ICS 35.240.50
CCS L 67

DB21

辽　宁　省　地　方　标　准

DB21/TXXXX—XXXX

5G+工业互联网园区网络安全要求

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

辽宁省市场监督管理局　发布

目　　次

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。

请注意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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：东北大学等。

本文件主要起草人：

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

归口管理部门通信地址：辽宁省沈阳市皇姑区北陵大街45-2号。

归口管理部门联系电话：024-86913384。

文件起草单位通讯地址：

文件起草单位联系电话：

5G+工业互联网园区网络安全要求

1 范围

本文件规定了5G工业互联网园区的安全通信网络、安全区域边界、安全管理中心、其他安全要求等方面的要求。

本文件适用于5G+工业互联网园区的安全功能的规划、设计、建设、优化和监督管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35673-2017 工业通信网络 网络和系统安全 系统安全要求和安全等级

GB/T 42021-2022 工业互联网 总体网络架构

3GPP TS 33.310 网络域安全性(NDS):认证框架(AF)(NetworkDomainSecurity (NDS):Authentication Framework(AF))

3 术语和定义

GB/T 35673-2017界定的及以下术语和定义适用于本文件。

3.1

工业互联网 industrial internet

新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，通过对人、机、物、系统等的全面连接，构建起覆盖全产业链、全价值链的全新制造和服务体系。

[来源：GB/T 42021-2022,3.1]

3.2

第5代移动网络 5th generation mobile networks

是一种具有高速率、低时延和大连接特点的新一代宽带移动通信技术，5G通讯设施是实现人机物互联的网络基础设施。

3.3

网络安全 cyber security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.4

身份核验 identity proofing

基于身份证据，旨在达到具体确保级的验证。

注1:身份核验通常作为登记的组成部分来进行。在维护已登记的身份信息(例如,用户账户恢复)期间,也可能需要身份证据。

注2:身份核验通常涉及所提供的身份信息的验证,并可能包括有可能基于生物特征识别技术的唯一性检查。

注3:对身份核验的验证通常基于登记策略,其中包括对实体所提供的身份证据的验证准则的规范。

注4:在进行身份核验时获得的经验证的身份信息,能包括在注册中,并能有助于日后对此实体的识别。

[来源:ISO/IEC 24760-1:2019.3.4.2]

3.5

访问控制 access control

一种确保数据处理系统的资源只能由经授权实体以授权方式进行访问的手段。

[来源:GB/T 5271.8-2001,08.04.01,有修改]

4 缩略语

下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）

AMF：接入及移动性管理功能（Access And Mobile Management）

API：应用编程接口（Application Programming Interface）

AS：附属存储（Attached Storage）

AUSF：认证服务器功能（Authentication Server Function）

CU：中央单位（Central Unit）

DN：数据网络（Data Network）

DNN：数据网络名称（Data Network Name）

EAP：可扩展的身份验证协议（Extensible Authentication Protocol）

EPS：演进分组系统（Evolved Packet System）

E2E：端到端（End To End）

FlexE：灵活以太网（Flex Ethernet）

FW：防火墙（Fire Wall）

gNB：基站协议功能实体（gNodeB）

GUTI：全球唯一的临时用户设备身份（Globally Unique Temporary UE Identity）

HPLMN：归属公共陆地移动网（Home Public Land Mobile Network）

ID：标识符（Identifier）

IEC：国际电工委员会（International Electrotechnical Commission）

IOPS：公共安全网络中陆地无线接入网的隔离操作（Isolated E-UTRAN Operation for Public Safety）

IoT：物联网（Internet of Things）

IP：互联网协议（Internet Protocol）

IPS：入侵防护系统（Intrusion Prevention System）

IPSec：网际协议安全（Internet Protocol Security）
LAN：局域网（Local Area Network）
LAN-VN：局域网-虚拟网络（Local Area Network-Virtual Network）
ME：移动设备（Mobile Equipment）
MEC：多接入边缘计算（Multi-access Edge Computing）
MNO：移动网络运营商（Mobile Network Operator）
NAS：非接入层（Non-Access Stratum）
NEF：网络曝光功能（Network Exposure Function）
NF：网络功能（Network Function）
NR：网络无线电（Network Radio）
NRF：网络存储库功能（Network Repository Functionality）
NSSAI：网络片选择辅助信息（Network Slice Selection Auxiliary Information）
PDU：分组数据单元（Packet Data Unit）
PEI：永久设备标识符（Permanent Device Identifier）
PLMN：公共陆地移动网（Public Land Mobile Network）
QoS：服务质量（Quality of Service）
RAN：无线接入网络（Radio Access Network）
RRC：无线资源控制（Radio Resource Control）
SEAF：安全锚功能（Safety Anchor function）
SEPP：安全边缘保护代理（Security Edge Protection Proxy）
SHA：安全哈希算法（Secure Hash Algorithm）
SIDF：用户标识符隐藏功能（Subscription Identifier Function）
SMF：会话管理功能（Session Management Function）
SSL：安全套接层（Secure Sockets Layer）
SUCI：用户隐藏标识符（subscription Concealed Identifier）
SUPI：用户永久标识符（User Permanent Identifier）
TLS：传输层安全（Transport Layer Security）
UDM：统一数据管理（Unied Data Management）
UE：用户设备（User Equipment）
uRLLC：超高可靠性与超低时延通信（Ultra Reliable & Low Latency Communication）
USIM：全球用户识别卡（Universal Subscriber Identity Module）
VLAN：虚拟局域网（Virtual Local Area Network）
VPLMN：访问公共陆地移动网（Visited Public Land Mobile Network）
VPN：虚拟专用网络（Virtual Private Network ）
WAF：Web应用防护系统/网站应用级入侵防御系统（Web Application Firewall）
3GPP：第三代合作伙伴计划（Third Generation Partnership Project）
5GC：5G核心网络（5G Core Network）
5G-RAN：5G无线电接入网（Radio Access Network）

