ICS 33.020
CCS M 04

中华人民共和国国家标准

GB/T 46462—2025

5G 移动通信网通信安全技术要求

Technical requirements on communication security of 5G mobile communication network

2025-10-31 发布　　2026-02-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅶ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 4
3.1　术语和定义 …… 4
3.2　缩略语 …… 6
4　安全架构概述 …… 9
4.1　安全域 …… 9
4.2　5G 核心网络边缘的安全功能 …… 10
4.3　5G 核心网络中的安全功能 …… 10
5　安全需求与功能要求 …… 11
5.1　通用安全要求 …… 11
5.2　UE 安全要求 …… 11
5.3　gNB 安全要求 …… 13
5.4　ng-eNB 安全要求 …… 15
5.5　AMF 安全要求 …… 15
5.6　SEAF 安全要求 …… 15
5.7　UDM 安全要求 …… 16
5.8　核心网安全要求 …… 16
5.9　安全可视性与可配置性要求 …… 19
5.10　算法与算法选择要求 …… 20
5.11　5G-RG 安全要求 …… 21
5.12　NSSAAF 安全要求 …… 21
6　UE 与 5G 网络功能实体间的安全流程 …… 21
6.1　主认证与密钥协商 …… 21
6.2　密钥的分层结构及推衍与分发机制 …… 30
6.3　安全上下文 …… 36
6.4　非接入层安全机制 …… 38
6.5　RRC 安全机制 …… 42
6.6　接入层用户面安全机制 …… 42
6.7　安全算法协商 …… 45
6.8　状态转换安全处理 …… 50
6.9　移动性管理安全 …… 58

6.10 双连接安全 …… 67
6.11 RRC 连接重建过程的安全处理 …… 73
6.12 用户隐私保护 …… 74
6.13 PDCP COUNT 核查的信令流程 …… 77
6.14 漫游引导安全机制 …… 77
6.15 通过 UDM 控制面的 UE 参数更新的安全机制 …… 81
6.16 5G 蜂窝物联网安全 …… 83
7 非蜂窝接入 5G 核心网络的安全 …… 87
7.1 接入安全原则 …… 87
7.2 对不可信的非蜂窝接入的认证安全流程 …… 88
7.3 可信非蜂窝无线接入的安全流程 …… 91
7.4 有线接入安全流程 …… 96
8 互操作安全 …… 100
8.1 通用安全要求 …… 100
8.2 基于 N26 接口的从 EPS 到 5GS 的移动性注册安全流程 …… 100
8.3 基于 N26 接口的从 5GS 到 EPS 的切换流程 …… 101
8.4 基于 N26 接口的从 EPS 到 5GS 的切换流程 …… 104
8.5 基于 N26 接口的从 5GS 到 EPS 的空闲态移动安全流程 …… 107
8.6 安全上下文的映射 …… 109
8.7 无 N26 接口的单注册互操作安全 …… 110
9 非服务化接口安全 …… 110
9.1 基本原则 …… 110
9.2 N2 接口的安全机制 …… 110
9.3 N3 接口的安全机制 …… 111
9.4 Xn 接口的安全机制 …… 111
9.5 使用 GTP 或者 DIAMETER 协议接口的安全机制 …… 111
9.6 gNB 内部接口的安全保护机制 …… 111
9.7 5G 核心网内部非基于服务的接口安全机制 …… 112
10 IMS 紧急呼叫安全 …… 113
10.1 通过身份认证的 IMS 紧急呼叫 …… 113
10.2 未经身份认证的 IMS 紧急呼叫 …… 114
11 UE 通过 5G 网络与外部数据网络之间交互的安全流程 …… 116
11.1 基于 EAP 的与外部数据网络的 AAA 服务器之间的次认证通用要求 …… 116
11.2 次认证流程 …… 116
11.3 重认证流程 …… 119
11.4 次认证授权的撤回 …… 120
12 网络开放功能实体(NEF)的安全保护 …… 120

