 mode only, or to both N1 mode and S1 mode.

When no PDU session context is active and the UE has not registered to S1 mode yet, the UE may initiate the attach procedure if EMM-REGISTERED without PDN connection is not supported by the MME. If EMM-REGISTERED without PDN connection is supported by the MME, the UE may initiate either the attach procedure without PDN connection establishment or the attach procedure.

When at least one PDU session context is active and the UE has not registered to S1 mode yet, the UE may initiate the attach procedure. If necessary, the UE may transfer an active PDU session from N1 mode to S1 mode by initiating the attach procedure with request type set to "handover" in the PDN CONNECTIVITY REQUEST message. After succesfully attached in S1 mode, if necessary, the UE may transfer other active PDU sessions from N1 mode to S1 mode by initiating the PDN connectivity procedure with request type set to "handover" in the PDN CONNECTIVITY REQUEST message.

NOTE 1: It is up to UE implementation to determine which active PDU session is transferred from N1 mode to S1 mode.

When the UE has not registered to N1 mode, the UE may initiate the initial registration procedure. After succesfully registered in N1 mode, if necessary, the UE may transfer one or more active PDN connections from S1 mode to N1 mode by initiating the PDU session establishment procedure with request type set to "existing PDU session".

NOTE 2: It is up to UE implementation to determine which active PDN connection is transferred from S1 mode to N1 mode.

If both the UE and the MME support EMM-REGISTERED without PDN connection, the UE that transferred all PDN connections to the 5GS, may stay in state EMM-REGISTERED. Otherwise, the UE shall enter state EMM-DEREGISTERED upon transferring all PDN connection to the 5GS.

## 11.4 Core Network selection

If the UE is capable of both N1 mode and S1 mode, when the UE needs to use one or more functionalities not supported in 5GS but supported in EPS, the UE may disable the N1 mode radio capabilities (see subclause 8.2.6).

If the UE is capable of both N1 mode and S1 mode and lower layers provide an indication that the current E-UTRA cell is connected to both EPC and 5GCN, the UE shall select a core network type (EPC or 5GCN) and provide the selected core network type information to the lower layer during the initial registration procedure.

Editor's note: The indication of the current E-UTRA cell is connected to both 5GCN and EPC provided by lower layers need to be defined by RAN WGs.

Editor's note: It is FFS how the UE selects a core network type, e.g. based on UE local configuration on core network preference.

# 12 5G System core network impact on services, network functions and capabilities

## 12.1 Specific services

### 12.1.1 Public warning system

#### 12.1.1.1 General

##### 12.1.1.1.1 Service Requirements

5G PWS will have the same functionality as E-UTRAN PWS for 4G.

##### 12.1.1.1.2 Technology Framework Assumptions

PWS in LTE is realized using cell broadcast technology (see 3GPP TS 22.268 [4] and 3GPP TS 23.041 [6]). It is expected that same CBS technology framework is used for technical realization of PWS in 5GS.

#### 12.1.1.2 Architecture alternative 1: Supporting PWS in 5GS via Service based Interface

##### 12.1.1.2.1 Overview

In this architecture alternative, the AMF interfaces with CBCF and NG-RAN to enable PWS service with the interface between AMF and CBCF implemented as service based interface. CBCF uses AMF communication services to forward warning messages to NG-RAN and to subscribe to receive warning delivery related notifications.

##### 12.1.1.2.2 Architecture description

###### 12.1.1.2.2.1 PWS architecture

Figure 12.1.1.2.2.1.1 shows the basic network structure of PWS architecture in 5GS.



Figure 12.1.1.2.2.1.1: PWS architecture

The cell broadcast centre function (CBCF) is part of the core network and connected to the AMF via the Ncbcf service based interface.

Reference point to support PWS architecture:

**N2:** Reference point between the NG-RAN and the AMF.

NOTE: NG-RAN can be NR based or E-UTRA based (See 3GPP TS 23.501 [9] and 3GPP TS 38.413 [28]).

Service based interface to support PWS in 5GS

**Namf:** Service-based interface exhibited by AMF.

**Ncbcf:** Service-based interface exhibited by CBCF.

The CBE and the interface between CBE and CBCF are out of scope of 3GPP specifications.

###### 12.1.1.2.2.2 AMF functionality

The AMF may interface to one CBCF or multiple CBCFs. An AMF may interface to several NG-RANs (i.e. combinations of gNodeBs and/or eNodeBs).

The AMF is responsible for:

1) Interpretation of commands from the CBC;

2) Storage of messages from the CBC;

3) Routing the WRITE-REPLACE-WARNING-REQUEST message to the appropriate NG-RAN entities upon receiving warning message request from CBCF;

4) Routing the STOP-WARNING-REQUEST message to the appropriate NG-RAN entities upon receiving STOP-WARNING-REQUEST message from CBCF;

5) Warning message delivery success or failure notification

- Providing to the CBCF acknowledgement of successful execution of commands received from the CBCF;

- Reporting to the CBCF failure when a command received from the CBCF is not understood or cannot be executed; and

- Reporting to the CBCF the Broadcast completed area list, the Broadcast cancelled area list; and

6) Forwarding PWS RESTART-INDICATION message and the PWS FAILURE-INDICATION message received from NG-RAN entities to all CBCFs that the AMF interfaces with.

###### 12.1.1.2.2.3 CBCF functionality

CBCF is a network function in the 5G core network. The CBCF may be connected to several AMFs. The CBCF may be connected to several CBEs. The CBCF shall be responsible for the management of CBS messages as specified in subclause 5 of 3GPP TS 23.041 [16].

CBCF supports service based interface. CBCF uses AMF communication services to forward warning messages to NG-RAN and to subscribe to receive warning delivery related notifications.

###### 12.1.1.2.2.4 NG-RAN functionality

The NG-RAN may interface to multiple AMFs.

The NG-RAN is responsible for:

1) Upon receipt of the WRITE-REPLACE-WARNING-REQUEST message, prioritise its resources and broadcast the warning message to the warning areas indicated in the requested Warning area list;

2) Upon receipt of the KILL-REQUEST message, stop broadcasting the warning message within for that area indicated in the requested Warning area list and discard the warning message;

3) Inform the AMF that PWS information for some or all cells of the NG-RAN are available for reloading from the CBCF if needed by sending a PWS RESTART-INDICATION message to the AMF; and

4) Inform the AMF that ongoing PWS operation for one or more cells of the NG-RAN has failed by sending a PWS FAILURE-INDICATION message to the AMF.

##### 12.1.1.2.3 Protocol Stack Overview



**Legend:**

- NG application protocol information for cell broadcast (NG-AP-CB): Subset of NG-AP information that the AMF relays between the AN and the CBCF. NG-AP-CB corresponds to a subset of NG-AP defined in 3GPP TS 38.413 [28].

- NG application protocol (NGAP): Application layer protocol between the NG-RAN entity (eNodeB and/or gNodeB) and the AMF. The NGAP protocol is defined in 3GPP TS 38.413 [28].

- SCTP for the control plane (SCTP): This protocol guarantees delivery of signalling messages between AMF and NG-RAN (N2) and between CBCF and AMF (NBc). SCTP is defined in IETF RFC 4960 [34].

Figure 12.1.1.2.3.1: CBCF - NG-RAN

##### 12.1.1.2.4 CBCF-AMF interface operations

The CBCF network function uses Namf\_Communication service to communicate with the NG-RAN for sending warning request primitives and receiving warning message delivery indication or restart/failure indication primitives.

The requirements are described by primitives.

The following table shows primitives that are expected to be supported using AMF via Namf interface:

Table 12.1.1.2.4.1: CBC-AMF primitives via Namf interface

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Originator** | **Type** | **Namf** **Service operations** |
| WRITE-REPLACE-WARNING-REQUEST | CBCF | Request/Indication | Namf\_Communication\_N2MessageTrigger  Namf\_Communication\_N2InfoSubscribe |
| WRITE-REPLACE-WARNING-CONFIRM | AMF | Response/Confirm | Namf\_Communication\_N2InfoNotify |
| STOP-WARNING-REQUEST | CBCF | Request/Indication | Namf\_Communication\_N2MessageTrigger  Namf\_Communication\_N2InfoSubscribe |
| STOP-WARNING-CONFIRM | AMF | Response/Confirm | Namf\_Communication\_N2InfoNotify |
| WRITE-REPLACE-WARNING-INDICATION | AMF | Request/Indication | Namf\_Communication\_N2InfoSubscribe  Namf\_Communication\_N2InfoNotify |
| STOP-WARNING-INDICATION | AMF | Request/Indication | Namf\_Communication\_N2InfoSubscribe  Namf\_Communication\_N2InfoNotify |
| RESTART-INDICATION-NG-RAN | AMF | Request/Indication | Namf\_Communication\_N2InfoSubscribe  Namf\_Communication\_N2InfoNotify |
| FAILURE-INDICATION-NG-RAN | AMF | Request/Indication | Namf\_Communication\_N2InfoSubscribe  Namf\_Communication\_N2InfoNotify |

#### 12.1.1.3 Architecture alternative 2: Supporting PWS in 5GS via SBc like Interface

##### 12.1.1.3.1 Overview

In this architecture alternative, the AMF interfaces with CBC and NG-RAN to enable PWS service by using SBc-like protocol interface (see 3GPP TS 29.168 [22]) referred to as "NBc" interface between AMF and CBC. Same protocol stack and procedures for SBc interface will be re-used for NBc interface.

##### 12.1.1.3.2 Architecture description

###### 12.1.1.3.2.1 PWS architecture

Figure 12.1.1.3.2.1.1 shows the basic network structure of PWS architecture in 5GS.



Figure 12.1.1.3.2.1.1: PWS architecture

The cell broadcast centre function (CBC) is part of the core network and connected to the AMF via the NBc interface.

Reference point to support PWS architecture:

**N2:** Reference point between the NG-RAN and the AMF.

**NBc:** Reference point between the AMF and the CBC.

NOTE: NG-RAN can be NR based or E-UTRA based (See 3GPP TS 23.501 [9] and 3GPP TS 38.413 [28]).

The CBE and the interface between CBE and CBC are out of scope of 3GPP specifications.

###### 12.1.1.3.2.2 AMF functionality

The AMF may interface to one CBC or multiple CBCs (i.e. the AMF is allowed to have SCTP transport associations established with one or multiple CBCs). An AMF may interface to several NG-RANs (i.e. combinations of gNodeBs and/or eNodeBs).

The AMF is responsible for:

1) Interpretation of commands from the CBC;

2) Storage of messages from the CBC;

3) Routing the WRITE-REPLACE-WARNING-REQUEST message to the appropriate NG-RAN entities upon receiving warning message request from CBC;

4) Routing the STOP-WARNING-REQUEST message to the appropriate NG-RAN entities upon receiving STOP-WARNING-REQUEST message from CBC;

5) Warning message delivery success or failure notification

- Providing to the CBC acknowledgement of successful execution of commands received from the CBC;

- Reporting to the CBC failure when a command received from the CBC is not understood or cannot be executed; and

- Reporting to the CBC the Broadcast completed area list, the Broadcast cancelled area list; and

6) Forwarding PWS RESTART-INDICATION and the PWS FAILURE-INDICATION received from NG-RAN entities to all CBCs that the AMF interfaces with.

###### 12.1.1.3.2.3 CBC functionality

CBC is integrated as a node in the 5G core network. The CBC may be connected to several AMFs. The CBC may be connected to several CBEs. The CBC shall be responsible for the management of CBS messages as specified in subclause 5 of 3GPP TS 23.041 [16].

CBC reuses existing SBc protocol interface for warning message delivery between AMF and CBC.

###### 12.1.1.3.2.4 NG-RAN functionality

The NG-RAN may interface to multiple AMFs.

The NG-RAN is responsible for:

1) Upon receipt of the WRITE-REPLACE WARNING REQUEST message, prioritise its resources and broadcast the warning message to the warning areas indicated in the requested Warning area list;

2) Upon receipt of the KILL REQUEST message, stop broadcasting the warning message within for that area indicated in the requested Warning area list and discard the warning message;

3) Inform the AMF that PWS information for some or all cells of the NG-RAN are available for reloading from the CBC if needed by sending a PWS RESTART-INDICATION message to the AMF; and

4) Inform the AMF that ongoing PWS operation for one or more cells of the NG-RAN has failed by sending a PWS FAILURE-INDICATION message to the AMF.

##### 12.1.1.3.3 NG-RAN Protocol Overview



**Legend:**

- NBc application protocol (NBc-AP): Application layer protocol between CBC and AMF. This protocol supports transfer of warning messages.

- NG application protocol (NGAP): Application layer protocol between the 5G-RAN entity (eNodeB and/or gNodeB) and the AMF. The NGAP protocol is defined in 3GPP TS 38.413 [28].

- SCTP for the control plane (SCTP): This protocol guarantees delivery of signalling messages between AMF and NG-RAN (N2) and between CBC and AMF (NBc). SCTP is defined in IETF RFC 4960 [34].

Figure 12.1.1.3.3.1: CBC - NG-RAN

##### 12.1.1.3.4 CBC-AMF interface

The CBC network function uses Namf\_Communication service to communicate with the NG-RAN for sending warning request primitives and receiving warning message delivery indication or restart/failure indication primitives.

The requirements are described by primitives.

The following table shows primitives that are expected to be supported using AMF via Namf interface:

Table 12.1.1.3.4.1: CBC-AMF primitives via Namf interface

|  |  |  |
| --- | --- | --- |
| **Name** | **Originator** | **Type** |
| WRITE-REPLACE-WARNING-REQUEST | CBC | Request/Indication |
| WRITE-REPLACE-WARNING-CONFIRM | AMF | Response/Confirm |
| STOP-WARNING-REQUEST | CBC | Request/Indication |
| STOP-WARNING-CONFIRM | AMF | Response/Confirm |
| WRITE-REPLACE-WARNING-INDICATION | AMF | Request/Indication |
| STOP-WARNING-INDICATION | AMF | Request/Indication |
| RESTART-INDICATION-NG-RAN | AMF | Request/Indication |
| FAILURE-INDICATION-NG-RAN | AMF | Request/Indication |

#### 12.1.1.4 Architecture alternative 3: Supporting PWS in 5GS to CBCF and via PWS-IWF to CBC

##### 12.1.1.4.1 Overview

In this architecture alternative, the AMF interfaces with CBCF and NG-RAN to enable PWS service with the interface between AMF and CBCF implemented as service based interface. CBCF uses AMF communication services to forward warning messages to NG-RAN and to subscribe to receive warning delivery related notifications. As a deployment option an PWS-IWF can be used as termination point of the service based interface (Ncbcf) and connect to a CBC via SBc.

##### 12.1.1.4.2 Architecture description

###### 12.1.1.4.2.1 PWS architecture

Figure 12.1.1.4.2.1.1 shows the basic network structure of PWS architecture in 5GS.



Figure 12.1.1.4.2.1.1: PWS architecture

The cell broadcast centre function (CBCF) is part of the core network and connected to the AMF via the Ncbcf service based interface. The cell broadcast centre (CBC) is part of the core network and connected to the PWS-IWF via the SBc interface. The PWS-IWF is part of the core network, connected to the AMF via the Ncbcf service based interface and to the CBC via the SBc interface.

Reference point to support PWS architecture:

**N2:** Reference point between the NG-RAN and the AMF.

NOTE: NG-RAN can be NR based or E-UTRA based (See 3GPP TS 23.501 [9] and 3GPP TS 38.413 [28]).

**SBc:** Reference point between the PWS-IWF and the CBC.

NOTE: SBc is specified for EPS (see 3GPP TS 23.041 [6]).

Service based interface to support PWS in 5GS:

**Namf:** Service-based interface exhibited by AMF.

**Ncbcf:** Service-based interface exhibited by CBCF or PWS-IWF.

The CBE and the interface between CBCF or CBC, and CBE are out of scope of 3GPP specifications.

###### 12.1.1.4.2.2 AMF functionality

The AMF may interface to one CBCF or PWS-IWF, or multiple CBCFs/PWS-IWFs (i.e. combinations of CBCFs and/or PWS-IWFs). An AMF may interface to several NG-RANs (i.e. combinations of gNodeBs and/or eNodeBs).

The AMF is responsible for:

1) Interpretation of commands from the CBCF or the CBC;

2) Storage of messages from the CBCF or the CBC;

3) Routing the WRITE-REPLACE-WARNING-REQUEST message to the appropriate NG-RAN entities upon receiving warning message request from the CBCF or the CBCF;

4) Routing the STOP-WARNING-REQUEST message to the appropriate NG-RAN entities upon receiving STOP-WARNING-REQUEST message from CBCF or the CBC;

5) Warning message delivery success or failure notification

- Providing to the CBCF, or optionally CBC via an PWS-IWF, acknowledgement of successful execution of commands received from the CBCF or CBC;

- Reporting to the CBCF, or optionally CBC via an PWS-IWF, failure when a command received from the CBCF is not understood or cannot be executed; and

- Reporting to the CBCF, or optionally CBC via an PWS-IWF, the Broadcast completed area list, the Broadcast cancelled area list received from NG-RAN; and

6) Forwarding PWS RESTART-INDICATION message and the PWS FAILURE-INDICATION message received from NG-RAN entities to all CBCFs or CBCs that the AMF interfaces with.

###### 12.1.1.4.2.3 CBCF functionality

CBCF is a network function in the 5G core network. The CBCF may be connected to several AMFs. The CBCF may be connected to several CBEs. The CBCF shall be responsible for the management of CBS messages as specified in subclause 5 of 3GPP TS 23.041 [16].

CBCF supports service based interface. CBCF uses AMF communication services to forward warning messages to NG-RAN and to subscribe to receive warning delivery related notifications.

###### 12.1.1.4.2.4 CBC functionality

CBC is a network function in the EPS core network. In the deployment option using an PWS-IWF, the CBC functionality and requirements are specified 3GPP TS 23.041 [16].

###### 12.1.1.4.2.5 PWS-IWF functionality

The PWS-IWF is a logical function which functionality is to translate from Ncbcf to SBc. The PWS-IWF may interface to one or multiple AMFs. The PWS-IWF may interface to one or multiple CBCs.

NOTE: The present document describes logical functional entities, and how these are realized in actual deployments is an implementation and deployment issue. It can however be foreseen that the PWS-IWF functionality can be co-located with the AMF, with the CBC, or deployed as a stand-alone network function. At AMF/PWS-IWF co-location, the AMF/PWS-IWF entity provides a SBc interface towards the CBC. At CBC/PWS-IWF co-location, the CBC/PWS-IWF provides the Ncbcf interface towards the AMF. At stand-alone PWS-IWF, the PWS-IWF provides the Ncbcf interface towards the AMF and the SBc interface towards the CBC.

###### 12.1.1.4.2.6 NG-RAN functionality

The NG-RAN may interface to multiple AMFs.

The NG-RAN is responsible for:

1) Upon receipt of the WRITE-REPLACE-WARNING-REQUEST message, prioritise its resources and broadcast the warning message to the warning areas indicated in the requested Warning area list;

2) Upon receipt of the KILL-REQUEST message, stop broadcasting the warning message within for that area indicated in the requested Warning area list and discard the warning message;

3) Inform the AMF that PWS information for some or all cells of the NG-RAN are available for reloading from the CBCF if needed by sending a PWS RESTART-INDICATION message to the AMF; and

4) Inform the AMF that ongoing PWS operation for one or more cells of the NG-RAN has failed by sending a PWS FAILURE-INDICATION message to the AMF.

##### 12.1.1.4.3 Protocol Stack Overview

Figure 12.1.1.4.3.1 shows the protocol stacks of architecture alternative 3 without PWS-IWF. This alternative is identical to Architecture alternative 1.



Figure 12.1.1.4.3.1: CBCF - NG-RAN, without PWS-IWF

Figure 12.1.1.4.3.2 shows the protocol stacks of architecture alternative 3 with PWS-IWF. In this alternative the AMF protocol stack is identical to architecture alternative 3 without PWS-IWF and to architecture alternative 1. Additionally, in this alternative the CBC protocol stack is identical to the CBC protocol stack in EPS PWS.



Figure 12.1.1.4.3.2: CBC - NG-RAN, with PWS-IWF

#### 12.1.1.5 Overall evaluation

Evaluation of the two architecture options is shown below:

**Table 12.1.1.4.1.1: PWS Architectur**e Option Evaluation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Option 1**  **(Direct SBI between AMF<->CBCF )** | **Option 2**  **(AMF<->CBC via SBc like interface)** | **Option 3**  **(AMF<->CBC via IWF)**  (SBI between AMF<-> IWF**/**CBCF and SBc between IWF<->CBC) | **Comments** |
| **Pros** | + Supports 5GS CN Service based interface  + Supports 5GS PWS evolution and enhancement. | + Supports existing CBC/PWS deployments,  + No impact to CBC  + Reuses existing EPS interface, less implementation efforts  + Less standardization efforts, SBc protocol already specified  + Support future PWS enhancement. | + Supports existing CBC/PWS deployments  + No impact to CBC  + Reuses existing EPS interface  + Supports 5GS CN Service based interface  + Supports independent 5GS PWS evolution.  + Allows flexible deployments of CBCF, IWF and CBC  + Meets all operator requirements. | Option 3 implies a single interface supporting both CBCF and CBC.  IWF can be implemented in a number of ways in networks and products, and allows practical deployments:  - if IWF is co-located with AMF, AMF connects CBC via SBc interface  - if IWF is co-located with CBC, CBC becomes CBCF, AMF connects CBC via SBI interface |
| **Cons** | - Does not support existing CBC/PWS deployments  - Requires upgrading all CBC to CBCF  - Additional standardization efforts  - Requires more efforts to implement new protocol stack and SBI interface on both AMF and CBCF  - Does not meet all operator requirements | - Does not meet all operator requirements. | - Additional network function introduced |  |

CBC is a legacy network element that is already widely deployed. It may be already connected to BSCs/RNCs/MMEs as well as CBEs. Also NG-RAN can be either NR or E-UTRA based. NG-eNB can connect to 5GC via N2 interface.

For operators that already deployed PWS services in their network, since SBc is already used as interface between CBC and MME in the EPC network for interfacing eNB, it would be desired that the same SBc interface can be used between CBC and AMF in the NG-CN for interfacing NG-RAN including NG-eNB. If the interface between AMF and CBC is defined to be service based, besides implementation efforts, it would also require CBC to maintain separate interfaces for same warning message delivery operations which is not desired. For operators that have not deployed PWS services in their network, above considerations due to existing deployment do not apply.

From the evaluation it can be seen that option 3 is the only option that allows both new deployments of a fully service based core network and inter-connection with existing non-service based CBC deployments. Therefore, option 3 is the most flexible alternative supporting legacy deployments, initial service based and smooth migration from legacy to service based.

### 12.1.2 SMS over NAS

Editor’s note: Both the names and codings of the SMS parameters sent from the UE to the network and from the network to the UE are FFS.

#### 12.1.2.1 Registration requirements

##### 12.1.2.1.1 Initial registration initiation

If the UE requests to use SMS over NAS, the UE shall include the SMS requested IE in the REGISTRATION REQUEST message and set:

1) the "supported accesses" bits of the SMS requested IE to:

A) "SMS over NAS supported via 3GPP access only" if the UE supports SMS delivery over NAS via 3GPP access only; or

B) "SMS over NAS supported via both 3GPP access and non-3GPP access" if the UE supports SMS delivery over NAS via both 3GPP access and non-3GPP access; and

2) the "one step" bit of the SMS requested IE to:

A) "MO SMS using one step approach not supported" if the UE does not support MO SMS using the one step approach in 5GMM-IDLE mode; or

B) "MO SMS using one step approach supported" if the UE supports MO SMS using the one step approach in 5GMM-IDLE mode.