5 总体架构

5G+工业互联网园区网络安全要求分为功能安全和信息安全的两方面，以工业自动化和控制系统通信网络安全为基础，融合5G+工业互联网园区网络增强安全要求、网络安全等级保护通用要求和5G+工业互联网园区网络通用安全要求等不同视角的安全要求，形成了5G+工业互联网园区安全要求。图1给出了5G+工业互联网园区网络安全要素的技术参考模型。具体包括：

a） 工业通信网络安全。包括标识控制、使用控制、系统完整、数据保密、网络控制、及时响应、资源可用等安全要素，是安全要求的基础；

b） 5G+工业互联网园区网络通用安全要求包括能力开放、身份鉴别、安全服务、网络安全、端到端核心网安全、安全可视化和安全可配置，是 5G+工业互联网园区网络通用安全的最低限度要求；

c） 5G+工业互联网园区网络增强安全要求。包括无线接入安全、5GC 安全、MEC 安全和切片安全，是针对 5G+工业互联网园区网络安全自身安全风险而设置的增强要求；

d） 网络安全等级保护要求包括物理环境安全、通信网络安全、区域边界安全、计算环境安全、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理；

本文件以GB/T 22239-2019的10个安全要素为框架，将工业通信网络安全、5G+工业互联网园区网络通用安全要求和5G+工业互联网园区网络增强安全要求融合在其中。

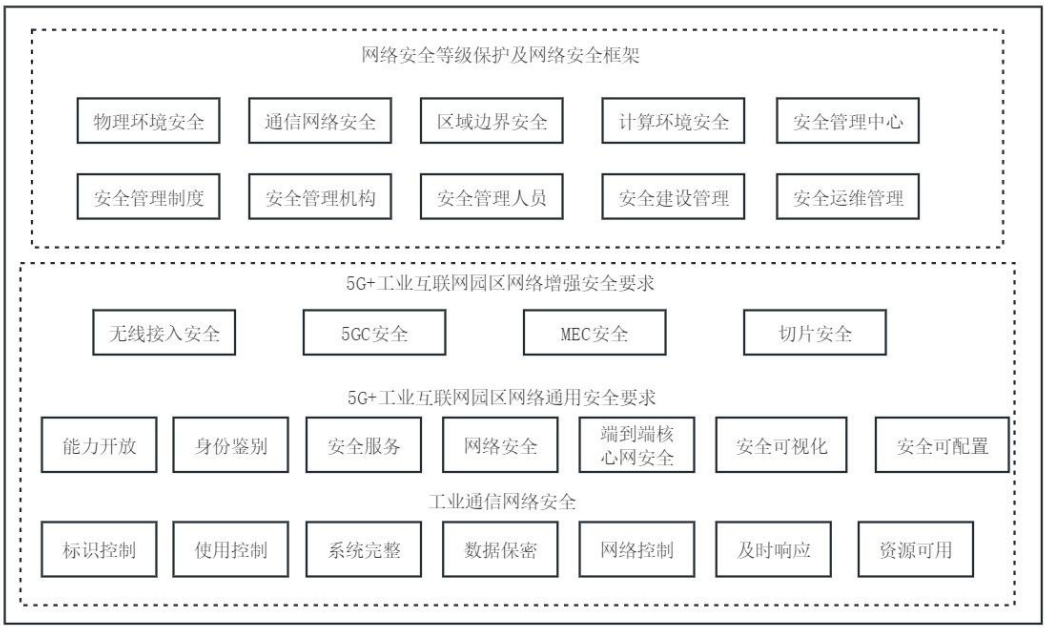

图 1　5G+工业互联网园区网络安全技术参考模型图

6　安全通信网络

6.1　网络安全能力开放要求

基于运营商策略，5G+工业互联网园区网络应开放合适的 API 向已授权的第三方提供 UE 的安全日志信息，例如，活动的 3GPP 安全机制（如数据隐私、认证、完整性保护等）。

6.2　身份鉴别要求

安全通信网络身份鉴别应满足以下要求：

a) 5G+工业互联网园区通信系统能够独立于物联网设备的识别来支持用户的识别；
b) 5G+工业互联网园区通信系统支持提供按需连接的机制（如用于远程配置的 IP 连接），使用户能够请求现场网络连接，同时为运营商提供所提供连接的识别和安全工具；
c) 5G+工业互联网园区通信系统应支持本地运营商的安全机制，远程提供唯一可识别且可验证的安全 IoT 设备的 3GPP 凭证。