12.1 基本原则 …… 120
12.2 双向认证 …… 120
12.3 NEF 与 AF 之间的安全保护 …… 120
12.4 对 AF 请求的授权验证 …… 120
12.5 对 CAPIF 的支持 …… 121
13 服务化接口安全 …… 121
13.1 网络层或传输层的安全保护 …… 121
13.2 N32 接口上的应用层安全保护 …… 123
13.3 认证和静态授权 …… 137
13.4 NF 服务请求时的授权 …… 140
13.5 SEPP 间的安全能力协商 …… 151
14 安全服务 …… 152
14.1 AUSF 提供的安全服务 …… 152
14.2 UDM 提供的安全服务 …… 153
14.3 NRF 提供的安全服务 …… 154
15 网络切片管理安全 …… 154
15.1 概述 …… 154
15.2 双向认证 …… 154
15.3 管理服务生产者与使用者之间管理交互的安全保护 …… 155
15.4 管理服务请求消息的授权验证 …… 155
15.5 网络切片安全流程 …… 155
16 非独立组网的双连接安全 …… 161
16.1 基本原则 …… 161
16.2 X2 接口的保护 …… 162
16.3 SgNB 中 DRB(数据无线承载)和/或 SRB(信令无线承载)的增加和修改 …… 162
16.4 DRB 加/解密/完整性保护和 SRB 加/解密/完整性保护的激活 …… 162
16.5 在 SgNB 的 PDCP 中为无线承载推衍密钥 …… 164
16.6 S-K_{gNB}更新 …… 165
16.7 切换流程 …… 165
16.8 周期性本地认证流程 …… 166
16.9 无线连接失效恢复 …… 166
16.10 避免因 DRB 类型改变引起的密钥流重用 …… 166
16.11 UE 和 SgNB 间安全 …… 166
17 5G 到 3G 的呼叫连续性安全 …… 167
17.1 NR 到 UTRAN 的呼叫连续性 …… 167
17.2 NR 到 UTRAN 呼叫连续性的紧急呼叫 …… 168
18 5G 局域网服务安全 …… 168

18.1 概述 …… 168
18.2 认证和授权 …… 168
18.3 UP 安全策略的处理 …… 169
19 时间敏感网络服务安全 …… 169
19.1 概述 …… 169
19.2 启用 5GS TSC 的 UE 的接入安全性 …… 169
19.3 在 TSC 中保护用户平面数据包括桥接模式下的(g)PTP 控制消息 …… 169
19.4 时间同步的接口开放 …… 169
20 5G 高可靠低时延安全要求 …… 169
20.1 概述 …… 169
20.2 冗余传输的安全保障 …… 169
20.3 N3/N9 接口的冗余传输 …… 170
21 边缘计算安全 …… 170
21.1 概述 …… 170
21.2 网络开放给边缘应用服务器的安全 …… 170
22 用户许可要求 …… 171
22.1 概述 …… 171
22.2 用户同意要求 …… 171
23 增强的 5G 多播广播业务安全机制 …… 172
23.1 MBSF 的要求 …… 172
23.2 MBSTF 的要求 …… 172
23.3 xMB-C/MB2-C 与 xMB-U/MB2-U 接口的安全机制 …… 172
23.4 MBS 流传输的安全机制 …… 172
23.5 5MBS 与 eMBMS 互通的安全保护 …… 174
24 大规模物联网消息安全 …… 174
24.1 概述 …… 174
24.2 5G 物联网消息终端和 5G 物联网消息服务器之间的认证和授权 …… 174
24.3 5G 物联网消息系统接口安全保护 …… 175
24.4 应用服务器与 5G 物联网消息服务器之间的身份认证与授权 …… 175
24.5 消息网关与 5G 物联网消息服务器之间的认证与授权 …… 175
附录 A（规范性） 加密与完整性保护算法 …… 176
A.1 空加密和完整性保护算法 …… 176
A.2 128 比特加密算法 …… 176
A.3 128 比特完整性保护算法 …… 177
A.4 安全算法的测试数据 …… 178
附录 B（资料性） 基于额外的 EAP 方式实现主认证 …… 180
B.1 基本原则 …… 180

