

中华人民共和国通信行业标准

YD/T XXXXX—XXXX

5G 多接入边缘计算平台通用安全防护要求

General security protection requirements for 5G multi-access edge computing platform

(点击此处添加与国际标准一致性程度的标识)

草案版次选择

行业标准信息服务平台

XXXX—XX—XX 发布

XXXX—XX—XX 实施

目 次

前 言	1
1 范围	1
2 规范性引用文件	1
3 术语和定义	2
4 缩略语	2
5 5G 多接入边缘计算平台安全防护概述	3
5.1 5G 多接入边缘计算平台安全防护范围	3
5.2 5G 多接入边缘计算平台安全风险分析	4
5.2.1 概述	4
5.2.2 应用安全风险	4
5.2.3 网络安全风险	5
5.2.4 设备安全风险	5
5.2.5 数据安全风险	6
5.2.6 物理环境安全风险	6
5.2.7 管理安全风险	6
5.3 5G 多接入边缘计算平台安全防护内容	6
5.4 5G 多接入边缘计算平台安全防护要求等级划分	7
6 5G 多接入边缘计算平台安全防护要求	7
6.1 第 1 级要求	7
6.2 第 2 级要求	7
6.2.1 应用安全要求	7
6.2.2 网络安全要求	9
6.2.3 设备安全要求	10
6.2.4 数据安全要求	12
6.2.5 物理环境安全要求	13
6.2.6 管理安全要求	13
6.3 第 3 级要求	15
6.3.1 应用安全要求	15
6.3.2 网络安全要求	16
6.3.3 设备安全要求	17
6.3.4 数据安全要求	18
6.3.5 物理环境安全要求	19
6.3.6 管理安全要求	19
6.4 第 4 级要求	20
6.5 第 5 级要求	20
附 录 A （规范性） 5G 多接入边缘计算平台各个主体的责任范围	21
附 录 B （资料性） 5G 多接入边缘计算平台风险分析	23

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。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、中国移动通信集团有限公司、中国移动通信集团浙江有限公司、华为技术有限公司、中兴通讯股份有限公司、启明星辰信息技术集团股份有限公司、恒安嘉新（北京）科技股份有限公司、亚信安全科技股份有限公司、北京网宿科技有限公司、武汉绿色网络信息服务有限责任公司、杭州电子科技大学、山石网科通信技术股份有限公司、中国联合网络通信集团有限公司。

本文件主要起草人：孟楠、戴方芳、王晗、邱勤、徐思嘉、蒋熠、薛永刚、殷浩、周继华、赵马煜、徐昕白、薛辉、赵亮、马涛、周书兵、王赞、张操、赵雨佳、高云园、余滔、任亮、李宇、谢泽铖、张曼君。

行业标准信息服务平台

5G 多接入边缘计算平台通用安全防护要求

1 范围

本文件规定了5G多接入边缘计算平台按安全防护等级的安全防护要求，涉及应用安全、网络安全、设备安全、数据安全、物理环境安全和管理安全。

本文件适用于基础电信业务经营者独立或与第三方合作建设运营以及用户自身建设运营的5G多接入边缘计算平台。本文件主要针对5G多接入边缘计算平台提出安全防护要求，与其相关的其他网络和系统单元如核心网、数据中心、公有云、企业本地网络等的安全防护要求见相应网络和系统单元类型的安全防护标准。

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 1731-2008	电信网和互联网灾难备份及恢复实施指南
YD/T 1754-2008	电信网和互联网物理环境安全等级保护要求
YD/T 2698-2014	电信网和互联网安全防护基线配置要求及检测要求 网络设备
YD/T 2699-2014	电信网和互联网安全防护基线配置要求及检测要求 安全设备
YD/T 2700-2014	电信网和互联网安全防护基线配置要求及检测要求 数据库
YD/T 2701-2014	电信网和互联网安全防护基线配置要求及检测要求 操作系统
YD/T 2702-2014	电信网和互联网安全防护基线配置要求及检测要求 中间件
YD/T 2703-2014	电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统
3GPP TS 33.513	5G 安全保证规范 (SCAS); 用户平面功能 (UPF) (5G Security Assurance Specification (SCAS); User Plane Function (UPF))

3 术语和定义

下列术语和定义适用于本文件。

3.1

多接入边缘计算 multi-access edge computing
在涵盖一种或多种接入技术的接入网边缘、靠近用户的位置，提供IT服务环境和云计算能力的系统。