6.3 安全服务要求

6.3.1 一般要求

安全通信网络服务一般要求包括：
a) 5G+工业互联网园区通信系统应支持存储缓存数据的安全机制；
b) 5G+工业互联网园区通信系统应支持接入内容缓存应用程序的安全机制；
c) 5G+工业互联网园区通信系统应支持接入服务或运营商服务托管环境中的应用程序的安全机制；
d) 5G+工业互联网园区通信系统应支持接入独立安全框架；
e) 5G+工业互联网园区通信系统应支持运营商授权其他 PLMN 的用户接收临时服务（例如，关键任务服务）的机制；
f) 5G+工业互联网园区通信系统应能够为没有接入到其本地网络的授权用户提供临时服务（例如：IOPS、关键任务服务）；
g) 根据第三方与网络运营商之间的协议，5G+工业互联网园区通信系统应允许运营商授权第三方创建、修改和删除网络片；
h) 5G+工业互联网园区通信系统应支持一种安全机制，以保护中继数据不被中继 UE 拦截；
i) 根据 HPLMN 政策及其服务和运营需求，任何能够使用接入 EPS（不是蜂窝网络 USIM）的 USIM 可用于对接入支持的服务进行身份验证；
j) 5G+工业互联网园区通信系统应为使用蜂窝网络 LAN类型服务的授权UE之间的通信提供完整性保护和机密性；
k) 5G+工业互联网园区网络 LAN-VN 应能够验证请求加入特定私人通信的 UE 的身份；
l) 5G+工业互联网园区通信系统应提供合适的 API，以允许在私有片服务的任何 UE 与该私有片中的核心网络实体之间使用受信任的第三方提供的加密。

6.3.2 认证要求

安全通信网络认证要求包括：
a) 5G+工业互联网园区网络应支持用于认证 IoT 设备组的资源有效机制；
b) 5G+工业互联网园区通信系统应支持向 IoT 设备验证用户的有效手段（如生物识别）；
c) 5G+工业互联网园区通信系统应能够使用 3GPP 凭证支持非 3GPP 接入技术的认证；
d) 对于隔离部署方案中的物联网设备，5G+工业互联网园区通信系统应支持运营商控制的替代认证方法，其具有用于网络接入的不同类型的凭证；
e) 5G+工业互联网园区通信系统应支持合适的框架（如 EAP），允许具有非 3GPP 身份和凭证的替代认证方法用于非公共网络中的 UE 网络接入认证；
f) 根据 MNO 与第三方之间的协议，5G+工业互联网园区通信系统应支持 PLMN 对托管的非公共网络和与托管的 PLMN 相关联的私有片的接入进行认证和授权的机制；
g) 5G+工业互联网园区网络应支持 3GPP 支持的机制，以对蜂窝网络 LAN-VN 接入的传统非 3GPP 设备进行身份验证。

6.3.3 授权要求

安全通信网络授权要求包括：

a) 5G+工业互联网园区通信系统应允许运营商授权物联网设备使用仅限于物联网设备的一个或多个蜂窝通信系统功能；
b) 5G+工业互联网园区通信系统应允许运营商授权/取消授权 UE 使用蜂窝网络 LAN 类型的服务；
c) 基于运营商策略，在使用非 3GPP 接入技术建立直接设备连接之前，IoT 设备应使用 3GPP 凭证来确定它们是否被授权参与直接设备连接；
d) 根据运营商政策，5G+工业互联网园区通信系统应提供一种方法来验证 UE 是否被授权为特定服务使用优先级网络接入。

6.3.4 身份管理要求

安全通信网络身份管理要求包括：

a) 5G+工业互联网园区通信系统应为运营商提供一种机制，允许 UE 使用隐藏其用户身份的临时标识符来进行接入；
b) 5G+工业互联网园区通信系统应为运营商提供一种机制，允许接入来自使用隐藏其用户身份的临时标识符在间接网络连接中连接的 UE；
c) HPLMN 应能够将临时标识符与 UE 的用户标识相关联；
d) 5G+工业互联网园区通信系统应能够保护用户身份和其他用户识别信息免受被动攻击；
e) 根据地区或国家监管要求，5G+工业互联网园区通信系统应能够保护用户身份和其他用户识别信息免受主动攻击；
f) 5G+工业互联网园区通信系统应允许合法实体收集设备标识符；
g) 5G+工业互联网园区通信系统应能够独立于设备识别而支持识别用户；
h) 5G+工业互联网园区通信系统应支持收集系统信息的安全机制，同时确保用户应用程序隐私；
i) 根据地区或国家监管要求，5G+工业互联网园区通信系统应能够提供 5G+工业互联网园区网络定位服务，同时确保保护 UE 用户或所有者的隐私，包括尊重其对定位服务的同意；
j) 对于使用蜂窝网络技术的专用网络，5G+工业互联网园区通信系统应使用由第三方提供和管理并由 3GPP 支持的身份、凭证和身份验证方法来支持网络接入。

6.3.5 监管要求

安全通信网络监管要求包括：

a) 5G+工业互联网园区通信系统应满足接入网络的区域或国家监管要求；
b) 5G+工业互联网园区通信系统应支持合法拦截，但应符合地区或国家监管要求；
c) 连接到多个国家的蜂窝核心网络的通信卫星接入网络应符合这些国家(例如 LI)的相应监管要求；
d) 5G+工业互联网园区通信系统应支持蜂窝网络 LAN 类型服务的监管要求。