##### 12.1.2.1.2 Initial registration accepted by the network

If the REGISTRATION REQUEST message contained the SMS requested IE with the supported accesses bits indicating that the UE supports SMS delivery over NAS via 3GPP access only, or via both 3GPP access and non-3GPP access, and SMSF selection is successful, then the AMF shall send the REGISTRATION ACCEPT message either:

a) prior to requesting activation of the SMS service from the SMSF; or

b) after the SMSF has confirmed that the activation of the SMS service was successful;

NOTE: The decision in the AMF to perform a) or b) above is based upon implementation.

Editor's note: For case a), consideration is needed when SMS activation subsequently fails at the SMSF.

When sending the REGISTRATION ACCEPT message, the AMF shall:

a) store the SMSF address and the contents of the SMS requested IE in the UE 5GMM context, and consider the UE available for SMS; and

b) include the SMS allowed IE in the REGISTRATION ACCEPT message with:

1) the "allowed accesses" bits of the SMS allowed IE to:

A) "SMS over NAS supported via 3GPP access only" if:

i) the UE has set the "supported accesses" bits of the SMS requested IE to "SMS over NAS supported via 3GPP access only" and the network allows the SMS delivery over NAS via 3GPP access; or

ii) the UE has set the "supported accesses" bits of the SMS requested IE to "SMS over NAS supported via both 3GPP access and non-3GPP access" and the network allows the SMS delivery over NAS via 3GPP access only; or

B) "SMS over NAS supported via both 3GPP access and non-3GPP access" if the UE has set the "supported accesses" bits of the SMS requested IE to "SMS over NAS supported via both 3GPP access and non-3GPP access" and the network allows the SMS delivery over NAS via both 3GPP access and non-3GPP access; and

2) the "one step" bit of the SMS allowed IE to:

A) "MO SMS using one step approach not allowed" if the UE indicated the support of the MO SMS using one step approach in 5GMM-IDLE mode or the network does not allow the MO SMS using one step approach; or

B) "MO SMS using one step approach allowed" if the UE indicated the support of the MO SMS using one step approach in 5GMM-IDLE mode and the network allows the MO SMS using one step approach.

If SMSF selection in the AMF or SMS activation via the SMSF is not successful, then the AMF shall not include the SMS allowed IE in the REGISTRATION ACCEPT message.

If the AMF does not allow the use of SMS over NAS, then the AMF shall not include the SMS allowed IE in the REGISTRATION ACCEPT message.

##### 12.1.2.1.3 Mobility and periodic registration update initiation

The UE in state 5GMM-REGISTERED shall initiate the mobility registration updating procedure by sending a REGISTRATION REQUEST message to the AMF when the UE needs to request the use of SMS over NAS transport or the current requirements to use SMS over NAS transport change in the UE, as specified in subclause 12.1.2.1.1.

When initiating a periodic registration update and the requirements to use SMS over NAS transport have not changed in the UE, the UE shall not include the SMS requested IE in the REGISTRATION REQUEST message.

If the UE no longer requires the use of SMS over NAS transport, then the UE shall include the SMS requested IE in the REGISTRATION REQUEST message with the "supported accesses" bits set to "SMS over NAS not supported".

##### 12.1.2.1.4 Mobility and periodic registration update accepted by the network

If the UE requests the use of SMS over NAS transport or the requirements to use SMS over NAS transport change in the UE, the AMF shall follow the procedures specified in subclause 12.1.2.1.2.If the REGISTRATION REQUEST message contained the SMS requested IE with the "supported accesses" bits set to "SMS over NAS not supported", then the AMF shall:

a) if an SMSF address is present in the 5GMM context, delete the SMSF address from the 5GMM context;

b) mark the 5GMM context to indicate that SMS over NAS is not required by the UE; and

NOTE: The AMF notifies the SMSF that the UE is deregistered from SMS over NAS.

c) not include the SMS allowed IE in the REGISTRATION ACCEPT message.

### 12.1.3 Emergency services

#### 12.1.3.1 Indication of support of emergency services

During the registration procedure the AMF includes the emergency PDU session service support indicator in the REGISTRATION ACCEPT message (see subclause 8.5.2.1).

Editor’s note: The emergency PDU session service support indicator needs to be aligned with the stage 2 as soon as procedural requirements are in place.

Editor’s note: The emergency service support indicator needs to be added in the subclause 8.5.2.1.

Editor’s note: It is FFS in which information element of the REGISTRATION ACCEPT message the emergency service support indicator is included.

The received emergency PDU session service support indicator shall be provided to the upper layers in the UE.

Editor’s note: The use of the emergency PDU session service support indicator by upper layers is FFS.

#### 12.1.3.2 Handling of emergency service for the UE in limited service state

If the UE in the 5GMM-DEREGISTERED.LIMITED-SERVICE state requests to use emergency services, the UE shall send REGISTRATION REQUEST message with the 5GS registration type IE set to "emergency registration".

The UE sending a REGISTRATION REQUEST message with the 5GS registration type IE set to "emergency registration" shall handle identities as follows:

- if the UE has a valid 5G-GUTI, then indicate the 5G-GUTI in the REGISTRATION REQUEST message;

- if the UE does not have a valid 5G-GUTI and has a valid SUPI, then indicate the SUPI in the REGISTRATION REQUEST message; and

- if the UE does not have a valid 5G-GUTI and does not have a SUPI, then indicate the PEI in the REGISTRATION REQUEST message.

Editor's note: When REGISTRATION REQUEST message layout is defined, 5GS registration type IE and 5GS mobile identity IE need to be included.

Editor's note: This subclause describes how to provide emergency bearer services to the UE in limited services state.

#### 12.1.3.3 Emergency PDU session setup

Editor's note: This subclause describes the procedure of PDU session setup.

#### 12.1.3.4 Handling of local emergency numbers

The following mechanism of handling of local emergency numbers applies when the UE accesses the 5GCN via 3GPP access and non-3GPP access.

Editor’s note: The handling of the case where the UE registers to different PLMNs via 3GPP access and non-3GPP access simultaneously and receive the emergency number list from different PLMNs is FFS.

At successful completion of the registration procedure the operator of this network may provide a list of local emergency numbers to the UE. Optionally to each local emergency number either an emergency service category or an associated sos-URN (i.e. URN with top level service type of "sos" as specified in IETF RFC 5031 [69]) may be provided in the local emergency number list. The emergency number list can be downloaded by the network to the UE at successful completion of the registration procedure.

The UE shall store and use the local emergency number list received from the network in addition to the emergency numbers stored on the UICC or user equipment to detect if the user dialled number is an emergency number and use the corresponding sos-URN to initiate an UE detected emergency session. The UE shall delete the emergency number list received from the network after successful registration to a different network.

NOTE 1: The sos-URN used by the UE to setup the emergency session is either the associated sos-URN or the sos-URN mapped to the emergency service category (as defined in 3GPP TS 24.229 [13]) if these additional information are provided.

NOTE 2: The option to provide an emergency list to an UE and the related content of this emergency list is optional and in responsibility of the network operator where the UE is registered. This enables the network operator to identify an emergency service and route the emergency session to the responsible PSAP in accordance to national regulation.

Editor’s note: It is FFS if there is a potential conflict with the emergency numbers list received via an access and those on the UICC.

The network may send a list of local emergency numbers in the REGISTRATION ACCEPT message (see subclause 8.5.2.1).

Editor’s note: The emergency number list needs to be added in the subclause 8.5.2.1.

Editor’s note: It is FFS in which information element of the REGISTRATION ACCEPT message the emergency number list is included.

The local emergency numbers received from the network are valid only in networks in the same country as where the UE received them and are only used to establish emergency sessions in the PS domain.

#### 12.1.3.5 Security procedures for handling emergency services

Editor's note: This subclause describes the difference on the security aspect between emergency services procedure and normal procedure.

#### 12.1.3.6 IMS emergency call reattempt

Upon request from upper layers to establish a PS emergency call, if the 5G core network does not support the emergency PDU session service as described in subclause 12.1.3.1 and when the UE selects the E-UTRA connected to EPC according to the core network selection (5GC or EPC) as specified in 3GPP TS 23.501 [9], the UE shall:

- if the UE operates in single-registration mode, disable the N1 mode radio capabilities and then proceed with the domain selection as specified in 3GPP TS.23.167 [8] annex H; and

- if the UE operates in dual-registration mode, proceed with the domain selection as specified in 3GPP TS.23.167 [8] annex H.

Editor's note: The requirement will be updated by taking RAN definition of emergency service support indication into account for e.g., UE behavior when the 5G core network supports the emergency PDU session service but the current RAT does not.

Editor's note: The 5G core network selection requirement for emergency call needs to be clarified in SA2.

### 12.1.4 Location services

LPP messages shall be transported between the UE and the AMF using the NAS transport procedures specified in subclause 8.5.1.3.

Editor’s note: It is FFS whether transport of supplementary service messages for location services as specified in 3GPP TS 24.030 is needed in 5G System.

### 12.1.5 Multimedia priority services

#### 12.1.5.1 General

5GS supports MPS with functionality as described in subclause 5.16.5 in 3GPP TS 23.501 [9]. MPS priority mechanisms can be classified as subscription-related, invocation-related, and those applied to existing QoS Flows, as described in subclause 5.22 of 3GPP TS 23.501 [9].

MPS-specific exemptions are provided for 5GS mobility management and 5GS session management.

#### 12.1.5.2 5GS mobility management priority mechanisms

Membership in the unique special access class assigned for MPS (based on subclause 4.4A of 3GPP TS 22.011 [2]) provides certain 5GMM priority treatments and exemptions to MPS-subscribed UEs.

An MPS-subscribed UE is configured with at least one access class in the range 11-15 on the USIM. A UE configured to use AC11 – 15 in selected PLMN shall be exempt from NAS level 5GMM congestion controls.

Editor’s note: NAS level 5GMM congestion control is FFS and will be captured by CT1 based on stage 2 requirements.

A UE configured to use AC11 – 15 in selected PLMN shall be exempt from 5GMM procedure backoff timers.

Editor’s note: 5GMM procedure backoff timers are FFS.

A UE configured to use AC11 – 15 in selected PLMN shall be exempt from failed service request procedure retry counter limitations.

Editor’s note: Service request procedure retry counters are FFS.

For initial paging to deliver an MPS packet, the network shall initiate paging procedure with paging priority.

If paging is in progress without priority, and an MPS packet arrives, the network shall re-start the paging procedure with paging priority.

#### 12.1.5.3 5GS session management priority mechanisms

Membership in the unique special access class assigned for MPS (based on subclause 4.4A of 3GPP TS 22.011 [2]) provides certain 5GSM priority treatments and exemptions to UEs configured to use AC11 – 15 in selected PLMN.

A UE configured to use AC11 – 15 in selected PLMN shall be exempt from 5GSM procedure backoff timers associated with network congestion at the AMF or SMF.

Editor’s note: DN level based congestion control is FFS and will be captured by CT1 based on stage 2 requirements. 5GSM procedure backoff timers are FFS.

A UE configured to use AC11 – 15 in selected PLMN shall be exempt from 5GSM procedure backoff timers associated with signaling for PDU sessions to specific DNs.

## 12.2 Access control

### 12.2.1 Unified access control (Alternative 1)

#### 12.2.1.1 General

5GS supports a unified access control by which each access attempt is categorized into one access category. The network can restrict the access on a per-access category basis according to the requirement specified in 3GPP TS 22.261 [3].

Access categories include:

- a set of standardized access categories specified in 3GPP TS 22.261 [3]; and

- optionally, operator-specific categories defined using the format specified in subclause 12.2.1.2.

An access attempt when the UE is in 5GMM-IDLE mode is defined as any event that requires a transition to 5GMM-CONNECTED mode.

An access attempt when the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication is defined as one of the following events:

1) an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication received from upper layers;

2) a request to send a mobile originated SMS over NAS from upper layers

3) a request for a new PDU session establishment from upper layers;

4) a request for an existing PDU sessions modification from upper layers;

5) a request for a PDU session release from upper layers; and

6) a request to re-establish the user plane for an existing PDU session from upper layers.

Editor's note: Additional vents qualifying as access attempts in 5GMM-CONNECTED mode with RRC inactive indication are FFS.

#### 12.2.1.2 Operator-specific access categories

Operator-specific access categories can be signalled to the UE using the NAS transport procedure specified in subclause 8.5.1.3, with:

- the payload container IE of the DL NAS TRANSPORT message containing one or more access category definitions, each consisting of the following parameters:

Editor's note: The encoding of the operator-specific access categories in the Payload container IE is FFS.

1) an access category number in the 32-63 range that uniquely identifies the access category in the PLMN in which the access categories are being sent to the UE;

2) a precedence value which indicates in which order the UE shall evaluate the operator-specific categories for a match; and

3) one or more access category criteria type and associated access category criteria type values. The access category criteria type can be set to one of the following:

i) DNN name;

ii) QFI;

iii) 5QI;

iv) OS Id + OS App Id of application triggering the access attempt; or

v) S-NSSAI.

Editor's note: Other access category criteria types are FFS.

NOTE: An access category criteria type can be associated with more than one access category criteria values. In this case, the access attempt matches the access category if the access criteria for the access attempt matches any of the associated access criteria type values.

- the Payload container type IE of the DL NAS TRANSPORT message indicating that the Payload container IE contains operator-specific access category definitions:

Editor's note: The encoding of the Payload container type IE for operator-specific access category definitions is FFS.

Upon receiving a DL NAS TRANSPORT message with a Payload container IE indicating that the Payload container IE contains operator-specific access category definitions, the UE shall store the operator-specific access category definitions for the registered PLMN.

Editor's note: It is FFS whether additional mechanisms are needed to ensure operator-specific access categories sent to the UE using NAS transport are delivered reliably.

Editor's note: It is FFS whether other NAS control plane messages can be used to send operator-specific access categories to the UE.

#### 12.2.1.3 Mapping of an access attempts to access category

When the UE is in 5GMM-IDLE mode, upon receiving a request from the upper layers for an access attempt, the NAS shall categorize the access attempt into one access category by performing the following steps in order until a match between the access attempt and an access category is found:

- The NAS shall evaluate whether the access attempt matches standardized access category 0 as specified in 3GPP TS 22.261 [3];

- the NAS shall evaluate whether the access attempt matches standardized access category 1 as specified in 3GPP TS 22.261 [3];

- the NAS shall evaluate whether the access attempt matches standardized access category 3 as specified in 3GPP TS 22.261 [3];

- the NAS shall evaluate whether the access attempt matches any of the operator-specific access categories stored in the UE for the registered PLMN, in order of increasing precedence value; and

- the NAS shall evaluate whether the access attempt matches any of the remaining standardized access categories as specified in 3GPP TS 22.261 [3].

Editor's note: The precedence order of the access categories needs to be confirmed by SA1.

When a match is found, the NAS shall pass the access category for which there was a match to the lower layers.

NOTE 1: The access barring check is performed by the lower layers.

NOTE 2: If, during an MMTEL voice session, MMTEL video session, SMSoIP transport or emergency PDU session, the UE has moved back to 5GMM-IDLE mode and needs to go to 5GMM-CONNECTED mode, this is considered a new access attempt and a new access barring check is performed by the lower layers.

If the lower layers indicate that the access attempt is allowed, the NAS shall initiate the procedure to send the initial NAS message for the access attempt. If the lower layers indicate that the access attempt is barred, the NAS shall not initiate the procedure to send the initial NAS message for the access attempt. Upon receiving an indication from the lower layers that access is granted, the NAS may initiate the procedure to send the initial NAS message, if still needed.

When the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication, upon detecting one of events 1) through 6) listed in subclause 12.2.1.1,, the NAS shall categorize the corresponding access attempt into on access category by performing the following steps in order until a match between the access attempt and an access category is found:

- the NAS shall evaluate whether the access attempt matches standardized access category 0 as specified in 3GPP TS 22.261 [3]; and

- the NAS shall evaluate whether the access attempt matches standardized access category 1 as specified in 3GPP TS 22.261 [3];

- the NAS shall evaluate whether the access attempt matches standardized access category 3 as specified in 3GPP TS 22.261 [3];

- the NAS shall evaluate whether the access attempt matches any operator-specific access categories stored in the UE for the registered PLMN in order of increasing precedence value; and

- the NAS shall evaluate whether the access attempt matches any of the remaining standardized access categories as specified in 3GPP TS 22.261 [3].

Editor's note: The precedence order of the access categories needs to be confirmed by SA1.

When a match is found, the NAS shall pass the access category for which there was a match to the lower layers.

NOTE 3: The access barring check is performed by the lower layers.

If the lower layers indicate that the access attempt is allowed, the NAS shall take the following action depending on the event which triggered the access attempt:

- if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication, the NAS shall notify the upper layers that the access attempt is allowed;

- if the event which triggered the access attempt was a request from upper layers to send a mobile originated SMS over NAS, the NAS shall initiate the NAS transport procedure as specified in subclause 8.5.1.2.3 to send the SMS in an UL NAS TRANSPORT message;

- if the event which triggered the access attempt was a request from upper layers for a new PDU session establishment, the NAS shall initiate the UE-requested PDU session establishment procedure as specified in subclause 9.5.2.2;

- if the event which triggered the access attempt was a request from upper layers for an existing PDU session modification, the NAS shall initiate the UE-requested PDU session modification procedure as specified in subclause 9.5.4.2; and

- if the event which triggered the access attempt was a request from upper layers to re-establish the user plane for an existing PDU session, the NAS shall initiate the service request procedure as specified in subclause 8.5.3.1.2.

If the lower layers indicate that the access attempt is barred, the NAS shall take the following action depending on the event which triggered the access attempt:

- if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication, the NAS shall notify the upper layers that the access attempt is barred. Upon receiving an indication from the lower layers that access is granted, the NAS shall notify the upper layers that access is granted;

NOTE 4: In this case prohibiting the initiation of the MMTEL voice session, MMTEL video session or prohibiting sending of the SMS over IP is performed by the upper layers.

- if the event which triggered the access attempt was a request from upper layers to send a mobile originated SMS over NAS, the NAS shall not initiate the NAS transport procedure as specified in subclause 8.5.1.2.3 to send the SMS in an UL NAS TRANSPORT message. Upon receiving an indication from the lower layers that access is granted, the NAS may initiate the NAS transport procedure as specified in subclause 8.5.1.2.3 to send the SMS in an UL NAS TRANSPORT message, if still needed;

- if the event which triggered the access attempt was a request from upper layers for a new PDU session establishment, the NAS shall not initiate the UE-requested PDU session establishment procedure as specified in subclause 9.5.2.2. Upon receiving an indication from the lower layers that access is granted, the NAS may initiate the UE-requested PDU session establishment procedure as specified in subclause 9.5.2.2, if still needed;

- if the event which triggered the access attempt was a request from upper layers for an existing PDU session modification, the NAS shall not initiate the UE-requested PDU session modification procedure as specified in subclause 9.5.4.2. Upon receiving an indication from the lower layers that access is granted, the NAS may initiate the UE-requested PDU session modification procedure as specified in subclause 9.5.4.2, if still needed; and

- if the event which triggered the access attempt was a request from upper layers to re-establish the user plane for an existing PDU session, the NAS shall not initiate the service request procedure as specified in subclause 8.5.3.1.2. Upon receiving an indication from the lower layers that access is granted, the NAS may initiate the service request procedure as specified in subclause 8.5.3.1.2, if still needed.

### 12.2.2 Access categories, access categorization and access control checking (combined Alternative 2 and Alternative 1)

#### 12.2.2.1 General

When the UE wants to access the 5GS, the UE must first perform access control checks to determine if the access is allowed. Access control checks shall be perfomed for the access attempts defined by the following list of events:

- the UE is in 5GMM-IDLE mode over 3GPP access and an event that requires a transition to 5GMM-CONNECTED mode occurs;

- the UE is in 5GMM-CONNECTED mode over 3GPP access or 5GMM-CONNECTED mode with RRC inactive indication and one of the following events occurs:

1) 5GMM receives an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication from upper layers;

2) 5GMM receives a request from upper layers to send a mobile originated SMS over NAS;

3) 5GMM receives a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session establishment;

4) 5GMM receives a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session modification; and

5) 5GMM receives a request to re-establish the user plane for an existing PDU session.

NOTE 1: 5GMM specific procedures initiated by NAS in 5GMM-CONNECTED mode are not subject to access control. E.g. a registration procedure after PS handover will not be prevented by access control.

Editor's note: For the case that the UE is in 5GMM-IDLE  mode when 5GMM receives a request from an upper layer to send an UL NAS TRANSPORT message, so that the procedure for the initial NAS message is followed by a NAS transport procedure, resolution of double barring is FFS.

Editor's note: Whether other events need to be considered in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication, is FFS.

When the NAS detects one of the above events, the NAS needs to perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

NOTE 2: The NAS is aware of the above events through indications provided by upper layers or when determing the need to start 5GMM procedures through normal NAS behaviour, or both.

To determine the access identities and the access category for a request, the NAS checks the reason for access, types of service requested and profile of the UE including UE configurations, against a set of access identities and access categories defined in 3GPP TS 22.261 [3], namely:

- a set of standardized access identities;

- a set of standardized access categories; and

- a set of operator-defined access categories, if available.

For the purpose of determining the applicable access identities from the set of standardized access identities defined in 3GPP TS 22.261 [3], the NAS shall follow the requirements set out in subclause 12.2.2.2 and the rules and actions defined in table 12.2.2.2.1.

For the purpose of determining the applicable access category from the set of standardized access categories and operator-defined access categories defined in 3GPP TS 22.261 [3], the NAS shall follow the requirements set out in subclause 12.2.2.2 and the rules and actions defined in table 12.2.2.2.2.

#### 12.2.2.2 Determination of the access identities and access category associated with a request for access

When the UE needs to initiate an access attempt in one of the events listed in subclause 12.2.2.1, the UE shall determine one or more access identities from the set of standardized access identities, and one access category from the set of standardized access categories and operator-defined access categories, to be associated with that access attempt.

The set of the access identities applicable for the request is determined by the UE in the following way:

- for each of the access identities 1, 2, 11, 12, 13, 14 and 15 in table 12.2.2.2.1, the UE shall check whether the access identity is applicable in the selected PLMN, if a new PLMN is selected, or otherwise if it is applicable in the RPLMN or equivalent PLMN; and

- if none of the above access identities is applicable, then access identity 0 is applicable.

**Table 12.2.2.2.1: Access Identities (according to 3GPP TS 22.261 [3], table 6.22.2.2-1**)

|  |  |
| --- | --- |
| **Access Identity number** | **UE configuration** |
| 0 | UE is not configured with any parameters from this table |
| 1 (NOTE 1) | UE is configured for Multimedia Priority Service (MPS). |
| 2 (NOTE 2) | UE is configured for Mission Critical Service (MCS). |
| 3-10 | Reserved for future use |
| 11 (NOTE 3) | Access Class 11 is configured in the UE. |
| 12 (NOTE 3) | Access Class 12 is configured in the UE. |
| 13 (NOTE 3) | Access Class 13 is configured in the UE. |
| 14 (NOTE 3) | Access Class 14 is configured in the UE. |
| 15 (NOTE 3) | Access Class 15 is configured in the UE. |
| NOTE 1: Access Identity 1 is used to provide overrides according to the subscription information in UEs configured for MPS. The subscription information defines whether an overide applies to UEs within one of the following categories:  a) UEs that are configured for MPS;  b) UEs that are configured for MPS and are in the PLMN listed as most preferred PLMN of the country where the UE is roaming in the operator-defined PLMN selector list or in their HPLMN or in a PLMN that is equivalent to their HPLMN;  c) UEs that are configured for MPS and are in their HPLMN or in a PLMN that is equivalent to it.  NOTE 2: Access Identity 2 is used to provide overrides according to the subscription information in UEs configured for MCS. The subscription information defines whether an overide applies to UEs within one of the following categories:  a) UEs that are configured for MCS;  b) UEs that are configured for MCS and are in the PLMN listed as most preferred PLMN of the country where the UE is roaming in the operator-defined PLMN selector list or in their HPLMN or in a PLMN that is equivalent to their HPLMN;  c) UEs that are configured for MCS and are in their HPLMN or in a PLMN that is equivalent to it.  NOTE 3: Access Identities 11 and 15 are valid in Home PLMN only if the EHPLMN list is not present or in any EHPLMN. Access Identities 12, 13 and 14 are valid in Home PLMN and visited PLMNs of home country only. For this purpose the home country is defined as the country of the MCC part of the IMSI. | |

In order to determine the access category applicable for the access attempt, the NAS shall check the rules in table 12.2.2.2.2, and use the access category for which there is a match for barring check. If the access attempt matches more than one rule, the access category of the lowest rule number shall be selected.