4 缩略语

下列缩略语适用于本文件。

ACL	访问控制列表	Access Control Lists
API	应用程序编程接口	Application Programming Interface
APP	应用程序	Application
CPE	客户前置设备	Customer Premise Equipment
CPU	中央处理器	Central Processing Unit
DDoS	分布式拒绝服务	Distributed Denial of Service
DNS	域名系统	Domain Name System
EMS	网元管理系统	Element Management System
GTP	GPRS隧道协议	GPRS Tunneling Protocol
ICT	信息与通信技术	Information and Communications Technology
ID	身份证明文件	Identity Document
IDS	入侵检测系统	Intrusion Detection System
IP	互联网协议	Internet Protocol
IPS	入侵防御系统	Intrusion Prevention System
IPSec	互联网安全协议	Internet Protocol Security
L2TP	第二层隧道协议	Layer 2 Tunneling Protocol
MEAO	MEC应用编排器	MEC Application Orchestrator
MEC	多接入边缘计算	Multi-Access Edge Computing
MEP	多接入边缘计算平台	Multi-Access Edge Computing Platform
MEPM	多接入边缘计算平台管理器	Multi-Access Edge Computing Platform Manager
MITM	中间人	Man-in-the-Middle
NFV	网络功能虚拟化	Network Functions Virtualization
NFVI	网络功能虚拟化基础设施	Network Functions Virtualization Infrastructure
NFVO	网络功能虚拟化编排器	Network Functions Virtualization Orchestrator
NTA	网络流量分析	Network Traffic Analysis
OTII	开放IT基础设施	Open Telecom IT Infrastructure
PBKDF2	基于密码的密钥衍生函数2	Password-Based Key Derivation Function 2
PDP	分组数据协议	Packet Data Protocol
QoS	服务质量	Quality of Service
SDK	软件开发工具包	Software Development Kit
SLA	服务等级协议	Service-Level Agreement
UPF	用户面功能	User Plane Function
VIM	虚拟化基础设施管理器	Virtualized Infrastructure Manager
VLAN	虚拟局域网	Virtual Local Area Network
VXLAN	虚拟扩展局域网	Virtual Extensible Local Area Network
WAF	网络应用程序防火墙	Web Application Firewall

