



# 中华人民共和国公共安全行业标准

GA/T 2348—2025

## 信息安全技术 网络安全等级保护 5G 接入安全测评要求

Information security technology—Evaluation requirements for  
5G access security for classified protection of cyber security

2025-10-13 发布

2026-02-01 实施

中华人民共和国公安部 发布

目次

前言 ..... III

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 3

5 测评工作流程 ..... 3

6 第一级测评扩展要求 ..... 4

6.1 安全通信网络 ..... 4

6.2 安全建设管理 ..... 4

6.3 安全运维管理 ..... 4

7 第二级测评扩展要求 ..... 4

7.1 安全物理环境 ..... 4

7.2 安全通信网络 ..... 5

7.3 安全区域边界 ..... 6

7.4 安全计算环境 ..... 6

7.5 安全建设管理 ..... 7

7.6 安全运维管理 ..... 8

8 第三级测评扩展要求 ..... 8

8.1 安全物理环境 ..... 8

8.2 安全通信网络 ..... 9

8.3 安全区域边界 ..... 14

8.4 安全计算环境 ..... 16

8.5 安全管理中心 ..... 17

8.6 安全建设管理 ..... 18

8.7 安全运维管理 ..... 20

9 第四级测评扩展要求 ..... 21

9.1 安全物理环境 ..... 21

9.2 安全通信网络 ..... 22

9.3 安全区域边界 ..... 27

9.4 安全计算环境 ..... 29

9.5 安全管理中心 ..... 31

9.6 安全建设管理 ..... 32

9.7 安全运维管理 .....34

10 第五级测评扩展要求 .....35

附录 A(规范性) 测评单元编码规则 .....36

参考文献 .....37

## 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。

本文件由公安部网络安全保卫局提出。

本文件由公安部信息系统安全标准化技术委员会归口。

本文件起草单位：公安部第三研究所、公安部网络安全保卫局、中国移动通信有限公司研究院、西安电子科技大学、华为技术有限公司、中国电信股份有限公司、北方实验室(沈阳)股份有限公司。

本文件主要起草人：陶源、李末岩、黄敏、张秀东、赵大鹏、刘秀龙、杨凯、马冰珂、李晖、游志勇、郑献春、沈雪丽、袁洪朋。

# 信息安全技术 网络安全等级保护 5G 接入安全测评要求

## 1 范围

本文件规定了采用 5G 技术的边缘计算网络系统(不含运营商核心网)的第一级到第四级的安全测评扩展要求。

本文件适用于指导安全测评服务机构、运营使用单位及主管部门对采用 5G 技术的边缘计算网络系统的安全状况进行安全测评,也适用于网络安全职能部门进行网络安全等级保护监督检查时参考使用。

注:采用 5G 技术的边缘计算网络系统(不含运营商核心网)的第五级安全测评不在本文件中进行描述。

## 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。

GB/T 22239	信息安全技术	网络安全等级保护基本要求
GB/T 22240	信息安全技术	网络安全等级保护定级指南
GB/T 25069	信息安全技术	术语
GB/T 25070	信息安全技术	网络安全等级保护安全设计技术要求
GB/T 25850	信息安全技术	网络安全等级保护实施指南
GB/T 28448	信息安全技术	网络安全等级保护测评要求
GB/T 36958	信息安全技术	网络安全等级保护安全管理中心技术要求

## 3 术语和定义

GB/T 22239、GB/T 22240、GB/T 25069、GB/T 25070、GB/T 25850、GB/T 28448 和 GB/T 36958 界定的以及下列术语和定义适用于本文件。

### 3.1

**边缘计算 edge computing**

在边缘或边缘附近进行数据处理与存储的分布式计算形式。

[来源:GB/T 42564—2023,3.2]

### 3.2

**多接入边缘计算 multi-access edge computing**

包含一种或多种类型的接入技术的边缘计算系统。

[来源:ETSI GS MEC 001 V2.1.1,3.1,有修改]

### 3.3

**MEC 平台 multi-access edge computing platform**

提供多接入边缘计算的所有相关软硬件资源。

3.4

**边缘应用 edge computing application**

部署并运行在边缘节点上的应用程序,在边缘实现对数据的本地处理和业务逻辑的本地执行。

[来源:GB/T 42564—2023,3.8]

3.5

**5G 5th generation**

符合第五代 3GPP 规范的电信系统。

注:由 5G 核心网、5G 接入网和用户设备组成。

[来源:3GPP TR 21.905 V17.1.0,4.1,有修改]

3.6

**5G 专网 5G private network**

采用 3GPP 5G 标准构建的不与公共网络交互的隔离网络。

[来源:3GPP TS 22.261 V19.4.0,3.1,有修改]

3.7

**网络切片 network slice**

在共享基础设施上构建的提供特定网络能力和网络特征的专用网络。

[来源:3GPP TS 23.501 V18.3.0,3.1,有修改]

3.8

**小区 cell**

可以被用户终端设备唯一标识的无线网络对象,该对象的标识用于无线接入网在特定地理区域广播。

[来源:3GPP TR 21.905 V17.1.0,3,有修改]

3.9

**访谈 interview**

测评人员通过引导等级保护对象相关人员进行有目的的(有针对性的)交流以帮助测评人员理解、澄清或取得证据的过程。

[来源:GB/T 28448—2019,3.1]

3.10

**核查 examine**

测评人员通过对测评对象(如制度文档、各类设备及相关安全配置等)进行观察、查验和分析,以帮助测评人员理解、澄清或取得证据的过程。

[来源:GB/T 28448—2019,3.2]

3.11

**测试 test**

测评人员使用预定的方法/工具使测评对象(各类设备或安全配置)产生特定的结果,将运行结果与预期的结果进行比对的过程。

[来源:GB/T 28448—2019,3.3]

3.12

**评估 evaluate**

对测评对象可能存在的威胁及其可能产生的后果进行综合评价和预测的过程。

[来源:GB/T 28448—2019,3.4]

3.13

**测评对象 target of testing and evaluation**

等级测评过程中不同测评方法作用的对象,主要涉及相关配套制度文档、设备设施及人员等。



[来源:GB/T 28448—2019,3.5]

### 3.14

#### 等级测评 **testing and evaluation for classified cybersecurity protection**

测评机构依据国家网络安全等级保护制度规定,按照有关管理规范和技术标准,对非涉及国家秘密的网络安全等级保护状况进行检测评估的活动。

[来源:GB/T 28448—2019,3.6]

### 3.15

#### 用户面功能 **user plane function**

提供用户面数据转发、处理的网络功能,负责与外部数据网络互连,分组路由转发,数据包检测和用户面策略执行等。

### 3.16

#### 会话管理功能 **session management function**

负责会话建立、修改和释放,IP 地址分配和管理,UPF 设备选择的网络功能。

## 4 缩略语

下列缩略语适用于本文件。

DDoS:分布式拒绝服务(Distributed Denial of Service)

GPS:全球卫星定位系统(Global Positioning System)

GUTI:全球唯一临时标识符(Globally Unique Temporary Identifier)

IPSec:IP 安全协议(Internet Protocol Security)

MEC:多接入边缘计算(Multi-access Edge Computing)

RRC:无线资源控制(Radio Resource Controller)

SMF:会话管理功能(Session Management Function)

SUCI:用户隐藏标识符(Subscription Concealed Identifier)

SUPI:用户永久标识符(Subscription Identifier)

UE:用户终端设备(User Equipment)

UPF:用户面功能(User Plane Function)

5G-GUTI:5G 全局唯一临时标识(5G Globally Unique Temporary Identifier)

## 5 测评工作流程

网络安全等级保护 5G 接入安全测评工作流程主要包括:对象识别、系统调研、指标映射和测评实施等环节。

对象识别是指在对采用 5G 技术的边缘计算系统进行测评时,需要明确测评对象的具体应用场景和架构,即明确测评对象是面向广域网采用 5G 技术的边缘计算系统,还是面向局域网采用 5G 技术的边缘计算系统。

系统调研是指调研测评对象的网络架构、边界防护、用户终端、无线安全等相关内容。

指标映射是指依据 GB/T 28448 中的安全测评通用要求和本文件中的测评要求,结合系统调研内容,选择和确定测评指标。

测评实施是指对测评对象开展单项测评和整体测评,形成测评报告。本文件中单项测评由测评指标、测评对象、测评实施和单元判定结果构成。为方便使用,针对每个测评单元进行编码,具体描述应符合附录 A 中测试单元编码规则。

## 6 第一级测评扩展要求

### 6.1 安全通信网络

网络架构测评单元(L1-CNS6-01)包括以下要求。

- a) 测评指标:应由电信运营商或其他外部单位运营维护的 5G 基站、UPF 设备、MEC 平台、核心网等系统或设备与用户自有系统之间划分为不同区域,并在区域间采用边界隔离与防护手段。
- b) 测评对象:路由器、交换机和防火墙等提供访问控制功能的设备。
- c) 测评实施包括以下内容:
  - 1) 应核查由电信运营商或其他外部单位运营维护的 UPF 设备、MEC 平台、核心网等系统或设备与用户自有系统之间是否部署边界隔离设备;
  - 2) 应核查是否采用了有效的边界隔离策略实施访问控制。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 6.2 安全建设管理

电信运营商选择测评单元(L1-CMS6-01)包括以下要求。

- a) 测评指标:应选择具有基础电信业务经营资质的 5G 电信运营商,其所提供的 5G 网络应为所承载的业务应用系统及数据传输业务提供不低于其安全保护等级的安全保护能力。
- b) 测评对象:系统安全管理员和服务合同。
- c) 测评实施包括以下内容:
  - 1) 应访谈系统安全管理员是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的 5G 电信运营商;
  - 2) 应核查 5G 电信运营商提供的相关服务合同,5G 网络的安全保护等级是否不低于其所承载的业务应用系统及数据传输业务。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 6.3 安全运维管理