Table 12.2.2.2.2: Mapping table for access categories

|  |  |  |  |
| --- | --- | --- | --- |
| **Rule #** | **Type of access attempt** | **Requirements to be met** | **Access Category** |
| 1 | Response to paging | Access attempt is for MT access | 0 (= MT\_acc) |
| 2 | Emergency | UE is attempting access for an emergency session (NOTE 1, NOTE 2) | 2 (= emergency) |
| 3 | Access attempt for operator-defined access category | UE was provided with operator-defined access categories for the current PLMN, and access attempt is matching criteria of an operator-defined access category | 32-63  (= based on operator classification) |
| 4 | Access attempt for delay tolerant service | UE is configured for delay tolerant service, the PLMN is broadcasting one of the categories a, b or c, and the UE is a member of the broadcasted category in the selected PLMN or RPLMN/equivalent PLMN (NOTE 3) | 1 (= delay tolerant) |
| 5 | MO MMTel voice call | Access attempt is for MO MMTel voice call  or for NAS signalling connection recovery during ongoing MO MMTel voice call (NOTE 2) | 4 (= MO MMTel voice) |
| 6 | MO MMTel video call | Access attempt is for MO MMTel video call  or for NAS signalling connection recovery during ongoing MO MMTel video call (NOTE 2) | 5 (= MO MMTel video) |
| 7 | MO SMS over NAS or MO SMSoIP | Access attempt is for MO SMS or SMSoIP transfer  or for NAS signalling connection recovery during ongoing MO SMS or SMSoIP transfer (NOTE 2) | 6 (= MO SMS and SMSoIP) |
| 8 | UE NAS initiated 5GMM specific procedures | Access attempt is for MO signalling | 3 (= MO\_sig) |
| 9 | UE NAS initiated 5GMM connection management procedures or 5GMM NAS transport procedure | Access attempt is for MO data | 7 (= MO\_data) |
| NOTE 1: This includes 5GMM specific procedures while the service is ongoing and 5GMM connection management procedures required to establish a PDU session with request type = "emergency" or to re-establish radio bearers for such a PDU session.  NOTE 2: Access for the purpose of NAS signalling connection recovery during an ongoing service is mapped to the access category of the ongoing service in order to derive an RRC establishment cause, but barring checks will be skipped for this access attempt.  NOTE 3: If the UE selects a new PLMN, then the selected PLMN is used to check the membership; otherwise the UE uses the RLPMN or a PLMN equivalent to the RPLMN. | | | |

Editor's note: The need for and the derivation of the RRC establishment cause (or its equivalence in 5GS) requires further work by RAN2.

#### 12.2.2.3 Operator-defined access categories

Operator-defined access categories can be signalled to the UE using NAS signalling. Each operator-defined category consists of the following parameters:

Editor's note: The encoding of the operator-defined access categories is FFS.

Editor's note: Whether the operator-defined access categories are sent to the UE in a CONFIGURATION UPDATE COMMAND message, a DL NAS TRANSPORT message or another NAS message, is FFS.

- a precedence value which indicates in which order the UE shall evaluate the operator-defined categories for a match;

- an access category number in the 32-63 range that uniquely identifies the access category in the PLMN in which the access categories are being sent to the UE; and

- one or more access category criteria type and associated access category criteria type values. The access category criteria type can be set to one of the following:

1) DNN name;

2) 5QI;

Editor's note: Whether the 5QI is a suitable access category criteria type is FFS.

3) OS Id + OS App Id of application triggering the access attempt; or

4) S-NSSAI.

Editor's note: Other access category criteria types, in particular whether QFI is a suitable parameter, are FFS.

NOTE: An access category criteria type can be associated with more than one access category criteria values. In this case, the access attempt matches the access category if the access criteria for the access attempt matches any of the associated access criteria type values.

If the UE is configured with operator-defined access categories for a PLMN, then access control in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication will only be performed for the events 1) to 5) defined in subclause 12.2.2.1.

Editor's note: Whether access control in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication also needs to be performed when 5GMM receives an indication that an application is started including the OS Id + OS App Id from the upper layers is FFS.

Upon receiving a NAS signalling message with operator-defined access category definitions, the UE shall store the operator-defined access category definitions for the registered PLMN.

#### 12.2.2.4 Access control and checking

Editor's note: it is FFS whether the alleviation of barring is or is not associated with the access category for which barring is alleviated.

##### 12.2.2.4.1 Access control and checking in 5GMM-IDLE mode

When the UE is in 5GMM-IDLE mode, upon receiving a request from the upper layers for an access attempt, the NAS shall categorize the access attempt into access identities and an access category following subclause 12.2.2.2, table 12.2.2.2.1 and table 12.2.2.2.2, and subclause 12.2.2.3, and provide the applicable access identities and the access category to the lower layers for the purpose of access control checking.

NOTE: The access barring check is performed by the lower layers.

Editor's note: Whether the applicable access identities also need to be provided to the lower layers based on other triggers is FFS.

If the lower layers indicate that the access attempt is allowed, the NAS shall initiate the procedure to send the initial NAS message for the access attempt.

If the lower layers indicate that the access attempt is barred, the NAS shall not initiate the procedure to send the initial NAS message for the access attempt. Additionally, if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication, the NAS shall notify the upper layers that the access attempt is barred. Upon receiving an indication from the lower layers that access is granted, the NAS may initiate the procedure to send the initial NAS message, if still needed.

##### 12.2.2.4.2 Access control and checking in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication

When the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication, upon detecting one of events 1) through 5) listed in subclause 12.2.2.1, the NAS shall categorize the corresponding access attempt into access identities and an access category following subclause 12.2.2.2, table 12.2.2.2.1 and table 12.2.2.2.2, and subclause 12.2.2.3, and provide the access identities and the access category to the lower layers for the purpose of access control checking.

Editor's note: Whether one or more applicable access identities also need to be provided to the lower layers based on other triggers is FFS.

If the lower layers indicate that the access attempt is allowed, the NAS shall take the following action depending on the event which triggered the access attempt:

- if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication, the NAS shall notify the upper layers that the access attempt is allowed;

- if the event which triggered the access attempt was a request from upper layers to send a mobile originated SMS over NAS, 5GMM shall initiate the NAS transport procedure as specified in subclause 8.5.1.3 to send the SMS in an UL NAS TRANSPORT message;

- if the event which triggered the access attempt was a request from upper layers to establish a new PDU session, 5GMM shall initiate the NAS transport procedure as specified in subclause 8.5.1.3 to send the PDU SESSION ESTABLISHMENT REQUEST message;

- if the event which triggered the access attempt was a request from upper layers to modify an existing PDU session, 5GMM shall initiate the NAS transport procedure as specified in subclause 8.5.1.3 to send the PDU SESSION MODIFICATION REQUEST message; and

- if the event which triggered the access attempt was a request to re-establish the user plane for an existing PDU session, 5GMM shall initiate the service request procedure as specified in subclause 8.5.3.1.2.

If the lower layers indicate that the access attempt is barred, the NAS shall take the following action depending on the event which triggered the access attempt:

- if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication, the NAS shall notify the upper layers that the access attempt is barred. Upon receiving an indication from the lower layers that access is granted, the NAS shall notify the upper layers that access is granted;

NOTE: In this case prohibiting the initiation of the MMTEL voice session, MMTEL video session or prohibiting sending of the SMS over IP is performed by the upper layers.

- if the event which triggered the access attempt was a request from upper layers to send a mobile originated SMS over NAS, 5GMM shall not initiate the NAS transport procedure as specified in subclause 8.5.1.3 to send the SMS in an UL NAS TRANSPORT message. Upon receiving an indication from the lower layers that access is granted, 5GMM may initiate the NAS transport procedure as specified in subclause 8.5.1.3 to send the SMS in an UL NAS TRANSPORT message, if still needed;

- if the event which triggered the access attempt was a request from upper layers to establish a new PDU session, 5GMM shall not initiate the NAS transport procedure to send the PDU SESSION ESTABLISHMENT REQUEST message. Upon receiving an indication from the lower layers that access is granted, the NAS may initiate the NAS transport procedure as specified in subclause 8.5.1.3, if still needed;

- if the event which triggered the access attempt was a request from upper layers to modify an existing PDU session modification, 5GMM shall not initiate the NAS transport procedure to send the PDU SESSION MODIFICATION REQUEST message. Upon receiving an indication from the lower layers that access is granted, the NAS may initiate the NAS transport procedure as specified in subclause 8.5.1.3, if still needed; and

- if the event which triggered the access attempt was a request to re-establish the user plane for an existing PDU session, the NAS shall not initiate the service request procedure as specified in subclause 8.5.3.1.2. Upon receiving an indication from the lower layers that access is granted, the NAS may initiate the service request procedure as specified in subclause 8.5.3.1.2, if still needed.

#### 12.2.2.5 Exception handling and avoiding double barring

There are several services for which the NAS needs to be informed when the service starts and stops,

- because, while the service is ongoing, the mapping of other access attempts to a specific access category can be affected; and

- in order to avoid double barring at the start of these services.

These services are:

i) emergency service;

ii) MMTEL voice;

iii) MMTEL video;

iv) SMSoIP; and

v) SMS over NAS.

The UE considers an emergency service i) as started when 5GMM receives a request from upper layers to attach for emergency services or to establish a PDU session with request type = "initial emergency request". It considers the emergency service as stopped when this PDU session is released.

While an emergency service i) is ongoing, any access attempt triggered by the initiation of a registration, deregistration or service request procedure is mapped to access category 2 = emergency.

Once the emergency service service has successfully passed access control, then as long as the service is ongoing, the following access attempts are allowed to proceed without further access control checking in order to avoid double barring:

- any service request procedure related to the PDU session associated with request type = "initial emergency request"; and

- any service request or registration procedure initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery.

NOTE 1: Although the access control checking is skipped, the mapping is performed in order to derive an RRC establishment cause.

Editor's note: The need for and the derivation of the RRC establishment cause (or its equivalence in 5GS) requires further work by RAN2.

Editor's note: If MT LCS are used during an emergency service to locate the UE, the 5GMM will transfer LCS messages to the network. It is FFS based on which criteria the UE will determine to skip access control for these messages.

For services ii) to v) the 5GMM receives explicit start and stop indications from the upper layers.

Editor's note: Whether explicit start and stop indications for SMS over NAS need to be defined is FFS.

Once the service has successfully passed access control, then as long as the service is ongoing, the following access attempts are allowed to proceed without further access control checking in order to avoid double barring:

- for services ii), iii) and iv), any service request procedure related to the PDU session established for DNN = "IMS"; and

Editor's note: It has been observed that some operators use an APN different from "IMS" for SMSoIP. How to handle that case when a DNN different from "IMS" is used, is FFS.

- for services ii), iii), iv) and v), any service request or registration procedure initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery.

While an MMTEL voice or video call, or SMS over IMS is ongoing, any of the above access attempts is mapped to access category 5, 6 or 7 respectively.

NOTE 2: Although the access control checking is skipped, the mapping is performed in order to derive an RRC establishment cause.

Editor's note: The need for and the derivation of the RRC establishment cause (or its equivalence in 5GS) requires further work by RAN2.

### 12.2.3 Alternative 3

#### 12.2.3.1 General

5GS supports a unified access control by which each access attempt is categorized into one access category. The network can restrict the access on a per-access category basis according to the requirement specified in 3GPP TS 22.261 [3].

The access attempts for standardized access categories are described in subclause 12.2.3.2.

Handling related to operator specific access categories is described in subclause 12.2.3.2A.

The layers detecting the access attempts are described in subclause 12.2.3.3.

Providing the access category selection assistance information enabling determination of applicability of access category 1 and of access category 2 is described in subclause 12.2.3.4.

Enforcement of unified access control is described in subclause 12.2.3.5.

#### 12.2.3.2 Access attempts for standardized access categories

Editor's note: precedence order among access categories potentially applicable to an access attempt needs to be checked against stage-1.

Access attempts for the standardized access categories are specified in table 12.2.3.2.1 and table 12.2.3.2.2.

Table 12.2.3.2.1: Access attempts started in 5GMM-IDLE mode.

|  |  |  |
| --- | --- | --- |
| **Access category number** | **Access attempt started in 5GMM-IDLE mode** | |
| **Start of the access attempt** | **Stop of the access attempt** |
| 0 | initiation of service request procedure triggered by paging. | completion of the service request procedure triggered by paging. |
| 3 (NOTE 1) | initiation of service request procedure preceding UE-initiated NAS transport of SM message establishing emergency PDU session. | rejection or abortion of the service request procedure preceding UE-initiated NAS transport of SM message establishing emergency PDU session, rejection or abortion of the PDU session establishment procedure establishing the emergency PDU session, or completion of the PDU session release procedure releasing the emergency PDU session. |
| 4 (NOTE 3) | Case 4-I-1) initiation of procedure of an initial 5GMM signalling message except service request and except a registration procedure for the purpose of NAS signalling connection recovery initiated when an access attempt of another access category is ongoing.  Case 4-I-2) initiation of service request procedure preceding 5GMM MO procedure except those identified for other categories. | Case 4-I-1) completion of the procedure of the initial 5GMM signalling message except service request.  Case 4-I-2) rejection or abortion of the service request procedure preceding the 5GMM MO procedure except those identified for other categories, or completion of the 5GMM MO procedure except those identified for other categories. |
| 5 (NOTE 3) | initiation of SIP session of MO MMTEL voice call. | rejection of initiation of SIP session of MO MMTEL voice call, or completion of release of the SIP session of the MO MMTEL voice call. |
| 6 (NOTE 3) | initiation of SIP session of MO MMTEL video call. | rejection of initiation of SIP session of MO MMTEL video call, or completion of release of the SIP session of the MO MMTEL video call. |
| 7 (NOTE 3) | Case 7-I-1) initiation of SIP transaction of MO SMSoIP message.  Case 7-I-2) initiation of service request procedure preceding UE-initiated NAS transport of a MO SMS message. | Case 7-I-1) completion of the SIP transaction of the MO SMSoIP message.  Case 7-I-2) rejection or abortion of the service request procedure preceding the UE-initiated NAS transport of the MO SMS message, or completion of the UE-initiated NAS transport of the MO SMS message. |
| 8 (NOTE 3) | Case 8-I-1) initation of service request procedure due to uplink user data packet to be sent via a non-emergency PDU session other than "IMS" DNN PDU session.  Case 8-I-2) initiation of MO SIP transaction not related to MMTEL and not related to SMSoIP.  Case 8-I-3) initiation of SIP session of MO MMTEL call which is neither MO MMTEL voice call nor MO MMTEL video call.  Case 8-I-4) void.  Case 8-I-5) initiation of service request procedure preceding UE-initiated NAS transport of SM message establishing a non-emergency PDU session other than "IMS" DNN PDU session. | Case 8-I-1) completion of the service request procedure due to uplink user data packet to be sent via a non-emergency PDU session other than "IMS" DNN PDU session.  Case 8-I-2) completion of the MO SIP transaction not related to MMTEL and not related to SMSoIP.  Case 8-I-3) rejection of initiation of SIP session of MO MMTEL call which is neither MO MMTEL voice call nor MMTEL video call, or completion of release of the SIP session of the MO MMTEL call which is neither MO MMTEL voice call nor MMTEL video call.  Case 8-I-4) void.  Case 8-I-5) rejection or abortion of the service request procedure preceding UE-initiated NAS transport of SM message establishing the non-emergency PDU session or completion of the PDU session establishment procedure establishing the non-emergency PDU session other than "IMS" DNN PDU session. |
| NOTE 1: If access category 1 is applicable according to 3GPP TS 22.261 [3], then the access category 1 is used instead of the indicated access category. If access category 2 is applicable according to 3GPP TS 22.261 [3] and access category 1 not applicable according to 3GPP TS 22.261 [3], then the access category 2 is used instead of the indicated access category.  NOTE 2: access categories 9-31 are not shown as they are reserved.  NOTE 3: If access category 1 is applicable according to 3GPP TS 22.261 [3], then the access category 1 is used instead of the indicated access category. If access category 1 is not applicable according to 3GPP TS 22.261 [3], and an operator specific access category is applicable according to subclause 12.2.3.2A, then the applicable operator specific access category is used instead of the indicated access category. If access category 1 is not applicable according to 3GPP TS 22.261 [3], no operator specific access category is applicable according to subclause 12.2.3.2A, and access category 2 is applicable according to 3GPP TS 22.261 [3] then the access category 2 is used instead of the indicated access category.  NOTE 4: completion of a procedure encompasses both the succesful completion of the procedure and the unsuccessful completion (i.e. rejection or abortion) of the procedure. | | |

Table 12.2.3.2.2: Access attempts started in 5GMM-CONNECTED mode with RRC inactive indication and 5GMM-CONNECTED mode.

|  |  |  |
| --- | --- | --- |
| **Access category number** | **Access attempts started in 5GMM-CONNECTED mode with RRC inactive indication and 5GMM-CONNECTED mode** | |
| **Start of the access attempt** | **Stop of the access attempt** |
| 0 | initiation of service request procedure triggered by notification. | completion of the service request procedure triggered by notification. |
| 3 (NOTE 1) | initiation of establishment of the emergency PDU session. | rejection or abortion of the PDU session establishment procedure establishing the emergency PDU session, or completion of the PDU session release procedure releasing the emergency PDU session. |
| 4 (NOTE 3) | initiation of 5GMM MO procedure except those identified for other categories. | completion of the 5GMM MO procedure except those identified for other categories. |
| 5 (NOTE 3) | initiation of SIP session of MO MMTEL voice call. | rejection of initiation of SIP session of MO MMTEL voice call, or completion of release of the SIP session of the MO MMTEL voice call. |
| 6 (NOTE 3) | initiation of SIP session of MO MMTEL video call. | rejection of initiation of SIP session of MO MMTEL video call, or completion of release of the SIP session of the MO MMTEL video call. |
| 7 (NOTE 3) | Case 7-C-1) initiation of SIP transaction of MO SMSoIP message.  Case 7-C-2) initiation of UE-initiated NAS transport of a MO SMS message. | Case 7-C-1) completion of the SIP transaction of the MO SMSoIP message.  Case 7-C-2) completion of the UE-initiated NAS transport of the MO SMS message. |
| 8 (NOTE 3) | Case 8-C-1) initation of service request procedure due to uplink user data packet to be sent via a non-emergency PDU session other than "IMS" DNN PDU session.  Case 8-C-2) initiation of MO SIP transaction not related to MMTEL and not related to SMSoIP.  Case 8-C-3) initiation of SIP session of MO MMTEL call which is neither MO MMTEL voice call nor MO MMTEL video call.  Case 8-C-4) initiation of transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-CONNECTED mode caused by an uplink user data packet to be sent via an activated non-emergency PDU session other than "IMS" DNN PDU session.  Case 8-C-5) initiation of PDU session establishment procedure establishing a non-emergency PDU session other than "IMS" DNN PDU session. | Case 8-C-1) completion of the service request procedure due to uplink user data packet to be sent via a non-emergency PDU session other than "IMS" DNN PDU session.  Case 8-C-2) completion of the MO SIP transaction not related to MMTEL and not related to SMSoIP.  Case 8-C-3) rejection of initiation of SIP session of MO MMTEL call which is neither MO MMTEL voice call nor MMTEL video call, or completion of release of the SIP session of the MO MMTEL call which is neither MO MMTEL voice call nor MMTEL video call.  Case 8-C-4) completion of the transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-CONNECTED mode caused by an uplink user data packet to be sent via an activated non-emergency PDU session other than "IMS" DNN PDU session.  Case 8-C-5) completion of the PDU session establishment procedure establishing the non-emergency PDU session other than "IMS" DNN PDU session. |
| NOTE 1: If access category 1 is applicable according to 3GPP TS 22.261 [3], then the access category 1 is used instead of the indicated access category. If access category 2 is applicable according to 3GPP TS 22.261 [3] and access category 1 not applicable according to 3GPP TS 22.261 [3], then the access category 2 is used instead of the indicated access category.  NOTE 2: access categories 9-31 are not shown as they are reserved.  NOTE 3: If access category 1 is applicable according to 3GPP TS 22.261 [3], then the access category 1 is used instead of the indicated access category. If access category 1 is not applicable according to 3GPP TS 22.261 [3], and an operator specific access category is applicable according to subclause 12.2.3.2A, then the applicable operator specific access category is used instead of the indicated access category. If access category 1 is not applicable according to 3GPP TS 22.261 [3], no operator specific access category is applicable according to subclause 12.2.3.2A, and access category 2 is applicable according to 3GPP TS 22.261 [3] then the access category 2 is used instead of the indicated access category.  NOTE 4: completion of a procedure encompasses both the succesful completion of the procedure and the unsuccessful completion (i.e. rejection or abortion) of the procedure. | | |

#### 12.2.3.2A Operator specific access categories

The serving PLMN can provide operator specific access categorization policy (OSACP) to the UE.

The AMF shall include OSACP into the policy IE of the CONFIGURATION UPDATE COMMAND message and shall set the policy type IE of the CONFIGURATION UPDATE COMMAND message to "operator specific access categorization policy". The AMF shall require a confirmation response in order to ensure that the policy has been updated by the UE.

If the UE receives OSACP in the CONFIGURATION UPDATE COMMAND message, the UE shall shall delete any previously stored OSACP and shall store the received OSACP. The UE shall also delete the stored OSACP upon selection of a PLMN other than the PLMN providing the stored OSACP, and when the UICC containing the USIM is removed.

OSACP consists of OSACP rules.

Each OSACP rule consists of a precedence, a set of criteria and an operator specific access category number (a number from the range 32-63).

Each criteria can be one of the following:

a) the access attempt relates to a PDU session with the requested DNN set to a particular value.

b) the access attempt relates to an particular value of the 5QI of a QoS flow of an uplink user data packet.

Editor's note: Other access category criteria types are FFS.

When deriving an access category for an access attempt assigned to a standardized access category equal to or higher than 4 specified in table 12.2.x.2.1 and table 12.2.x.2.2, the UE evaluates whether the access attempt matches an OSACP rule in the stored OSACP in decreasing order of precedence of the OSACP rules.

If the access attempt matches an OSACP rule, the UE shall stop evaluation and the UE shall consider that the operator specific access category indicated by the operator specific access category number of the OSACP rule is applicable for the access attempt.

If the access attempt matches no OSACP rule, the UE shall consider that no operator specific access category is applicable for the access attempt.

The access attempt matches an OSACP rule if (and only if) all the criteria of the OSACP rule are satisfied.

#### 12.2.3.3 Layers detecting the access attempts

The layers indicated in table 12.2.3.3.1 shall detect the access attempts indicated in table 12.2.3.2.1 and table 12.2.3.2.2.

