3GPP TS 33.501 V15.3.1 (2018-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security architecture and procedures for 5G system
(Release 15)

A GLOBAL INITIATIVE

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 3GPP Organizational Partners and shall not be implemented

DOCKET ALARM

Find authenticated court documents without watermarks at docketalarm.com.

Keywords

security,5G

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.

© 2018, 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

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Contents

Foreword........11

1 Scope........12

2 References........12

3 Definitions and abbreviations........14
3.1 Definitions........14
3.2 Abbreviations........18

4 Overview of security architecture........19
4.1 Security domains........19
4.2 Security entity at the perimeter of the 5G Core network........20
4.3 Security entities in the 5G Core network........20

5 Security requirements and features........20
5.1 General security requirements........20
5.1.1 Mitigation of bidding down attacks........20
5.1.2 Authentication and Authorization........20
5.1.3 Requirements on 5GC and NG-RAN related to keys........21
5.2 Requirements on the UE........21
5.2.1 General........21
5.2.2 User data and signalling data confidentiality........21
5.2.3 User data and signalling data integrity........22
5.2.4 Secure storage and processing of subscription credentials........22
5.2.5 Subscriber privacy........23
5.3 Requirements on the gNB........23
5.3.1 General........23
5.3.2 User data and signalling data confidentiality........23
5.3.3 User data and signalling data integrity........24
5.3.4 Requirements for the gNB setup and configuration........24
5.3.5 Requirements for key management inside the gNB........24
5.3.6 Requirements for handling user plane data for the gNB........25
5.3.7 Requirements for handling control plane data for the gNB........25
5.3.8 Requirements for secure environment of the gNB........25
5.3.9 Requirements for the gNB F1 interfaces........25
5.3.10 Requirements for the gNB E1 interfaces........25
5.4 Requirements on the ng-eNB........26
5.5 Requirements on the AMF........26
5.5.1 Signalling data confidentiality........26
5.5.2 Signalling data integrity........26
5.5.3 Subscriber privacy........26
5.6 Requirements on the SEAF........26
5.7 Void........27
5.8 Requirements on the UDM........27
5.8.1 Generic requirements........27
5.8.2 Subscriber privacy related requirements to UDM and SIDF........27
5.8a Requirements on AUSF........27
5.9 Core network security........27
5.9.1 Trust boundaries........27
5.9.2 Requirements on service-based architecture........27
5.9.2.1 Security Requirements for service registration, discovery and authorization........27
5.9.2.2 NRF security requirements........28
5.9.2.3 NEF security requirements........28
5.9.3 Requirements for e2e core network interconnection security........28
5.9.3.1 General........28
5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP)........29
5.9.3.3 Protection of attributes........29
5.10 Visibility and configurability........30

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

5.10.1 Security visibility 30
5.10.2 Security configurability 30
5.11 Requirements for algorithms, and algorithm selection 30
5.11.1 Algorithm identifier values 30
5.11.1.1 Ciphering algorithm identifier values 30
5.11.1.2 Integrity algorithm identifier values 30
5.11.2 Requirements for algorithm selection 31

6 Security procedures between UE and 5G network functions 32
6.1 Primary authentication and key agreement 32
6.1.1 Authentication framework 32
6.1.1.1 General 32
6.1.1.2 EAP framework 32
6.1.1.3 Granularity of anchor key binding to serving network 33
6.1.1.4 Construction of the serving network name 33
6.1.1.4.1 Serving network name 33
6.1.1.4.2 Construction of the serving network name by the UE 33
6.1.1.4.3 Construction of the serving network name by the SEAF 33
6.1.2 Initiation of authentication and selection of authentication method 34
6.1.3 Authentication procedures 35
6.1.3.1 Authentication procedure for EAP-AKA' 35
6.1.3.2 Authentication procedure for 5G AKA 37
6.1.3.2.0 5G AKA 37
6.1.3.2.1 Void 39
6.1.3.2.2 RES* verification failure in SEAF or AUSF or both 39
6.1.3.3 Synchronization failure or MAC failure 40
6.1.3.3.1 Synchronization failure or MAC failure in USIM 40
6.1.3.3.2 Synchronization failure recovery in Home Network 40
6.1.4 Linking increased home control to subsequent procedures 41
6.1.4.1 Introduction 41
6.1.4.1a Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF 41
6.1.4.2 Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF 42
6.2 Key hierarchy, key derivation, and distribution scheme 43
6.2.1 Key hierarchy 43
6.2.2 Key derivation and distribution scheme 45
6.2.2.1 Keys in network entities 45
6.2.2.2 Keys in the UE 46
6.2.3 Handling of user-related keys 48
6.2.3.1 Key setting 48
6.2.3.2 Key identification 48
6.2.3.3 Key lifetimes 49
6.3 Security contexts 50
6.3.1 Distribution of security contexts 50
6.3.1.1 General 50
6.3.1.2 Distribution of subscriber identities and security data within one 5G serving network domain 50
6.3.1.3 Distribution of subscriber identities and security data between 5G serving network domains 50
6.3.1.4 Distribution of subscriber identities and security data between 5G and EPS serving network domains 50
6.3.2 Multiple registrations in same or different serving networks 51
6.3.2.0 General 51
6.3.2.1 Multiple registrations in different PLMNs 51
6.3.2.2 Multiple registrations in the same PLMN 51
6.4 NAS security mechanisms 51
6.4.1 General 51
6.4.2 Security for multiple NAS connections 51
6.4.2.1 Multiple active NAS connections with different PLMNs 51
6.4.2.2 Multiple active NAS connections in the same PLMN's serving network 52
6.4.3 NAS integrity mechanisms 52
6.4.3.0 General 52
6.4.3.1 NAS input parameters to integrity algorithm 52
6.4.3.2 NAS integrity activation 53