B.2 初始认证与密钥协商 …… 180
B.3 密钥推衍 …… 184
附录 C（规范性） 密钥推衍功能 …… 185
C.1 KDF 接口和输入参数构建 …… 185
C.2 K_{AUSF} 推衍函数 …… 185
C.3 CK′和 IK′推衍函数 …… 185
C.4 RES^* 和 $XRES^*$ 推衍函数 …… 185
C.5 $HRES^*$ 和 $HXRES^*$ 推衍函数 …… 186
C.6 K_{SEAF} 推衍函数 …… 186
C.7 K_{AMF} 推衍函数 …… 186
C.8 算法密钥推衍函数 …… 187
C.9 K_{gNB} 和 K_{N3IWF} 推衍函数 …… 187
C.10 NH 推衍函数 …… 188
C.11 目标基站 gNB 的 $K_{NG\text{-}RAN}{}^*$ 推衍函数 …… 188
C.12 目标基站 ng-eNB 的 $K_{NG\text{-}RAN}{}^*$ 推衍函数 …… 188
C.13 移动情况下 K_{AMF} 到 $K_{AMF}{}'$ 的推衍 …… 189
C.14 互操作下 K_{AMF} 到 $K_{ASME}{}'$ 推衍 …… 189
C.15 互操作下 K_{ASME} 到 $K_{AMF}{}'$ 推衍 …… 189
C.16 双连接的 K_{SN} 的推衍 …… 190
C.17 SoR-MAC-I_{AUSF} 生成函数 …… 190
C.18 SoR-MAC-I_{UE} 生成函数 …… 190
C.19 UPU-MAC-I_{AUSF} 生成函数 …… 191
C.20 UPU-MAC-I_{UE}/UPU-XMAC-I_{UE} 生成函数 …… 191
C.21 互操作下 K_{AMF} 到 K_{ASME_SRVCC} 推衍 …… 191
C.22 K_{TIPSec} 和 K_{TNAP} 推衍函数 …… 191
C.23 K_{IAB} 生成函数 …… 192
附录 D（规范性） 5G 中的 EAP-AKA′参数定义要求 …… 193
D.1 概述 …… 193
D.2 用户隐私 …… 193
D.3 用户身份和密钥推衍 …… 194
附录 E（规范性） 非公共网络 …… 195
E.1 概述 …… 195
E.2 SNPN 中的认证 …… 195
E.3 SNPN 的服务网络名称 …… 199
E.4 修改 UE 中的 CAG ID 列表 …… 199
E.5 SNPN 的 SUPI 隐私 …… 199
E.6 PNI-NPN 中的认证 …… 199

E.7 SNPN 的授权 …… 199
E.8 SEPP 和互联相关安全流程 …… 199
E.9 SNPN 中 UE 在线签约的安全性 …… 200
附录 F（规范性） SUCI 的保护方法 …… 202
F.1 基本原则 …… 202
F.2 空模式 …… 202
F.3 椭圆曲线加密方案(ECIES) …… 202
附录 G（规范性） 接入回传一体化安全要求 …… 206
G.1 概述 …… 206
G.2 安全要求和功能 …… 206
G.3 IAB 节点集成流程 …… 206
G.4 IAB 节点与 OAM 之间的管理数据保护 …… 208
附录 H（规范性） 5G 系统网络自动化使能安全 …… 209
H.1 概述 …… 209
H.2 NF 服务使用者通过 DCCF 访问数据的授权流程 …… 209
H.3 NF 服务使用者通过 DCCF 访问数据的授权流程(通过 MFAF 返回通知) …… 211
H.4 通过消息框架的数据的安全保护 …… 212
H.5 AF 和 NWDAF 间的数据传输保护 …… 212
H.6 NF 之间 UE 数据的传输保护 …… 212
H.7 用户同意需求 …… 212
参考文献 …… 213