隐私管理测评单元(L1-MMS6-01)包括以下要求:

- a) 测评指标:应具有使用 5G-GUTI 替代 SUPI 的能力,实现 5G 用户信息的隐私保护;
- b) 测评对象:5G 基站、UPF 设备、5G 用户终端设备;
- c) 测评实施:应核查用户手册、验收文档或第三方检测报告,是否具有在业务过程中使用 5G-GUTI 的能力;
- d) 单元判定:如果 c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

## 7 第二级测评扩展要求

### 7.1 安全物理环境

物理位置选择测评单元(L2-PES6-01)包括以下要求。



- a) 测评指标:在业务数据不出园区的场景下,应将 5G 基站、UPF 设备和 5G 用户终端设备部署在园区内。
- b) 测评对象:用户手册或验收文档。
- c) 测评实施包括以下内容:
  - 1) 应核查业务应用场景是否有业务数据不出园区的规定和要求;
  - 2) 应核查用户手册或验收文档,对于基站、UPF 设备和 5G 用户终端设备等由电信运营商或其他外部单位建设、运营与维护的系统或设备,核查系统或设备是否部署在园区内。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 7.2 安全通信网络

### 7.2.1 网络架构测评单元(L2-CNS6-01)

该测评单元包括以下要求:

- a) 测评指标:5G 行业应用系统不运行在低于其安全保护等级的 5G 网络上;
- b) 测评对象:5G 行业应用系统和 5G 网络定级备案材料;
- c) 测评实施:应核查 5G 行业应用系统和承载 5G 行业应用系统的 5G 网络的定级备案材料,5G 网络的安全保护等级是否不低于其承载的业务应用系统安全保护等级;
- d) 单元判定:如果 c) 测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

### 7.2.2 网络架构测评单元(L2-CNS6-02)

该测评单元包括以下要求。

- a) 测评指标:应由电信运营商或其他外部单位运营维护的 5G 基站、UPF 设备、MEC 平台、核心网等系统或设备与用户自有系统之间划分为不同区域,并在区域间采用边界隔离与防护手段。
- b) 测评对象:路由器、交换机和防火墙等提供访问控制功能的设备。
- c) 测评实施包括以下内容:
  - 1) 应核查由电信运营商或其他外部单位运营维护的 UPF 设备、MEC 平台、核心网等系统或设备与用户自有系统之间是否部署边界隔离设备;
  - 2) 应核查是否采用了有效的边界隔离策略实施访问控制。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 7.2.3 网络架构测评单元(L2-CNS6-03)

该测评单元包括以下要求。

- a) 测评指标:网络通信设备不包含其供应商、生产商或开发人员不再支持的软件和硬件组件,如已达到生命周期或不再支持的组件。
- b) 测评对象:5G 基站、路由器和 UPF 设备。
- c) 测评实施包括以下内容:
  - 1) 应使用工具或其他适当的确定手段,识别供应商、生产者、开发人员或经营者的其他合同伙伴提供的硬件和软件组件、版本信息及种类;
  - 2) 应验证在系统安装的硬件和软件列表中,没有供应商在所附文档中未提供的条目(含版本

信息和种类)。

- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 7.3 安全区域边界

#### 7.3.1 边界防护测评单元(L2-ABS6-01)

该测评单元包括以下要求:

- a) 测评指标:5G 网络 N6 接口与应用服务器网络之间的访问和数据流应通过边界网关设备,并设置访问控制规则。
- b) 测评对象:访问控制策略和网络边界设备。
- c) 测评实施包括以下内容:
  - 1) 应核查 5G 网络 N6 接口与应用服务器网络之间的访问和数据是否通过边界网关设备;
  - 2) 应核查并测试网络边界访问控制规则和访问控制策略是否正确配置、开启并生效。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 7.3.2 访问控制测评单元(L2-ABS6-02)

该测评单元包括以下要求:

- a) 测评指标:5G 用户终端设备应开启接入认证功能;
- b) 测评对象:5G 用户终端设备;
- c) 测评实施:应核查 5G 用户终端设备是否开启接入认证功能;
- d) 单元判定:如果 c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

#### 7.3.3 入侵防范测评单元(L2-ABS6-03)

该测评单元包括以下要求。

- a) 测评指标:边缘应用应具有安全防御能力。
- b) 测评对象:边缘应用、入侵防御系统或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查在边缘应用是否部署了入侵防御系统对网络入侵行为进行防范,其规则库是否为最新;
  - 2) 应核查部署的入侵防御系统或相关组件对异常的流量和未知的威胁监控策略是否正确配置、开启并生效,如核查入侵防御系统或相关组件是否能记录攻击类型、攻击时间等信息;
  - 3) 应核查部署的攻击防御检测设备或相关组件对攻击行为的报警策略是否正确配置、开启并生效,如核查入侵防御系统或相关组件是否具有实时报警日志等信息。
- d) 单元判定:如果 c)中 1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 7.4 安全计算环境

访问控制测评单元(L2-CES6-01)包括以下要求。

- a) 测评指标:应提供 MEC 平台用户设置其所属的不同虚拟机之间的访问控制策略的功能。
- b) 测评对象:MEC 的管理平台、5G 网络服务客户管理系统、网络边界访问控制设备。

- c) 测评实施包括以下内容：
  - 1) 应核查 MEC 的管理平台或安全设备,查看是否允许客户设置不同虚拟机间访问控制策略;
  - 2) 应核查 MEC 的管理平台,查看是否存在不同虚拟机间的访问控制管理模块,是否可以开启该访问控制功能;
  - 3) 应核查 MEC 平台中的客户虚拟机安全策略,查看不同虚拟机间访问控制策略是否有效。
- d) 单元判定:如果 c) 中 1)~3) 为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 7.5 安全建设管理

### 7.5.1 电信运营商选择测评单元(L2-CMS6-01)

该测评单元包括以下要求。

- a) 测评指标:应选择具有基础电信业务经营资质的 5G 电信运营商,其所提供的 5G 网络应为所承载的业务应用系统及数据传输业务提供不低于其安全保护等级的安全保护能力。
- b) 测评对象:系统安全管理员和系统定级备案材料。
- c) 测评实施包括以下内容：
  - 1) 应访谈系统安全管理员是否根据业务系统的安全保护等级选择不低于其安全保护等级的 5G 电信运营商;
  - 2) 应核查 5G 网络和业务应用系统相关定级备案材料,5G 网络的安全保护等级是否不低于其所承载的业务应用系统及数据传输业务。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 7.5.2 应用软件采购

#### 7.5.2.1 测评单元(L2-CMS6-02)

该测评单元包括以下要求。

- a) 测评指标:5G 用户终端设备、MEC 平台等安装、运行的应用软件来自可靠分发渠道或使用数字签名。
- b) 测评对象:5G 用户终端设备、MEC 平台。
- c) 测评实施包括以下内容：
  - 1) 应核查移动应用软件是否来自可靠分发渠道或使用数字签名;
  - 2) 应核查使用数字签名的证书是否在有效期内。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

#### 7.5.2.2 测评单元(L2-CMS6-03)

该测评单元包括以下要求。

- a) 测评指标:网络通信产品及服务应符合国家标准、行业标准。
- b) 测评对象:5G 基站、UPF 设备、路由器产品及服务。
- c) 测评实施包括以下内容：
  - 1) 应核查部署的网络通信设备的产品及服务是否符合国家标准或行业标准;
  - 2) 应核查引用的国家标准和行业标准是否处于现行状态。



- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 7.6 安全运维管理

### 7.6.1 5G 用户终端设备管理测评单元(L2-MMS6-01)

该测评单元包括以下要求。

- a) 测评指标:应指定人员定期巡视 5G 用户终端设备、网络接入设备的部署环境,对可能影响设备正常工作的环境异常进行记录和维护。
- b) 测评对象:维护记录。
- c) 测评实施包括以下内容:
  - 1) 应访谈系统运维负责人是否有专门的人员对 5G 用户终端设备进行定期维护,由何部门或何人负责,维护周期是否小于 1 年;
  - 2) 应核查 5G 用户终端设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 7.6.2 隐私管理测评单元(L2-MMS6-02)

该测评单元包括以下要求:

- a) 测评指标:应具有使用 5G-GUTI 替代 SUPI 的能力,实现 5G 用户信息的隐私保护;
- b) 测评对象:5G 基站、UPF 设备、5G 用户终端设备;
- c) 测评实施:应核查用户手册、验收文档或第三方检测报告,是否具有在业务过程中使用 5G-GUTI 的能力;
- d) 单元判定:如果 c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

## 8 第三级测评扩展要求

### 8.1 安全物理环境

物理位置选择测评单元(L3-PES6-01)包括以下要求。

- a) 测评指标:在业务数据不出园区的场景下,应将基站、UPF 设备和 5G 用户终端设备部署在园区内。
- b) 测评对象:用户手册或验收文档。
- c) 测评实施包括以下内容:
  - 1) 应核查业务应用场景是否有业务数据不出园区的规定和要求;
  - 2) 应核查用户手册或验收文档,对于基站、UPF 设备和 5G 用户终端设备等由电信运营商或其他外部单位建设、运营与维护的系统或设备,核查系统或设备是否部署在园区内。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 8.2 安全通信网络

### 8.2.1 网络架构

#### 8.2.1.1 测评单元(L3-CNS6-01)

该测评单元包括以下要求：

- a) 测评指标:5G行业应用系统不运行在低于其安全保护等级的5G网络上；
- b) 测评对象:5G行业应用系统和5G网络定级备案材料；
- c) 测评实施:应核查5G行业应用系统和承载5G行业应用系统的5G网络的定级备案材料,5G网络的安全保护等级是否不低于其承载的业务应用系统安全保护等级；
- d) 单元判定:如果c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