5 5G 多接入边缘计算平台安全防护概述

5.1 5G 多接入边缘计算平台安全防护范围

5G多接入边缘计算（MEC）平台的安全防护范围覆盖MEC平台以及平台对外的通信接口与链路等，如图1所示。

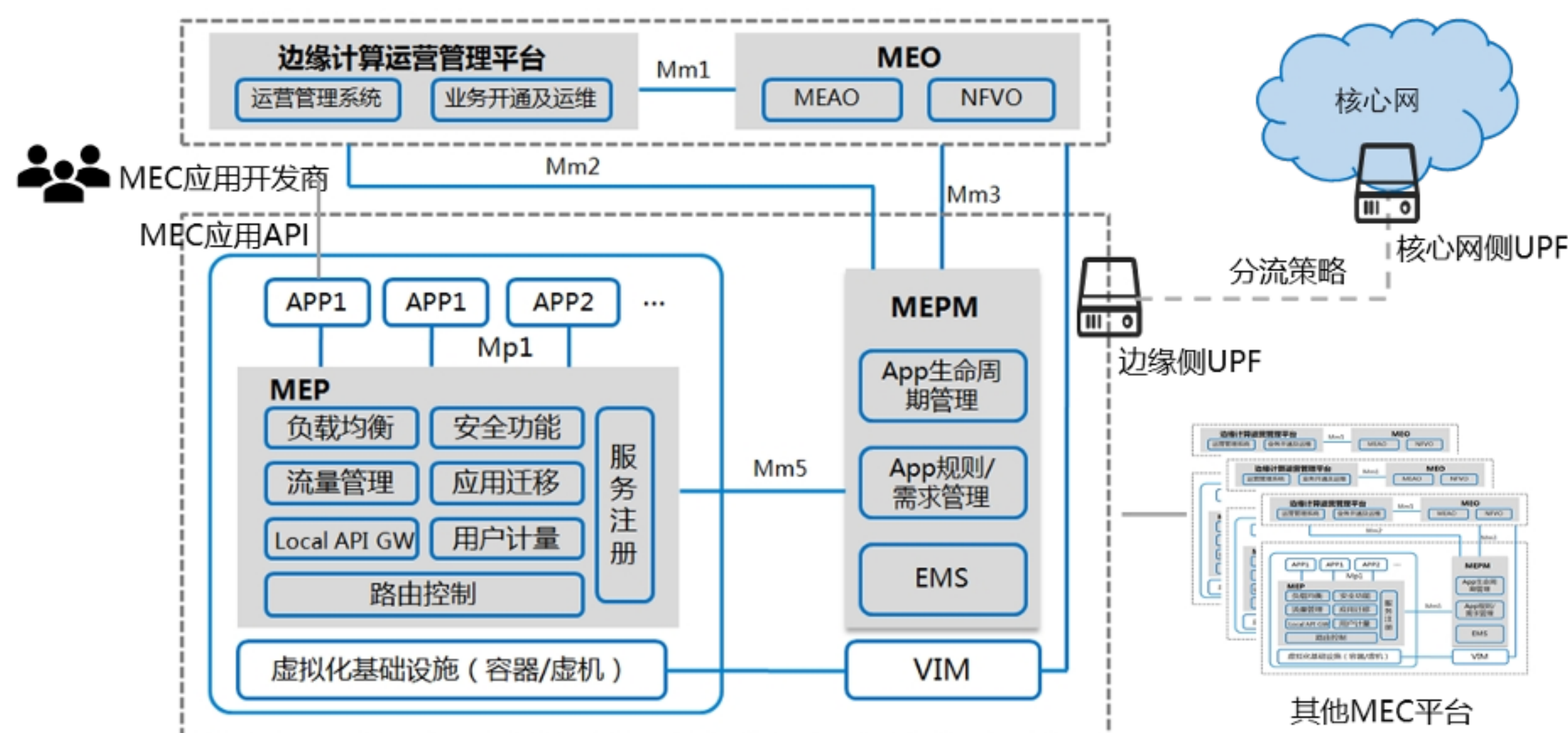


图1 5G 多接入边缘计算平台示意图

从外部看，MEC平台分流DNS策略以及相关基础能力受核心网控制面统一配置管理，并与其他MEC平台间实现横向的互联协作以提升资源利用率、增强用户体验；从内部看，MEC平台由主机和管理功能组成，其中：

- MEC 平台主机包含平台和虚拟化基础设施，以及上面运行的各种 MEC 应用和服务。虚拟化基础设施提供运行 MEC 应用所需的计算、存储、网络资源。平台提供 APP 运行环境和调用 MEC 服务，MEP 本身也可以提供服务，MEP 的功能包括负载均衡、安全功能、流量管理、对移动性的支持、Local API 网关功能、用户计量和能力开放代理等。
- MEC 平台管理功能包含 MEC 系统级管理功能和主机级管理功能。MEC 系统级管理功能包含用户应用生命周期管理代理、运营支撑系统和 MEAO，MEC 主机级管理功能包含平台管理器和虚拟化基础设施管理器。
- MEAO 主要功能包含维护 MEC 系统的整体视图；加载 MEC 应用包、对 MEC 应用包进行完整性检查、检查应用规则和需求的有效性；基于延迟、可用资源、可用服务等约束条件选择合适的 MEC 平台主机实例化边缘计算应用；触发 MEC 应用的实例化、终结、迁移。
- 平台管理器 MEPM 可以管理多个 MEP，可以和主机一起部署在边缘，也可以和系统级网元一起部署在相对集中的位置。MEPM 主要功能包含 MEC 应用的生命周期管理；为平台提供网元管理功能，可以管理多个 MEP；管理 MEC 应用的规则和需求；从虚拟化基础设施管理器接收资源故障报告和性能测量数据。
- 虚拟化基础设施管理器 VIM 主要功能包含分配、管理、释放虚拟化基础设施的虚拟化资源；接收和存储软件镜像；收集、上报虚拟化资源的性能和故障信息。

5G MEC平台的建设、运行等过程中涉及的主体包括：

- 建设部署方**：为用户提供 MEC 服务的主体，包括独立或与第三方合作建设运营 MEC 平台的运营商或厂商、系统集成商、运维合作商等。

——**第三方合作商**：为建设部署方建设、运营边缘计算平台提供服务或基础设施的厂商，包括电信设备制造商，云基础设施提供商、虚拟平台供应商、第三方能力供应商、MEC 应用开发商、服务提供商、内容提供商、安全合作商等。