Table 12.2.3.3.1: Layers detecting access attempts

|  |  |
| --- | --- |
| **Access category number** | **Layer detecting an access attempt** |
| 0 | NAS layer (5GMM entity). |
| 3 (NOTE 1) | NAS layer (5GSM entity). |
| 4 (NOTE 3) | NAS layer (5GMM entity). |
| 5 (NOTE 3) | MMTEL layer. |
| 6 (NOTE 3) | MMTEL layer. |
| 7 (NOTE 3) | SMSoIP layer (case 7-I-1 and case 7-C-1) and NAS layer (5GMM entity) (case 7-I-2 and case 7-C-2). |
| 8 (NOTE 3) | NAS layer (5GMM entity) (for case 8-I-1, case 8-C-1 and case 8-C-4), IMS layer (case 8-I-2 and case 8-C-2), MMTEL layer (for case 8-I-3 and case 8-C-3), and NAS layer (5GSM entity) (case 8-C-5). |
| NOTE 1: If access category 1 is applicable according to 3GPP TS 22.261 [3], then the access category 1 is used instead of the indicated access category. If access category 2 is applicable according to 3GPP TS 22.261 [3] and access category 1 not applicable according to 3GPP TS 22.261 [3], then the access category 2 is used instead of the indicated access category.  NOTE 2: access categories 9-31 are not shown as they are reserved.  NOTE 3: If access category 1 is applicable according to 3GPP TS 22.261 [3], then the access category 1 is used instead of the indicated access category. If access category 1 is not applicable according to 3GPP TS 22.261 [3], and an operator specific access category is applicable according to subclause 12.2.3.2A, then the applicable operator specific access category is used instead of the indicated access category. If access category 1 is not applicable according to 3GPP TS 22.261 [3], no operator specific access category is applicable according to subclause 12.2.3.2A, and access category 2 is applicable according to 3GPP TS 22.261 [3] then the access category 2 is used instead of the indicated access category.. | |

#### 12.2.3.4 Access category selection assistance information

In order to enable determination of applicability of access category 1 and of access category 2 according to 3GPP TS 22.261 [3], the AS layer shall provide to the NAS layer as shown in figure 12.2.3.4.1 an access category selection assistance information consisting of:

a) information whether the access category 1 is applicable to:

1) a UE with access classes 11 configured in UICC;

2) a UE with access classes 12 configured in UICC;

3) a UE with access classes 13 configured in UICC;

4) a UE with access classes 14 configured in UICC;

5) a UE with access classes 15 configured in UICC; or

6) any combination of these; and

b) information whether the access category 2 is applicable to:

1) a UE configured for delay tolerant service and registered in UE’s HPLMN or UE's EHPLMN;

2) a UE configured for delay tolerant service and registered in UEs' most preferred VPLMN;

3) a UE configured for delay tolerant service and registered in a PLMN other than UE’s HPLMN, other than UE's EHPLMN and other than UEs' most preferred VPLMN; or

4) any combination of these.

Figure 12.2.3.4.1: AS - NAS interface for providing access category selection assistance information.

#### 12.2.3.5 Enforcement of unified access control

The AS layer owns barring timers for all the access categories.

When an access attempt is about to start as shown in figure 12.2.3.5.1, the layer indicated in the table 12.2.3.3.1 shall inform the NAS layer about start of the access attempt NAS layer derives an access category for the access attempt and asks the AS layer for authorization for the access category. If not authorized, the layer indicated in the table 12.2.3.3.1 shall block the access attempt. If authorized, the layer indicated in the table 12.2.3.3.1 proceeds with the access attempt.

NOTE: The AS layer does not perform blocking of access attempts indicated in table 12.2.3.2.1 and table 12.2.3.2.2. The AS layer can perform blocking of any AS layer specific access attempts, unrelated to transmission of NAS control plane messages and unrelated to transmission of user data packets, if defined by RAN2.

Figure 12.2.3.5.1: information flow when access attempt is about to start.

When the authorized access attempt is completed as shown in figure 12.2.x.5.2, the layer indicated in the table 12.2.x.3.1 shall inform the NAS layer about completion of the access attempt for the category.



Figure 12.2.x.5.2: information flow when an authorized access attempt stops

The NAS layer shall keep track of access categories with an ongoing authorized access attempt.

Editors' note: FFS whether the NAS uses information about access categories with an ongoing authorized access attempt to derive establishment cause indicated to AS layer when moving from moving from 5GMM-IDLE mode to 5GMM-CONNECTED mode and when moving from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-CONNECTED mode.

## 12.3 Security

### 12.3.1 General

Security for the NAS signalling for 5GS Phase 1 is terminated in the UE and in the AMF. The security protection for the NAS signalling includes ciphering and integrity protection as specified in 3GPP TS 33.501 [24].

Security for the user-plane, as well as for AS signalling, is terminated in the UE and in the NG-RAN.

The keys for NAS signalling security and user-plane security are agreed between the AMF and the UE by means of a primary authentication and key agreement procedure as described in subclause 8.5.1.1.

Authentication and authorization of PDU session establishment to an external DN are performed between the SMF and the UE as described in subclause 9.5.3. The SMF relies on an external DN-AAA server to authenticate and authorize the UE's request for the establishment of a PDU sessions.

### 12.3.2 NAS security mode command

In order to provide NAS signalling security for 5GS there is an NAS security function in both the UE and the AMF which performs integrity/replay protection as well as enciphering/deciphering of NAS signalling messages. This NAS security function is achieved by means of the NAS security mode control procedure as described in subclause 8.5.1.2.

### 12.3.3 5G NAS security context

The security parameters for authentication, integrity protection and ciphering are tied together in a 5G NAS security context and identified by a key set identifier (ngKSI). The relationship between the security parameters is defined in 3GPP TS 33.501 [24].

Before security can be activated, the AMF and the UE need to establish a 5G NAS security context. Usually, the 5G NAS security context is created as the result of a primary authentication and key agreement procedure between the AMF and the UE. Alternatively, during inter-system handover from S1 mode to N1 mode, the AMF and the UE derive a mapped 5G security context from an EPS security context that has been established while the UE was in S1 mode.

The 5G NAS security context is taken into use by the UE and the AMF, when the AMF initiates a NAS security mode control procedure or during the inter-system handover procedure from S1 mode to N1 mode. The 5G NAS security context which has been taken into use by the network most recently is called current 5G NAS security context. This current 5G security context can be of type native or mapped, i.e. originating from a native 5G NAS security context or mapped 5G NAS security context.

The key set identifier ngKSI is assigned by the AMF either during the primary authentication and key agreement procedure procedure or, for the mapped 5G NAS security context, during the inter-system handover procedure. The ngKSI consists of a value and a type of security context parameter indicating whether a 5G NAS security context is a native 5G NAS security context or a mapped 5G NAS security context. When the 5G NAS security context is a native 5G NAS security context, the ngKSI has the value of KSIAMF, and when the current 5G NAS security context is of type mapped, the ngKSI has the value of KSIASME.

## 12.4 Quality of service (QoS)

### 12.4.1 General

Editor's note: The content of this sub-clause has been moved to 3GPP TS 24.501 [17], and therefore this sub-clause is no longer maintained.

#### 12.4.1.1 QoS rules

##### 12.4.1.1.1 General

In a PDU session of IPv4, IPv6, and Ethernet PDU session type, the NAS protocol enables different forwarding treatments of UL user data packets in one or more QoS flows based on signalled QoS rules, derived QoS rules or any combination of them.

In a PDU session of Unstructured PDU session type, all UL user data packets are associated with the same QoS flow.

##### 12.4.1.1.2 Signalled QoS rules

The NAS protocol enables the network to provide the UE with signalled QoS rules associated with a PDU session.

The network can provide the UE with one or more signalled QoS rules associated with a PDU session at the PDU session establishment or at QoS flow establishment.

Each signalled QoS rule contains:

a) an indication of whether the QoS rule is the default QoS rule;

b) a QoS rule identifier (QRI);

c) a QoS flow identifier (QFI);

d) optionally a set of packet filters. If the QoS rule is not the default QoS rule, the set of packet filters is included and contains at least one packet filter for UL direction or at least one packet filter for both UL and DL directions;

e) a precedence value;

f) if the flow is a GBR QoS flow:

1) Guaranteed flow bit rate (GFBR) for UL;

2) Guaranteed flow bit rate (GFBR) for DL;

3) Maximum flow bit rate (MFBR) for UL;

4) Maximum flow bit rate (MFBR) for DL;

5) optionally averaging window for UL; and

6) optionally averaging window for DL; and

g) 5QI, if the QFI is not the same as the 5QI of the QoS flow identified by the QFI; and

h) optionally a EPS bearer identity (EBI), mapped EPS QoS parameters, mapped extended EPS QoS parameters and mapped traffic flow template if the QoS flow can be mapped to an EPS bearer as specified in subclause 4.11.2 of 3GPP TS 23.501 [9].

If the UE requests a new QoS flow, it shall assign a precedence value for the signalled QoS rule which is not in the range from 70 to 99 (decimal).

If the averaging window for UL is not included in a QoS rule for a GBR QoS flow with a 5QI indicated in 3GPP TS 23.501 [9] table 5.7.4-1, the averaging window associated with the 5QI in 3GPP TS 23.501 [9] table 5.7.4-1 applies for the averaging window for UL. If the averaging window for DL is not included in a QoS rule for a GBR QoS flow with a 5QI indicated in 3GPP TS 23.501 [9] table 5.7.4-1, the averaging window associated with the 5QI in 3GPP TS 23.501 [9] table 5.7.4-1 applies for the averaging window for DL.

If the averaging window for UL is not included in a QoS rule for a GBR QoS flow with a 5QI not indicated in 3GPP TS 23.501 [9] table 5.7.4-1, the standardized value of two seconds is used as the averaging window for UL. If the averaging window for DL is not included in a QoS rule for a GBR QoS flow with a 5QI not indicated in 3GPP TS 23.501 [9] table 5.7.4-1, the standardized value of two seconds is used as the averaging window for DL.

Editor's note: The need of the averaging window for DL is FFS.

Within a PDU session:

a) each signalled QoS rule has a unique QRI;

b) there is at least one signalled QoS rule;

c) there can be zero, one or more signalled QoS rules associated with a given QFI; and

d) there can be up to one signalled QoS rule without a set of packet filters.

##### 12.4.1.1.3 Derived QoS rules

The reflective QoS in the UE creates derived QoS rules associated with a PDU session based on DL user data packets received via the PDU session.

Each derived QoS rule contains:

a) a QoS flow identifier (QFI);

b) a packet filter for UL direction; and

c) a precedence value of 80 (decimal).

NOTE: On the network side, the corresponding QoS rule can be associated with a different precedence value in the range from 70 to 99 (decimal).

Within a PDU session:

a) there can be zero, one or more derived QoS rules associated with a given QFI; and

b) there can be up to one derived QoS rule associated with a given packet filter for UL direction.

In the UE, a timer X runs for each derived QoS rule.

Editor’s note: Creation and maintaining of derived QoS rules generates additional requirements for the UE processing capacity. The UE can support only a limited number of concurrent derived QoS rules. Whether the maximum number of concurrent derived QoS rules should be standardized or implementation specific is FFS.

Editor’s note: The UE actions when the maximum number of concurrent derived QoS rules is exceeded (e.g. whether the UE deletes the least used derived QoS rule or stop deriving new QoS rules etc.) is FFS.

#### 12.4.1.2 Session-AMBR

The NAS protocol enables the network to provide the UE with the session-AMBR associated with a PDU session.

The standardized value of two seconds is used as the averaging window for the UE's enforcement of the UL rate limitation indicated by the session-AMBR.

#### 12.4.1.3 UL user data packet matching

Upon receiving an UL user data packet from the upper layers for transmission via a PDU session, the UE shall attempt to associate the UL user data packet with:

a) the QFI of a signalled QoS rule associated with the PDU session which has a set of packet filters containing a packet filter for UL direction matching the UL user data packet or containing a packet filter for both UL and DL directions matching the UL user data packet;

b) the QFI of a derived QoS rule associated with the PDU session which has the packet filter for UL direction matching the UL user data packet; or

c) the QFI of a signalled QoS rule associated with the PDU session which does not have a set of packet filters or has a set of packet filters not containing a packet filter for UL direction and not containing a packet filter for both UL and DL directions;

by evaluating the QoS rules in increasing order of their precedence values until the UL user data packet is associated with a QFI or all QoS rules are evaluated.

If the UL user data packet is associated with a QFI, the UE shall pass the QFI along the UL user data packet to the lower layers for transmission.

NOTE: Marking of the UL user data packet with the QFI is performed by the lower layers.

If all QoS rules are evaluated and the UL user data packet is not associated with a QFI, the UE shall discard the UL user data packet.

#### 12.4.1.4 Reflective QoS

##### 12.4.1.4.1 General

The UE may support reflective QoS.

If the UE supports the reflective QoS, the UE shall support the procedures in the following subclauses.

The reflective QoS is applicable in a PDU session of IPv4, IPv6 and Ethernet PDU session type. The reflective QoS is not applicable in a PDU session of Unstructured PDU session type.

##### 12.4.1.4.2 Derivation of packet filter for UL direction from DL user data packet

The UE shall derive a packet filter for UL direction from a DL user data packet as follows:

a) if the received DL user data packet belongs to a PDU session IPv4 PDU session type, the packet filter for UL direction contains the following packet filter components:

1) an IPv4 remote address component set to the source IP address of the received DL user data packet;

2) an IPv4 local address component set to the destination IP address of the received DL user data packet;

3) a Protocol identifier/Next header type component set to the value of the received protocol type field; and

4) if the received protocol type field indicates a protocol specifying usage of ports:

A) a Single local port type component set to value of the destination port in the received DL user data packet; and

B) a Single remote port type component set to the value of the source port in the received DL user data packet;

b) if the received DL user data packet belongs to a PDU session of IPv6 PDU session type, the packet filter for UL direction contains the following packet filter components:

1) an IPv6 remote address/prefix length component set to the source IP address of the received DL user data packet;

2) an IPv6 local address/prefix length component set to the destination IP address of the received DL user data packet;

3) a Protocol identifier/Next header type component set to the value of the last received next header field; and

4) if the last received next header field indicates a protocol specifying usage of ports:

A) a Single local port type component set to value of the destination port in the received DL user data packet; and

B) a Single remote port type component set to the value of the source port in the received DL user data packet; and

c) if the received DL user data packet belongs to a PDU session of Ethernet PDU session type, the packet filter for UL direction contains the following packet filter components:

1) a destination MAC address component set to the source MAC address of the received DL packet;

2) a source MAC address component set to the destination MAC address of the received DL packet;

3) if an 802.1Q C-TAG is included in the received DL packet, an 802.1Q C-TAG VID component set to the 802.1Q C-TAG VID of the received DL packet and an 802.1Q C-TAG PCP/DEI component set to the 802.1Q C-TAG PCP/DEI of the received DL packet;

4) if an 802.1Q S-TAG is included in the received DL packet, an 802.1Q S-TAG VID component set to the 802.1Q S-TAG VID of the received DL packet and an 802.1Q S-TAG PCP/DEI component set to the 802.1Q S-TAG PCP/DEI of the received DL packet;

5) If the Ethertype field of the received DL packet is set to a value of 1536 or above, an Ethertype component set to the Ethertype of the received DL packet;

6) if the Ethertype field of the Ethernet frame header indicates that the data carried in the Ethernet frame is IPv4 data, the UE shall also add to the packet filter for UL direction IP-specific components based on the contents of the DL user data IP header as described in bullet a) above; and

7) if the Ethertype field of the Ethernet frame header indicates that the data carried in the Ethernet frame is IPv6 data, the UE shall also add to the packet filter for UL direction IP-specific components based on the contents of the DL user data IP header as described in bullet b) above.

##### 12.4.1.4.3 Creating a derived QoS rule by reflective QoS in the UE

If the UE receives a DL user data packet marked with a QFI and an RQI, the DL user data packet belongs to a PDU session of IPv4, IPv6, or Ethernet PDU session type, and the UE does not have a derived QoS rule with the same packet filter for UL direction as the packet filter for UL direction derived from the DL user data packet as specified in subclause 12.4.1.4.2, then the UE shall create a new derived QoS rule as follows:

a) the QFI of the derived QoS rule is set to the received QFI;

b) the precedence value of the derived QoS rule is set to a default standardized precedence value; and

Editor's note: FFS what is the default standardized precedence value.

c) the packet filter for UL direction of the derived QoS rule is set to the derived packet filter for UL direction;

and the UE shall start the timer X associated with the derived QoS rule with the RQ timer value received during the UE-requested PDU session establishment procedure as specified in subclause 9.5.3. If the RQ timer value was not received in the UE-requested PDU session establishment procedure, the default standardized RQ timer value is used.

Editor's note: FFS what is the default standardized RQ timer value.

##### 12.4.1.4.4 fUpdating a derived QoS rule by reflective QoS in the UE

If the UE receives a DL user data packet associated with a QFI and an RQI, the DL user data packet belongs to a PDU session of IPv4, IPv6, or Ethernet PDU session type, and the UE has a derived QoS rule with the same packet filter for UL direction as the packet filter for UL direction derived from the DL user data packet as specified in subclause 12.4.1.4.2, then the UE shall re-start the timer X associated with the derived QoS rule with the RQ timer value received during the UE-requested PDU session establishment procedure as specified in subclause 9.5.3. If the RQ timer value was not received in the UE-requested PDU session establishment procedure, the default standardized RQ timer value is used.

Editor's note: FFS what is the default standardized RQ timer value.

Additionally, if the QFI value associated with the DL user data packet is different from the QFI value stored for the derived QoS rule, then the UE shall replace the QFI value stored for the derived QoS rule with the new QFI value for the derived QoS rule.

##### 12.4.1.4.5 Deleting a derived QoS rule by reflective QoS in the UE

Upon expiration of timer X associated with a derived QoS rule, the UE shall remove the derived QoS rule.

Upon release of the PDU session, the UE shall remove the derived QoS rule(s) associated with the PDU session.

### 12.4.2 QoS coding

#### 12.4.2.1 QoS rules coding

Editor's note: The content of this sub-clause has been moved to 3GPP TS 24.501 [17], and therefore this sub-clause is no longer maintained.

The purpose of the QoS rulesinformation element is to specify the set of parameters that are used by the UE:

- for classification and marking of uplink user traffic; and

- for identification of a QoS flow which the network is to use for a particular downlink user traffic.

NOTE: The UE needs to be aware of a QoS flow which the network is to use for a particular downlink user traffic e.g. to determine whether a resource is available for downlink media of a media stream of an SDP media description provided by the UE in an IMS session.

The QoS rules may contain a set of packet filters consisting of zero or more packet filters for UL direction, zero or more packet filters for DL direction, zero or more packet filters for both UL and DL directions or any combinations of these. The set of packet filters determine the traffic mapping to QoS flows. The QoS rules may contain a EPS bearer identity (EBI), mapped EPS QoS parameters, mapped extended EPS QoS parameters and mapped traffic flow template if the QoS flow can be mapped to an EPS bearer as specified in subclause 4.11.2 of 3GPP TS 23.501 [9].

The QoS *rules* information element is a type 6 information element with a minimum length of 7 octets. The maximum length for the information element is 65538 octets.

The QoS rulesinformation element is coded as shown in figure 12.4.2.1.1 and table 12.4.2.1.1.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | QoS rules IEI | | | | | | | | Octet 1 |
|  | Length of QoS rules IE | | | | | | | | Octet 2 |
|  | Octet 3 |
|  | QoS rule 1 | | | | | | | | Octet 4  Octet u |
|  | QoS rule 2 | | | | | | | | Octet u+1  Octet v |
|  | … | | | | | | | | Octet v+1  Octet w |
|  | QoS rule n | | | | | | | | Octet w+1  Octet x |

Figure 12.4.2.1.1: QoS rules information element

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | | 4 | | 3 | 2 | 1 |  |
|  | QoS rule identifier | | | | | | | | | | Octet 4 |
|  | Length of QoS rule | | | | | | | | | | Octet 5 |
|  | Octet 6 |
|  | Rule operation code | | | | DQR bit | | Number of packet filters | | | | Octet 7 |
|  | Packet filter list | | | | | | | | | | Octet 8\*  Octet z |
|  | 0  Spare | E | Number of parameters | | | | | | | | Octet z+1 |
|  | Parameters list | | | | | | | | | | Octet z+1  Octet u |
|  | QoS rule precedence | | | | | | | | | | Octet u+1\* |
|  | QoS flow identifier | | | | | | | | | | Octet u+2\* |

Figure 12.4.2.1.2: QoS rule

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 0 | 0 | 0 | 0 | Packet filter identifier 1 | | | | Octet 8 |
| Spare | | | |
|  | 0 | 0 | 0 | 0 | Packet filter identifier 2 | | | | Octet 9 |
| Spare | | | |
|  | … | | | | | | | |  |
|  | 0 | 0 | 0 | 0 | Packet filter identifier N | | | | Octet N+3 |
| Spare | | | |

Figure 12.4.2.1.3: Packet filter list when the rule operation is "modify existing QoS rule and delete packet filters" (z=N+3)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 0 | 0 | Packet filter direction 1 | | Packet filter identifier 1 | | | | Octet 8 |
| Spare | |
|  | Length of packet filter contents 1 | | | | | | | | Octet 9 |
|  | Packet filter contents 1 | | | | | | | | Octet 10  Octet m |
|  | 0 | 0 | Packet filter direction 2 | | Packet filter identifier 2 | | | | Octet m+1 |
| Spare | |
|  | Length of packet filter contents 2 | | | | | | | | Octet m+2 |
|  | Packet filter contents 2 | | | | | | | | Octet m+3  Octet n |
|  | … | | | | | | | | Octet n+1  Octet y |
|  | 0 | 0 | Packet filter direction N | | Packet filter identifier N | | | | Octet y+1 |
| Spare | |
|  | Length of packet filter contents N | | | | | | | | Octet y+2 |
|  | Packet filter contents N | | | | | | | | Octet y+3  Octet z |

Figure 12.4.2.1.4: Packet filter list when the rule operation is "create new QoS rule", or "modify existing QoS rule and add packet filters" or "modify existing QoS rule and replace packet filters"

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | Parameter identifier 1 | | | | | | | | Octet z+2 |
|  | Length of Parameter contents 1 | | | | | | | | Octet z+3 |
|  | Parameter contents 1 | | | | | | | | Octet z+4  Octet k |
|  | Parameter identifier 2 | | | | | | | | Octet k+1 |
|  | Length of Parameter contents 2 | | | | | | | | Octet k+2 |
|  | Parameter contents 2 | | | | | | | | Octet k+3  Octet p |
|  | … | | | | | | | | Octet p+1  Octet q |
|  | Parameter identifier N | | | | | | | | Octet q+1 |
|  | Length of Parameter contents N | | | | | | | | Octet q+2 |
|  | Parameter contents N | | | | | | | | Octet q+3  Octet v |