#### 8.2.1.2 测评单元(L3-CNS6-02)

该测评单元包括以下要求。

- a) 测评指标:应由电信运营商或其他外部单位运营维护的5G基站、UPF设备、MEC平台、核心网等系统或设备与用户自有系统之间划分为不同区域,并在区域间采用边界隔离与防护手段。
- b) 测评对象:路由器、交换机和防火墙等提供访问控制功能的设备。
- c) 测评实施包括以下内容:
  - 1) 应核查由电信运营商或其他外部单位运营维护的UPF设备、MEC平台、核心网等系统或设备与用户自有系统之间是否部署边界隔离设备；
  - 2) 应核查是否采用了有效的边界隔离策略实施访问控制。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.2.1.3 测评单元(L3-CNS6-03)

该测评单元包括以下要求。

- a) 测评指标:网络通信设备不包含其供应商、生产商或开发人员不再支持的软件和硬件组件,如已达到生命周期或不再支持的组件。
- b) 测评对象:5G基站、路由器和UPF设备。
- c) 测评实施:
  - 1) 应使用工具或其他适当的确定手段,识别供应商、生产者、开发人员或经营者的其他合同伙伴提供的硬件和软件组件、版本信息及种类；
  - 2) 应核查在系统安装的硬件和软件列表中,没有供应商在所附文档中未提供的条目(含版本信息和种类)。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.2.1.4 测评单元(L3-CNS6-04)

该测评单元包括以下要求。

- a) 测评指标:网络通信设备自身应具有入侵检测能力,防止对设备的攻击入侵。

- b) 测评对象:5G 基站、UPF 设备、路由器或防火墙等提供网络通信功能的设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查网络通信设备产品规格是否具有检测对设备攻击入侵能力;
  - 2) 应采用核查文档、测试策略、渗透测试等方式来验证网络通信设备能否检测对设备的入侵攻击,并给出相关处置措施建议。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 8.2.2 通信传输

### 8.2.2.1 测评单元(L3-CNS6-05)

该测评单元包括以下要求。

- a) 测评指标:通过 5G 网络的空口、UPF 设备承载的数据等应采用逻辑独立的信道传输。
- b) 测评对象:5G 基站和路由器设备。
- c) 测评实施包括以下内容:
  - 1) 应核查 5G 空口是否采用 5QI 技术提供逻辑信道隔离;
  - 2) 应核查 5G 基站和 UPF 设备间的数据传输是否采取 VLAN 等逻辑隔离措施。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

### 8.2.2.2 测评单元(L3-CNS6-06)

该测评单元包括以下要求:

- a) 测评指标:使用 5G 网络的空口、UPF 设备进行指令或相关数据交互的操作,应采用加密认证技术手段实现身份认证、访问控制和数据加密传输;
- b) 测评对象:加密认证设备、路由器、交换机和防火墙等提供访问控制功能的设备;
- c) 测评实施:应核查 5G 行业应用系统中使用 5G 网络的空口、UPF 设备进行指令或相关数据交互的操作是否采用加密认证技术实现身份认证、访问控制和数据加密传输;
- d) 单元判定:如果 c) 测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

### 8.2.2.3 测评单元(L3-CNS6-07)

该测评单元包括以下要求。

- a) 测评指标:应具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据完整性保护能力。
- b) 测评对象:5G 基站、UPF 设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查在 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口是否部署安全网关(内置或外置)并是否正确配置满足 GM/T 0022 要求的 IPsec;
  - 2) 应核查 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据是否具有完整性保护能力。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。



#### 8.2.2.4 测评单元(L3-CNS6-08)

该测评单元包括以下要求。

- a) 测评指标:应具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据机密性保护能力。
- b) 测评对象:5G 基站、UPF 设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查在 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口是否部署安全网关(内置或外置),并是否正确配置满足 GM/T 0022 要求的 IPsec;
  - 2) 应核查 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口用户面数据是否具有机密性保护能力。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 8.2.2.5 测评单元(L3-CNS6-09)

该测评单元包括以下要求。

- a) 测评指标:应具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据防重放保护能力。
- b) 测评对象:5G 基站、UPF 设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查在 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口是否部署安全网关(内置或外置),并是否正确配置满足 GM/T 0022 要求的 IPsec;
  - 2) 应核查 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口用户面数据是否具有防重放保护能力。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 8.2.2.6 测评单元(L3-CNS6-10)

该测评单元包括以下要求。

- a) 测评指标:应具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据完整性保护能力。
- b) 测评对象:UPF 设备、SMF 设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查在 UPF 设备和 SMF 设备之间 N4 接口是否部署安全网关(内置或外置),并是否正确配置满足 GM/T 0022 要求的 IPsec;
  - 2) 应核查 UPF 设备和 SMF 设备之间 N4 接口控制面数据是否具有完整性保护能力。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 8.2.2.7 测评单元(L3-CNS6-11)

该测评单元包括以下要求。

- a) 测评指标:应具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据机密性保护能力。
- b) 测评对象:UPF 设备、SMF 设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查在 UPF 设备和 SMF 设备之间 N4 接口是否部署安全网关(内置或外置),并是否正确配置满足 GM/T 0022 要求的 IPsec;
  - 2) 应核查 UPF 设备和 SMF 设备之间 N4 接口控制面数据是否具有机密性保护能力。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 8.2.2.8 测评单元(L3-CNS6-12)

该测评单元包括以下要求。

- a) 测评指标:应具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据防重放保护能力。
- b) 测评对象:UPF 设备、SMF 设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查在 UPF 设备和 SMF 设备之间 N4 接口是否部署安全网关(内置或外置),并是否正确配置满足 GM/T 0022 要求的 IPsec;
  - 2) 应核查 UPF 设备和 SMF 设备之间 N4 接口控制面数据是否具有防重放保护能力。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 8.2.2.9 测评单元(L3-CNS6-13)

该测评单元包括以下要求。

- a) 测评指标:应具有 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间的应用数据完整性保护能力。
- b) 测评对象:提供校验技术或密码技术功能的设备或组件。
- c) 测评实施包括以下内容:
  - 1) 应核查是否在 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间数据传输过程中使用校验技术或密码技术来保护数据;
  - 2) 应核查数据传输过程中是否具有数据完整性保护能力。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.2.2.10 测评单元(L3-CNS6-14)

该测评单元包括以下要求。

- a) 测评指标:应具有 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间的应用数据机密性保护能力。
- b) 测评对象:提供校验技术或密码技术功能的设备或组件。
- c) 测评实施包括以下内容:
  - 1) 应核查是否在 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间数据传输过程中使用校验技术或密码技术来保护数据;
  - 2) 应核查数据传输过程中是否具有数据机密性保护能力。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本

测评单元指标要求。

### 8.2.3 无线安全测评单元(L3-CNS6-15)

该测评单元包括以下要求：

- a) 测评指标：应具有空口干扰检测和干扰定位能力；
- b) 测评对象：5G 基站；
- c) 测评实施：应核查 5G 基站的用户手册、验收文档或第三方检测报告，是否具有干扰检测和干扰定位功能；
- d) 单元判定：如果 c) 测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

### 8.2.4 入侵防范

#### 8.2.4.1 测评单元(L3-CNS6-16)

该测评单元包括以下要求。

- a) 测评指标：应具有伪造北斗、GPS 等信号的检测和防御能力。
- b) 测评对象：5G 基站。
- c) 测评实施包括以下内容：
  - 1) 应核查 5G 基站的用户手册、验收文档或第三方检测报告，是否具有伪造 GPS、北斗等信号的检测和防御功能；
  - 2) 应核查 5G 基站对北斗、GPS 等伪造信号的检测和防御功能是否开启。
- d) 单元判定：如果 c) 中 1) 和 2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

#### 8.2.4.2 测评单元(L3-CNS6-17)

该测评单元包括以下要求。

- a) 测评指标：应具有空口信令面 DDoS 攻击的检测和防御能力。
- b) 测评对象：5G 基站。
- c) 测评实施包括以下内容：
  - 1) 应核查 5G 基站的用户手册、验收文档或第三方检测报告，是否具有 DDoS 攻击的检测和防御功能；
  - 2) 应核查验证 5G 基站对空口信令面 DDoS 攻击的检测和防御功能是否开启。
- d) 单元判定：如果 c) 中 1) 和 2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

#### 8.2.4.3 测评单元(L3-CNS6-18)

该测评单元包括以下要求。

- a) 测评指标：应具有传输端口的访问控制能力，设置访问控制规则。
- b) 测评对象：5G 基站和 UPF 设备。
- c) 测评实施包括以下内容：
  - 1) 应核查 5G 基站、UPF 设备是否具有传输端口的访问控制能力，是否启用访问控制策略；
  - 2) 应核查 5G 基站、UPF 设备是否具有传输端口的单包攻击防御、DDoS 攻击防御等的的能力；
  - 3) 应核查 5G 基站、UPF 设备对传输端口入侵行为(单包攻击、DDoS 攻击)是否开启检测和防

御功能。

- d) 单元判定:如果 c)中 1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.2.4.4 测评单元(L3-CNS6-19)

该测评单元包括以下要求。

- a) 测评指标:应具有用户面数据的流量检测能力。
- b) 测评对象:流量检测设备或组件。
- c) 测评实施包括以下内容:
  - 1) 应核查是否部署流量检测设备或组件,流量检测策略是否正确配置、开启并生效;
  - 2) 应核查流量检测设备或组件是否能够检测用户面数据的流量。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 8.3 安全区域边界

#### 8.3.1 边界防护测评单元(L3-ABS6-01)

该测评单元包括以下要求。

- a) 测评指标:5G 网络 N6 接口与应用服务器网络之间的访问和数据流通过边界网关设备,并设置访问控制规则。
- b) 测评对象:访问控制策略和网络边界设备。
- c) 测评实施包括以下内容:
  - 1) 应核查 5G 空口与应用服务器网络之间是否部署边界网关设备;
  - 2) 应核查网络边界访问控制规则和访问控制策略是否正确配置、开启并生效。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.3.2 访问控制