——**MEC 平台用户**：使用 MEC 服务的行业和个人用户。

在5G MEC平台的安全防护中，各个主体采用责任共担模型，划定责任边界。具体各个主体的责任范围见附录A中表A.1、表A.2、表A.3。

从资产的角度看，5G MEC平台防护范畴涵盖构建5G MEC平台的通用/专用设备、软件、数据、文档和资料、人员、物理环境等，具体见附录B中表B.1。

5.2 5G 多接入边缘计算平台安全风险分析

5.2.1 概述

以5G MEC平台的资产为核心，可从技术脆弱性和管理脆弱性两个方面识别5G MEC平台脆弱性。5G MEC平台的脆弱性分析应包括附录B中表B.2所列范围。表B.3列举出5G多接入边缘计算主要面临的威胁。结合5G MEC平台技术架构和运行模式，平台可能面临的安全风险主要包括应用安全风险、网络安全风险、设备安全风险、数据安全风险、物理环境安全风险和管理安全风险几个方面。

5.2.2 应用安全风险

5G MEC平台通过开发的原生应用或入驻平台的第三方应用，将平台相关基础网络能力、通用安全能力、第三方能力等开放给平台用户，涉及的应用安全风险包括：

- MEC 应用安全隔离风险**：在多个第三方边缘计算应用托管、入驻的情况下，应用与应用、应用与网元，以及多用户应用环境中用户与应用间的隔离不当，可能导致用户访问权限越界、数据丢失和泄露等安全风险。
- 接口开放的风险**：MEC 为边缘计算提供了一个应用承载的平台。为了便于用户开发所需的应用，MEC 需要为用户提供一系列的开放 API，允许用户访问 MEC 相关的数据和功能。这些 API 为应用的开发和部署带来了便利，同时也成为了攻击者的目标。如果缺少有效的认证和鉴权手段，或者 API 的安全性没有得到充分的测试和验证，那么攻击者将有可能通过仿冒终端接入、漏洞攻击、侧信道攻击等手段，达到非法调用 API、非法访问或篡改用户数据等恶意攻击目的。
- 应用级安全配套能力不足**：因没有为入驻平台的 MEC 应用提供恰当的防火墙、IDS/IPS、WAF 等通用安全保障能力，或对应应用、API 等缺乏对应的安全管理、配置和监测能力等，导致无法及时发现、拦截和响应针对应用的非法访问、入侵等安全风险。
- 恶意应用**：因未设置应用资产管理清单、未实施应用安全检测等原因，导致恶意应用入驻平台，进而引发恶意消耗平台资源引发 DDoS 攻击、窃取数据和用户信息、传播或扩散非法内容等安全风险。
- 应用管理编排不当**：因对应应用获取 MEC 能力访问的分级管理、冲突检测、安全部署指南等管理的缺乏，引起应用过度授权或权限滥用，或因应用的调用、编排、协作管理等策略设置不当，导致应用对平台资源的过度消耗或滥用。
- 安全漏洞**：包括 MEC 管理模块、MEC 应用、API 接口等在开发、部署、更新等过程中可能引入的安全漏洞，serverless、service mesh、微服务框架等技术架构安全漏洞，监控工具、调试工具等组件安全漏洞等。利用相关漏洞实施网络攻击以 MEC 应用作为突破口，进而向 MEC 平台核心部分甚至核心网、其他 MEC 平台、接入侧等多向渗透。

5.2.3 网络安全风险

5G MEC平台在组网方面北向与5G核心网连接，接受核心网分流策略、DNS策略等统一配置管理，并与其他MEC平台间实现横向的互联协作。从组网架构、服务提供方式、运营模式等方面看，涉及的网络安全风险包括：

- 设备接入风险**：包括各类边缘设备不安全的通信协议接入、非法设备接入平台。
- 远程管理风险**：主要涉及远程管理控制软件与平台相关功能网元之间的控制传输安全性问题，包括控制传输流量、上报资源状态和业务信息被监听、窃取、篡改等安全风险。
- 网络攻击威胁**：攻击者可通过实施针对 MEC 平台 UPF 网元的欺骗、流量劫持、信息窃取等攻击，Restful 接口攻击等，进而入侵核心网。
- 网络级安全防护措施不当**：因未部署恰当的网络级 IDS、抗 DDoS、防火墙等防攻击手段，或网络告警管理、安全资源管理、安全审计措施等，导致无法及时发现、拦截和响应来自网络层面的非法访问、入侵等安全风险。
- 网络配置缺陷**：包括网络连接配置不当、资源分配配置不当、UPF 的访问控制策略配置不当、多 MEC 平台间管理编排调度不当等配置缺陷引入的安全风险。