Figure 12.4.2.1.5: Parameters list

Table 12.4.2.1.1: QoS rules information element

|  |
| --- |
| QoS rule identifier (octet 4)  The QoS rule identifier field is used to identify the QoS rule.  QoS rule precedence (octet u+1)  The QoS rule precedence field is used to specify the precedence of the QoS rule among all QoS rules and derived QoS rules associated with the PDU session of the QoS flow. This field includes the binary coded value of the QoS rule precedence in the range from 0 to 255 (decimal). The higher the value of the QoS rule precedence field, the lower the precedence of that QoS rule is.  The value 80 (decimal) is reserved.  QoS flow identifier (octet u+2)  The QoS flow identifier field is used to identify the QoS flow.  DQR bit (bit 5 of octet 7)  The DQR bit indicates whether the QoS rule is the default QoS rule and it is encoded as follows:  Bit  5  0 the QoS rule is not the default QoS rule.  1 the QoS rule is the default QoS rule.  Rule operation code (bits 8 to 6 of octet 7) Bits 8 7 6  0 0 0 Reserved 0 0 1 Create new QoS rule  0 1 0 Delete existing QoS rule  0 1 1 Modify existing QoS rule and add packet filters  1 0 0 Modify existing QoS rule and replace packet filters  1 0 1 Modify existing QoS rule and delete packet filters  1 1 0 Modify existing QoS rule without modifying packet filters  1 1 1 Reserved  E bit (bit 7 of octet z+1)  For the "create new QoS rule" operation, the E bit is encoded as follows:  Bit  7  0 parameters list is not included  1 parameters list is included  For the "modify existing QoS rule and add packet filters" operation, the "modify existing QoS rule and replace packet filters", the "modify existing QoS rule and delete packet filters" operation and the "modify existing QoS rule without modifying packet filters" operation, the E bit is encoded as follows:  Bit  7  0 previously provided parameters list extension  1 previously provided parameters list replacement  If the E bit is set to "parameters list is not included", the number of parameters field has zero value. If the E bit is set to "parameters list is included", the number of parameters field has non-zero value. If the E bit is set to "previously provided parameters list extension" or "previously provided parameters list replacement", the number of parameters field can have zero or non-zero value.  Number of packet filters (bits 4 to 1 of octet 7  The number of packet filters contains the binary coding for the number of packet filters in the packet filter list. The number of packet filters field is encoded in bits 4 through 1 of octet 7 where bit 4 is the most significant and bit 1 is the least significant bit. For the "delete existing QoS rule" operation and for the "modify existing QoS rule without modifying packet filters" operation, the number of packet filters shall be coded as 0. For the "create new QoS rule" operation and the "modify existing QoS rule and replace packet filters" operation, the number of packet filters shall be greater than or equal to 0 and less than or equal to 15. For all other operations, the number of packet filters shall be greater than 0 and less than or equal to 15.  Packet filter list (octets 8 to z)  The packet filter list contains a variable number of packet filters.  For the "delete existing QoS rule" operation, the length of QoS rule field is set to one.  For the "delete existing QoS rule" operation and the "modify existing QoS rule without modifying packet filters" operation, the packet filter list shall be empty.  For the "modify existing QoS rule and delete packet filters" operation, the packet filter list shall contain a variable number of packet filter identifiers. This number shall be derived from the coding of the number of packet filters field in octet 7.  For the "create new QoS rule" operation and for the "modify existing QoS rule and replace packet filters" operation, the packet filter list shall contain 0 or a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.  For the "modify existing QoS rule and add packet filters" operation, the packet filter list shall contain a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.  Each packet filter is of variable length and consists of  a packet filter direction (2 bits);  - a packet filter identifier (4 bits);  - the length of the packet filter contents (1 octet); and - the packet filter contents itself (variable amount of octets).  The packet filter direction field is used to indicate for what traffic direction the filter applies.  Bits  6 5  0 0 reserved  0 1 downlink only  1 0 uplink only  1 1 bidirectional (see NOTE 1)  The packet filter identifier field is used to identify each packet filter in a QoS rule. The least significant 4 bits are used.  The length of the packet filter contents field contains the binary coded representation of the length of the packet filter contents field of a packet filter. The first bit in transmission order is the most significant bit.  The packet filter contents field is of variable size and contains a variable number (at least one) of packet filter components. Each packet filter component shall be encoded as a sequence of a one octet packet filter component type identifier and a fixed length packet filter component value field. The packet filter component type identifier shall be transmitted first.  In each packet filter, there shall not be more than one occurrence of each packet filter component type. Among the "IPv4 remote address type" and "IPv6 remote address/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "IPv4 local address type" and "IPv6 local address/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "single local port type" and "local port range type" packet filter components, only one shall be present in one packet filter. Among the "single remote port type" and "remote port range type" packet filter components, only one shall be present in one packet filter.  The term local refers to the UE and the term remote refers to an external network entity.  Packet filter component type identifier Bits 8 7 6 5 4 3 2 1  0 0 0 1 0 0 0 0 IPv4 remote address type 0 0 0 1 0 0 0 1 IPv4 local address type  0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type 0 0 1 0 0 0 1 1 IPv6 local address/prefix length type 0 0 1 1 0 0 0 0 Protocol identifier/Next header type 0 1 0 0 0 0 0 0 Single local port type 0 1 0 0 0 0 0 1 Local port range type 0 1 0 1 0 0 0 0 Single remote port type  0 1 0 1 0 0 0 1 Remote port range type 0 1 1 0 0 0 0 0 Security parameter index type 0 1 1 1 0 0 0 0 Type of service/Traffic class type 1 0 0 0 0 0 0 0 Flow label type  1 0 0 0 0 0 0 1 Destination MAC address type 1 0 0 0 0 0 1 0 Source MAC address type 1 0 0 0 0 0 1 1 802.1Q C-TAG VID type 1 0 0 0 0 1 0 0 802.1Q S-TAG VID type 1 0 0 0 0 1 0 1 802.1Q C-TAG PCP/DEI type 1 0 0 0 0 1 1 0 802.1Q S-TAG PCP/DEI type 1 0 0 0 0 1 1 1 Ethertype type  All other values are reserved.  The description and valid combinations of packet filter component type identifiers in a packet filter are defined in 3GPP TS 23.501 [9].  For "IPv4 remote address type", the packet filter component value field shall be encoded as a sequence of a four octet IPv4 address field and a four octet IPv4 address mask field. The IPv4 address field shall be transmitted first.  For "IPv4 local address type", the packet filter component value field shall be encoded as defined for "IPv4 remote address type".  For "IPv6 remote address/prefix length type", the packet filter component value field shall be encoded as a sequence of a sixteen octet IPv6 address field and one octet prefix length field. The IPv6 address field shall be transmitted first.  For "IPv6 local address/prefix length type", the packet filter component value field shall be encoded as defined for "IPv6 remote address /prefix length".  For "protocol identifier/Next header type", the packet filter component value field shall be encoded as one octet which specifies the IPv4 protocol identifier or IPv6 next header.  For "single local port type" and "single remote port type", the packet filter component value field shall be encoded as two octet which specifies a port number.  For "local port range type" and "remote port range type", the packet filter component value field shall be encoded as a sequence of a two octet port range low limit field and a two octet port range high limit field. The port range low limit field shall be transmitted first.  For "security parameter index", the packet filter component value field shall be encoded as four octets which specifies the IPSec security parameter index.  For "type of service/traffic class type", the packet filter component value field shall be encoded as a sequence of a one octet type-of-service/traffic class field and a one octet type-of-service/traffic class mask field. The type-of-service/traffic class field shall be transmitted first.  For "flow label type", the packet filter component value field shall be encoded as three octets which specifies the IPv6 flow label. The bits 8 through 5 of the first octet shall be spare whereas the remaining 20 bits shall contain the IPv6 flow label.  For "destination MAC address type" and "source MAC address type", the packet filter component value field shall be encoded as 6 octets which specify a MAC address.  For "802.1Q C-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the customer-VLAN tag (C-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.  For "802.1Q S-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the service-VLAN tag (S-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.  For "802.1Q C-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q C-TAG PCP and DEI. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.  For "802.1Q S-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q S-TAG PCP. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.  For "ethertype type", the packet filter component value field shall be encoded as two octets which specify an ethertype.  Number of parameters (bits 6 to 1 of octet z+1)  The number of parameters field contains the binary coding for the number of parameters in the parameters list field. The number of parameters field is encoded in bits 6 through 1 of octet z+1 where bit 6 is the most significant and bit 1 is the least significant bit.  Parameters list (octets z+2 to v)  The parameters list contains a variable number of parameters.  Each parameter included in the parameters list is of variable length and consists of:  - a parameter identifier (1 octet);  - the length of the parameter contents (1 octet); and - the parameter contents itself (variable amount of octets).  The parameter identifier field is used to identify each parameter included in the parameters list and it contains the hexadecimal coding of the parameter identifier. Bit 8 of the parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following parameter identifiers are specified:  - 01H (5QI); - 02H (GFBR uplink);  - 03H (GFBR downlink);  - 04H (MFBR uplink);  - 05H (MFBR downlink);  - 06H (Averaging window for uplink);  - 07H (Averaging window for downlink);  08H (EPS bearer identity);  - 09H (Mapped EPS QoS parameters);  - 10H (Mapped extended EPS QoS parameters); and  - 11H (Traffic flow template).  If the parameters list contains a parameter identifier that is not supported by the receiving entity the corresponding parameter shall be discarded.  The length of parameter contents field contains the binary coded representation of the length of the parameter contents field. The first bit in transmission order is the most significant bit.  When the parameter identifier indicates 5QI, the parameter contents field contains the binary representation of 5G QoS identifier (5QI) that is one octet in length.  5QI:  Bits  8 7 6 5 4 3 2 1  In network to UE direction:  0 0 0 0 0 0 0 0 Reserved  0 0 0 0 0 0 0 1 5QI 1  0 0 0 0 0 0 1 0 5QI 2  0 0 0 0 0 0 1 1 5QI 3  0 0 0 0 0 1 0 0 5QI 4  0 0 0 0 0 1 0 1 5QI 5  0 0 0 0 0 1 1 0 5QI 6  0 0 0 0 0 1 1 1 5QI 7  0 0 0 0 1 0 0 0 5QI 8  0 0 0 0 1 0 0 1 5QI 9  0 0 0 0 1 0 1 0  to Spare  0 1 0 0 0 0 0 0  0 1 0 0 0 0 0 1 5QI 65  0 1 0 0 0 0 1 0 5QI 66  0 1 0 0 0 0 1 1  to Spare  0 1 0 0 0 1 0 0  0 1 0 0 0 1 0 1 5QI 69  0 1 0 0 0 1 1 0 5QI 70  0 1 0 0 0 1 1 1  to Spare  0 1 0 0 1 0 1 0  0 1 0 0 1 0 1 1 5QI 75  0 1 0 0 1 1 0 0  to Spare  0 1 0 0 1 1 1 0  0 1 0 0 1 1 1 1 5QI 79  0 1 0 1 0 0 0 0  to Spare  0 1 1 1 1 1 1 1  1 0 0 0 0 0 0 0  to Operator-specific 5QIs  1 1 1 1 1 1 1 0  1 1 1 1 1 1 1 1 Reserved  The network shall consider all other values not explicitly defined in this version of the protocol as unsupported.  If the UE receives a 5QI value (excluding the reserved 5QI values) that it does not understand, the UE shall choose a 5QI value from the set of 5QI values defined in this version of the protocol (see 3GPP TS 23.501 [9]) and associated with:  - GBR QoS flows, if the QoS flow includes a GFBR uplink parameter and a GFBR dowlinkink parameter; and  - non-GBR QoS flows, if the QoS flow does not include a GFBR uplink parameter or does not include a GFBR downlink parameter.  The UE shall use this chosen 5QI value for internal operations only. The UE shall use the received 5QI value in subsequent NAS signalling procedures.  When the parameter identifier indicates "GFBR uplink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for uplink followed by two octets containing the value of the guaranteed flow bit rate for uplink.  Unit of the guaranteed flow bit rate for uplink (octet 1):  Bits  8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 0 0 value is not used  0 0 0 0 0 0 0 0 1 value is incremented in multiples of 1 Kbps  0 0 0 0 0 0 0 1 0 value is incremented in multiples of 4 Kbps  0 0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps  0 0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps  0 0 0 0 0 0 1 0 1 value is incremented in multiples of 256 Kbps  0 0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps  0 0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps  0 0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps  0 0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps  0 0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps  0 0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps  0 0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps  0 0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps  0 0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps  0 0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps  0 0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps  0 0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps  0 0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps  0 0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps  0 0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps  0 0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps  0 0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps  0 0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps  0 0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps  0 0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps  Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol.  Value of the guaranteed flow bit rate for uplink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for uplink in units defined by the unit of the guaranteed flow bit rate for uplink.  When the parameter identifier indicates "GFBR downlink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for downlink followed by two octets containing the value of the guaranteed flow bit rate for downlink.  Unit of the guaranteed flow bit rate for downlink (octet 1):  The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.  Value of the guaranteed flow bit rate for downlink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for downlink in units defined by the unit of the guaranteed flow bit rate for downlink.  When the parameter identifier indicates "MFBR uplink", the parameter contents field contains the one octet indicating the unit of the maximum flow bit rate for uplink followed by two octets containing the value of maximum flow bit rate for uplink.  Unit of the maximum flow bit rate for uplink (octet 1):  The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.  Value of the maximum flow bit rate for uplink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for uplink in units defined by the unit of the maximum flow bit rate for uplink.  When the parameter identifier indicates "MFBR downlink", the parameter contents field contains one octet indicating the unit of the maximum flow bit rate for downlink followed by two octets containing the value of the maximum flow bit rate for downlink.  Unit of the maximum flow bit rate for downlink (octet 1):  The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.  Value of the maximum flow bit rate for downlink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for downlink in units defined by the unit of the maximum flow bit rate for downlink.  When the parameter identifier indicates "averaging window for uplink", the parameter contents field contains the binary representation of the averaging window for uplink in milliseconds and the parameter contents field is two octets in length.  When the parameter identifier indicates "averaging window for downlink", the parameter contents field contains the binary representation of the averaging window for downlink in milliseconds and the parameter contents field is two octets in length.  When the parameter identifier indicates EPS bearer identity, the length of EPS bearer identity is one octet and parameter contents field is coded as specified in subclause 9.3.2 of 3GPP TS 24.301 [15] (see NOTE 2).  When the parameter identifier indicates mapped EPS QoS parameters, the length and parameter contents field are coded as specified in subclause 9.9.4.3 of 3GPP TS 24.301 [15].  When the parameter identifier indicates mapped extended EPS QoS parameters, the length and parameter contents field are coded as specified in subclause 9.9.4.30 of 3GPP TS 24.301 [15].  When the parameter identifier indicates traffic flow template, the length and parameter contents field are coded from octet 2 as shown figure 10.5.144 and table 10.5.162 of 3GPP TS 24.008 [12]. |
| NOTE 1: A packet filter with the "bidirectional" packet filter direction is used both as a packet filter with the "downlink only" packet filter direction and a packet filter with the "uplink only" packet filter direction.  NOTE 2: The total number of EPS bearer identities included in all QoS rules of a UE cannot exceed eleven. |

#### 12.4.2.2 Session-AMBR coding

Editor's note: The content of this sub-clause has been moved to 3GPP TS 24.501 [17], and therefore this sub-clause is no longer maintained.

The purpose of the Session-AMBR information element is to indicate the initial subscribed PDU session aggregate maximum bit rate when the UE establishes a PDU session or to indicate the new subscribed PDU session aggregate maximum bit rate if it is changed by the network.

The Session-AMBR information element is coded as shown in figure 12.4.2.2.1 and table 12.4.2.2.1.

The Session-AMBR is a type 4 information element with a length of 8 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Session-AMBR IEI | | | | | | | | octet 1 |
| Length of Session-AMBR contents | | | | | | | | octet 2 |
| Unit for Session-AMBR for downlink | | | | | | | | octet 3 |
| Session-AMBR for downlink | | | | | | | | octet 4-5 |
| Unit for Session-AMBR for uplink | | | | | | | | octet 6 |
| Session-AMBR for uplink | | | | | | | | octet 7-8 |

Figure 12.4.2.2.1: Session-AMBR information element

Table 12.4.2.2.1: Session-AMBR information element

|  |
| --- |
| Unit for Session-AMBR for downlink (octet 3)  0 0 0 0 0 0 0 0 value is not used  0 0 0 0 0 0 0 1 value is incremented in multiples of 1 Kbps  0 0 0 0 0 0 1 0 value is incremented in multiples of 4 Kbps  0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps  0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps  0 0 0 0 0 1 0 1 value is incremented in multiples of 256 kbps  0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps  0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps  0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps  0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps  0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps  0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps  0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps  0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps  0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps  0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps  0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps  0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps  0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps  0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps  0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps  0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps  0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps  0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps  0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps  0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps  Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol.  Session-AMBR for downlink (octets 4 and 5)  Octets 4 and 5 represent the binary coded value of PDU session aggregated maximum bit rate for downlink in units defined by octet 3.  Unit for Session-AMBR for uplink (octet 6)  The coding is identical to the unit coding defined for Session-AMBR for downlink (octet 3)  Session-AMBR for uplink (octets 7 and 8)  Octets 7 and 8 represent the binary coded value of PDU session aggregated maximum bit rate for uplink in units defined by octet 6. |

## 12.5 IM CN subsystem

### 12.5.1 IMS voice over PS Session supported Indication

The network informs the UE about the support of IMS voice over PS session during the registration procedure. In a UE with IMS voice over PS session capability, the IMS voice over PS session indicator (IMS VoPS) shall be provided to the upper layers. When initiating a voice call, the upper layers take the IMS voice over PS session support indicator into account for the access domain selection.

During the registration procedure the AMF includes the IMS voice over PS session supported indicator in the REGISTRATION ACCEPT message (see subclause 8.5.1.1).

Editor’s note: The emergency PDU session service support indicator needs to be aligned with the stage 2 as soon as procedural requirements are in place.

Editor’s note: The emergency service support indicator needs to be added in the subclause 8.5.2.1.

Editor’s note: It is FFS in which information element of the REGISTRATION ACCEPT message the emergency service support indicator is included.

When indicating support of IMS voice over PS session to the UE, the AMF should take into account the following factors:

1) the local policy of the PLMN to which the AMF belongs;

2) the capabilities of the network including: IMS voice over PS session capability of 5GCN and EPC, IMS voice over PS session capability of NR connected to 5GCN, IMS voice over PS session capability of E-UTRA connected to 5GCN, PS handover to E-UTRA connected to 5GCN capability of NR connected to 5GCN, and PS handover to E-UTRA connected to EPC capability of NR connected to 5GCN;

3) the capabilities of the UE including: PS handover to E-UTRAN capability; and

4) the roaming agreement between the VPLMN and the HPLMN.

### 12.5.2 P-CSCF address delivery

When the UE requests to establish a PDU session, which can be used for IMS services, the UE includes in the ePCO IE contained in the PDU SESSION ESTABLISHMENT REQUEST message (see subclause 9.6.3) the request for P-CSCF IPv4 address or P-CSCF IPv6 address or both. The AMF forwards the ePCO IE transparently via N11 interface towards the SMF.

When receiving an 5GSM request message containing a P-CSCF address request on the N11 interface, the SMF includes the locally configured P-CSCF address(es) in the ePCO IE of the corresponding 5GSM response message.

## 12.6 Network sharing

Within the 5GS, a single network can be shared by multiple participating operators. The shared network includes the NG-RAN and the shared resources include radio resources.

In a shared network, the UE shall choose one of the PLMN identifiers as specified in 3GPP TS 23.122 [7].

Editor's note: It is expected that 3GPP TS 23.122 is updated to refer 3GPP TS 38.304 in describing that the AS indicates multiple PLMN identifiers to the NAS in case of a shared NG-RAN.

In case of a shared network, one or more TACs and multiple PLMN identifiers are broadcast and the UE shall construct the TAI of the cell from the chosen PLMN identifier and the TAC associated with the chosen PLMN identifier, if needed.

Editor's note: The above paragraph can be modified according to the information broadcast by a shared NG-RAN.

## 12.7 Congestion and overload control

### 12.7.1 Handling of NAS level mobility management congestion control

The AMF may detect 5GMM signalling congestion and perform General NAS level congestion control. Under the 5GMM signalling congestion conditions the AMF may reject 5GMM signalling requests from UEs as specified in 3GPP TS 23.501 [9]. The AMF should not reject the following request:

- requests for emergency services; and

- requests from UEs configured to use AC11 – 15 in selected PLMN.

When General NAS level congestion control is active, the AMF may include a value for the mobility management back-off timer T3346 in the reject messages. The UE starts the timer T3346 with the value received in the 5GMM reject messages. To avoid that large numbers of UEs simultaneously initiate deferred requests, the AMF should select the value for the timer T3346 for the rejected UEs so that timeouts are not synchronised.

If the timer T3346 is running when the UE enters state 5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then the timer T3346 is kept running until it expires or it is stopped.

If the UE is switched off when the timer T3346 is running, the UE shall behave as follows when the UE is switched on and the USIM in the UE remains the same:

- let t1 be the time remaining for T3346 timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

Editor's note: Whether dual priority is supported in 5GS and how it is handled in the NAS level 5GMM congestion control are FFS.

If the UE enters a new PLMN while timer T3346 is running, and the new PLMN is not equivalent to the PLMN where the UE started timer T3346, the UE shall stop timer T3346 when initiating 5GMM procedures in the new PLMN.

### 12.7.2 Handling of DNN based congestion control

The network may detect and start performing DNN based congestion control when one or more DNN congestion criteria as specified in 3GPP TS 23.501 [9] are met. The network may store a DNN congestion back-off timer on a per UE and congested DNN basis. If the UE does not provide a DNN for a non-emergency PDU session, then the SMF uses the selected DNN.

In the UE, 5GS session management timers T35ab for DNN based congestion control are started and stopped on a per DNN basis.

In case the timer T35ab is provided during the PDU session establishment procedure, the DNN associated with T35ab is the DNN provided by the UE when the PDU session is established. If no DNN is provided by the UE along the PDU SESSION ESTABLISHMENT REQUEST, then T35ab is associated with no DNN. For this purpose the UE shall memorize the DNN provided to the network during the PDU session establishment. The timer T35ab associated with no DNN will never be started due to any 5GSM procedure related to an emergency PDU session. If the timer T35ab associated with no DNN is running, it does not affect the ability of the UE to request an emergency PDU session.

In case the timer T35ab is provided during the UE-requested PDU session modification procedure or the network-requested PDU session release procedure, the DNN associated with T35ab is the DNN associated with the PDU session corresponding to the 5GSM procedure.

If T35ab is running or is deactivated, and the UE is a UE configured to use AC11 – 15 in selected PLMN, then the UE is allowed to initiate 5GSM session management procedure for the respective DNN.

Editor's note: How to capture the aspect of Group specific NAS level congestion control is FFS.

### 12.7.3 Handling of S-NSSAI based congestion control

The network may detect and start performing S-NSSAI based congestion control when one or more S-NSSAI congestion criteria as specified in 3GPP TS 23.501 [9] are met. The network may store a S-NSSAI congestion back-off timer on a per UE, S-NSSAI, and DNN basis. If the UE does not provide a DNN for a non-emergency PDU session, then the SMF uses the selected DNN.

In the UE, 5GS session management timers T35cd for the S-NSSAI based congestion control are started and stopped on a per DNN and S-NSSAI basis.

In case the timer T35cd is provided during the PDU session establishment procedure, the S-NSSAI associated with T35cd is the S-NSSAI provided by the UE when the PDU session is established. The DNN associated with T35cd is the DNN provided by the UE when the PDU session is established. If no DNN is provided by the UE along the PDU SESSION ESTABLISHMENT REQUEST, then T35cd is associated with no DNN and S-NSSAI provided to the network during the PDU session establishment. For this purpose the UE shall memorize the DNN and S-NSSAI provided to the network during the PDU session establishment. The timer T35cd associated with no DNN and an S-NSSAI will never be started due to any 5GSM procedure related to an emergency PDU session. If the timer T35cd associated with no DNN and a S-NSSAI is running, it does not affect the ability of the UE to request an emergency PDU session.