##### 8.3.2.1 测评单元(L3-ABS6-02)

该测评单元包括以下要求。

- a) 测评指标:5G 用户终端设备应开启接入认证功能,并支持采用 5G 网络进行双向认证。
- b) 测评对象:5G 用户终端设备。
- c) 测评实施:
  - 1) 应核查 5G 用户终端设备是否开启接入认证功能;
  - 2) 应核查是否采用 5G 网络或认证服务器等进行双向认证。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

##### 8.3.2.2 测评单元(L3-ABS6-03)

该测评单元包括以下要求。

- a) 测评指标:对 5G 专网中存在多种业务系统的情况,应通过 DNN 或网络切片等方式对不同业务系统进行安全隔离,并限制无权限访问相关业务系统的 5G 用户终端设备接入业务系统所在的



网络。

b) 测评对象:5G 专网。

c) 测评实施包括以下内容:

- 1) 应核查当 5G 专网中存在多个业务系统时,是否按照业务特点采取隔离机制(如 DNN 或切片等方式)实现业务系统的安全隔离;
- 2) 应核查当 5G 专网中存在多个业务系统时,是否有相关的授权访问控制措施限制无权限 5G 用户终端设备接入对应的 5G 专网各业务系统。

d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 8.3.2.3 测评单元(L3-ABS6-04)

该测评单元包括以下要求:

- a) 测评指标:应能根据 5G 用户终端设备所在的区域,控制其接入相应 5G 专网权限,限制 5G 用户终端设备在非授权区域访问 5G 专网及相关业务系统;
- b) 测评对象:5G 专网;
- c) 测评实施:应核查是否能够提供基于 5G 用户终端设备所在的小区限制其接入相应 5G 专网权限的能力,阻止 5G 用户终端设备在非授权区域访问 5G 专网及相关业务系统;
- d) 单元判定:如果 c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

## 8.3.3 入侵防范

### 8.3.3.1 测评单元(L3-ABS6-05)

该测评单元包括以下要求。

- a) 测评指标:边缘应用应具有抗击多种高级攻击的安全防御能力。
- b) 测评对象:边缘应用、入侵防御系统或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查在边缘应用是否部署了入侵防御系统对网络入侵行为进行防范(如抗 DDoS 能力、抗入侵能力),其规则库是否为最新;
  - 2) 应核查部署的入侵防御系统或相关组件对异常的流量和未知的威胁监控策略是否有效,如核查入侵防御系统或相关组件是否能记录攻击类型、攻击时间等信息;
  - 3) 应核查部署的攻击防御检测设备或相关组件对攻击行为的报警策略是否有效,如核查入侵防御系统或相关组件是否具有实时报警日志等信息。
- d) 单元判定:如果 c)中 1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 8.3.3.2 测评单元(L3-ABS6-06)

该测评单元包括以下要求。

- a) 测评指标:应具有对 5G 用户终端设备恶意行为(如 UE 互访、地址欺骗等)的检测,并对存在恶意行为的 5G 用户终端设备进行处置的能力。
- b) 测评对象:入侵防御系统或相关组件、UPF 设备。
- c) 测评实施包括以下内容:
  - 1) 应核查是否具有检测、防御 5G 用户终端设备的恶意攻击行为(如 UE 互访、地址欺骗等)的

能力；

2) 应核查是否具有对恶意 5G 用户终端设备进行处置的能力。

d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 8.4 安全计算环境

### 8.4.1 身份鉴别测评单元(L3-CES6-01)

该测评单元包括以下要求。

a) 测评指标:应具有主认证之外的二次认证方式,以确保仅授权的 UE 访问用户所属网络。

b) 测评对象:认证方案建议书或验收文档及认证相关组件。

c) 测评实施包括以下内容:

1) 应核查二次认证方案建议书或验收文档是否有主认证之外的二次认证方式以确保授权的 UE 访问用户所属网络;

2) 应核查相关二次认证方式是否配置、开启并生效。

d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 8.4.2 5G 用户终端设备安全

#### 8.4.2.1 测评单元(L3-CES6-02)

该测评单元包括以下要求:

a) 测评指标:固件及固件升级包上线前应进行安全性检测;

b) 测评对象:5G 用户终端设备;

c) 测评实施:应核查固件及固件升级包上线前是否完成安全性检测,是否具有安全检测报告;

d) 单元判定:如果 c) 测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

#### 8.4.2.2 测评单元(L3-CES6-03)

该测评单元包括以下要求。

a) 测评指标:应具有软件白名单控制能力,应根据白名单控制应用软件安装、运行。

b) 测评对象:5G 用户终端设备。

c) 测评实施包括以下内容:

1) 应核查 5G 用户终端设备系统是否具有软件白名单功能;

2) 应核查 5G 用户终端设备系统的白名单功能是否能控制应用软件的安装和运行。

d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.4.3 访问控制测评单元(L3-CES6-04)

该测评单元包括以下要求。

a) 测评指标:应提供 MEC 平台用户设置其所属的不同虚拟机之间的访问控制策略的功能。

b) 测评对象:MEC 的管理平台、5G 网络服务客户管理系统、网络边界访问控制设备。



- c) 测评实施包括以下内容：
  - 1) 应核查 MEC 的管理平台或安全设备,查看是否允许客户设置其所属的不同虚拟机间访问控制策略;
  - 2) 应核查 MEC 平台的管理平台,查看是否存在不同虚拟机间的访问控制管理模块,是否开启访问控制功能;
  - 3) 应核查 MEC 平台中的客户虚拟机安全策略,查看不同虚拟机间访问控制策略是否有效。
- d) 单元判定:如果 c)中 1)~3)为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.4.4 入侵防范测评单元(L3-CES6-05)

该测评单元包括以下要求。

- a) 测评指标:应在 MEC 平台提供虚拟机逃逸攻击的检测能力,防止虚拟机对虚拟化管理平台的入侵攻击。
- b) 测评对象:MEC 平台。
- c) 测评实施包括以下内容：
  - 1) 应访谈并核查 MEC 平台中是否具有应用安全防护、主机安全防护等入侵检测的措施;
  - 2) 应核查在边缘应用发生入侵事件时,安全防护措施是否提供安全报警。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.4.5 数据安全测评单元(L3-CES6-06)

该测评单元包括以下要求。

- a) 测评指标:应具有空口用户面数据和控制面数据的机密性和完整性功能。
- b) 测评对象:5G 基站的用户手册或验收文档。
- c) 测评实施：
  - 1) 应核查 5G 基站的用户手册或验收文档,是否具有空口用户面数据和控制面(RRC)数据的机密性功能;
  - 2) 应核查 5G 基站的用户手册或验收文档,是否具有空口用户面数据和控制面(RRC)数据的完整性功能。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 8.5 安全管理中心

#### 8.5.1 集中管控测评单元(L3-SMC6-01)

该测评单元包括以下要求。

- a) 测评指标:分离业务系统流量与 5G 网络管理流量。
- b) 测评对象:网络架构。
- c) 测评实施包括以下内容：
  - 1) 应核查网络架构是否采用带外管理或策略配置等方式实现 5G 网络管理流量和业务系统流量分离;
  - 2) 应核查 5G 网络管理流量与业务系统流量是否分离。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本

测评单元指标要求。

#### 8.5.2 集中管控测评单元(L3-SMC6-02)

该测评单元包括以下要求。

- a) 测评指标:应能够建立设备管理的安全传输通道,对 5G 电信运营商提供的网元设备进行安全管理。
- b) 测评对象:5G 基站、UPF 设备、防火墙、路由器。
- c) 测评实施包括以下内容:
  - 1) 应核查是否采用安全传输协议对设备或组件进行管理;
  - 2) 应核查是否使用独立的带外管理网络对设备或组件进行管理。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 8.5.3 集中管控测评单元(L3-SMC6-03)

该测评单元包括以下要求。

- a) 测评指标:应具有安全配置核查能力,避免不安全配置导致的安全风险。
- b) 测评对象:5G 基站、路由器和 UPF 设备。
- c) 测评实施包括以下内容:
  - 1) 应核查 5G 基站、路由器和 UPF 设备的运维系统是否具有安全配置核查(安全策略相关配置数据)的能力;
  - 2) 应核查是否制定安全配置基线并启用安全配置核查功能。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.5.4 集中管控测评单元(L3-SMC6-04)

该测评单元包括以下要求。

- a) 测评指标:应具有空口用户面和控制面的安全算法优先级配置行为的安全审计功能。
- b) 测评对象:MEC 平台或业务应用平台。
- c) 测评实施包括以下内容:
  - 1) 应核查 MEC 平台或业务应用平台,是否对空口用户面和控制面(RRC)的安全算法优先级配置行为进行安全审计;
  - 2) 应核查 MEC 平台或业务应用平台,是否具有审计记录。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 8.6 安全建设管理

#### 8.6.1 电信运营商选择测评单元(L3-CMS6-01)

该测评单元包括以下要求。

- a) 测评指标:应选择具有基础电信业务经营资质的 5G 电信运营商,其所提供的 5G 网络应为所承载的业务应用系统及数据传输业务提供不低于其安全保护等级的安全保护能力。
- b) 测评对象:系统安全管理员、电信运营商资质文件和系统定级备案材料。
- c) 测评实施包括以下内容:

- 1) 应访谈系统安全管理员是否根据业务系统的安全保护等级选择不低于其安全保护等级的5G电信运营商;
- 2) 应核查5G网络和业务应用系统相关定级备案材料,5G网络的安全保护等级是否不低于其所承载的业务应用系统及数据传输业务。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 8.6.2 应用软件采购