5.2.4 设备安全风险

5G MEC平台设备主要包括定制化服务器、通用服务器、网络设备、安全设备等用于搭建平台的实体，负责承载MEC平台核心能力、构建网络连接、提供安全防护能力等，其涉及的安全风险包括：

- 设备配置缺陷**：包括各类设备基线配置不当、设备登录和访问控制策略配置不当、设备资源管理策略配置不当等引发的非法用户登录、非授权攻击等安全问题。
- 设备管理安全**：包括因设备维护的管理通道缺乏双向认证或匹配的加密算法引发的窃听、劫持和篡改攻击，设备安全漏洞更新不及时导致的安全隐患等。
- 设备安全漏洞**：包括设备涉及的硬件漏洞、软件漏洞，以及容器、Kubernetes、数据库开发等第三方组件漏洞等。
- 设备级安全防护措施不当**：因未部署恰当的设备级 IDS、抗 DDoS、防火墙等防攻击手段，导致无法及时发现、拦截和响应针对设备的非法访问、入侵等安全风险。
- 供应链安全风险**：包括因设备整机、关键芯片、核心部件、软件功能等断供引发的供应链完备性问题，以及因设备研发、生产、组装、存储、运输过程引入安全隐患而引发的供应链安全性问题等。

5.2.5 数据安全风险

5G MEC平台可收集、存储、使用或共享与其连接设备的数据，包括应用数据、用户数据等，其涉及的数据安全风险包括：

- 数据损毁风险**：包括因 5G MEC 平台设备毁坏、设备遭受攻击、重要数据未备份、未具备数据容灾备份、数据恢复机制等造成的数据损毁风险。
- 数据篡改风险**：包括因 SQL 注入、XSS 注入等外部攻击入侵造成的数据篡改风险。
- 数据泄露风险**：5G MEC 平台业务开展过程中可获得和处理业务应用数据和用户个人敏感隐私数据，因未实施数据分级分类管理、访问控制，未部署敏感数据加密、脱敏手段，或开展不合规的数据开放共享等，可能导致数据泄露等安全风险。

5.2.6 物理环境安全风险

5G MEC平台部署物理环境可包括地市级、区县级、单位或机构内部机房，以及边缘云、微型数据中心，或现场设备、智能网关等网络设备等，其涉及的物理环境安全风险包括：

- 机房环境安全风险：**包括因 5G MEC 平台机房位置、电力供应、防火、防水、防静电、温湿度控制、机柜安装等设置不合规、缺少必要的监控系统及设备而引发的设备断电、网络断连、平台瘫痪等安全风险。
- 开放环境安全风险：**主要针对部署于现场设备或智能网关等设备上的轻量级 MEC 平台，因物理攻击，以及设备被窃、被盗、被劫持、软硬件被篡改等引发的安全风险。

5.2.7 管理安全风险

5G MEC平台管理安全风险包括涉及平台自身的管理安全风险，以及与其他相关方合作过程中的管理安全风险等，主要包括：

- 平台管理安全风险：**主要涉及因平台安全管理制度缺乏、灾难恢复预案不恰当、安全责任划分制度不明确等引发的平台安全防护措施未落实、安全事件应急恢复不及时等安全风险。
- 第三方管理安全风险：**包括在 MEC 应用上线、升级时缺乏对第三方应用开发商的安全评估和审核，对于多用户的 MEC 应用缺乏区分用户的业务运维和安全管理，设备供应商的安全管理、持续性评估不足等安全隐患。

5.3 5G 多接入边缘计算平台安全防护内容

从5G多接入边缘计算平台的资产和脆弱性分析看，保障MEC应用的安全稳定运行对于平台是否能顺利对外提供MEC服务至关重要，除此之外，保障MEC平台的网络安全、设备安全、数据安全、物理环境安全和管理安全等也是安全防护的主要内容。5G多接入边缘计算平台的安全防护内容具体包括：