In case the timer T35cd is provided during the UE-requested PDU session modification procedure or the network-requested PDU session release procedure, the S-NSSAI and DNN associated with T35cd are the S-NSSAI and DNN associated with the PDU session corresponding to the 5GSM procedure.

If T35cd is running or is deactivated, and the UE is a UE configured to use AC11 – 15 in selected PLMN, then the UE is allowed to initiate 5GSM session management procedure for the respective DNN and an S-NSSAI.

Editor's note: How to capture the aspect of Group specific NAS level congestion control is FFS.

Editor's note: S-NSSAI based congestion control by AMF is FFS.

## 12.8 Charging

The charging architecture and functionalities for 5GS Phase 1 are studied in 3GPP TR 32.899 [23]. Network slicing aspects and provisioning for 5GS Phase 1 are captured in 3GPP TS 28.530 [20] and 3GPP TS 28.531 [21].

At present, no 5GS Phase 1 charging reqjuirements to NAS protocols have been identified but are not excluded.

NOTE: Charging aspects for 5GS Phase 1 which can impact NAS protocols has to be considered and depend on SA5 work but currently not outlined in 3GPP TS 28.530, 3GPP TS 28.531 or 3GPP TR 32.899.

## 12.9 Mission critical services

3GPP TS 23.501 [9] specifies that a mission critical service (MCS) requires a subscription in place for both 5G QoS profile and the necessary policies. The standardized 5QI values 65, 69 and 70 are mapped to QoS characteristics for MCS (see 3GPP TS 23.501 [9] subclause 5.7.4).

When the network needs to provide the UE with signalled QoS rules that includes a 5QI associated with a PDU session for MCS, a standardized 5QI value may be used for MCS (see sub-clause 12.4.2.1).

# 13 Network slicing

## 13.1 General

The 5GS supports network slicing as described in 3GPP TS 23.501 [9]. Within a PLMN, a network slice is identified by an S-NSSAI, which is comprised of a slice/service type (SST) and a slice differentiator (SD). Inclusion of an SD in an S-NSSAI is optional. A set of one or more S-NSSAIs is called the NSSAI. There are multiple types of NSSAI (see 3GPP TS 23.501 [9]):

- configured NSSAI;

- requested NSSAI;

- allowed NSSAI;

- subscribed NSSAI;

- temporarily rejected NSSAI for the current PLMN;

- permanently rejected NSSAI for the current PLMN.

- temporarily rejected NSSAI for the current PLMN and registration area combination; and

- permanently rejected NSSAI for the current PLMN and registration area combination.

The HPLMN may configure a UE with the configured NSSAI per PLMN.

Editor's note: Terms on network slicing can be revisited.

## 13.2 Mobility management aspects

### 13.2.1 General

Upon registration to a PLMN, the UE shall send to the AMF the requested NSSAI including one or more S-NSSAIs corresponding to the slice(s) to which the UE wishes to register if the UE has a configured NSSAI and/or an allowed NSSAI for the PLMN according to the rules defined in 3GPP TS 23.501 [9]. The UE NAS shall also provide the lower layers with the requested NSSAI, if available. If the UE has neither a configured NSSAI nor an allowed NSSAI for a PLMN, the UE does not send a requested NSSAI when requesting registration towards the PLMN. In roaming scenarios the requested NSSAI, included in the REGISTRATION REQUEST message shall include only the S-NSSAI values that are valid in the VPLMN. The AMF verifies if the requested NSSAI is permitted based on the subscribed NSSAI in the UE subscription, and if so then the AMF may provide the UE with the allowed NSSAI for the PLMN. The AMF may also query the NSSF to determine the allowed NSSAI for a given registration area. See subclause 8.5.2.2for further details.

The set of network slice(s) for a UE can be changed at any time while the UE is registered to a PLMN, and may be initiated by the network, or the UE. In this case, the allowed NSSAI and associated registration area may be changed during the registration procedure. The network may notify the UE of the change of the supported network slice(s) in order to trigger the registration procedure. Change in the allowed NSSAI may lead to AMF relocation subject to operator policy.

A single UE can be served by at most eight slices at a time. Multiple instances of S-NSSAI may be deployed in a given registration area; each of the network slice instance can correspond to one or more S-NSSAIs in the allowed NSSAI. The AMF is common across multiple such slice instances.

Editor's note: The subclause for the notification procedure will be included in the TR and the subclause will be referred.

### 13.2.2 NSSAI storage

Each of the configured NSSAI, allowed NSSAI, temporarily rejected NSSAI(s), and permanently rejected NSSA(s)I is a set composed of at most 8 S-NSSAIs associated with a PLMN identity. The S-NSSAI(s) in the temporarily rejected NSSAI for the current PLMN and registration area combination and permanently rejected NSSAI for the current PLMN and registration area combination may be further associated with a registration area where the rejected S-NSSAI is not available. There shall be no duplicated PLMN identities in each of the list of configured NSSAI(s), allowed NSSAI(s) , temporarily rejected NSSAI(s), and permanently rejected NSSAI(s).

If available, the configured NSSAI(s), allowed NSSAI(s) , temporarily rejected NSSAI(s), and permanently rejected NSSAI(s) shall be stored in a non-volatile memory in the ME together with the SUPI from the USIM per PLMN. Those NSSAIs can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME; else the UE shall delete them.

The UE stores (S-)NSSAIs as follows:

The configured NSSAI shall be stored until a new configured NSSAI is received for a given PLMN. When provisioned with a new configured NSSAI for a PLMN, the UE shall replace any stored configured NSSAI for this PLMN with the new configured NSSAI, and delete any stored allowed NSSAI, temporarily rejected NSSAI(s), and permanently rejected NSSAI(s) for the current PLMN.

The allowed NSSAI shall be stored, including when the UE is switched off, until a new allowed NSSAI is received for a given PLMN. When a new allowed NSSAI for a PLMN is received, the UE shall replace any stored allowed NSSAI for the current PLMN with this new allowed NSSAI.

When the UE receives the S-NSSAI(s) included in rejected NSSAI in the REGISTRATION ACCEPT message, the UE shall store the S-NSSAI(s) into temporarily rejected NSSAI(s) or permanently rejected NSSAI based on the associated rejection cause(s). Once the UE is deregistered, the temporarily rejected NSSAI(s) and permanently rejected NSSAI(s) for the current PLMN shall be deleted.

Editor's note: Other conditions when the UE shall delete S-NSSAI(s) from temporarily rejected NSSAI are FFS.

The network may provide to the UE mapping information as to how the S-NSSAI(s) in the allowed NSSAI maps to S-NSSAI(s) in the configured NSSAI in the UE. The UE shall store this mapping information in the ME and use this information for creating appropriate PDU requests.

Editor’s note: The content of the mapping information as to how a particular S-NSSAI in the allowed NSSAI maps to a S-NSSAI in the configured NSSAI in the UE, and how it is conveyed to the UE, are FFS.

## 13.3 Session management aspects

### 13.3.1 General

In order to enable PDU transmission in a network slice, the UE may request establishment of a PDU session in a network slice towards a data network (DN) which is associated with an S-NSSAI and a data network name (DNN) if there is no established PDU session adequate for the PDU transmission. The S-NSSAI included is part of allowed NSSAI and in roaming scenarios the S-NSSAI value is valid in VPLMN. See subclause 9.5.3 for further details. The UE determines whether to establish a new PDU session or use one of the established PDU session(s) based on NSSP.

### 13.3.2 NSSP

NSSP is a set of one or more NSSP rules, where an NSSP rule is either:

1) a non-default NSSP rule including:

A) an application identifier;

B) an S-NSSAI and/or a DNN; and

C) a precedence value of the NSSP rule; or

2) a default NSSP rule including an S-NSSAI and/or a DNN.

Only one NSSP rule in NSSP can be a default NSSP rule. If a default NSSP rule and one or more non-default NSSP rules are included in NSSP, any non-default NSSP rule shall be prioritized over the default NSSP rule.

Editor's note: Coding of the NSSP rule is FFS.

When a PDU from an application needs to be transmitted and there exists an NSSP rule matching the application (including a default NSSP rule):

1) if there exists a PDU session associated with S-NSSAI and/or DNN in the NSSP rule, the UE shall transmit the PDU via the PDU session; or

2) otherwise, the UE establishes a PDU session with the S-NSSAI and/or DNN in the NSSP rule in case other conditions do not prohibits the UE from the PDU session establishment.

The HPLMN may provision the UE with NSSP. The NSSP shall be stored in a non-volatile memory in the ME together with the SUPI from the USIM. The NSSP shall be stored until new NSSP are provisioned by HPLMN or the USIM is removed. The NSSP can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME; else the UE shall delete them.

Editor's note: Whether the generic UE configuration update procedure can be used to provision NSSP is FFS.

# 14 Conclusions and recommendations

## 14.1 Work plan and procedures

CT1 have reached the following agreements with regard to the work plan and procedures to be used for the start of the normative phase of 5GS:

1. New TSs are started for the specification work as described in Annex A.1.

2. The rapporteurs of new TSs are tasked to provide a mapping proposal of the sections from 3GPP TR 24.890 or any other applicable TS to the new TSs. The agreed mapping proposals will be documented in the TR.

3. The rapporteurs will produce new reference versions of the new TSs based on agreed mapping proposals which will then be used for CT1 as the reference versions for contributions.

4. Impacts to existing specifications are described in Annex A.2.

5. Updates to existing specifications stored in 3GPP TR 24.890 will be transferred to appropriate TSs.

6. CT1 will not continue maintaining material in 3GPP TR 24.890 which is transferred to new or existing TSs to avoid duplication of documentation and work. Material transferred out of 3GPP TR 24.890 will be marked by means of editor’s note to indicate that has been moved and no longer maintained in the TR

7. No new study work would be added to 3GPP TR 24.890 after its approval. Exceptionally, unresolved contentious issues in 3GPP TR 24.890 could continue being worked till the next 3GPP TSG CT plenary meeting after approval.

## 14.2 Alternatives on NAS transport mechanism

CT1 have studied two alternatives for the NAS transport mechanism as described in subclause 8.5.1.3.2 and 8.5.1.3.3. CT1 have done an evaluation of the alternatives as documented in subclause 8.5.1.3.4 and 8.5.1.3.5. CT1 have decided to select the alternative 2 as the NAS transport mechanism to be used (see subclause 8.5.1.3.6).

## 14.3 Mapping to 3GPP TS 24.501

The table 14.3.1 identifies the mapping of sections from 3GPP TR 24.890 to 3GPP TS 24.501 [17].

Table 14.3.1: Mapping of sections from 3GPP TR 24.890 to 3GPP TS 24.501

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 3GPP TR 24.890 | | 3GPP TS 24.501 | |
| General message format and information elements coding | 6.6 (including all sub-clauses) | | 9 (9.1 – 9.7) | |
| Handling of unknown, unforeseen, and erroneous protocol data | 6.7 (including all sub-clauses) | | 7 | |
| Coordination between the protocols for 5GMM and 5GSM | 7 | | 4.2 | |
| UE domain selection | 8.1.2 (including all sub-clauses) | | 4.3 | |
| Network slicing | 13 (including all sub-clauses) | | 4.6 | |
| 5GMM; general, states and procedures | 8.1.1 | | 5.1.1 | |
| 8.1.3 | | 5.12 | |
| 8.1.4 (8.1.4.1 – 8.1.4.2) | | 5.1.3 | |
| 8.1.4.3 (including all sub-clauses) | | 5.2 (5.2.1 – 5.2.3) | |
| 8.3 | | 5.3.1.1 | |
| 8.4 | | 5.3.1.2 | |
| 8.2.5 | | 5.3.1.3 | |
| 8.1.5 | | 5.3.2 | |
| 8.1.6 | | 5.3.3 | |
| 8.2.1 (excluding 8.2.1.2) | | 5.3.4 | |
| 8.2.2 | | 5.3.5 | |
| 8.1.7 | | 5.3.6 | |
| 8.1.8 | | 5.3.7 | |
| 8.5.1 | 8.5.1.1 | 5.4.1 | 5.4 |
| 8.5.1.3.3 | 5.4.4 |
| 8.5.1.4 | 5.4.2 |
| 8.5.1.5 | 5.4.3 |
| 8.5.1.6 | 5.4.5 |
| 8.5.2 (including all sub-clauses) | | 5.5 | |
| 8.5.3 (including all sub-clauses) | | 5.6 | |
| 5GMM; messages, IEs, timers and cause values | 8.6 (including all sub-clauses but 8.6.9 – 8.6.11, and 8.6.13) | | 8.2 | |
| 8.7 (including all sub-clauses but 8.7.5, 8.7.9 and 8.7.10) | | 9.8.3 | |
| 8.9 | | 10.2 | |
| 8.10 (including all sub-clauses) | | Annex A | |
| 5GSM; general, states and procedures | 9.2.2 | | 6.1.1 | |
| 9.3 (including all sub-clauses) | | 6.1.3 | |
| 9.2.1 | | 6.2 | |
| 9.4 (including all sub-clauses) | | 6.2 | |
| 9.2.3 | | 6.2 | |
| 9.5 | 9.5.1.1 | 6.2.1 | 6 |
| 9.5.3 | 6.4.1 |
| 9.5.4 | 6.3.1 |
| 9.5.5 | 6.4.2 |
| 9.5.6 | 6.3.2 |
| 9.5.7 | 6.4.3 |
| 9.5.8 | 6.3.3 |
| 9.5.9 | 6.5 |
| 5GSM; messages, IEs, timers and cause values | 9.6 (including all sub-clauses) | | 8.3 | |
| 9.7 (including all sub-clauses) | | 9.9.4 | |
| 9.8 | | 10.3 | |
| 9.9 (including all sub-clauses) | | Annex B | |
| QoS | 12.4.1 | | 6.2.5 | |
| 12.4.2.1 | | 9.8.4 | |
| 12.4.2.2 | | 9.8.4 | |
| References | 2 (only references used by the text moved to 3GPP TS 24.501)) | | 2 | |
| Definitions and abbreviations | 3.1 (only definitions used by the text moved to 3GPP TS 24.501) | | 3.1 | |
| 3.2 (only abbreviations used by the text moved to 3GPP TS 24.501)) | | 3.2 | |

## 14.4 Mapping to 3GPP TS 24.502

The table 14.4.1 identifies the mapping of sections from 3GPP TR 24.890 to 3GPP TS 24.502 [18].

Table 14.4.1: Mapping of sections from 3GPP TR 24.890 and 3GPP TS 24.302 to 3GPP TS 24.502

|  |  |  |
| --- | --- | --- |
|  | 3GPP TR 24.890 | 3GPP TS 24.502 |
| Security association management procedures | 10.5 | 7.2 N3IWF selection procedure |
| 10.7.1 | 7.3 IKEv2 SA establishment procedure |
| 10.7.5  (10.7.5.1 - 10.7.5.6) | 7.4 IKEv2 SA disconnection procedure |
| 10.7.2  (10.7.2.1 -10.7.2.6) | 7.5 IPSec SA creation procedure |
| 10.7.3 | 7.6 IPSec SA modification procedure |
| 10.7.4  (10.7.4.1 - 10.7.4.6) | 7.7 IPSec SA deletion procedure |

## 14.5 Alternatives on architecture for PWS in 5GS

CT1 have studied three alternatives for the architecture for PWS in 5GS as described in subclause 12.1.1.2, 12.1.1.3 and 12.1.1.4. CT1 have done an evaluation of the alternatives as documented in subclause 12.1.1.5. CT1 have decided to select the alternative in subclause 12.1.1.4 as the architecture for PWS in 5GS.

## 14.6 Alternatives on unified access control

CT1 have studied three alternatives for the unified access control as described in subclause 12.2.1, 12.2.2 and 12.2.3. CT1 have discussed during their #108 meeting the alternatives and decided to select the alternative in subclause 12.2.2 as the unified access control mechanism.

NOTE: The alternative 2 indicated by subclause 12.2.2 existed in earlier versions of this technical report.

## 14.7 Alternatives on steering of UE in VPLMN

CT1 have studied three alternatives for the steering of UE in VPLMN as described in subclause 5.2.4.1, 5.2.4.2 and 5.2.4.3. CT1 have discussed during their #108 meeting the alternatives and decided to select the alternative subclause 5.2.4.1 as the steering of UE in VPLMN mechanism.

The legacy steering of roaming mechanism as specified in 3GPP TS 23.122 [3] subclause 4.4.6 is still available.

Annex A:  
Impacts to specifications

## A.1 New specifications

The table A.1.1 identifies new specifications that are required to define the CT1 aspects of the 5GS.

Table A.1.1: New specifications for the CT1 aspects of the 5GS

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Series | Title | Scope |
| TS | 24.501 [17] | Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 | This TS will be the stage 3 part of 3GPP TS 23.501 [9] and 3GPP TS 23.502 [10] covering protocols for mobility management, session management, and control of NAS security for both 3GPP access and non-3GPP access. Furthermore, the TS would provide support of inter-system mobility between; NG-RAN and E-UTRAN, and between NG-RAN and non-3GPP access network |
| TS | 24.502 [18] | Access to the 5G System (5GS) via non-3GPP access networks; Stage 3 | This TS will cover the particular aspects of non-3GPP access network discovery and selection procedures which differ from 3GPP access, the authentication and tunnel management procedures with N3IWF, IP mobility mode selection, and in general, any procedure associated with accessing the 5GCN via non-3GPP accesses until the UE has gained IP connectivity through the N3IWF |
| TS | 24.568 [19] | WLAN connectivity for 5GS Management Object (MO) | This TS will cover provisioning of configuration parameters for WLAN connectivity for 5GS based on stage 2 requirements in 3GPP TS 23.501 [9]. |

## A.2 Impacted existing specifications

The table A.2.1 identifies impacted existing specifications that are required to define the CT1 aspects of the 5GS.

Table A.2.1: Impacted specifications for the CT1 aspects of the 5GS

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Series | Title | Brief description of the impacts |
| TS | 23.122 | Non-Access-Stratum functions related to Mobile Station (MS) in idle mode | Enhancements of PLMN selection procedures and access control to support NR |
| TS | 23.040 | Technical realization of Short Message Service (SMS) | Support of SMS for 5G System |
| TS | 23.041 | Technical realization of Cell Broadcast Service (CBS) | Support of PWS for 5G System |
| TS | 24.007 | Mobile radio interface signalling layer 3; General aspects | Protocol principles for the NAS protocol for 5G System |
| TS | 24.301 | Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 | Inter-system mobility between NR and E-UTRAN. Updates to IEs which can be used by 5GS protocols |
| TS | 24.008 | Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3 | Possible impacts, e.g. updates to Ies which can be used by 5GS protocols |
| TS | 24.302 | Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 | Possible impacts, e.g. updates to Ies which can be used by 5GS protocols |
| TS | 24.011 | Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface | Updates to the SMS protocols for 5G System |
| TS | 24.312 | Access Network Discovery and Selection Function (ANDSF) Management Object (MO) | Possible impacts, e.g. update to ANDSF Mos to include aspects of the 5G System |
| TS | 24.305 | Selective Disabling of 3GPP User Equipment Capabilities (SdoUE) Management Object (MO) | Updates to selective disabling of UE (SdoUE) for 5G System procedures |
| TS | 24.368 | Non-Access Stratum (NAS) configuration Management Object (MO) | Possible impacts, e.g. update to existing or new leaves to support 5G System |

Annex B (informative):  
Proposed changes to 3GPP TS 23.040

# B.1 First Change

# 1 Scope

The present document describes the Short Message Service (SMS) for GSM/UMTS/EPS/5GS networks. It defines:

- the services and service elements;

- the network architecture;

- the Service Centre functionality;

- the SMS Router functionality;

- the MSC functionality (with regard to the SMS);

- the SGSN functionality (with regard to the SMS);

- the MME functionality (with regard to the SMS);

- the SMSF functionality;

- the routing requirements;

- the protocols and protocol layering;

for the Mobile Originated and Mobile Terminated Short Message Service Teleservices, as specified in 3GPP TS 22.003 [2] and 3GPP TS 22.105 [32].

The use of radio resources for the transfer of short messages between the MS and the MSC or the SGSN or the MME is described in 3GPP TS 24.011 [13].

The present document also describes the Short Message Service (SMS) for EPS networks supported via "SMS in MME" (see 3GPP TS.23.272 [45], annex C).

The present document also describes the SGSN supporting Diameter based protocol for SMS between the SGSN and the central SMS functions (SMS-GMSC, SMS-IWMSC, SMS-Router) in annex J.

The present document describes SMS for 5GS networks (see 3GPP TS 23.501 [xx] and 3GPP TS 23.502 [yy]).

The network aspects of Short Message Service provision are outside the scope of the present document (i.e. the provision of network connectivity between the PLMN subsystems). There is no technical restriction within the present document for the transfer of short messages between different PLMNs. Any such restriction is likely to be subject to commercial arrangements and PLMN operators must make their own provision for interworking or for preventing interworking with other PLMNs as they see fit.

The required and assumed network service offered to the higher layers is defined in the present document.

# B.2 Next 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] Void

[2] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)".

[3] 3GPP TS 22.004: "General on supplementary services".

[4] 3GPP TS 22.041: "Operator Determined Barring (ODB)".

[5] 3GPP TS 23.002: "Network architecture".

[6] 3GPP TS 23.008: "Organization of subscriber data".

[7] 3GPP TS 23.011: "Technical realization of supplementary services".

[8] 3GPP TS 23.015: "Technical realization of Operator Determined Barring (ODB)".

[9] 3GPP TS 23.038: "Alphabets and language‑specific information".

[10] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[11] Void

[12] 3GPP TS 44.008: "Mobile radio interface layer 3 specification".

[13] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[14] 3GPP TS 27.005: "Use of Data Terminal Equipment ‑ Data Circuit terminating Equipment (DTE ‑ DCE) interface for Short Message Service (SMS) and Cell Broadcast Service (CBS)".

[15] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[16] 3GPP TS 51.011 Release 4 (version 4.x.x): "Specification of the Subscriber Identity Module ‑ Mobile Equipment (SIM‑ ME) interface".

[17] CCITT Recommendation E.164 (Blue Book): "The international public telecommunication numbering plan".

[18] CCITT Recommendation E.163 (Blue Book): "Numbering plan for the international telephone service".

[19] CCITT Recommendation Q.771: "Specifications of Signalling System No.7; Functional description of transaction capabilities".

[20] CCITT Recommendation T.100 (Blue Book): "International information exchange for interactive videotex".

[21] CCITT Recommendation T.101 (Blue Book): "International interworking for videotex services".

[22] CCITT Recommendation X.121 (Blue Book): "International numbering plan for public data networks".

[23] CCITT Recommendation X.400 (Blue Book): "Message handling services: Message handling system and service overview".

[24] ISO/IEC10646: "Universal Multiple‑Octet Coded Character Set (USC); UCS2, 16 bit coding".

[25] 3GPP TS 22.022: "Personalisation of Mobile Equipment (ME); Mobile functionality specification".

[26] 3GPP TS 23.042: "Compression Algorithm for Text Messaging Services".

[27] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[28] 3GPP TS 31.115: "Secured packet structure for (U)SIM toolkit application".

[29] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[30] 3GPP TS 31.102: "Characteristics of the USIM application".

[31] 3GPP TS 31.101: "UICC – Terminal interface; Physical and logical characteristics".

[32] 3GPP TS 22.105: "Services and Service Capabilites".

[33] Infrared Data Association. Specifications for Ir Mobile Communications (IrMC).  
iMelody.

[34] IETF RFC 5322 (October 2008): "Internet Message Format".

[35] Void

[36] "vCard - The Electronic Business Card", version 2.1,The Internet Mail Consortium (IMC), September 18, 1996,   
[URL:http://www.imc.org/pdi/vcard-21.doc](url:http://www.imc.org/pdi/vcard-21.doc)".