### 8.6.2.1 测评单元(L3-CMS6-02)

该测评单元包括以下要求。

- a) 测评指标:5G用户终端设备、MEC平台等安装、运行的应用软件来自可靠分发渠道或使用数字签名。
- b) 测评对象:5G用户终端设备、MEC平台。
- c) 测评实施包括以下内容:
  - 1) 应核查移动应用软件是否来自可靠分发渠道或使用数字签名;
  - 2) 应核查使用数字签名的证书是否在有效期内。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

### 8.6.2.2 测评单元(L3-CMS6-03)

该测评单元包括以下要求。

- a) 测评指标:网络通信设备的产品及服务符合国家标准、行业标准。
- b) 测评对象:5G基站、UPF设备、路由器产品及服务。
- c) 测评实施包括以下内容:
  - 1) 应核查部署的网络通信设备的产品及服务是否符合国家标准或行业标准;
  - 2) 应核查引用的国家标准和行业标准是否处于现行状态。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 8.6.2.3 测评单元(L3-CMS6-04)

该测评单元包括以下要求:

- a) 测评指标:5G用户终端设备、MEC平台等安装、运行的应用软件由授权的开发者开发;
- b) 测评对象:5G用户终端设备、MEC平台;
- c) 测评实施:应核查应用软件是否由授权的开发者开发;
- d) 单元判定:如果c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

### 8.6.2.4 测评单元(L3-CMS6-05)

该测评单元包括以下要求。

- a) 测评指标:5G基站和UPF设备的软件实现安全自动化构建。
- b) 测评对象:5G基站和UPF设备。
- c) 测评实施包括以下内容:

- 1) 应访谈5G基站和UPF设备供应商,设计开发过程中是否具有软件的安全自动化构建;
- 2) 应核查5G基站和UPF设备的用户手册或验收文档,是否具有软件安全自动化构建能力。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 8.6.2.5 测评单元(L3-CMS6-06)

该测评单元包括以下要求。

- a) 测评指标:5G基站和UPF设备的软件实现版本控制和配置管理。
- b) 测评对象:5G基站和UPF设备。
- c) 测评实施包括以下内容:
  - 1) 应访谈5G基站和UPF设备的软件供应商,设计开发过程中是否具有软件的版本控制和配置管理;
  - 2) 应核查5G基站和UPF设备的用户手册或验收文档,是否具有变更跟踪管理,确保变更有效实施并可追溯。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 8.7 安全运维管理

#### 8.7.1 5G用户终端设备管理

##### 8.7.1.1 测评单元(L3-MMS6-01)

该测评单元包括以下要求。

- a) 测评指标:应指定人员定期巡视5G用户终端设备的部署环境,对可能影响设备正常工作的环境异常进行记录和维护。
- b) 测评对象:维护记录。
- c) 测评实施包括以下内容:
  - 1) 应访谈系统运维负责人是否有专门的人员对5G用户终端设备进行定期维护,由何部门或何人负责,维护周期是否小于1年;
  - 2) 应核查5G用户终端设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

##### 8.7.1.2 测评单元(L3-MMS6-02)

该测评单元包括以下要求:

- a) 测评指标:应对5G用户终端设备的入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定,并进行全程管理;
- b) 测评对象:安全管理文档;
- c) 测评实施:应核查5G用户终端设备安全管理文档是否覆盖5G用户终端设备入库、存储、部署、携带、维修、丢失和报废等方面;
- d) 单元判定:如果c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。



## 8.7.2 隐私管理

### 8.7.2.1 测评单元(L3-MMS6-03)

该测评单元包括以下要求：

- a) 测评指标：应具有使用5G-GUTI替代SUPI的能力，实现5G用户信息的隐私保护；
- b) 测评对象：5G基站、UPF设备、5G用户终端设备；
- c) 测评实施：应核查用户手册、验收文档或第三方检测报告，是否具有在业务过程中使用5G-GUTI的能力；
- d) 单元判定：如果c)测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

### 8.7.2.2 测评单元(L3-MMS6-04)

该测评单元包括以下要求：

- a) 测评指标：应具有增强的用户身份保密措施，除紧急呼叫外，使用SUCI或5G-GUTI在注册过程中传输SUPI；
- b) 测评对象：5G基站、UPF设备、5G用户终端设备；
- c) 测评实施：应核查用户手册、验收文档或第三方检测报告，是否具有在非紧急呼叫的注册过程中，使用SUCI或5G-GUTI作为5G用户身份标识；
- d) 单元判定：如果c)测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

### 8.7.3 网络开放能力测评单元(L3-MMS6-05)

该测评单元包括以下要求：

- a) 测评指标：应加强网络能力开放接口安全防护能力，防止攻击者从网络能力开放接口渗透进入行业应用网络；
- b) 测评对象：网络开放接口相关组件的用户手册或验收文档；
- c) 测评实施：应核查网络开放接口相关组件的用户手册或验收文档是否有加强网络能力开放接口暴露面收敛的安全措施；
- d) 单元判定：如果c)测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

## 9 第四级测评扩展要求

### 9.1 安全物理环境

物理位置选择测评单元(L1-PES6-01)包括以下要求。

- a) 测评指标：在业务数据不出园区的场景下，应将5G基站、UPF设备和5G用户终端设备部署在园区内。
- b) 测评对象：用户手册或验收文档。
- c) 测评实施包括以下内容：
  - 1) 应核查业务应用场景是否有业务数据不出园区的规定和要求；
  - 2) 应核查用户手册或验收文档，对于基站、UPF设备和5G用户终端设备等由电信运营商或其他外部单位建设、运营与维护的系统或设备，核查系统或设备是否部署在园区内。

- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 9.2 安全通信网络

### 9.2.1 网络架构

#### 9.2.1.1 测评单元(L4-CNS6-01)

该测评单元包括以下要求:

- a) 测评指标:5G行业应用系统不运行在低于其安全保护等级的5G网络上;
- b) 测评对象:5G行业应用系统和5G网络定级备案材料;
- c) 测评实施:应核查5G行业应用系统和承载5G行业应用系统的5G网络的定级备案材料,5G网络的安全保护等级是否不低于其承载的业务应用系统安全保护等级;
- d) 单元判定:如果 c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

#### 9.2.1.2 测评单元(L4-CNS6-02)

该测评单元包括以下要求。

- a) 测评指标:应由电信运营商或其他外部单位运营维护的5G基站、UPF设备、MEC平台、核心网等系统或设备与用户自有系统之间划分为不同区域,并在区域间采用边界隔离与防护手段。
- b) 测评对象:路由器、交换机和防火墙等提供访问控制功能的设备。
- c) 测评实施包括以下内容:
  - 1) 应核查由电信运营商或其他外部单位运营维护的UPF设备、MEC平台、核心网等系统或设备与用户自有系统之间是否部署边界隔离设备;
  - 2) 应核查是否设置并启用边界隔离策略实施访问控制;
  - 3) 应核查边界隔离策略是否有效。
- d) 单元判定:如果 c)中 1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.2.1.3 测评单元(L4-CNS6-03)

该测评单元包括以下要求。

- a) 测评指标:网络通信设备不包含其供应商、生产商或开发人员不再支持的软件和硬件组件,如已达到生命周期或不再支持的组件。
- b) 测评对象:5G基站、路由器和UPF设备。
- c) 测评实施包括以下内容:
  - 1) 应使用工具或其他适当的确定手段,识别供应商、生产者、开发人员或经营者的其他合同伙伴提供的硬件和软件组件、版本信息及种类;
  - 2) 应核查在系统安装的硬件和软件列表中,没有供应商在所附文档中未提供的条目(含版本信息和种类)。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。



#### 9.2.1.4 测评单元(L4-CNS6-04)

该测评单元包括以下要求。

- a) 测评指标:网络通信设备自身应具有入侵检测能力,防止对设备的攻击入侵。
- b) 测评对象:5G 基站、UPF 设备、路由器和防火墙等提供网络通信功能的设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查网络通信设备产品规格是否具有检测对设备攻击入侵能力;
  - 2) 应采用核查文档、测试策略、渗透测试等方式来验证网络通信设备能否检测对设备的入侵攻击,并给出相关处置措施建议。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

### 9.2.2 通信传输

#### 9.2.2.1 测评单元(L4-CNS6-05)

该测评单元包括以下要求。

- a) 测评指标:通过 5G 网络的空口、UPF 设备承载的数据等应采用硬隔离机制(无线采用 5G 专用基站或载波隔离或资源块预留,传输采用 FlexE、TDM、光波长切分等方式隔离,UPF 设备采用专用部署模式)的信道传输。
- b) 测评对象:5G 基站、路由器和 UPF 设备。
- c) 测评实施包括以下内容:
  - 1) 应核查 5G 基站是否采用专用基站或载波隔离或资源块预留措施;
  - 2) 应核查 5G 基站和 UPF 设备间的数据传输是否采用 FlexE、TDM、光波长切分等隔离措施;
  - 3) 应核查是否使用专用 UPF 设备提供隔离措施。
- d) 单元判定:如果 c)中 1)~3)均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 9.2.2.2 测评单元(L4-CNS6-06)

该测评单元包括以下要求:

- a) 测评指标:使用 5G 网络的空口、UPF 设备进行指令或相关数据交互的操作,应采用加密认证技术手段实现身份认证、访问控制和数据加密传输;
- b) 测评对象:加密认证设备、路由器、交换机和防火墙等提供访问控制功能的设备;
- c) 测评实施:应核查 5G 行业应用系统中使用 5G 网络的空口、UPF 设备进行指令或相关数据交互的操作是否采用加密认证技术实现身份认证、访问控制和数据加密传输;
- d) 单元判定:如果 c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

#### 9.2.2.3 测评单元(L4-CNS6-07)

该测评单元包括以下要求。

- a) 测评指标:应具有 5G 基站和 UPF 设备之间 N3 接口、UPF 设备和 UPF 设备之间 N9 接口、UPF 设备和企业网边界之间 N6 接口的用户面数据完整性保护能力。
- b) 测评对象:5G 基站、UPF 设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:

- 1) 应核查5G基站和UPF设备之间N3接口、UPF设备和UPF设备之间N9接口、UPF设备和企业网边界之间N6接口是否部署安全网关(内置或外置)并是否正确配置满足GM/T 0022要求的IPsec;
- 2) 应核查5G基站和UPF设备之间N3接口、UPF设备和UPF设备之间N9接口、UPF设备和企业网边界之间N6接口的用户面数据是否具有完整性。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 9.2.2.4 测评单元(L4-CNS6-08)

该测评单元包括以下要求。

- a) 测评指标:应具有5G基站和UPF设备之间N3接口、UPF设备和UPF设备之间N9接口、UPF设备和企业网边界之间N6接口的用户面数据机密性保护能力。
- b) 测评对象:5G基站、UPF设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查5G基站和UPF设备之间N3接口、UPF设备和UPF设备之间N9接口、UPF设备和企业网边界之间N6接口是否部署安全网关(内置或外置),并是否正确配置满足GM/T 0022要求的IPsec;
  - 2) 应核查5G基站和UPF设备之间N3接口、UPF设备和UPF设备之间N9接口、UPF设备和企业网边界之间N6接口用户面数据是否具有机密性。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 9.2.2.5 测评单元(L4-CNS6-09)

该测评单元包括以下要求。

- a) 测评指标:应具有5G基站和UPF设备之间N3接口、UPF设备和UPF设备之间N9接口、UPF设备和企业网边界之间N6接口的用户面数据防重放保护能力。
- b) 测评对象:5G基站、UPF设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查5G基站和UPF设备之间N3接口、UPF设备和UPF设备之间N9接口、UPF设备和企业网边界之间N6接口是否部署安全网关(内置或外置),并是否正确配置满足GM/T 0022要求的IPsec;
  - 2) 应核查5G基站和UPF设备之间N3接口、UPF设备和UPF设备之间N9接口、UPF设备和企业网边界之间N6接口用户面数据是否具有防重放。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 9.2.2.6 测评单元(L4-CNS6-10)

该测评单元包括以下要求。

- a) 测评指标:应具有UPF设备和SMF设备之间N4接口的控制面数据完整性保护能力。
- b) 测评对象:UPF设备、SMF设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查UPF设备和SMF设备之间N4接口是否部署安全网关(内置或外置),并是否正确

配置满足 GM/T 0022 要求的 IPsec;

- 2) 应核查 UPF 设备和 SMF 设备之间 N4 接口控制面数据是否具有完整性。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 9.2.2.7 测评单元(L4-CNS6-11)

该测评单元包括以下要求。

- a) 测评指标:应具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据机密性保护能力。
- b) 测评对象:UPF 设备、SMF 设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查 UPF 设备和 SMF 设备之间 N4 接口是否部署安全网关(内置或外置),并是否正确配置满足 GM/T 0022 要求的 IPsec;
  - 2) 应核查 UPF 设备和 SMF 设备之间 N4 接口控制面数据是否具有机密性。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 9.2.2.8 测评单元(L4-CNS6-12)

该测评单元包括以下要求。

- a) 测评指标:应具有 UPF 设备和 SMF 设备之间 N4 接口的控制面数据防重放保护能力。
- b) 测评对象:UPF 设备、SMF 设备和安全网关设备或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查 UPF 设备和 SMF 设备之间 N4 接口是否部署安全网关(内置或外置),并是否正确配置满足 GM/T 0022 要求的 IPsec;
  - 2) 应核查 UPF 设备和 SMF 设备之间 N4 接口控制面数据是否具有防重放。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 9.2.2.9 测评单元(L4-CNS6-13)

该测评单元包括以下要求。

- a) 测评指标:应具有 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间的应用数据完整性保护能力。
- b) 测评对象:提供校验技术或密码技术功能的设备或组件。
- c) 测评实施包括以下内容:
  - 1) 应核查是否在 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户间数据传输过程中使用校验技术或密码技术来保护数据;
  - 2) 应核查数据传输过程中是否具有数据完整性。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.2.2.10 测评单元(L4-CNS6-14)

该测评单元包括以下要求。

- a) 测评指标:应具有 5G 用户终端设备间,或 5G 行业应用服务器与 5G 用户终端设备间的应用数



据机密性保护能力。

- b) 测评对象:提供校验技术或密码技术功能的设备或组件。
- c) 测评实施包括以下内容:
  - 1) 应核查是否在5G用户终端设备间,或5G行业应用服务器与5G用户间数据传输过程中使用校验技术或密码技术来保护数据;
  - 2) 应核查数据传输过程中是否具有数据机密性。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 9.2.3 无线安全

#### 9.2.3.1 测评单元(L4-CNS6-15)

该测评单元包括以下要求。

- a) 测评指标:应具有空口干扰检测和干扰定位能力。
- b) 测评对象:5G基站。
- c) 测评实施包括以下内容:
  - 1) 应核查5G基站的用户手册、验收文档或第三方检测报告,是否具有干扰检测和干扰定位功能;
  - 2) 应测试验证5G基站对干扰是否可以成功检测并上报测量;
  - 3) 网管侧基于基站上报的测量,分析检测是否存在干扰及干扰的种类,同时给出干扰源的位置。
- d) 单元判定:如果c)中1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.2.3.2 测评单元(L4-CNS6-16)

该测评单元包括以下要求。

- a) 测评指标:在5G基站工作范围内,应具有对发射仿冒无线信号的伪基站进行检测的能力。
- b) 测评对象:5G基站。
- c) 测评实施包括以下内容:
  - 1) 应核查5G基站对工作范围内的发射无线信号的伪基站具有检测功能,与用户手册或验收文档说明一致;
  - 2) 应核查5G基站是否启用伪基站检测,分析伪基站的信息并定位伪基站(呈现时间相关摘要、伪基站特征、处置建议及定位信息,辅助定位伪基站位置)。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 9.2.4 入侵防范

#### 9.2.4.1 测评单元(L4-CNS6-17)

该测评单元包括以下要求。

- a) 测评指标:应具有伪造北斗、GPS等信号的检测和防御能力。
- b) 测评对象:5G基站。
- c) 测评实施包括以下内容:
  - 1) 应核查5G基站的用户手册、验收文档或第三方检测报告,是否具有伪造北斗、GPS等信号

的检测和防御功能；

- 2) 应核查5G基站对北斗、GPS等伪造信号的检测和防御功能是否开启。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.2.4.2 测评单元(L4-CNS6-18)

该测评单元包括以下要求。

- a) 测评指标:应具有空口信令面DDoS攻击的检测和防御能力。
- b) 测评对象:5G基站。
- c) 测评实施包括以下内容:
  - 1) 应核查5G基站的用户手册、验收文档或第三方检测报告,是否具有DDoS攻击的检测和防御功能;
  - 2) 应核查验证5G基站对空口信令面DDoS攻击的检测和防御功能是否开启。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.2.4.3 测评单元(L4-CNS6-19)

该测评单元包括以下要求。

- a) 测评指标:应具有传输端口的访问控制能力,设置访问控制规则。
- b) 测评对象:5G基站和UPF设备。
- c) 测评实施包括以下内容:
  - 1) 应核查5G基站、UPF设备是否具有传输端口的访问控制能力,是否启用访问控制策略;
  - 2) 应核查5G基站、UPF设备是否具有传输端口的单包攻击防御、DDoS攻击防御等的的能力;
  - 3) 应核查5G基站、UPF设备对传输端口入侵行为(单包攻击、DDoS攻击)是否开启检测和防御功能。
- d) 单元判定:如果c)中1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.2.4.4 测评单元(L4-CNS6-20)

该测评单元包括以下要求。

- a) 测评指标:应具有用户面数据的流量检测能力。
- b) 测评对象:流量检测设备或组件。
- c) 测评实施包括以下内容:
  - 1) 应核查是否部署流量检测设备或组件,流量检测策略是否正确配置、开启并生效;
  - 2) 应核查流量检测设备或组件是否具有用户面数据的流量检测能力。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 9.3 安全区域边界

#### 9.3.1 边界防护测评单元(L4-ABS6-01)

该测评单元包括以下要求。

- a) 测评指标:5G网络N6接口与应用服务器网络之间的访问和数据流通过边界网关设备,并设置

访问控制规则。

- b) 测评对象:访问控制策略和网络边界设备。
- c) 测评实施包括以下内容:
  - 1) 应核查5G网络N6接口与应用服务器网络之间的访问和数据是否通过边界网关设备;
  - 2) 应核查网络边界访问控制规则和访问控制策略是否正确配置、开启并生效。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 9.3.2 访问控制

#### 9.3.2.1 测评单元(L4-ABS6-02)

该测评单元包括以下要求。

- a) 测评指标:5G用户终端设备应开启接入认证功能,并支持采用5G网络进行双向认证。
- b) 测评对象:5G用户终端设备。
- c) 测评实施:
  - 1) 应核查5G用户终端设备是否开启接入认证功能;
  - 2) 应核查是否采用5G网络或认证服务器进行双向认证。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.3.2.2 测评单元(L4-ABS6-03)

该测评单元包括以下要求。

- a) 测评指标:对5G专网中存在多种业务系统的,应通过硬隔离机制(无线采用5G专用基站或载波隔离或资源块预留,传输采用FlexE、TDM、光波长切分等方式隔离,UPF设备采用专用部署模式)对不同业务系统进行安全隔离,并限制无权限访问相关业务系统的5G用户终端设备接入业务系统所在的网络。
- b) 测评对象:5G专网。
- c) 测评实施包括以下内容:
  - 1) 应核查当5G专网中存在多个业务系统时,是否按照业务特点采取硬隔离机制(无线采用5G专用基站或载波隔离或资源块预留,传输采用:FlexE、TDM、光波长切分等方式隔离,UPF设备采用专用部署模式)实现业务系统的安全隔离;
  - 2) 应核查当5G专网中存在多个业务系统时,是否有相关的授权访问控制措施限制无权限5G用户终端设备接入对应的5G专网各业务系统。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.3.2.3 测评单元(L4-ABS6-04)