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

6.4.3.3 NAS integrity failure handling 53
6.4.4 NAS confidentiality mechanisms 53
6.4.4.0 General 53
6.4.4.1 NAS input parameters to confidentiality algorithm 53
6.4.4.2 NAS confidentiality activation 53
6.4.5 Handling of NAS COUNTs 53
6.4.6 Protection of initial NAS message 54
6.4.7 Security aspects of SMS over NAS 55
6.5 RRC security mechanisms 55
6.5.1 RRC integrity mechanisms 55
6.5.2 RRC confidentiality mechanisms 55
6.6 UP security mechanisms 56
6.6.1 UP security policy 56
6.6.2 UP security activation mechanism 57
6.6.3 UP confidentiality mechanisms 58
6.6.4 UP integrity mechanisms 58
6.7 Security algorithm selection, key establishment and security mode command procedure 58
6.7.1 Procedures for NAS algorithm selection 58
6.7.1.1 Initial NAS security context establishment 58
6.7.1.2 AMF change 58
6.7.2 NAS security mode command procedure 59
6.7.3 Procedures for AS algorithm selection 60
6.7.3.0 Initial AS security context establishment 60
6.7.3.1 Xn-handover 61
6.7.3.2 N2-handover 61
6.7.3.3 Intra-gNB-CU handover 61
6.7.3.4 Transitions from RRC-INACTIVE to RRC-CONNECTED states 61
6.7.3.5 RNA Update procedure 62
6.7.3.6 Algorithm negotiation for unauthenticated UEs in LSM 62
6.7.4 AS security mode command procedure 62
6.8 Security handling in state transitions 63
6.8.1 Key handling at connection and registration state transitions 63
6.8.1.1 Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states 63
6.8.1.1.0 General 63
6.8.1.1.1 Transition from RM-REGISTERED to RM-DEREGISTERED 64
6.8.1.1.2 Transition from RM-DEREGISTERED to RM-REGISTERED 65
6.8.1.1.2.1 General 65
6.8.1.1.2.2 Full native 5G NAS security context available 65
6.8.1.1.2.3 Full native 5G NAS security context not available 66
6.8.1.1.2.4 UE registration over a second access type to the same AMF 66
6.8.1.2 Key handling at transitions between CM-IDLE and CM-CONNECTED states 66
6.8.1.2.0 General 66
6.8.1.2.1 Transition from CM-IDLE to CM-CONNECTED 67
6.8.1.2.2 Establishment of keys for cryptographically protected radio bearers in 3GPP access 67
6.8.1.2.3 Establishment of keys for cryptographically protected traffic in non-3GPP access 68
6.8.1.2.4 Transition from CM-CONNECTED to CM-IDLE 68
6.8.1.3 Key handling for the Registration procedure when registered in NG-RAN 68
6.8.2 Security handling at RRC state transitions 69
6.8.2.1 Security handling at transitions between RRC_INACTIVE and RRC-CONNECTED states 69
6.8.2.1.1 General 69
6.8.2.1.3 State transition from RRCINACTIVE to RRCCONNECTED to a new gNB 69
6.8.2.1.4 State transition from RRCINACTIVE to RRCCONNECTED to the same gNB 71
6.8.2.2 Key handling during mobility in RRC-INACTIVE state 71
6.8.2.2.1 General 71
6.8.2.2.2 RAN-based notification area update to a new gNB 71
6.8.2.2.3 RAN-based notification area update to the same gNB 71
6.9 Security handling in mobility 71
6.9.1 General 71
6.9.2 Key handling in handover 72
6.9.2.1 General 72
6.9.2.1.1 Access stratum 72
6.9.2.1.2 Non access stratum 73

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**