6.3.6 欺诈保护要求

根据地区或国家监管要求，安全通信网络欺诈保护要求包括：

a) 5G+工业互联网园区通信系统应允许授权实体禁止被盗 UE 的正常运行；
b) 5G+工业互联网园区通信系统应允许授权实体恢复被盗 UE 重新启用至正常运行；
c) 5G+工业互联网园区通信系统应能够保护用户位置信息免受攻击；

d) 5G+工业互联网园区通信系统应支持保护用户位置信息和用户定位相关数据的生成，以防止篡改和欺骗的机制；
e) 5G+工业互联网园区通信系统应支持检测用户位置信息和用户位置相关数据生成的篡改和欺骗尝试的机制。

6.3.7 资源效率安全要求

安全通信网络资源效率安全要求包括：
a) 5G+工业互联网园区通信系统应在不影响 3GPP 系统安全级别的情况下最小化安全信令开销；
b) 5G+工业互联网园区通信系统应支持有效的安全机制，能够将相同的数据发送到多个 UE。

6.3.8 数据安全和隐私要求

安全通信网络数据安全和隐私要求包括：
a) 5G+工业互联网园区通信系统应支持为 URLLC 和能量受限设备提供服务的数据完整性保护和机密性方法；
b) 5G+工业互联网园区通信系统应能够验证消息的完整性以及消息发送者的真实性；
c) 5G+工业互联网园区通信系统应支持在请求的端到端延迟内对 URLLC 服务进行加密。

6.4 网络安全要求

6.4.1 一般安全要求

6.4.1.1 身份鉴别和授权

本项要求包括：
a) 用户认证：服务网络应在 UE 与网络之间的认证和密钥协商过程中认证订购永久标识符（SUPI）；
b) 服务网络认证：UE 应通过隐式密钥认证服务网络标识符；
c) UE 授权：服务网络应通过从归属网络获得的用户简单授权 UE，UE 授权基于经过身份验证的 SUPI；
d) 由归属网络提供网络授权：应向 UE 提供保证，确保它连接到由归属网络授权为 UE 提供服务的服务网络；

注：这种授权是“隐含的”，因为它是由成功的身份验证和密钥协议运行所暗示的。

e) 接入网络授权：应向 UE 提供保证，确保它连接到由服务网络授权为 UE 提供服务的接入网络；

注：这种授权是“隐含的”，因为它是由成功建立接入网络安全所暗示的。此接入网络授权适用于所有类型的接入网络。

f) 未经认证的紧急服务：5G+工业互联网园区通信系统应支持未经认证的接入用于紧急服务。

注：此要求适用于所有 ME，仅适用于存在未经认证的紧急服务的监管要求的服务网络。位于禁止未经认证的紧急服务的地区的服务网络不得支持此功能。

6.4.1.2 与密钥相关的 5GC 和 5G-RAN 要求

本项要求包括：
a) 5GC 和 5G-RAN 应允许使用加密和完整性保护算法，用于具有 128 位长度密钥的 AS 和 NAS 保护；
b) 网络接口应支持 256 位密钥的传输；
c) 用于 UP，NAS 和 AS 保护的密钥应取决于使用它们的算法。

6.4.2 对 UE 的要求

6.4.2.1 一般要求

PEI 应安全存储在 UE 中，以确保 PEI 的完整性。

6.4.2.2 用户数据和信令数据机密性

本项要求包括：

a) UE 应支持在 UE 和 gNB 之间加密用户数据；
b) UE 应根据 gNB 发送的指示激活用户数据的加密；
c) UE 应支持 RRC 和 NAS 信令的加密；
d) RRC 信令的机密性保护和 NAS 信令是可选的，应在相关法律的允许下使用保密措施。

6.4.2.3 用户数据和信令数据完整性

本项要求包括：

a) UE 应支持 UE 和 gNB 之间用户数据的完整性保护和重放保护，UE 应根据 gNB 发送的指示激活用户数据的完整性保护；
b) UE 应支持 RRC 和 NAS 信令的完整性保护和重放保护；
c) UE 应实现 NIA0，以实现对 NAS 和 RRC 信令的完整性保护，NIA0 仅允许使用未经认证的紧急会话。

6.4.2.4 安全存储和处理用户凭据

本项要求包括：

a) 用户凭证应使用防篡改安全硬件组件以实现在 UE 内完整性保护；
b) 用户凭证（即 K）的长期密钥应使用防篡改安全硬件组件以实现在 UE 内受到机密性保护，用户凭证的长期密钥不应在防篡改安全硬件组件的外部清晰可用；
c) 使用用户凭证的认证算法应始终在防篡改安全硬件组件内执行；
d) 应根据防篡改安全硬件组件的相应安全要求执行安全评估。