a) 应用安全

应用安全包括向用户提供MEC服务的相关MEC应用在设计技术、安全隔离、防攻击、应用备案和版本管理、安全管理和控制等方面的安全要求。

b) 网络安全

网络安全主要包括5G MEC平台内、外部组网架构安全，网络攻击防范和安全审计等方面的安全防护要求。

c) 设备安全

设备安全主要包括5G MEC平台所涉及的网络及安全设备、操作系统、数据库、中间件在身份鉴别、访问控制、安全审计、入侵防范、资源控制等方面的安全防护要求。

d) 数据安全

数据安全主要包括5G MEC平台所涉及的在数据加密、数据存储、敏感数据处理、数据传输、数据共享等方面的安全防护要求。

e) 物理安全

物理安全主要包括5G MEC平台基础设施所处的物理环境在机房位置、电力供应、防火、防水、防静电、温湿度控制、机柜安装、监控等方面的安全防护要求。

f) 管理安全

管理安全主要包括管理制度、人员和技术支持能力、运行维护管理能力、灾难恢复预案等方面的安全防护要求。

5.4 5G 多接入边缘计算平台安全防护要求等级划分

5G多接入边缘计算平台安全防护要求的等级应与根据中华人民共和国工业和信息化部令第11号《通信网络安全防护管理办法》中向电信管理机构备案定级情况确定的安全等级一致。

6 5G 多接入边缘计算平台安全防护要求

6.1 第1级要求

本项要求包括：

- a) 操作系统的安全基线配置应满足 YD/T 2701—2014 的安全要求。
- b) 数据库的安全基线配置应满足 YD/T 2700—2014 的安全要求。
- c) WEB 应用系统的安全基线配置应满足 YD/T 2703—2014 的安全要求。
- d) 中间件的安全基线配置应满足 YD/T 2702—2014 的安全要求。
- e) 网络设备的安全基线配置应满足 YD/T 2698—2014 的安全要求。
- f) 安全设备的安全基线配置应满足 YD/T 2699—2014 的安全要求。
- g) 用户个人电子信息保护应满足 YD/T 2692—2014 的安全要求。
- h) MEC 的原生安全能力应满足 3GPP TS 33.513 的安全要求。

6.2 第2级要求

6.2.1 应用安全要求

6.2.1.1 应用清单管理

本项要求包括：

- a) 应建立并维护 MEC 应用资产清单，包括 MEC 应用名称、服务内容、资源分配、权限分配、应用数量、应用类型、开发者、用户类型、应用状态、应用镜像存储路径等信息管理，其中，应用名称和资源分配应一一对应。
- b) 应具备应用黑白名单功能，能根据白名单控制 MEC 应用的注册、安装、运行等。

6.2.1.2 身份鉴别

本项要求包括：

- a) 应对登录 MEC 应用的用户进行身份标识和鉴别，身份标识具有唯一性，口令等身份鉴别信息应有复杂度要求并定期更换。
- b) 应对 MEC 应用启用登录连接超时自动退出功能，应启用登录失败处理功能，可采取结束会话、限制非法登录次数等措施。
- c) 若 MEC 应用存在初始口令，应强制用户首次登陆时修改初始口令。
- d) 用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全。

6.2.1.3 访问控制

本项要求包括：

- a) 应建立并应用访问控制策略，覆盖 MEC 平台用户与应用、网元与应用、应用与应用等的访问控制规则，对不同的访问行为分配相应的读取、写入等资源访问权限。
- b) 应重命名或删除默认账户，及时删除或停用多余、过期账户，避免共享账户的存在。

6.2.1.4 应用安全部署

本项要求包括：

- a) 应对 MEC 应用开发者、用户等提供 MEC 应用安全部署指南、安全规则公示和主动安全提示等。

- b) 使用第三方 SDK 对 MEC API 进行封装，或集成视频编解码能力、算法库等第三方组件时，应遵循安全安装和配置流程，及时更新第三方组件版本，及时修复安全漏洞，以减少因安装使用第三方组件而引发的安全问题。
- c) 应建立 MEC 应用的注册、激活、去激活、发布、更新、注销等机制，对 MEC 应用进行全流程的管理和控制。
- d) 应对 MEC 应用的注册、加载、更新等过程提供必要的完整性校验和认证鉴权。
- e) 应对 MEC 应用提供日常安全扫描和基线核查等安全机制，在应用上线前，对应用进行代码审计和基线核查，以确保代码未遗留已知高危安全漏洞。
- f) 应对 MEC 应用对 API 的调用等进行安全检测，并对 MEC 应用下线后的 API 调用取消授权。
- g) 应对 MEC 应用提供 WAF、主机安全（如防病毒、EDR 等）等安全防护能力，MEC 用户可以按需选择必要的安全防护能力。