[37] "vCalendar - the Electronic Calendaring and Scheduling Format", version 1.0,  
The Internet Mail Consortium (IMC), September 18, 1996,  
[URL:http://www.imc.org/pdi/vcal-10.doc](url:http://www.imc.org/pdi/vcal-10.doc%0D)

[[38] Scalable Polyphony MIDI Specification, MIDI Manufacturers Association (2002);](url:http://www.imc.org/pdi/vcal-10.doc%0D) [http://www.midi.org](http://www.midi.org/)

[39] Scalable Polyphony MIDI Device 5-to-24 Note Profile for 3GPP, MIDI Manufacturers Association (2002); [http://www.midi.org](http://www.midi.org/)

[40] The Complete MIDI 1.0 Detailed Specification, Incorporating all Recommended Practices, MIDI Manufacturers Association, Document version 96.1, 1996; [http://www.midi.org](http://www.midi.org/)

[41] 3GPP TS 23.097: Multiple Subscriber Profile (MSP) (Phase 2) - Stage 2

[42] 3GPP TS 23.204: "Support of SMS over generic 3GPP IP access; Stage 2".

[43] IETF RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[44] IETF RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[45] 3GPP TS 23.272: "Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2".

[46] 3GPP TS 29.272: "Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

[47] 3GPP TS 29.118: "Mobility Management Entity (MME) – Visitor Location Register (VLR) SGs interface specification".

[48] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[49] Void.

[50] 3GPP TS 29.338: "Diameter based protocols to support of SMS capable MMEs".

[xx] 3GPP TS 23.501: " System Architecture for the 5G System; Stage 2".

[yy] 3GPP TS 23.502: " Procedures for the 5G System; Stage 2".

# B.3 Next Change

Annex L (normative):  
SMS in 5GS

# L.1 General

A 5GS network delivers short message services over 5GS NAS signalling.

For the architecture and the definition of reference points for SMS in 5GS see 3GPP TS 23.501 [xx], subclause 4.2.

Between the architecture and the reference points for SMS in 5GS and the architecture and the reference points shown in subclause 4.1, and figure 5, of the present specification the following mapping is used:

Table L.1: Mapping between architecture and reference points for SMS in 5GS and the present specification

|  |  |  |
| --- | --- | --- |
|  | SMS in 5GS | present specification |
|  | UDM | HLR |
| Network entities | SMSF | MSC + VLR |
|  | UE | MS |
|  | AMF | MME (NOTE 1) |
|  | N20/Namf/Nsmsf | (not shown in figure 5) |
|  | N21/Nsmsf | (not shown in figure 5) |
|  | N8/Nudm | (not shown in figure 5) |
|  | Not shown in 3GPP TS 23.501 (NOTE 3) | 2 |
| Reference points | Not shown in 3GPP TS 23.501 (NOTE 2) | 3 |
|  | (not applicable) | 4 |
|  | N1 | 5 |
|  | (not applicable) | 6 |
| NOTE 1: In figure 5, the MME is only acting as a relay for SMS transfer via the SGs.  NOTE 2: Reference point 3 is used as reference from SMSF to/from SMS-GMSC/IWMSC and SMS Router.  NOTE 3: Reference point 2 is used as reference from UDM to/from SMS-GMSC and SMS Router. | | |

For the purpose of supporting SMS in 5GS, the SMSF shall implement the requirements specified in the present specification for the MSC and the VLR with the following modifications:

1) "GSM/UMTS system" is to be replaced with "5GS".

2) Throughout the text and in the figures, message names, parameter names and cause values:

"MSC" is to be replaced with "SMSF";

"VLR" is to be replaced with "SMSF internal subscriber register";

"HLR" is to be replaced with "UDM/HLR";

"MS" is to be replaced with "UE"; and

"non GPRS" is to be replaced with "5GS".

3) Reference point 4 is SMSF internal, and operations performed on this reference point are not standardized. In the message flows of clause 10, the SMSF replaces the combination of MSC and VLR, and messages exchanged between MSC and VLR are replaced with MME internal communication.

The architecture for SMS in 5GS is defined in 3GPP TS 23.501 [xx] and uses the following reference points:

**N1**: Reference point between the UE and the AMF.

**N8**: Reference point between the UDM and the AMF.

**N20**: Reference point between the AMF and the SMSF.

**N21**: Reference point between SMSF and the UDM.

The following service based interfaces are used for SMS in 5GS:

**Namf:** Service-based interface exhibited by AMF. Usage of Namf service operations for SMS in 5GS is defined in 3GPP TS 23.502 [yy].

**Nsmsf:** Service-based interface exhibited by SMSF. Usage of Nsmsf service operations for SMS in 5GS is defined in 3GPP TS 23.502 [yy].].

**Nudm:** Service-based interface exhibited by UDM. Usage of Nudm service operations for SMS in 5GS is defined in 3GPP TS 23.502 [yy].

# B.4 Next Change

# L.2 Support for SMS when UE is registered to both 5GS and EPS

When a UE is operating in dual-registration mode as specified 3GPP TS 23.501 [8] and is registered to the network via:

- MME; and

- AMF;

and SMS in EPS uses SMS over SGs, the network shall deliver an MT short message either via SMS over SGs in EPS or SMS over NAS in 5GS based on local policy. In case the network determines the MT short message delivery fails, e.g. the UE is not reachable, the network may try delivering the short message via the not yet tried option for delivering of the MT short message. If the network tries to deliver an MT short message via SMS over SGs in EPS and SMS over NAS in 5GS then the mobile not reachable flags specified in subclause 3.2.8 of this specification are only set if MT short message delivery fails via both options.

NOTE 1: This version of the specification does not specify an architecture that provides a standardized interface between SMSF and VLR.

Editor’s note: Support for SMS in MME specified in Annex I for dual registration requires further study.

Annex C (informative):  
Proposed changes to 3GPP TS 24.011

# C.1 First Change

# 1 Scope

The present document specifies the procedures used across the mobile radio interface by the signalling layer 3 function Short Message Control (SMC) and Short Message Relay function (SM‑RL) for circuit switched in A/Gb mode, GPRS, EPS, and 5GS.

## 1.1 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] Void.

[1a] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS) Point‑to‑Point (PP)".

[3a] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[3] 3GPP TS 44.006: "Mobile Station ‑ Base Station System (MS ‑ BSS) interface; Data Link (DL) layer specification".

[4] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[5] 3GPP TS 24.008: "Mobile radio interface layer 3 specification".

[5a] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[5b] 3GPP TS 33.102: "3G Security; Security Architecture".

[5c] 3GPP TS 42.017: "Subscriber Identity Modules (SIM); Functional characteristics".

[6a] 3GPP TS 44.064: "General Packet Radio Service (GPRS); Logical Link Control (LLC) layer specification ".

[6] ISO 7498: "Information processing systems ‑ Open Systems Interconnection ‑ Basic Reference Model".

[7] 3GPP TS 44.018: "Mobile radio interface layer 3 specification; Radio Resource Control Protocol".

[8] 3GPP TS 25.413: "UTRAN Iu interface RANAP signalling".

[9] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"

[10] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3"

[11] 3GPP TS 23.272: "Circuit Switched Fallback in Evolved Packet System; Stage 2"

[12] 3GPP TS 29.118: "Mobility Management Entity (MME) – Visitor Location Register (VLR) SGs interface specification"

[xx] 3GPP TS 23.501: " System Architecture for the 5G System; Stage 2".

[yy] 3GPP TS 23.502: " Procedures for the 5G System; Stage 2".

[zz] 3GPP TS 24.501: "Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

## 1.2 Abbreviations

For the purpose of the present document, the abbreviations given in 3GPP TR 21.905 [1a] and the following apply:

**RR connection:** a RR connection is a dedicated physical circuit switched domain connection used by the two RR or RRC peer entities to support the upper layers' exchange of information flows.

**PS signalling connection:** is a peer to peer UMTS connection between MS and CN packet domain node.

**GPRS:** Packet Services for GSM and UMTS system.

The label **(A/Gb mode only):** indicates this section or paragraph applies only to GSM system. For multi system case this is determined by the current serving radio access network.

The label **(Iu mode only):** indicates this section or paragraph applies only to UMTS system. For multi system case this is determined by the current serving radio access network.

The label **(S1 mode only):** indicates this section or paragraph applies only to Evolved Packet Core (EPC) and E-UTRAN access. For multi system case this is determined by the current serving radio access network.

**In A/Gb mode,...:** Indicates this paragraph applies only to GSM System. For multi system case this is determined by the current serving radio access network.

**In Iu mode,...:** Indicates this paragraph applies only to UMTS System. For multi system case this is determined by the current serving radio access network.

**In S1 mode,...:** Indicates this paragraph applies only to Evolved Packet Core and E-UTRAN access. For multi system case this is determined by the current serving radio access network.

**In N1 mode:** Indicates this paragraph applies only to 5G System access and that a N1 NAS signaling connection as defined in 3GPP TS 24.501 [zz] is used.

**SIM:** Subscriber Identity Module (see 3GPP TS 42.017 [5c]). This specification makes no distinction between SIM and USIM.

**MS:** Mobile Station. This specification makes no distinction between MS and UE.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.301 [10] apply:

**UE using EPS services with control plane CIoT EPS optimization**

# C.2 Next Change

# 2 Overview of Short Message Service (SMS) support

The purpose of the Short Message Service is to provide the means to transfer messages between a GSM PLMN Mobile Station (MS) and a Short Message Entity via a Service Centre, as described in 3GPP TS 23.040 [2]. The terms "MO" ‑ Mobile Originating ‑ and "MT" ‑ Mobile Terminating ‑ are used to indicate the direction in which the short message is sent.

The present document describes the procedures necessary to support the Short Message Service between the MS and the MSC or SGSN or MME or SMSF and vice versa, as described in 3GPP TS 23.040 [2].

The procedures are based on services provided by the Mobility Management sublayer as described in 3GPP TS 24.007 [11]/3GPP TS 24.008 [12] for CS in A/Gb mode and CS/PS services in Iu mode, 3GPP 24.301 [10] for CS/PS services in S1 mode, and the Logical Link Control layer described in 3GPP TS 44.064 [6a] for GPRS services. For CS/PS service in S1 mode, depending on network configuration and UE subscription data, network may choose to use either packet-switched service or circuit-switched service to provide SMS service. If circuit-switched service is used instead of packet-switched service, then the messages are tunneled through the MME. In this case the network also uses procedures described in 3GPP 29.118 [12].

Editor's note: Mobility management for UE in N1 mode to be included, only possible once the new NAS technical specification is available.

## 2.1 Protocols and protocol architecture

In Iu mode only, integrity protected signalling (see 3GPP TS 24.008 [5], subclause 'Integrity Protection of Signalling Messages' and in general, see 3GPP TS 33.102 [5b]) is mandatory. In Iu mode only, all protocols shall use integrity protected signalling. Integrity protection of all SMS signalling messages is the responsibility of lower layers. It is the network which activates integrity protection. This is done using the security mode control procedure (3GPP TS 25.331 [5a]).

The hierarchical model in figure 2.1a shows the layer structure of the MSC and the MS in A/Gb mode. The hierarchical model in figure 2.1c shows the layer structure of the SGSN and the MS in Iu mode. The hierarchical model in figure 2.1d shows the layer structure of the MSC and the MS in S1 mode. The hierarchical model in figure 2.1e shows the layer structure of the MME and the MS in S1 mode. The hierarchical model in figure 2.1f shows the layer structure of the SMSF and MS in N1 mode.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | MSC |  |  |  | MS |  |
|  |  |  |  |  |  |  |  |  |  |
| SM‑AL |  |  |  |  |  |  |  |  |  |
| SM‑TL |  |  |  |  |  |  |  |  |  |
| SM‑RL |  |  |  | SMR |  | < SM‑RP protocol > |  | SMR |  |
| CM‑sublayer |  |  |  | SMC |  | < SM‑CP protocol > |  | SMC |  |
| MM‑sublayer |  |  |  |  |  |  |  |  |  |
| RR‑sublayer |  |  |  |  |  |  |  |  |  |

Figure 2.1a/3GPP TS 24.011: Protocol hierarchy for circuit-switched service

The hierarchical model in figure 2.1b shows the layer structure of the SGSN and the MS in A/Gb mode.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | SGSN |  |  |  | MS |  |
|  |  |  |  |  |  |  |  |  |  |
| SM‑AL |  |  |  |  |  |  |  |  |  |
| SM‑TL |  |  |  |  |  |  |  |  |  |
| SM‑RL |  |  |  | SMR |  | < SM‑RP protocol > |  | SMR |  |
| CM‑sublayer |  |  |  | SMC |  | < SM‑CP protocol > |  | SMC |  |
| LLC‑sublayer |  |  |  |  |  |  |  |  |  |
| GRR‑sublayer |  |  |  |  |  |  |  |  |  |

Figure 2.1b/3GPP TS 24.011: Protocol hierarchy for GPRS in A/Gb mode

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | SGSN |  |  |  | MS |  |
|  |  |  |  |  |  |  |  |  |  |
| SM‑AL |  |  |  |  |  |  |  |  |  |
| SM‑TL |  |  |  |  |  |  |  |  |  |
| SM‑RL |  |  |  | SMR |  | < SM‑RP protocol > |  | SMR |  |
| CM‑sublayer |  |  |  | SMC |  | < SM‑CP protocol > |  | SMC |  |
| GMM‑sublayer |  |  |  |  |  |  |  |  |  |

Figure 2.1c/3GPP TS 24.011: Protocol hierarchy for packet-switched service in Iu mode

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | MSC |  |  |  | MS |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| SM‑AL |  |  |  |  |  |  |  |  |  |  |  | SM‑AL |
| SM‑TL |  |  |  |  |  |  |  |  |  |  |  | SM‑TL |
| SM‑RL |  |  |  | SMR |  | < SM‑RP protocol > |  | SMR |  |  |  | SM‑RL |
| CM‑sublayer |  |  |  | SMC |  | < SM‑CP protocol > |  | SMC |  |  |  | CM‑sublayer |
| SGs layer |  |  |  |  |  |  |  |  |  |  |  | EMM-sublayer |

NOTE: SM-CP messages are transferred between the MSC and the MS through the MME. The protocol stack on the MME is not shown.

Figure 2.1d/3GPP TS 24.011: Protocol hierarchy for circuit-switched service in S1 mode

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | MME |  |  |  | MS |  |
|  |  |  |  |  |  |  |  |  |  |
| SM‑AL |  |  |  |  |  |  |  |  |  |
| SM‑TL |  |  |  |  |  |  |  |  |  |
| SM‑RL |  |  |  | SMR |  | <¾¾¾¾¾¾ SM‑RP protocol ¾¾¾¾¾> |  | SMR |  |
| CM‑sublayer |  |  |  | SMC |  | <¾¾¾¾¾¾ SM‑CP protocol ¾¾¾¾¾> |  | SMC |  |
| EMM‑sublayer |  |  |  |  |  |  |  |  |  |

Figure 2.1e/3GPP TS 24.011: Protocol hierarchy for packet-switched service in S1 mode

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | SMSF |  |  |  | MS |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| SM‑AL |  |  |  |  |  |  |  |  |  |  |  | SM‑AL |
| SM‑TL |  |  |  |  |  |  |  |  |  |  |  | SM‑TL |
| SM‑RL |  |  |  | SMR |  | < SM‑RP protocol > |  | SMR |  |  |  | SM‑RL |
| CM‑sublayer |  |  |  | SMC |  | < SM‑CP protocol > |  | SMC |  |  |  | CM‑sublayer |
| N20-layer |  |  |  |  |  |  |  |  |  |  |  | 5GMM-sublayer |

NOTE: SM-CP messages are transferred between the SMSF and the MS through the AMF. The protocol stack on the AMF is not shown.

Figure 2.1f/3GPP TS 24.011: Protocol hierarchy in N1 mode

The CM‑sublayer, in terms of the Short Message Service Support, provides services to the Short Message Relay Layer.

On the MS‑side the Short Message Relay Layer provides services to the Short Message Transfer Layer. The Short Message Relay Layer is the upper layer on the network side (MSC or SGSN or MME), and the SM‑user information elements are mapped to TCAP/MAP.

The peer protocol between two SMC entities is denoted SM‑CP, and between two SMR entities, SM‑RP.

Abbreviations:

SM‑AL Short Message Application Layer

SM‑TL Short Message Transfer Layer

SM‑RL Short Message Relay Layer

SM‑RP Short Message Relay Protocol

SMR Short Message Relay (entity)

CM‑sub Connection Management sublayer

SM‑CP Short Message Control Protocol

SMC Short Message Control (entity)

MM‑sub Mobility Management sublayer

GMM-sub GPRS Mobility Management sublayer

RR‑sub Radio Resource Management sublayer

LLC-sub Logical Link Control sublayer

GRR-sub GPRS Radio Resource sublayer in GSM

EMM-sub EPS Mobility Management sublayer

5GMM-sub 5G Mobility Management sublayer

# C.3 Next Change

## 2.5B 5GSMS entity in N1 mode

It shall be possible for an MS in N1 mode that is attached to the 5GCN to send and receive short messages.

The 5GSMS entity for an MS in N1 mode is shown in figure 2.5B.



Figure 2.5B/3GPP TS 24.011: 5GSMS entity for MS in N1 mode

# C.4 Next Change

## 3.2 Service provided by the CM‑sublayer

In order to support the Short Message Service, the CM‑sublayer provides services to the Short Message Relay Layer.

The CM‑sublayer services are provided using layer specific functions and lower layer services offered to the CM‑sublayer, controlled by short message service control entities called SMCs.

An SMC entity in the MS communicates with an SMC entity in the MSC or the SGSN or the MME or the SMSF by means of a peer protocol, SM‑CP (Short Message Service Control Protocol). The arrow diagrams in annex A give an overview of the messaging on the CM‑sublayer during a short message transfer.

A mobile station supporting the Short Message Service shall have a minimum of two SMC entities per service type (i.e. two for CS GSM and two for GPRS). This enables the MS to receive MT messages during an MO message transfer.

To ensure that an MS having the minimum of two SMC entities is able to receive MT messages during an MO message transfer, and to send MO messages during MT message transfer, parallel message transfer in the same direction is prohibited. This means that the SMC entities shall not simultaneously perform messaging in the same direction. The rules for concatenation of message transfers are described in subclause 5.4.

The MSC or the SGSN or the MME or the SMSF shall have a minimum of two SMC entities available each during an MT message transfer to a mobile station, one being reserved for MO message transfer. In an MO message transfer, the MSC or the SGSN or the MME or the SMSF shall have one SMC entity reserved for handling of an MT message.

# C.5 Next Change

# 5 CM‑procedures

## 5.1 General

This clause describes the procedures used by the SMC entity on the Connection Management sublayer. An SMC entity communicates with a corresponding peer entity using an MM‑connection for CS in A/Gb and Iu mode, or the LLC layer for GPRS in A/Gb mode, or the GMM-connection for PS in Iu mode, or the EMM-connection for EPS in S1 mode if packet-switched service is used, or through the MME for S1 mode if circuit-switched service is used, or through the AMF for N1 mode.

Editor's note: The impact of MO SMS using one step approach in 5GMM-IDLE mode in case of SMS in N1 mode requires further study.

Multiple MM‑connections may be established at the same time, allowing parallel transactions. The description of the procedures is related to one single transaction.

For circuit switched service, the CM‑procedures described can only be performed if an MM‑connection has been established between the mobile station and the network.

For GPRS, no connection has to be established, and thus the CM procedures for GPRS reflect this. Detailed SDL diagrams for SMC entities are contained in annex B.

For EPS when packet-switched service is used, detailed SDL diagrams for SMC entities are contained in annex B.

# C.6 Next Change

### 5.2.2 SMC-GP, SMC-EP and SMC-5G states at the MS side of the radio interface

#### 5.2.2.1 Mobile Originating Case

The states described in this clause are for an SMC-GP entity in a GPRS MS, and for an SMC-EP entity in an EPS MS, and for an SMC-5G entity in a 5GS MS handling mobile originating short message transfer and notification to the network that the mobile has memory available to receive one or more short messages (referred to below as "notification").

# C.7 Next Change

### 5.2.4 SMC-GP, SMC-EP and SMC-5G states at the network side of the radio interface

#### 5.2.4.1 Mobile Originating Case

The states described in this subclause are for an SMC-GP entity in an SGSN and for an SMC-EP entity in an MSC or an MME and an SMC-5G entity in a SMSF handling both mobile originating short message transfer and notification to the network that the mobile has memory available to receive one or more short messages (referred to below as "notification").

# C.8 Next Change

#### 5.3.2.2 RPDU transfer for GPRS, EPS and 5GS

In A/Gb mode, when an SMC-GP or SMC-EP entity or SMC-5G entity is in the Idle state and transfer of an RPDU is requested, the SMC-GP or SMC-EP or SMC-5G entity on the originating side forwards the CP-DATA message containing the RPDU to the lower layer, and sets the timer TC1\* and enters the Wait for CP-ACK state. In A/Gb mode, for the SMC-GP entity, the lower layer is the LLC sublayer. For the SMC-EP entity on the MS side, the lower layer is EMM. For the SMC-EP entity on the network side, the lower layer can be either the SGs association as described in 3GPP TS 29.118 [12] or the EMM sublayer. For the SMC-5G entity on the MS side, the lower layer is 5GMM. For the SMC-5G entity on the network side the lower layer is provided by the N20 interface.

Editor’s note: Appropriate reference for N20 interface to be included once available.

In Iu mode, when an SMC-GP entity in the MS side is in the Idle state and transfer of an RPDU is requested:

- the SMC-GP entity on the originating side requests the GMM sublayer to establish a PS signalling connection, and enters the GMM-Connection Pending state.

- after completion of the PS signalling connection establishment, a confirmation is given to the originating side to indicate that the GMM sublayer is ready for RPDU transfer; and.

- after confirmation of the PS signalling connection establishment, the SMC-GP entity on the originating side forwards the CP-DATA message to the GMM sublayer. This contains the RPDU, and also the SMC-GP entity sets the timer TC1\* and enters the Wait for CP-ACK state.

In S1 mode, when an SMC-EP entity in the MS side is in the Idle state and transfer of an RPDU is requested:

- if the MS is not using Control plane CIoT EPS optimization:

1) the SMC-EP entity on the originating side requests the EMM sublayer to establish a NAS signalling connection, and enters the EMM-Connection Pending state;

2) after completion of the NAS signalling connection establishment, a confirmation is given to the originating side to indicate that the EMM sublayer is ready for RPDU transfer; and

3) after confirmation of the NAS signalling connection establishment, the SMC-EP entity on the originating side forwards the CP-DATA message to the EMM sublayer. This contains the RPDU, and also the SMC-EP entity sets the timer TC1\* and enters the Wait for CP‑ACK state; or

- if the MS is using Control plane CIoT EPS optimization, the SMC-EP entity on the originating side forwards the CP-DATA message that contains the RPDU to the EMM sublayer when requesting the EMM sublayer to establish a NAS signalling connection. The SMC-EP entity then sets the timer TC1\* and enters the Wait for CP-ACK state immediately.

NOTE: If the MS in idle mode is using Control plane CIoT optimization, the first CP-DATA message is sent by piggybacking on the CONTROL PLANE SERVICE REQUEST message during the service request procedure as specified in 3GPP 24.301 [10].

In N1 mode, when an SMC-5G entity in the MS side is in the Idle state and transfer of an RPDU is requested:

1) the SMC-5G entity on the originating side requests the 5GMM sublayer to establish a NAS signalling connection;

2) after completion of the NAS signalling connection establishment, a confirmation is given to the originating side to indicate that the 5GMM sublayer is ready for RPDU transfer; and

3) after confirmation of the NAS signalling connection establishment, the SMC-5G entity on the originating side forwards the CP‑DATA message to the 5GMM sublayer. This contains the RPDU, and also the SMC-5G entity sets the timer TC1\* and enters the Wait for CP-ACK state.