6.4.2.5 用户隐私

本项要求包括：

a) UE 应支持 5G-GUTI；
b) 除路由信息外，不应通过 5G-RAN 以明文形式传送 SUPI，例如移动国家代码（MCC）和移动网络代码（MNC），归属网络公钥应存储在 USIM 中；
c) 保护方案标识符应存储在 USIM 中，ME 应支持零方案；
d) 如果归属网络尚未在 USIM 中配置归属网络公钥，则不提供初始注册过程中的 SUPI 保护，在这种情况下，ME 应使用零方案；
e) 根据 USIM 指示的归属运营商的决定，SUCI 的计算应由 USIM 或 ME 执行；
f) 如果是未经认证的紧急呼叫，则不需要 SUPI 的隐私保护；
g) 在 USIM 中供应和更新归属网络公钥应由归属网络运营商控制；
h) 用户隐私启用应在用户的归属网络的控制之下；
i) 在 NAS 安全上下文建立后，UE 只应在 NAS 协议中发送 PEI，除非在紧急注册期间不能建立 NAS 安全上下文。

6.4.3 对 gNB 的要求

6.4.3.1 用户数据和信令数据机密性

本项要求包括：

a) gNB 应支持在 UE 和 gNB 之间加密用户数据；
b) gNB 应根据 SMF 发送的安全策略激活用户数据的加密；
c) gNB 应支持 RRC 信令的加密；
d) UE 和 gNB 之间的用户数据的机密性保护应是可选的；
e) RRC 信令的机密性保护应是可选的；
f) 相关法律允许的前提下，应使用保密措施。

6.4.3.2 用户数据和信令数据完整性

本项要求包括：

a) gNB 应支持 UE 和 gNB 之间的用户数据的完整性保护和重放保护；
b) gNB 应根据 SMF 发送的安全策略激活用户数据的完整性保护；
c) gNB 应支持 RRC 信令的完整性保护和重放保护；
d) UE 和 gNB 之间的用户数据的完整性保护是可选的，不应使用 NIA0；
e) 在未经认证的紧急会话支持不是监管要求的部署中，应在 gNB 中禁用 NIA0。

6.4.3.3 gNB 设置和配置的要求

本项要求包括：

a) 通过 O&M 系统设置和配置 gNB，应由 gNB 进行认证和授权，以便攻击者无法通过本地或远程接入修改 gNB 设置和软件配置；
b) 对于 gNB，应支持 3GPP TS 33.310 中为基站指定的证书注册机制，关于是否使用注册机制由运营商决定；
c) O&M 系统与 gNB 之间的通信应保密、完整和重播，防止未经授权的各方窃听、篡改或伪造通信数据。，应支持 gNB 与运营商信任的 5G 蜂窝网络核心或 O&M 域中的实体之间的安全关联，这些安全关联机构应相互认证；
d) gNB 应能够确保授权软件/数据更改尝试，gNB 应使用授权数据/软件；
e) 启动过程的敏感部分应在安全环境的帮助下执行，应确保 gNB 传输软件的机密性；
f) 应确保软件向 gNB 传输的完整性；
g) gNB 软件更新应在安装前进行验证。

6.4.3.4 gNB 内部密钥管理的要求

gNB 部署中以明文存储或处理密钥的任何部分均应受到保护，以免受到物理攻击；如果不是，则应将整个实体放置在物理上安全的位置，然后将在安全的环境中存储和处理明文中的密钥。

6.4.3.5 处理 gNB 的用户平面数据的要求

gNB 部署中以明文形式存储或处理用户平面数据的任何部分都应受到保护，以免受到物理攻击。如果不是，则应将整个实体放置在物理上安全的位置，然后将在安全的环境中存储和处理明文中的用户平面数据。

6.4.3.6 处理 gNB 的控制平面数据的要求

gNB 部署中以明文形式存储或处理控制平面数据的任何部分都应受到保护，以免受物理攻击。如果不是，则应将整个实体放置在物理上安全的位置，然后以安全的环境存储和处理明文中的控制平面数据。

6.4.3.7 对 gNB 安全环境的要求

本项要求包括：

a) 安全环境应支持敏感数据的安全存储，例如长期加密的机密和重要配置数据；
b) 安全环境应支持敏感功能的执行，例如用户数据的解密以及使用长期秘密协议内的基本步骤等；
c) 安全环境应支持执行引导过程的敏感部分；
d) 应确保安全环境的完整性；
e) 只有授权的接入才能被授予安全环境。

6.4.3.8 gNB F1 接口的要求

F1 接口指 gNB 的 CU 和 DU 功能实体之间互联的接口，具体要求包括：

a) F1-C 接口应支持机密性，完整性和重播保护；
b) 通过 CU-DU 链路承载的所有管理流量应保持完整性，机密性和重播保护；
c) gNB 应支持用户平面的 gNB DU-CU F1-U 接口的机密性、完整性和重放保护；
d) 通过 CU-DU 链路承载的 F1-C 和管理流量应独立于 F1-U 流量进行保护。

6.4.3.9 gNB E1 接口的要求

CU-CP 和 CU-UP 之间的 E1 接口应具有机密性，完整性和重放保护。

6.4.4 对 AMF 的要求

6.4.4.1 信令数据机密性

本项要求包括：

a) AMF 应支持 NAS 信令的加密；
b) 机密性保护 NAS 信令应为可选；
c) 在相关法律允许的前提下，应使用保密措施。

6.4.4.2 信令数据完整性

本项要求包括：

a) AMF 应支持 NAS 信令的完整性保护和重放保护。在未经认证的紧急会话的部署中，AMF 应在 AMF 中禁用；
b) 除 TS 24.501 [35]中明确列出的那些例外之外，所有 NAS 信令消息都应该使用与 NIA-0 不同的算法进行完整性保护，紧急呼叫除外。