该测评单元包括以下要求:

- a) 测评指标:应能根据5G用户终端设备所在的区域,控制其接入相应5G专网权限,限制5G用户终端设备在非授权区域访问5G专网及相关业务系统;
- b) 测评对象:5G专网;
- c) 测评实施:应核查是否能够提供基于5G用户终端设备所在的小区限制其接入相应5G专网权限的能力,阻止5G用户终端设备在非授权区域访问5G专网及相关业务系统;



- d) 单元判定:如果c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

### 9.3.3 入侵防范

#### 9.3.3.1 测评单元(L4-ABS6-05)

该测评单元包括以下要求。

- a) 测评指标:边缘应用应具有抗击多种高级攻击的安全防御能力。
- b) 测评对象:边缘应用、入侵防御系统或相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查在边缘应用上是否部署了入侵防御系统对网络入侵行为进行防范(如抗DDoS能力、防恶意代码能力、抗入侵能力、病毒检测和防护等),其规则库是否为最新;
  - 2) 应核查部署的入侵防御系统或相关组件对异常的流量和未知的威胁监控策略是否有效,如核查入侵防御系统或相关组件是否能记录攻击类型、攻击时间等信息;
  - 3) 应核查部署的攻击防御检测设备或相关组件对攻击行为的报警策略是否有效,如核查入侵防御系统或相关组件是否具有实时报警日志等信息。
- d) 单元判定:如果c)中1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.3.3.2 测评单元(L4-ABS6-06)

该测评单元包括以下要求。

- a) 测评指标:应具有对5G用户终端设备恶意行为(如UE互访、地址欺骗等)的检测,并对存在恶意行为的5G用户终端设备进行处置的能力。
- b) 测评对象:入侵防御系统或相关组件、UPF设备。
- c) 测评实施包括以下内容:
  - 1) 应核查是否具有检测、防御5G用户终端设备的恶意攻击行为(如UE互访、地址欺骗等)的能力;
  - 2) 应核查是否具有对恶意5G用户终端设备进行处置的能力。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 9.4 安全计算环境

### 9.4.1 身份鉴别测评单元(L4-CES6-01)

该测评单元包括以下要求。

- a) 测评指标:应具有主认证之外的二次认证方式,以确保仅授权的UE访问用户所属网络。
- b) 测评对象:认证方案建议书或验收文档及认证相关组件。
- c) 测评实施包括以下内容:
  - 1) 应核查二次认证方案建议书或验收文档是否有主认证之外的二次认证方式以确保授权的UE访问用户所属网络;
  - 2) 应核查相关二次认证方式是否正确配置、开启并生效。
- d) 单元判定:如果c)中1)和2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

## 9.4.2 5G 用户终端设备安全

### 9.4.2.1 测评单元(L4-CES6-02)

该测评单元包括以下要求：

- a) 测评指标：固件及固件升级包上线前应进行安全性检测；
- b) 测评对象：5G 用户终端设备；
- c) 测评实施：应核查固件及固件升级包上线前是否完成安全性检测，是否具有安全检测报告；
- d) 单元判定：如果 c) 测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

### 9.4.2.2 测评单元(L4-CES6-03)

该测评单元包括以下要求。

- a) 测评指标：应具有软件白名单控制能力，应能根据白名单控制应用软件安装、运行。
- b) 测评对象：5G 用户终端设备。
- c) 测评实施包括以下内容：
  - 1) 应核查 5G 用户终端设备系统是否具有软件白名单功能；
  - 2) 应核查 5G 用户终端设备系统的白名单功能是否能控制应用软件的安装和运行。
- d) 单元判定：如果 c) 中 1) 和 2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

### 9.4.3 访问控制测评单元(L4-CES6-04)

该测评单元包括以下要求。

- a) 测评指标：应提供 MEC 平台用户设置其所属的不同虚拟机之间的访问控制策略的功能。
- b) 测评对象：MEC 的管理平台、5G 网络服务客户管理系统、网络边界访问控制设备。
- c) 测评实施包括以下内容：
  - 1) 应核查 MEC 的管理平台或安全设备，查看是否允许客户设置不同虚拟机间访问控制策略；
  - 2) 应核查 MEC 的管理平台，查看是否存在不同虚拟机间的访问控制管理模块，是否可以开启该访问控制功能；
  - 3) 应核查 MEC 平台中的客户虚拟机安全策略，查看不同虚拟机间访问控制策略是否有效。
- d) 单元判定：如果 c) 中 1)~3) 为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

### 9.4.4 入侵防范测评单元(L4-CES6-05)

该测评单元包括以下要求。

- a) 测评指标：应在 MEC 边平台提供虚拟机逃逸攻击的检测能力，防止虚拟机对虚拟化管理平台的入侵攻击。
- b) 测评对象：MEC 平台。
- c) 测评实施包括以下内容：
  - 1) 应访谈并核查 MEC 平台中是否具有应用安全防护、主机安全防护等入侵检测的措施；
  - 2) 应核查在边缘应用发生入侵事件时，安全防护措施是否提供安全报警。
- d) 单元判定：如果 c) 中 1) 和 2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

#### 9.4.5 数据安全测评单元(L4-CES6-06)

该测评单元包括以下要求。

- a) 测评指标:应具有空口用户面数据和控制面数据的机密性和完整性功能。
- b) 测评对象:5G 基站的用户手册或验收文档。
- c) 测评实施:
  - 1) 应核查 5G 基站的用户手册或验收文档,是否具有空口用户面数据和控制面(RRC)数据的机密性功能;
  - 2) 应核查 5G 基站的用户手册或验收文档,是否具有空口用户面数据和控制面(RRC)数据的完整性功能;
  - 3) 应核查 5G 基站的用户手册或验收文档,是否具有空口用户面数据和控制面(RRC)数据的防重放功能。
- d) 单元判定:如果 c)中 1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 9.5 安全管理中心

#### 9.5.1 集中管控测评单元(L4-SMC6-01)

该测评单元包括以下要求。

- a) 测评指标:分离业务系统流量与 5G 网络管理流量。
- b) 测评对象:网络架构。
- c) 测评实施包括以下内容:
  - 1) 应核查网络架构是否采用带外管理或策略配置等方式实现 5G 网络管理流量和业务系统流量分离;
  - 2) 应核查 5G 网络管理流量与业务系统流量是否分离。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.5.2 集中管控测评单元(L4-SMC6-02)

该测评单元包括以下要求。

- a) 测评指标:应能够建立设备管理的安全传输通道,对 5G 电信运营商提供的网元设备进行安全管理。
- b) 测评对象:5G 基站、UPF 设备、防火墙、路由器。
- c) 测评实施包括以下内容:
  - 1) 应核查是否采用安全传输协议对设备或组件进行管理;
  - 2) 应核查是否使用独立的带外管理网络对设备或组件进行管理。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测试单元指标要求,否则不符合或部分符合本测试单元指标要求。

#### 9.5.3 集中管控测评单元(L4-SMC6-03)

该测评单元包括以下要求。

- a) 测评指标:应具有安全配置核查能力,避免不安全配置导致的安全风险。
- b) 测评对象:5G 基站、路由器和 UPF 设备。

- c) 测评实施包括以下内容:
  - 1) 应核查 5G 基站、路由器和 UPF 设备的运维系统是否具有安全配置核查(安全策略相关配置数据)的能力;
  - 2) 应核查是否制定安全配置基线并启用安全配置核查功能。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.5.4 集中管控测评单元(L4-SMC6-04)

该测评单元包括以下要求。

- a) 测评指标:应具有空口用户面和控制面的安全算法优先级配置行为的安全审计功能。
- b) 测评对象:MEC 平台或业务应用平台。
- c) 测评实施:
  - 1) 应核查 MEC 平台或业务应用平台,是否对空口用户面和控制面(RRC)的安全算法优先级配置行为进行安全审计;
  - 2) 应核查 MEC 平台或业务应用平台,是否具有审计记录查看界面或者通过集中审计平台收集审计记录。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

### 9.6 安全管理

#### 9.6.1 电信运营商选择测评单元(L4-CMS6-01)

该测评单元包括以下要求。

- a) 测评指标:应选择具有基础电信业务经营资质的 5G 电信运营商,其所提供的 5G 网络应为所承载的业务应用系统及数据传输业务提供不低于其安全保护等级的安全保护能力。
- b) 测评对象:系统安全管理员、电信运营商资质文件和系统定级备案材料。
- c) 测评实施包括以下内容:
  - 1) 应访谈系统安全管理员是否根据业务系统的安全保护等级选择不低于其安全保护等级的 5G 电信运营商;
  - 2) 应核查 5G 网络和业务应用系统相关定级备案材料,5G 网络的安全保护等级是否不低于其所承载的业务应用系统及数据传输业务。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.6.2 应用软件采购

##### 9.6.2.1 测评单元(L4-CMS6-02)

该测评单元包括以下要求。

- a) 测评指标:5G 用户终端设备、MEC 平台等安装、运行的应用软件来自可靠分发渠道或使用数字签名。
- b) 测评对象:5G 用户终端设备、MEC 平台。
- c) 测评实施包括以下内容:
  - 1) 应核查移动应用软件是否来自可靠分发渠道或使用数字签名;



- 2) 应核查使用数字签名的证书是否在有效期内。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

#### 9.6.2.2 测评单元(L4-CMS6-03)

该测评单元包括以下要求。

- a) 测评指标:网络通信设备的产品及服务符合国家标准、行业标准。
- b) 测评对象:5G 基站、UPF 设备、路由器产品及服务。
- c) 测评实施包括以下内容:
  - 1) 应核查部署的网络通信设备的产品及服务是否符合国家标准或行业标准;
  - 2) 应核查引用的国家标准和行业标准是否处于现行状态。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.6.2.3 测评单元(L4-CMS6-04)