6.2.1.5 攻击防范

本项要求包括：

- a) 应配置 WAF、主机安全（如防病毒、EDR 等）攻击防范机制，对 MEC 应用进行安全隔离和攻击防范。
- b) MEC 应用镜像快照应加密存储于安全路径下，以防止非授权的访问，并进行镜像安全漏洞扫描和病毒扫描、基线核查，对镜像采取完整性保护措施，对镜像快照采取加密保护措施，保证镜像的存储安全、防篡改和传输安全等。
- c) 应对应用容器镜像进行漏洞扫描，发现已知漏洞并及时进行修复。
- d) 应对应用容器实例进行进程监控，对异常进程行为进行告警。

6.2.1.6 安全审计

本项要求包括：

- a) 应提供安全审计功能，并根据运营商和 MEC 平台用户的职责划分，对各自部分的用户行为和安全事件进行审计。其中，运营商负责对应用开放能力（位置服务能力、无线信息能力、QoS 服务能力、安全能力）等的安全审计，MEC 平台用户负责对 MEC 应用的安全审计。
- b) 应确保运营商对 MEC 应用的操作可被 MEC 平台用户审计。
- c) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，并确保审计记录的留存时间符合有关法律法规要求。
- d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等，保证审计数据的真实性和完整性，应保证不同 MEC 应用的审计数据隔离存放，并对审计数据进行定期备份。

6.2.1.7 资源安全管控

本项要求包括：

- a) 应能够对 MEC 应用全生命周期的运行状况进行统一的监控管理，包括 API 状态、并发量、调用成功/失败信息、调用时延、应用调用统计等，并在发现异常时告警。
- b) 应支持对能力 API 调用的优先级、顺序与逻辑进行设置，并具备编排的冲突检测能力。
- c) 应能够对 MEC 应用的存储资源、计算资源、时延、带宽等平台资源使用情况进行限制，对 MEC 应用的资源使用情况进行 QoS 和 SLA 管理。

6.2.2 网络安全要求

6.2.2.1 结构安全

本项要求包括：

- a) 应确保 MEC 平台不承载高于其安全防护等级的业务应用系统。
- b) 应绘制与 MEC 平台运行情况相符的网络拓扑结构图，维护网络设备、虚拟化网络资源、网络配置等资产清单，并能够对网络拓扑结构图和资产清单进行及时更新。
- c) 应根据网元业务属性等划分不同的安全域，控制面网元、管理面网元和数据面网元应划分在不同安全域。安全域之间应采用物理隔离或逻辑隔离（如部署防火墙等）的技术隔离手段。
- d) 应实现不同 MEC 服务客户虚拟网络之间的隔离，确保虚拟机虚拟网络只能接收到目的地址包括自己地址的报文。
- e) 应规划关键节点设备（如 UPF、虚拟化基础设施和硬件基础设施等）的硬件冗余，保障网络和高系统的高可用性。
- f) 对于部署在非电信机房环境的 MEC 平台，应采用集成化、内生的网络安全防护，避免采用外置式网络安全设备，防止安全防护被物理绕过。

6.2.2.2 访问控制

本项要求包括：

- a) 应在网络边界、虚拟化网络边界、安全域之间等根据访问控制策略设置访问控制规则，严格控制 MEC 平台不同网络功能间、MEC 运营管理平台对 MEC 平台等的访问控制。
- b) 应及时对访问控制规则进行更新，删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。
- c) 应确保当 MEC 应用迁移时，访问控制策略随其迁移。
- d) 应允许 MEC 应用服务用户设置不同虚拟机之间的访问控制策略。
- e) 应允许 MEC 应用服务用户设置不同容器（部署和服务）之间的访问控制策略。

6.2.2.3 安全审计

本项要求包括：

- a) 应在网络边界、重要网络节点（如 MEC 平台管理层、MEC 应用 API、UPF、与其他 MEC 平台的通信链路出入口等）进行安全审计，审计范围覆盖到每个用户，对重要的用户行为、资源使用情况、相关安全事件等进行审计。
- b) 审计记录应包括事件的日期和事件、用户、事件类型、事件是否成功及其他与审计相关的信息。
- c) 应对审计记录进行保护，定期备份，避免受到未经授权的删除、修改或覆盖等，审计记录的留存时间应符合相关法律法规要求。
- d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