6.4.4.3 用户隐私

本项要求包括：

a) AMF 应支持使用 SUCI 触发主要认证；
b) AMF 应支持将 5G-GUTI 分配给 UE；
c) AMF 应能够从 UE 和归属网络确认 SUPI，如果此确认失败，AMF 应拒绝向 UE 提供服务。

6.4.5 对 SEAF 的要求

SEAF 应支持使用 SUCI 的主要认证。

6.4.6 对 UDM 的要求

6.4.6.1 通用要求

用于认证和安全关联设置目的的长期密钥应受到保护，免受物理攻击，并且不应离开 UDM 的安全环境。

6.4.6.2 与 UDM 和 SIDF 相关的用户隐私相关要求

本项要求包括：

a) SIDF 应是 UDM 提供的服务；
b) SIDF 应将基于用于生成 SUCI 的保护方案从 SUCI 解析 SUPI；
c) 用于保护用户隐私的归属网络密钥应受到保护，以免受 UDM 中的物理攻击，当私有/公共密钥对用于用户隐私时，UDM 应保存密钥标识符；
d) 用于用户隐私的算法应在 UDM 的安全环境中执行。

6.4.7 对 AUSF 的要求

本项要求包括：

a) 认证服务器功能（AUSF）应处理 3GPP 接入和非 3GPP 接入的认证请求；
b) 如果 VPLMN 发送了 SUCI 的认证请求，AUSF 应仅在认证确认后向 VPLMN 提供 SUPI，AUSF 应通知 UDM 已成功或不成功的用户认证。

6.4.8 核心网络安全

6.4.8.1 基于服务的体系结构的要求

本项要求包括：

a) 基于 NF 服务的发现和注册应支持机密性，完整性和重播保护，NRF 应能够确保 NF 发现和注册请求得到授权；
b) 基于 NF 服务的发现和注册应能够在一个管理/信任域中隐藏来自不同信任/管理域中的实体的可用/支持的 NF 的拓扑；
c) NF 服务请求和响应流程应支持 NF 消费者和 NF 生产者之间的相互认证；
d) 每个 NF 都应验证所有传入的消息。根据协议规范和网络状态无效的消息应被 NF 拒绝或丢弃。

6.4.8.2 NRF 安全要求

本项要求包括：

a) 网络存储库功能（NRF）从 NF 实例接收 NF 发现请求，应将所发现的 NF 实例的信息提供给 NF 实例，并维护 NF 配置文件；
b) 请求服务的 NRF 和 NF 应相互认证；
c) NRF 应向 NF 提供认证和授权，以在彼此之间建立安全通信。

6.4.8.3 NEF 安全要求

本项要求包括：

a) 网络曝光功能（NEF）应支持将网络功能的功能外部暴露给应用功能，应用功能通过 NEF 与相关的网络功能进行交互；
b) 应支持 NEF 和应用功能之间通信的完整性保护，重放保护和机密性保护；
c) 应支持 NEF 和应用功能之间的相互认证；
d) 内部 5G 蜂窝核心信息（如 DNN，S-NSSAI 等）不应发送到 3GPP 运营商域之外；
e) NEF 不应将 SUPI 发送到 3GPP 运营商域之外；
f) NEF 应能够确定应用功能是否被授权与相关的网络功能进行交互。

6.4.8.4 核心网互联安全要求

本项要求包括：
a) 应为源文件和目标网络之间的端到端提供本文档中标识的特定消息元素的机密性和完整性；
b) 应能够确定发送根据前一个项目保护的特定消息元素的源网络的真实性；
c) 应对 3GPP 定义的网络元素产生最小的影响和增加；
d) 应使用标准安全协议；
e) 应涵盖用于漫游目的的接口；
f) 应包括防止重放攻击、防止降价攻击和算法协商等；

6.4.8.5 安全边缘保护代理（SEPP）要求

本项要求包括：
a) SEPP 应充当非透明代理节点；
b) SEPP 应保护属于使用 N32 接口的不同 PLMN 的两个 NF 之间的应用层控制平面消息；
c) SEPP 应在漫游网络中与 SEPP 进行密码套件的相互认证和协商；
d) SEPP 将处理密钥管理方面，应在两个 SEPP 之间设置保护 N32 接口上消息所需的加密密钥；
e) SEPP 应通过限制外部各方可见的内部拓扑信息来执行拓扑隐藏；
f) 作为反向代理，SEPP 应提供单点接入并控制内部 NF；
g) 接收 SEPP 应能够验证发送的 SEPP 是否被授权在接收的 N32 消息中使用 PLMN ID；
h) SEPP 应能够清楚地区分用于认证对等 SEPP 的证书和用于认证执行消息修改的中间体的证书；
i) SEPP 应丢弃格式错误的 N32 信令消息；
j) SEPP 应实施速率限制功能，以保护自身和随后的 NF 免受过度 CP 信号的影响，包括 SEPP 到 SEPP 信令消息；
k) SEPP 应实现反欺骗机制，以实现源和目标地址和标识符（例如 FQDN 或 PLMNID）的跨层验证。