该测评单元包括以下要求:

- a) 测评指标:5G 用户终端设备、MEC 平台等安装、运行的应用软件由授权的开发者开发;
- b) 测评对象:5G 用户终端设备、MEC 平台;
- c) 测评实施:应核查应用软件是否由授权的开发者开发;
- d) 单元判定:如果 c)测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

#### 9.6.2.4 测评单元(L4-CMS6-05)

该测评单元包括以下要求。

- a) 测评指标:5G 基站和 UPF 设备的软件实现安全自动化构建。
- b) 测评对象:5G 基站和 UPF 设备。
- c) 测评实施包括以下内容:
  - 1) 应访谈 5G 基站和 UPF 设备供应商,设计开发过程中是否具有软件的安全自动化构建能力;
  - 2) 应核查 5G 基站和 UPF 设备的用户手册或验收文档,是否具有软件安全自动化构建能力。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.6.2.5 测评单元(L4-CMS6-06)

该测评单元包括以下要求。

- a) 测评指标:5G 基站和 UPF 设备的软件实现版本控制和配置管理。
- b) 测评对象:5G 基站和 UPF 设备。
- c) 测评实施包括以下内容:
  - 1) 应访谈 5G 基站和 UPF 设备的软件供应商,设计开发过程中是否具有软件的版本控制和配置管理;
  - 2) 应核查 5G 基站和 UPF 设备的用户手册或验收文档,是否具有变更跟踪管理,确保变更有效实施并可追溯。
- d) 单元判定:如果 c)中 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本

测评单元指标要求。

## 9.7 安全运维管理

### 9.7.1 5G 用户终端设备管理

#### 9.7.1.1 测评单元(L4-MMS6-01)

该测评单元包括以下要求。

- a) 测评指标:应指定人员定期巡视 5G 用户终端设备的部署环境,对可能影响设备正常工作的环境异常进行记录和维护。
- b) 测评对象:系统运维负责人和维护记录。
- c) 测评实施包括以下内容:
  - 1) 应访谈系统运维负责人是否有专门的人员对 5G 用户终端设备进行定期维护,由何部门或何人负责,维护周期是否小于 1 年;
  - 2) 应核查 5G 用户终端设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

#### 9.7.1.2 测评单元(L4-MMS6-02)

该测评单元包括以下要求。

- a) 测评指标:应对 5G 用户终端设备的入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定,并进行全程管理。
- b) 测评对象:安全管理文档、5G 用户终端设备管理记录。
- c) 测评实施:
  - 1) 应核查终端设备安全管理文档是否覆盖 5G 用户终端设备入库、存储、部署、携带、维修、丢失和报废等方面;
  - 2) 应核查是否具有终端设备管理记录,内容是否包含 5G 用户终端设备的入库、存储、部署、携带、维修、丢失和报废等记录。
- d) 单元判定:如果 c) 中 1) 和 2) 均为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

## 9.7.2 隐私管理

### 9.7.2.1 测评单元(L4-MMS6-03)

该测评单元包括以下要求:

- a) 测评指标:应具有使用 5G-GUTI 替代 SUPI 的能力,实现 5G 用户信息的隐私保护;
- b) 测评对象:5G 基站、UPF 设备、5G 用户终端设备;
- c) 测评实施:应核查用户手册、验收文档或第三方检测报告,是否具有在业务过程中使用 5G-GUTI 的能力;
- d) 单元判定:如果 c) 测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

### 9.7.2.2 测评单元(L4-MMS6-04)

该测评单元包括以下要求：

- a) 测评指标：应具有增强的用户身份保密措施，除紧急呼叫外，使用SUCI或5G-GUTI在注册过程中传输SUPI；
- b) 测评对象：5G基站、UPF设备、5G用户终端设备；
- c) 测评实施：应核查用户手册、验收文档或第三方检测报告，是否具有在非紧急呼叫的注册过程中，使用SUCI或5G-GUTI作为5G用户身份标识；
- d) 单元判定：如果c)测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

## 9.7.3 网络能力开放接口

### 9.7.3.1 测评单元(L4-MMS6-05)

该测评单元包括以下要求：

- a) 测评指标：应加强网络能力开放接口安全防护能力，防止攻击者从网络能力开放接口渗透进入行业应用网络；
- b) 测评对象：网络开放接口相关组件的用户手册或验收文档；
- c) 测评实施：应核查网络开放接口相关组件的用户手册或验收文档是否有加强网络能力开放接口暴露面收敛的安全措施；
- d) 单元判定：如果c)测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

### 9.7.3.2 测评单元(L4-MMS6-06)

该测评单元包括以下要求：

- a) 测评指标：应加强网络能力开放接口暴露面收敛；
- b) 测评对象：网络开放接口相关组件的用户手册或验收文档；
- c) 测评实施：应核查是否具有加强网络能力开放接口暴露面收敛的保护措施，如暴露的接口是否具有安全认证、加密、完整性保护等能力；
- d) 单元判定：如果c)测评实施为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

## 10 第五级测评扩展要求

略。

附录 A  
(规范性)  
测评单元编码规则

测评单元编码由安全级别、要求类别、要求顺序码三部分构成。编码编制形式应与图 A.1 相符,编码代号应符合表 A.1 规定。

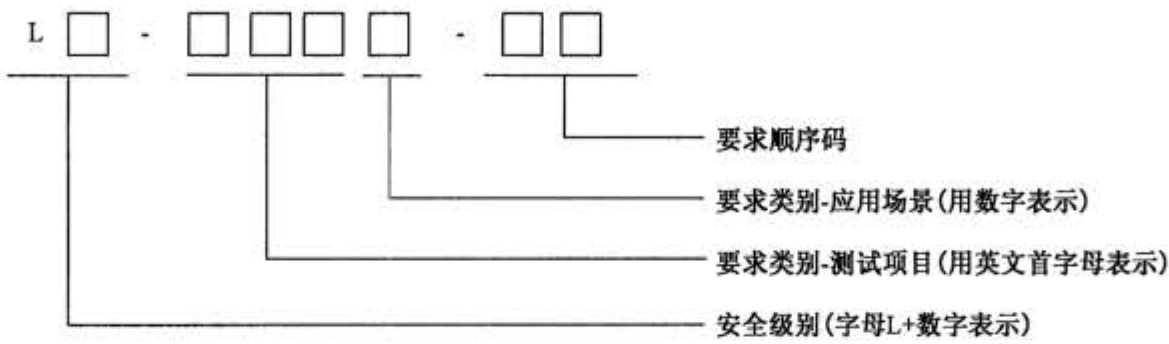


图 A.1 编码编制形式

表 A.1 编码代号

编码组成	代 码
安全级别	L:级别(Level); L1:第一级; L2:第二级; L3:第三级; L4:第四级; L5:第五级
要求类别——测试项目	ABS:安全区域边界(Area Boundary Security); BDS:大数据系统(Bigdata System); CES:安全计算环境(Computing Environment Security); CMS:安全建设管理(Construction Management Security); CNS:安全通信网络(Communication Network Security); MMS:安全运维管理(Maintenance Management Security); ORS:安全管理机构(Organization and Resource Security); PES:安全物理环境(Physical Environment Security); PSS:安全管理制度(Policy and System Security); HRS:安全管理人员(Human Resource Security); SMC:安全管理中心(Security Management Center)
要求类别——应用场景	1:安全测评通用要求; 2:云计算安全测评扩展要求; 3:移动互联安全测评扩展要求; 4:物联网安全测评扩展要求; 5:工业控制系统安全测评扩展要求; 6:边缘计算安全测评扩展要求

示例:测评单元编码为L1-PES6-01,代表源自边缘计算安全测评扩展要求部分的第一级安全物理环境类的第1项指标。



## 参 考 文 献

- [1] GB/T 42564—2023 信息安全技术 边缘计算安全技术要求
  - [2] 3GPP TR 21.905 V17.1.0 Vocabulary for 3GPP Specifications
  - [3] 3GPP TS 22.261 V19.4.0 Service requirements for the 5G system
  - [4] 3GPP TS 23.501 V18.3.0 System architecture for the 5G System
  - [5] 3GPP TS 33.501 V18.3.0 Security architecture and procedures for 5G System
  - [6] ETSI GS MEC 001 V2.1.1 Multi-access Edge Computing (MEC): Terminology
  - [7] GM/T 0022 IPsec VPN技术规范
-

中华人民共和国公共安全  
行业标准  
信息安全技术 网络安全等级保护 5G  
接入安全测评要求  
GA/T 2348—2025

\*

中国标准出版社出版发行  
北京市朝阳区和平里西街甲2号(100029)  
网址 [www.spc.net.cn](http://www.spc.net.cn)  
总编室:(010)68533533 发行中心:(010)51780238  
读者服务部:(010)68523946  
中国标准出版社秦皇岛印刷厂印刷  
各地新华书店经销

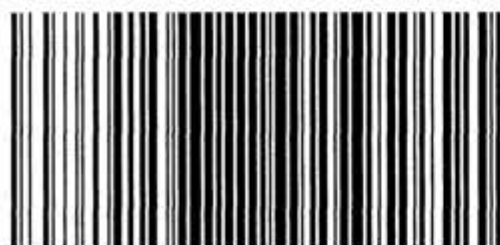
\*

开本 880×1230 1/16 印张 2.75 字数 73 千字  
2025 年 12 月第 1 版 2025 年 12 月第 1 次印刷

\*

书号: 155066 · 2-39560 定价 70.00 元

如有印装差错 由本社发行中心调换  
版权专有 侵权必究  
举报电话:(010)68510107



GA/T 2348-2025