In Iu mode, when an SMC-GP entity in the network side is in Idle state and transfer of an RPDU is requested, the SMC-GP entity on the originating side forwards the C-‑DATA message to the GMM sublayer. This contains the RPDU, and also the SMC-GP entity sets the timer TC1\* and enters the Wait for CP-ACK state.

In S1 mode and the circuit-switched service is used, when an SMC-EP entity in the network side is in Idle state and transfer of an RPDU is requested, the SMC-EP entity on the MSC forwards the CP-DATA message to the SGs sublayer. This contains the RPDU, and also the SMC-EP entity sets the timer TC1\* and enters the Wait for CP-ACK state. The SGs layer transfers the CP-DATA message by using the procedures specified in 3GPP 24.301 [10].

In S1 mode and the packet-switched service is used, when an SMC-EP entity in the network side is in Idle state and transfer of an RPDU is requested, the SMC-EP entity on the originating side forwards the CP-DATA message to the EMM sublayer. This contains the RPDU, and also the SMC-GP entity sets the timer TC1\* and enters the Wait for CP-ACK state.

In N1 mode and the packet-switched service is used, when an SMC-5G entity in the network side is in Idle state and transfer of an RPDU is requested, the SMC-EP entity on the SMSF forwards the CP-DATA message to the N20 sublayer. This contains the RPDU, and also the SMC-5G entity sets the timer TC1\* and enters the Wait for CP-ACK state.The value of TC1\* may vary with the length of the CP‑DATA. However, the value of TC1\* shall be sufficiently great to allow the lower layers to transmit the CP-DATA and CP-ACK messages and to allow for some re-transmissions of layer 2 frames.

If an SMC entity in the Wait for CP-ACK state gets an indication that the CP-DATA message has probably been lost then, as an implementation option, that SMC-GP entity may reduce the time until expiry of TC1\*.

If the timer TC1\* expires in the Wait for CP-ACK state, the CP-DATA message is retransmitted and the state Wait for CP-ACK is re‑entered. The maximum number of CP-DATA message re-transmissions is an implementation option but shall be either 1, 2 or 3. If the timer TC1\* expires after the maximum number of retransmission attempts, an error indication is passed to SM-RL. The Idle state is then entered.

On receipt of the CP-ACK message in response to the CP-DATA (RP DATA) message in the Wait for CP-ACK state, the SMC-GP resets the timer TC1\* and enters the Wait for CP DATA state.

On receipt of the CP‑ACK message in response to the CP-DATA (RP ACK) message in the Wait for CP-ACK state, the SMC-GP resets the timer TC1\* and enters the Idle State.

On receipt of the CP-ACK message in response to the CP-DATA (RP DATA) message in the Wait for CP-ACK state, the SMC-5G resets the timer TC1\* and enters the Wait for CP DATA state.

On receipt of the CP-ACK message in response to the CP-DATA (RP ACK) message in the Wait for CP-ACK state, the SMC-5G resets the timer TC1\* and enters the Idle State.

In A/Gb mode or S1 mode or N1 mode, when receiving a CP-DATA message from the lower layer, the SMC-GP or SMC-EP or SMC5G entity checks the parameters relevant to the CP protocol. If these are valid, the RPDU is passed to the SM-RL, the CP-ACK message is sent.

In Iu mode, when receiving a CP-DATA message from the GMM sublayer, the SMC-GP entity checks the parameters relevant to the CP protocol. If these are valid, the RPDU is passed to the SM-RL, the CP-ACK message is sent.

In S1 mode, when receiving a CP-DATA message from the lower layer, the SMC-EP entity checks the parameters relevant to the CP protocol. If these are valid, the RPDU is passed to the SM-RL, the CP-ACK message is sent.

In N1 mode, when receiving a CP-‑DATA message from the lower layer, the SMC-5G entity checks the parameters relevant to the CP protocol. If these are valid, the RPDU is passed to the SM-‑RL, the CP-‑ACK message is sent

If an SMC entity in the Idle state is unable to accept a CP-DATA message, it sends a CP-ERROR message and then enters the Idle state.

# C.9 Next Change

## 5.4 Concatenating short message or notification transfers

If an entity has more than one short message or notification to send, then it is useful to maintain the Radio Resource (RR) connection (in A/Gb mode) or the signalling connection (in Iu mode, in S1 mode if packet-switched service is used, and in N1 mode) in between transfers. For mobile terminated short messages this is simple because the network decides when, and whether, to release the RR connection (in A/Gb mode) or the signalling connection (in Iu mode, in S1 mode if packet-switched service is used, and in N1 mode). However, for mobile originated transfers, the network does not know whether or not the mobile has more messages to transfer. For short message transfer through the EPS in S1 mode if circuit-switched service is used, the network side has no knowledge of the signalling connection in for both mobile originated and mobile terminated transfers.

If another short message or a memory available notification is to be sent, an originating SMR entity in the MS may choose to continue to use the same RR connection (in A/Gb mode) or the same signalling connection (in Iu mode or in N1 mode).

In the case of a SMS transfer via the CS domain, when the MS chooses to use the same RR connection (in A/Gb mode) or CS signalling connection (in Iu mode), then:

- the MS shall transmit a CM SERVICE REQUEST for the new CM connection before the final CP‑ACK (i.e. the one that acknowledges the CP‑DATA that carried the RP‑ACK) for the old MM connection is transmitted;

- before transmission of the first CP‑DATA on the new MM connection, the MS may transmit the CP‑ACK for the old MM connection; the MS shall not transmit the final CP-ACK after the new CP-DATA;

- the Transaction Identifier used on the new MM connection shall be different to that used on the old MM connection; and

- the MS shall not initiate establishment of the new MM connection before the final CP‑DATA (e.g. the one carrying the RP‑ACK) has been received.

In the case of a SMS transfer via the PS domain, when the MS chooses to use the same PS signalling connection (in Iu mode and in S1 mode if packet-switched service is used); or in the case of a SMS transfer via the PS domain in A/Gb mode; or in the case of SMS transfer through the EPS; or in the case of SMS transfer in N1 mode, then:

- the MS shall transmit the CP-DATA for the successive RPDU and shall not transmit the final CP‑ACK for the current SMS (i.e. the one that acknowledges the CP‑DATA that carried the RP‑ACK);

- the Transaction Identifier used for the successive RPDU shall be different to that used for the current RPDU; and

- the MS shall not transmit the CP-DATA for the successive RPDU before the final CP‑DATA (i.e. the one that carried the RP‑ACK) has been received.

NOTE: When an MS sends successive memory available notifications and/or mobile originated short messages on different RR connections (in A/Gb mode) or signalling connections (in Iu mode and S1 mode), the MS is strongly recommended to use different Transaction Identifiers for the old and new MM connections.

It is possible that the final CP‑ACK of a short message transfer may not be received (e.g. due to transmission errors and/or hand overs).

For mobile terminated transfers, if the CP‑ACK is lost, the reception of a CP‑DATA with a different transaction identifier and carrying an RPDU shall be interpreted as the implicit reception of the awaited CP‑ACK followed by the reception of the new CP‑DATA message.

For mobile originated transfers, if the CP‑ACK is lost or not sent by the MS, the following events shall be interpreted as the implicit reception of the awaited CP‑ACK:

- in the case of a SMS transfer via the CS domain,, the reception of a CM SERVICE REQUEST followed by a CP‑DATA with a different transaction identifier and carrying an RPDU; or

- in the case of a SMS transfer via the PS domain, the reception of a CP-DATA with a different transaction identifier and carrying an RPDU.

Annex D (informative):  
Proposed changes to 3GPP TS 24.301

# D.1 Summary of changes

The list of impacts that should be captured in 3GPP TS 24.301 [15] is as follows:

1) Attach procedure for EPS services and combined attach procedure for EPS services and non-EPS services

A) Mode selection for intersystem change with 5GS

i) If the UE supports N1 mode, the UE shall set the N1 mode supported bit to "N1 mode supported" in the UE network capability IE of the ATTACH REQUEST message.

ii) If the MME received the N1 mode supported bit set to "N1 mode supported" in the UE network capability IE of the ATTACH REQUEST message and the MME supports intersystem change with 5GS, in the ATTACH ACCEPT message the MME shall indicate either:

a) "dual-registration not supported" if the MME supports interworking procedures with N26 interface; or

b) "dual-registration supported" if the MME supports interworking procedures without N26 interface.

iii) If the MME indicated "dual-registration not supported", the UE shall operate in single-registration mode. If the MME indicated "dual-registration supported" and the UE supports dual-registration mode, the UE shall operate in dual-registration mode. If the MME indicated "dual-registration supported" and the UE only supports single-registration mode, the UE shall operate in single-registration mode. If the MME indicated neither "dual-registration not supported" nor "dual-registration supported", the UE shall operate in single-registration mode. The interworking procedures required for coordination between 5GMM and EMM without N26 interface are specified in subclause 11.2.3.

B) Temporary identity

i) At inter-system change from N1 mode to S1 mode the UE operating in the single-registration mode that has a valid 5G-GUTI shall include a 4G-GUTI mapped from map the 5G-GUTI as specified in 3GPP TS 23.003 [5] in the EPS mobile identity IE, and include Old GUTI type IE with GUTI type set to "native GUTI".

ii) If the UE operating in the single-registration mode holds a valid 4G-GUTI and a valid 5G-GUTI, it shall include in the EPS mobile identity IE of the ATTACH REQUEST message either 4G-GUTI or 4G-GUTI mapped from the 5G-GUTI (as specified in 3GPP TS 23.003 [5]) according to the system (i.e. either EPS or 5GS), where the last successful EPS attach, tracking area updating or registration procedure was performed. In this case, the GUTI type field of the Old GUTI type IE shall be set to "native GUTI".

iii) At inter-system change from N1 mode to S1 mode, the UE operating in the dual-registration mode that has a valid 4G-GUTI shall include the 4G-GUTI in the EPS mobile identity IE, and include Old GUTI type IE with GUTI type set to "native GUTI". The UE operating in the dual-registration mode shall not use the 5G-GUTI even if the UE has a valid 5G-GUTI.

C) Mobility indication

i) The UE shall include a UE status IE with a 5GMM registration status set to "UE is in 5GMM-REGISTERED state"n in the ATTACH REQUEST message.

Editor's note: The enconding of the UE status IE indication is FFS.

2) Normal tracking area updating procedure and combined tracking area updating procedure

A) At inter-system change from N1 mode to S1 mode the UE operating in the single-registration mode shall include a 4G-GUTI mapped from the 5G-GUTI as specified in 3GPP TS 23.003 [5] in the EPS mobile identity IE, and include Old GUTI type IE with GUTI type set to "native GUTI".

B) The UE operating in the dual-registration mode that has a valid 4G-GUTI shall include the 4G-GUTI in the EPS mobile identity IE, and include Old GUTI type IE with GUTI type set to "native GUTI". The UE operating in the dual-registration mode shall not use the 5G-GUTI even if the UE has a valid 5G-GUTI.

C) The UE shall include a UE status IE with a 5GMM registration status set to "UE is in 5GMM-REGISTERED state" indication in the TRACKING AREA UPDATE REQUEST message.

3) UE requested PDN connectivity procedure

A) The PDU CONNECTIVITY REQUEST message(s) triggered by the UE operating in the dual-registration mode intending to transfer PDU sessions from the 5GS to the EPS, shall include the request type IE set to "Handover" in the PDN CONNECTIVITY REQUEST message.

NOTE: The usage of "Handover" value in the request type IE needs to be extended to cover transferring PDU sessions from 5GC to EPS.

B) The PDU Session ID is sent to the network in the protocol configuration options IE or extended protocol configuration options IE in the PDN CONNECTIVITY REQUEST message if the UE is operating in the single-registration mode.

C) 5G QoS parameters including session-AMBR and QoS rules are sent to the UE in the protocol configuration options IE or extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER REQUEST message.

D) The PDU CONNECTIVITY REQUEST message(s) triggered by the UE operating in the dual-registration mode intending to transfer PDU sessions with PDU session type "Ethernet" or "Unstructured" from the 5GS to the EPS, shall include the PDN type IE set to "non-IP" in the PDN CONNECTIVITY REQUEST message.

4) Dedicated EPS bearer context activation procedure

A) The 5G QoS parameters including session-AMBR and QoS rules are sent to the UE in the protocol configuration options IE or in the extended protocol options IE in the ACTIVATE DEDICATED EPS BEARER REQUEST message.

5) EPS bearer context modification procedure

A) The 5G QoS parameters including session-AMBR and QoS rules are sent to the UE in the protocol configuration options IE or in the extended protocol configuration options IE in the MODIFY EPS BEARER REQUEST message.

Annex E (informative):  
Proposed changes to 3GPP TS 24.007

# E.1 First change

##### 11.2.3.1.X PDU session identity

A L3 protocol may define that octet 2 of a standard L3 message of the protocol contains the PDU session identity. The PDU session identity is used to identify a PDU session.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | PDU session identity | | | | | | | | octet 1 |

Figure 11.9Y: PDU session identity

Table 11.5Z: PDU session identity

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PDU session identity value (octet 1, bit 1 to bit 8) | | | | | | | | |
| Bits | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | No PDU session identity assigned |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | Reserved |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | Reserved |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | Reserved |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | Reserved |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | PDU session identity value 5 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | PDU session identity value 6 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | PDU session identity value 7 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | PDU session identity value 8 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | PDU session identity value 9 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | PDU session identity value 10 |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | PDU session identity value 11 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | PDU session identity value 12 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | PDU session identity value 13 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | PDU session identity value 14 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | PDU session identity value 15 |
| All other values are spare values | | | | | | | | |

Annex F (informative):  
Proposed changes to 3GPP TS 24.008

The list of impacts that should be captured in 3GPP TS 24.008 [12] is as follows:

1) The coding of the protocol configuration options

A) The PDU Session ID, 5G QoS parameters including session-AMBR and QoS rules are added in the protocol configuration options.

Annex G:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **Tdoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2017-04 | CT1#103 | C1-171624 |  |  |  | Draft skeleton provided by the rapporteur. | 0.0.0 |
| 2017-04 | CT1#103 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-171512, C1-171516, C1-171623, C1-171632, C1-171634, C1-171638, C1-171959, C1-171960, C1-171662, C1-171971, C1-171973, C1-171974, C1-171975. | 0.1.0 |
| 2017-05 | CT1#104 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-172298, C1-172410, C1-172411, C1-172412, C1-172628, C1-172643, C1-172416, C1-172427, C1-172429, C1-172430, C1-172431, C1-172432, C1-172630, C1-172632, C1-172654, C1-172655, C1-172769, C1-172770, C1-172771, C1-172772, C1-172773, C1-172780, C1-172786, C1-172633, C1-172634, C1-172635, C1-172636, C1-172637, C1-172645, C1-172646, C1-172647, C1-172656, C1-172775, C1-172472, C1-172777, C1-172640, C1-172659, C1-172661, C1-172662, C1-172776, C1-172778, C1-172779 | 0.2.0 |
| 2017-06 | CT1 e-mail review |  |  |  |  | Implementation of C1-172773 under clause 6 instead of clause 10. Also, the TR clauses from clause 11 onwards have been renumbered due to the move of the previous clause 10. | 0.2.1 |
| 2017-08 | CT1#105 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-173180, C1-173076, C1-173181, C1-173189, C1-173183, C1-173352, C1-173799, C1-173804, C1-173195, C1-173198, C1-173358, C1-173359, C1-173360, C1-173361, C1-173362, C1-173363, C1-173364, C1-173550, C1-173555, C1-173556, C1-173358, C1-173714, C1-173715, C1-173716, C1-173717, C1-173728, C1-173729, C1-173730, C1-173762, C1-173763, C1-173764, C1-173800, C1-173801, C1-173803, C1-173809, C1-173367, C1-173511, C1-173718, C1-173819, C1-173740, C1-173742, C1-173766, C1-173771, C1-173787, C1-173802, C1-173798, C1-173803, C1-173805, C1-173581, C1-173743, C1-173745, C1-173788, C1-173789, C1-173790, C1-173791, C1-173795, C1-173397, C1-173500, C1-173501, C1-173191, C1-173344, C1-173388, C1-173394, C1-173502, C1-173508, C1-173509, C1-173578, C1-173579, C1-173595, C1-173722, C1-173767, C1-173768, C1-173792, C1-173793, C1-173794, C1-173185, C1-173011, C1-173559, C1-173723, C1-173769, C1-173562 | 0.3.0 |
| 2017-09 | CT1 e-mail review |  |  |  |  | Implementation of part of C1-173364 as some changes were missing.  Editorial corrections. | 0.3.1 |
| 2017-09 | CT1 e-mail review |  |  |  |  | Editorial corrections. | 0.3.2 |
| 2017-09 |  | CP-173035 |  |  |  | Version 1.0.0 created for presentation to TSG CT#77 for information. | 1.0.0 |
| 2017-09 | CT1 e-mail review |  |  |  |  | Implementation of missing parts of C1-172803, C1-173508, C1-173719, C1-173766. | 1.0.1 |
| 2017-09 | CT1 e-mail review |  |  |  |  | Re-implementation of the missing part of C1-173508 which was introduced in a wrong bullet list in the previous version.  Implementation of missing parts of C1-173714.  Editorial corrections. | 1.0.2 |
| 2017-09 | CT1 e-mail review |  |  |  |  | Implementation of missing parts of C1-173550.  Editorial corrections. | 1.0.3 |
| 2017-11 | CT1#106 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-174132, C1-174216, C1-174188, C1-174201, C1-174165, C1-174289, C1-174292, C1-174570, C1-174571, C1-174645, C1-174646, C1-173821, C1-174145, C1-174202, C1-174204, C1-173913, C1-174137, C1-174208, C1-174141, C1-174206, C1-173842, C1-174269, C1-174302, C1-174304, C1-174307, C1-174312, C1-174313, C1-174381, C1-174396, C1-174503, C1-174558, C1-174559, C1-174574, C1-174575, C1-174580, C1-174582, C1-174584, C1-174586, C1-174591, C1-174599, C1-174600, C1-174601, C1-174602, C1-174603, C1-174604, C1-174605, C1-174606, C1-174607, C1-174625, C1-174632, C1-174633, C1-174648, C1-174649, C1-174650, C1-174668, C1-174670, C1-174673, C1-174187, C1-173822, C1-174315, C1-174320, C1-174321, C1-174588, C1-174608, C1-174609, C1-174610, C1-174674, C1-174179, C1-174327, C1-174328, C1-174329, C1-174613, C1-174615, C1-174343, C1-174547, C1-174550, C1-174551, C1-174553, C1-174554, C1-174590, C1-174614, C1-174652, C1-174667, C1-174093, C1-174094, C1-174009, C1-174342, C1-174347, C1-174349, C1-174538, C1-174569, C1-174616, C1-174635, C1-174659, C1-174642, C1-174644, C1-174653, C1-174654, C1-174655, C1-174656, C1-174675, C1-174540, C1-174541, C1-174669 | 1.1.0 |
| 2017-11 | CT1 e-mail review |  |  |  |  | Implementation of part of C1-174538, C1-174632, C1-174645, C1-174675 as some changes were missing or were implemented with editorial mistakes.  C1-174655 implemented again in order to be located under the correct sub-clause.  Editorial corrections. | 1.1.1 |
| 2017-12 | CT1#107 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-174877, C1-175093, C1-175096, C1-175097, C1-175313, C1-175314, C1-175315, C1-175334, C1-175375, C1-175417, C1-175086, C1-175087, C1-175093, C1-175089, C1-175336, C1-174894, C1-174700, C1-174699, C1-174887, C1-175050, C1-174896, C1-174893, C1-174819, C1-175035, C1-174960, C1-174899, C1-174821, C1-174931, C1-174927, C1-174995, C1-175100, C1-175101, C1-175103, C1-175104, C1-175105, C1-175107, C1-175111, C1-175112, C1-175114, C1-175116, C1-175117, C1-175118, C1-175119, C1-175120, C1-175180, C1-175181, C1-175184, C1-175185, C1-175186, C1-175187, C1-175194, C1-175300, C1-175301, C1-175303, C1-175305, C1-175333, C1-175337, C1-175338, C1-175339, C1-175349, C1-175355, C1-175356, C1-175366, C1-175369, C1-175385, C1-175391, C1-175400, C1-175401, C1-175402, C1-175403, C1-175404, C1-175405, C1-175410, C1-175411, C1-174895, C1-174788, C1-175068, C1-174885, C1-175121, C1-175122, C1-175123, C1-175125, C1-175127, C1-175128, C1-175129, C1-175130, C1-175177, C1-175341, C1-175342, C1-175343, C1-175357, C1-175358, C1-175360, C1-175361, C1-175399, C1-175051, C1-175131, C1-175132, C1-175386, C1-175135, C1-175136, C1-175141, C1-175142, C1-175344, C1-175347, C1-175396, C1-175397, C1-175398, C1-174769, C1-174963, C1-174966, C1-174852, C1-175144, C1-175150, C1-175151, C1-175153, C1-175154, C1-175173, C1-175175, C1-175179, C1-175192, C1-175370, C1-175371, C1-175387, C1-175357, C1-175406, C1-175155, C1-175156, | 1.2.0 |
| 2017-12 | CT-78 | CP-173043 |  |  |  | Version 2.0.0 created for presentation to TSG CT#77 for approval. | 2.0.0 |
| 2017-12 | CT-78 |  |  |  |  | Version 15.0.0 created after approval | 15.0.0 |
| 2018-03 | CT-79 | CP-180075 | 0002 | 4 | B | Extension of alternative 1 for steering of roaming | 15.1.0 |
| 2018-03 | CT-79 | CP-180075 | 0005 | 6 | B | Update of Alternative 1 for steering of UE in VPLMN | 15.1.0 |
| 2018-03 | CT-79 | CP-180076 | 0006 |  | F | Fixing missing parts of the security mode command procedure from C1-175411 | 15.1.0 |
| 2018-03 | CT-79 | CP-180077 | 0008 |  | F | Correction to the mapping table to 3GPP TS 24.501 | 15.1.0 |
| 2018-03 | CT-79 | CP-180076 | 0009 | 1 | F | Conclusion on alternatives on archictecure for PWS in 5GS | 15.1.0 |
| 2018-03 | CT-79 | CP-180076 | 0010 | 1 | F | Conclusion on alternatives on unified access control | 15.1.0 |
| 2018-03 | CT-79 | CP-180075 | 0011 | 2 | F | Conclusion on steering of UE in VPLMN | 15.1.0 |
| 2018-03 | CT-79 | CP-180075 | 0012 | 1 | F | Update to impacts to specifications | 15.1.0 |
| 2018-03 | CT-79 | CP-180076 | 0013 | 3 | B | Stage 2 solution of Steering Of Roaming (SOR) based on Authentication procedure during Registration (Alternative 3) | 15.1.0 |
| 2018-03 | CT-79 | CP-180076 | 0015 | 2 | B | 5GS PWS evaluation and conclusion | 15.1.0 |
| 2018-03 | CT-79 | CP-180076 | 0016 | 2 | F | Unified Access Control – Merging alternative 2 and alternative1 | 15.1.0 |
| 2018-03 | CT-79 | CP-180076 | 0017 | 3 | B | 5GS PWS architecture option with and without IWF | 15.1.0 |
| 2018-03 | CT-79 | CP-180075 | 0022 | 2 | B | NAS signaling encapsulation over non-3GPP untrusted access | 15.1.0 |
| 2020-07 | SA-88e | - | - | - | - | Update to Rel-16 version (MCC) | **16.0.0** |