6.4.9 算法选择要求

本项要求包括：
a) RRC_Connected 中的 UE 和服务网络应具有一致的算法；
b) 如果 UE 支持连接到 5GC 的 E-UTRAN，则 UE 安全功能应包括用于 NAS 级别的 NR NAS 算法，用于 AS 层的 NR AS 算法和用于 AS 级别的 LTE 算法；

注：如果 UE 同时支持连接到 5GC 的 E-UTRAN 和 NR，则 UE 5G 安全功能包括 LTE 和 NR 算法。

c) 应以受保护的方式向 UE 指示每个所选算法，以便确保 UE 保护算法选择的完整性免于操纵；
d) 应保护 UE 安全功能免受“降维攻击”；
e) 服务网络应根据 UE 的安全能力或当前服务网络已配置的允许安全功能列表选择依赖的算法。

6.5 端到端核心网安全要求

6.5.1 通用要求

端到端核心网通用要求包括：

a) 应支持应用层机制，用于由中间节点添加，删除和修改消息元素，本文件中描述的特定消息元素除外；

注：这种情况的典型例子是 IPX 运营商修改消息以用于路由目的。

b) 应为源网络和目标网络之间特定消息元素提供端到端机密性和完整性保护；

c) 目标网络应能够确定发送由前一个项目保护的特定消息元素的源网络的真实性；

d) 应对 3GPP 定义的网络元素产生最小的影响；

e) 应使用标准的安全协议；

f) 应涵盖用于漫游目的的接口；

g) 应包括抗重放攻击保护、算法协商和防降级攻击；

6.5.2 SEPP 安全要求

本项要求包括：

a) SEPP 应充当非透明代理节点；

b) SEPP 应保护属于不同 PLMN 的两个 NF 之间的使用 N32 接口通信的应用层控制面消息；

c) SEPP 应在漫游网络中与 SEPP 进行密码组建的相互认证和协商；

d) SEPP 应处理密钥管理方面，涉及设置在两个 SEPP 之间保护 N32 接口上的消息所需的加密密钥；

e) SEPP 应通过限制外部各方可见内部拓扑信息来执行拓扑隐藏；

f) 作为反向代理，SEPP 应提供内部 NF 的单点接入控制；

g) 接收方 SEPP 应能够验证在接收的 N32 消息中，发送方 SEPP 是否被授权使用 PLMNID；

h) SEPP 应能够清楚地区分用于认证对等 SEPP 的证书和用于认证执行消息修改的中间体的证书，例如通过实施单独的证书存储，可以实现这种区分。

i) SEPP 应丢弃格式错误的 N32 信令消息；

j) SEPP 应实施速率限制功能，以保护自身和随后的 NF 免受过度控制面信令的影响，包括 SEPP 到 SEPP 信令消息；

k) SEPP 应实现反欺骗机制，以实现源和目标地址和标识符（例如 FQDN 或 PLMNID）的跨层验证。

示例：如果消息的不同层之间存在不匹配或者目的地地址不属于 SEPP 自己的 PLMN，则丢弃该消息。

6.5.3 保护属性

本项要求包括：

a) 完整性保护应适用于通过 N32 接口传输的所有属性；

b) 机密性保护应适用于 SEPP 的数据加密策略中指定的所有属性。无论数据加密策略如何，通过 N32 接口发送时，应受到机密性保护的属性包括：认证向量、密钥素材、位置数据（例如小区 ID 和物理小区 ID）。

6.5.4 数据传输安全

本项要求包括：

a) 应采用 5G 网络的 AES、SNOW 3G、ZUC 等算法，以保护数据传输的机密性；

b) 应建立 TLS 安全传输通道，对需要保护的信息进行机密性和完整性保护，有效防止数据在网间传输时被篡改或窃听；
c) 应提供工业互联网中的数据产生、处理、使用等环节的安全保护；
d) 应采用基于会话的加密机制，按需配置加密算法与密钥强度，如建立 IPSec/SSL VPN 隧道。

6.6 接入安全

本项要求包括：
a) 应采用终端接入认证、终端访问控制和安全数据传输设计；
b) 应采用多重接入认证、切片认证、数据网络认证和信息加密方式；
c) 应针对不同业务，灵活配置不同级别的认证策略或策略组合；
d) 针对安全等级高的工业系统提供定制化的服务过程，应采用切片二次认证机制；
e) 应提供多种访问控制方式，以避免不可靠来源用户接入；
f) 应对关键敏感数据采用 SHA256、AES256 等加密算法进行加密存储。

6.7 5GC 安全

本项要求包括：
a) 应针对 5G 核心网络功能虚拟化特点，划分不同的安全等级，并设置不同的安全域；
b) 每个安全域应分配专用的硬件资源池；
c) 域间访问应通过虚拟安全设备做防护；
d) 域内应根据网元种类、归属地区等划分子域；
e) 安全资源池应提供 FW/VPN/WAF/IPS 等安全服务，并进行 MANO 统一编排。

6.8 MEC 安全 5G

本项要求包括：
a) 应满足 5G 业务本地化、差异化、低延时的要求；
b) 应根据 MEC 自身业务特点，从物理安全、基础设施安全、系统及平台安全、业务及数据安全、管理与运维安全等端到端的安全解决方案出发，构建“放心”的边缘计算平台；
c) 应采用安全隔离手段，如部署 FW、划分 VLAN 等；
d) 应满足虚拟层安全要求和容器安全要求，采用安全措施实现虚拟 CPU、虚拟内存以及 I/O 等资源与其它虚拟机或容器使用的资源间的隔离；
e) 应保证平台镜像仓库具有完整性、机密性和访问控制的安全保护。

