

ICS 33.020
CCS M 04



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 46462-2025

**Technical requirements on communication security of 5G
mobile communication network**

5G移动通信网通信安全技术要求

Issued on: October 31, 2025

Implemented on: February 1, 2026

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

1.Scope	1
2 Normative References	1
3.1 Terms and Definitions	4
3.2 Abbreviations	6
4.Security Architecture Overview	9
4.1 Security Domain	9
4.2 Security Functions at the Edge of the 5G Core Network	10
4.3 Security Functions in 5G Core Networks	10
5.Safety Requirements and Functional Requirements	11
5.1 General Safety Requirements	11
5.2 UE Security Requirements	11
5.3 gNB Security Requirements	13
5.4 ng-eNB Security Requirements	15
5.5 AMF Safety Requirements	15
5.6 SEAF Safety Requirements	15
5.7 UDM Security Requirements	16
5.8 Core Network Security Requirements	16
5.9 Security Visibility and Configurability Requirements	19
5.10 Algorithms and Algorithm Selection Requirements 20 5.11 5G-RG Security Requirements	21
5.12 NSSAAF Safety Requirements	21
6.Security procedures between UE and 5G network functional entities	21
6.1 Master Authentication and Key Negotiation	21
6.2 Hierarchical structure of keys and derivation and distribution mechanism	30
6.3 Security Context	36
6.4 Non-access stratum security mechanisms	38
6.5 RRC Security Mechanism	42
6.6 Access Layer User Plane Security Mechanisms	42
6.7 Security Algorithm Negotiation	45
6.8 State Transition Safety Handling	50
6.9 Mobility Management Security	58
6.10 Dual-Connect Security	67

6.11 Safety procedures during RRC connection reconstruction	73
6.12 User Privacy Protection	74
6.13 Signaling Flow of PDCPCOUNT Verification	77
6.14 Roaming Guidance Security Mechanism	77
6.15 Security Mechanism for UE Parameter Update via UDM Control Plane 81 6.16 5G Cellular IoT Security	83
7.Security of non-cellular access to 5G core networks	87
7.1 Access Security Principles	87
7.2 Authentication Security Process for Untrusted Non-Cellular Access	88
7.3 Security Procedures for Trusted Non-Cellular Wireless Access	91
7.4 Wired Access Security Procedures	96
8.1 General Safety Requirements	100
8.2 Security process for mobility registration from EPS to 5GS based on N26 interface	100
8.3 Switching process from 5GS to EPS based on N26 interface	101
8.4 Switching process from EPS to 5GS based on N26 interface	104
26 Interface	107
8.6 Mapping of Security Contexts	109
9.1 Basic Principles	110
2 Interface	110
3 Interface	111
9.4 Security Mechanisms of the Xn Interface	111
9.5 Security mechanisms using GTP or DIAMETER protocol interfaces	111
9.6 Security Protection Mechanism for gNB Internal Interfaces	111
9.7 Security Mechanisms for Non-Service-Based Interfaces within the 5G Core Network 112 10 IMS Emergency Call Security	113
10.2 Unauthenticated IMS emergency calls to	114
11.Security procedures for UE interaction with external data networks via 5G network ..	116
11.1 General requirements for secondary authentication between EAP-based AAA servers and external data networks	116
11.2 Secondary Authentication Process	116
11.3 Re-authentication process	119
11.4 Revocation of Authentication Authorization	120
12 Security protection for Network Open Functional Entity (NEF)	120
12.1 Basic Principles	120
12.2 Two-way authentication	120

12.3 Safety protection between NEF and AF	120
12.4 Authorization Verification of AF Requests	120
12.5 Support for CAPIF	121
13 Service-Oriented Interface Security	121
13.1 Security protection at the network layer or transport layer	121
32 Interface	123
13.3 Authentication and Static Licensing	137
13.4 Authorization during NF service requests	140
13.5 Security Capability Negotiation among SEPPs	151
14 Security Services	152
14.1 Security Services Provided by AUSF	152
14.2 Security Services Provided by UDM	153
14.3 Security Services Provided by NRF	154
15 Network Slice Management Security	154
15.1 Overview	154
15.2 Two-way authentication	154
15.3 Security Protection for Management Interactions Between Service Producers and Users	155
15.4 Authorization Verification of Management Service Request Messages	155
16. Dual-connectivity security in non-standalone networking	161
2 Interface	162
16.3 Additions and modifications to DRB (Data Radio Bearer) and/or SRB (Signaling Radio Bearer) in SgNB	162
16.4 Activation of DRB encryption/decryption/integrity protection and SRB encryption/decryption/integrity protection	162
16.6 S-KgNB Update	165
16.7 Switching Process	165
16.8 Periodic Local Authentication Process	166
16.9 Wireless connection failure recovery	166
16.10 Avoid keystream reuse due to DRB type changes	166
16.11 Security between UE and SgNB	166
17.1 Call continuity from NR to UTRAN	167
17.2 Emergency Calls Continuing from NR to UTRAN 168 18 5G LAN Service Security	168
18.1 Overview	168
18.2 Authentication and Authorization	168

18.3 UP Security Policy Processing	169
19.Security of Time-Sensitive Network Services	169
19.1 Overview	169
19.2 Access Security for UEs with 5G STSC Enabled	169
19.3 Protecting user plane data in TSC includes (g)PTP control messages in bridged mode	169
19.4 Time synchronization interface exposed 169 20 5G High Reliability, Low Latency, and Security Requirements	169
20.1 Overview	169
20.2 Security Assurance for Redundant Transmission	169
20.3 Redundant transmission of N3/N9 interface	170
21 Edge computing security	170
21.1 Overview	170
21.2 Security of Network Exposure to Edge Application Servers	170
22 User license requirements	171
22.1 Overview	171
22.2 User consent required	171
23 Enhanced security mechanisms for 5G multicast services	172
23.1 MBSF Requirements	172
23.2 MBSTF requirement	172
23.3 Security Mechanisms for xMB-C/MB2-C and xMB-U/MB2-U Interfaces	172
23.4 MBS Streaming Security Mechanisms	172
23.5 Security protection for 5MBS and eMBMS interoperability	174
24 Large-Scale IoT Message Security	174
24.1 Overview	174
24.2 Authentication and Authorization between 5G IoT Messaging Terminals and 5G IoT Messaging Servers 174	
24.3 5G IoT Messaging System Interface Security Protection	175
24.4 Identity Authentication and Authorization between Application Server and 5G IoT Messaging Server	175

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1.Structure and Drafting Rules of Standardization Documents". Drafting. Some content in this document may involve patents. The issuing organization of this document assumes no