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会(SAC/TC 485)归口。

本文件起草单位：中国移动通信集团有限公司、中国信息通信研究院、中兴通讯股份有限公司、上海诺基亚贝尔股份有限公司、中国信息通信科技集团有限公司、中国联合网络通信集团有限公司、中国电子科技网络信息安全有限公司、高通无线通信技术(中国)有限公司、华为技术有限公司、北京小米移动软件有限公司、爱立信(中国)通信有限公司、中国电信集团有限公司、浪潮通信技术有限公司、北京紫光展锐通信技术有限公司、北京首信科技股份有限公司、郑州信大捷安信息技术股份有限公司、北京浩瀚深度信息技术股份有限公司、苹果研发(北京)有限公司、恒安嘉新(北京)科技股份公司、西安通和电信设备检测有限公司、博鼎实华(北京)技术有限公司、北京东方通网信科技有限公司、北京启明星辰信息安全技术有限公司、新华三技术有限公司。

本文件主要起草人：齐旻鹏、吴荣、平静、刘畅、游世林、袁琦、杨红梅、陆伟、刘为华、章乐怡、姚戈、徐晖、王俊、杜志敏、李娜、黄晓婷、谢泽铖、白景鹏、郭龙华、田永春、李晓华、张伟强、崔婷婷、陈涛、庞韶敏、佟婧、郭姝、宋华、孟娟、李星、蒋发群、周雷。

5G 移动通信网通信安全技术要求

1 范围

本文件确立了 5G 移动通信网通信安全架构，规定了 5G 移动通信网的接入安全、网络安全、用户隐私防护、安全服务等通信安全技术要求及安全功能，并描述了相关安全流程等。

本文件适用于面向个人、企业等场景下的 5G 移动通信网络安全架构搭建、安全要求定义与安全能力实施。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2910—2015 LTE/SAE 安全技术要求

YD/T 4743—2024 5G 移动通信网 核心网多播广播技术要求

YD/T 6423—2025 5G 移动通信网支持非公共网络（NPN）技术要求（第二阶段）

3GPP TR 21.905 3GPP 规范词汇表（Vocabulary for 3GPP specifications）

3GPP TS 22.261 下一代新的服务和市场的业务需求（Service requirements for next generation new services and markets）

3GPP TS 23.003 v17.9.0 编号，寻址和标识（Numbering，addressing and identification）

3GPP TS 23.122 v17.9.0 与处于空闲模式的移动站（MS）相关的非接入层（NAS）功能[Non-Access-Stratum（NAS）functions related to mobile station（MS）in idle mode]

3GPP TS 23.501 v17.8.0 5G 系统架构（System architecture for the 5G System）

3GPP TS 23.502 v17.8.0 5G 系统流程（Procedures for the 5G system）

3GPP TS 24.302 通过非蜂窝方式接入 3GPP 演进分组核心（EPC）协议；阶段 3[Access to the 3GPP evolved packet core（EPC）via non-3GPP access networks；Stage 3]

3GPP TS 24.501 v17.9.0 用于 5G 系统的非接入层（NAS）协议（5GS）；阶段 3[Non-access-stratum（NAS）protocol for 5G system（5GS）；Stage 3]

3GPP TS 28.533 管理和编排；架构框架（Management and orchestration；Architecture framework）

3GPP TS 31.111 USIM 应用工具箱[Universal Subscriber Identity Module（USIM），Application Toolkit（USAT）]

3GPP TS 31.115 USIM 应用工具箱安全包结构[Secured packet structure for（Universal）subscriber identity module（U）SIM toolkit applications]

3GPP TS 33.102 v17.0.0 3G 安全：安全架构（3G security；Security architecture）

3GPP TS 33.117 v17.3.0 通用安全保障要求目录（Catalogue of general security assurance requirements）

3GPP TS 33.122 v17.1.0 用于 3GPP 北向 API 的通用 API 框架的安全性方面（Security aspects of common API framework for 3GPP northbound APIs）