6.9 切片安全

本项要求包括：
a) 应建立在共享资源之上的虚拟化专用网络；
b) 应提供传统移动网络安全机制，包括接入认证、接入层和非接入层信令和数据的加密与完整性保护等；
c) 应提供网络切片之间端到端安全隔离机制，包括端到端切片隔离、切片与用户间安全隔离、切片与 DN 间安全隔离；
d) 针对面向无线频谱资源以及基站处理资源应采用 RAN 侧隔离；
e) 最高安全等级的工业控制类切片应采用独立的基站或者频谱独享；

f) 应通过软隔离、硬隔离和QoS资源保障等多种方案，实现网络切片在承载侧的隔离，如VPN/VLAN隔离、FlexE隔离等；
g) 应采用多重隔离机制，实现核心网侧的隔离。

7 安全区域边界

7.1 边界防护

本项要求包括：
a) 应满足GB/T 22239-2019中的相关要求；
b) 应基于零信任安全理念，启用新型身份验证管理模式，充分利用身份验证凭据、设备、网络、应用等多种资源组合安全边界；
c) 应采用边界防护方式，即在网络边界验证终端身份，确定用户是否被信任；
d) 应通过安全接入网关提供认证服务、安全策略管理能力。

7.2 访问控制

本项要求包括：
a) 应满足GB/T 22239-2019中的相关要求；
b) 应针对行业终端访问控制需求，通过安全接入网关对访问主体进行认证，对访问主体的权限进行判定。只有认证通过、并且具有访问权限的访问请求才予以放行。

7.3 入侵防范

本项要求包括：
a） 应满足GB/T22239-2019中的相关要求；
b） 应利用5G工业互联网态势感知技术覆盖5G资产，如5GC网元、切片、虚机、物理机、中间件等；
c） 应根据威胁事件（如漏洞、脆弱性和攻击事件），追踪威胁源头并分析可能波及的范围，以确定资产与业务安全的处置方式；
d） 应利用伪装性网络服务或系统（如蜜罐、蜜网等），构建主动且实时诱捕的网络安全防御体系；
e） 应在5G+工业互联网园区网络区域性边界处，部署单点、多点式工业蜜罐或集群式工业蜜网，主动增强工业网络的安全防护能力；
f） 应通过态势感知实现对网络攻击事件的深度挖掘，提供网络安全防御建议和措施；
g） 应利用蜜罐、蜜网所捕获的威胁信息，并结合多源异构的威胁情报实现关联风险分析；
h） 应根据工业威胁情报的可追溯性，对攻击目标实施主动追踪和动态溯源。

7.4 其他要求

恶意代码和垃圾邮件防范、安全审计、可信验证、拨号使用控制及无线使用控制应满足GB/T 22239-2019中的相关要求。

8 安全管理中心

8.1 安全管理

本项要求包括：

a) 应满足 GB/T 22239-2019 中的规定；
b) 应对网络运维和管理人员，提供统一的安全接入门户，实现用户的集中管理、接入认证、访问日志审计等功能；
c) 应按需编排安全并提供差异化安全服务；
d) 应开放网络安全管理能力，在运营商将网络能力开放之前，需要对能力开放给租户进行授权，租户需要在认证和授权通过之后，才能访问网络能力，不同的角色将获取不同的网络接入权限，租户和网络之间通过建立安全隧道，保证操作和运营数据的安全传输。

8.2 安全可视性

本项要求包括：

a) UE 应按照每个 PDU 会话粒度向 UE 中的应用流程提供以下安全信息：
   1） AS 机密性安全特征：包括 AS 机密性、机密性算法、承载信息；
   2） AS 完整性安全特征：包括 AS 完整性、完整性算法、承载信息；
   3） NAS 机密性安全特征：包括 NAS 机密性、机密性算法；
   4） NAS 完整性安全特征：包括 NAS 完整性、完整性算法；
b) 服务网络标识符应可用于 UE 中的应用。

8.3 安全可配置

本项要求包括：

a) 应允许用户在 UE 上配置特定的安全特征设置；
b) 应允许用户管理附加的能力或使用特定高级安全特征；
c) 应允许或拒绝未经认证访问 USIM。

8.4 其他要求

系统管理、审计管理及集中管控应满足GB/T 22239-2019中的相关要求。

9 其它安全要求

安全物理环境、安全计算环境、安全管理应满足GB/T 22239-2019中的相关要求。

参 考 文 献

[1] GB/T 18336.2-2015 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求

[2] GB/T 20270-2006 信息安全技术 网络基础安全技术要求

[3] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

[4] GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

[5] GB/T 25068.1-2020 信息技术 安全技术 网络安全 第1部分：综述和概念

[6] GB/T 25068.2-2020 信息技术 安全技术 网络安全 第2部分：网络安全设计和实现指南

[7] GB/T 37934-2019 信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求

[8] GB/T 37955-2019 信息安全技术 数控网络安全技术要求

[9] GB/T 38318-2019 电力监控系统网络安全评估指南