6.2.2.4 攻击防范

本项要求包括：

- a) 应制定 MEC 平台安全防护方案，部署 IDS 等同类安全检测设备、防火墙等同类访问控制设备。
- b) 应在关键网络节点处监测网络攻击行为，进行恶意代码检测和清除，并维护攻击监测、恶意代码防护等安全机制的升级和更新。
- c) 当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目标、攻击时间等攻击信息。

6.2.2.5 资源安全管控

本项要求包括：

- a) 应具备对平台的资源监控功能，包括网络链路、网络功能、网络设备、计算处理资源、存储资源、安全设备等运行状况监测，MEC 应用资源使用状况监测和流量管理等。
- b) 应提供负载均衡功能，实现 MEC 应用多实例的负载分担，能通过负载均衡等配置，避免资源负载和网络的阻塞。

6.2.2.6 通信安全

本项要求包括：

- a) 应采用校验码技术保证通信过程中的数据完整性，包括相关网络功能上报的资源状态信息、业务信息，核心网下发的配置信息等。
- b) 应对相关外部通信交互的接口进行认证授权，实施完整性和防重放攻击等保护。

6.2.2.7 安全能力开放

本项要求包括：

- a) 应支持将防火墙、入侵检测、抗 DDoS、WAF 等通用安全能力虚拟化、多用户化，以服务的形式向 MEC 应用提供。
- b) 应提供开放接口或开放性安全服务，允许 MEC 平台用户接入第三方安全产品或在平台上选择第三方安全服务。

6.2.3 设备安全要求

6.2.3.1 身份鉴别

本项要求包括：

- a) 应对登录用户进行身份标识和鉴别，身份标识具有唯一性，口令等身份鉴别信息应有复杂度要求并定期更换。
- b) 应启用登录连接超时自动退出功能，应启用登录失败处理功能，可采取结束会话、限制非法登录次数等措施。
- c) 所有登录后才能访问的界面都必须提供主动退出选项，当用户退出时，服务器端必须清除该用户的会话信息。
- d) 必须设置会话超时机制，在超时过后必须要清除该会话信息。
- e) 用户登陆认证通过后必须更换会话标识，以防止会话固定（session fixation）漏洞。
- f) 所有能对系统进行管理的人机接口以及跨信任网络的机机接口都需具备接入认证机制（标准协议定义中无认证机制的除外）。当进行远程管理时，应采取必要的安全措施，保护鉴别信息在网络传输过程中不被窃听。
- g) 系统禁止预留任何的未公开账号，所有账号都必须可被系统管理，并在资料中提供所有账号及管理操作说明。系统禁止存在用户无法修改的口令。

6.2.3.2 访问控制

本项要求包括：

- a) 应对登录的用户分配角色和权限，运行软件程序的账号要尽可能的使用操作系统低权限的账号；使用操作系统的非管理员权限账号来运行数据库；在程序中连接数据库系统的账号不能是数据库系统最高权限的账号。
- b) 应根据管理用户的角色授予其所需的最小权限，实现管理用户的权限分离。
- c) 应重命名或删除默认账户，修改默认账户的默认口令（需要满足口令复杂性的要求）。并及时删除或停用多余的、过期的账户，避免共享账户的存在。

- d) 应采用技术措施，通过设定终端接入方式、网络地址范围等对合法访问平台的终端进行限制。
- e) 应保证当发生虚拟设备迁移时，访问控制策略随之迁移。
- f) 应确保只有在 MEC 应用用户授权下，MEC 平台或第三方才具有 MEC 用户数据的管理权限。
- g) 包含敏感信息的文件（包括程序运行时产生的静态文件和临时文件）必须要有权限控制，只能被相应权限的用户访问。
- h) 资产的通信矩阵必须清楚地记录其正确操作所需的所有接口、服务、端口（源和目的地）和协议，包括任何可选的接口、服务、端口和协议，并明确服务与所需的网络接口、IP 地址和端口的对应关系。

6.2.3.3 攻击防范

本项要求包括：

- a) 应遵循最小安装的原则（安全软件除外），仅安装需要的组件和应用程序，并保持系统补丁及时得到更新。
- b) 应关闭不需要的系统服务、默认共享和不必要的开放端口。
- c) 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。
- d) 应部署防恶意代码软件、入侵检测系统等恰当的防攻击手段，并定期进行软件版本升级和恶意代码库更新。
- e) 应遵循电信网和互联网安全防护基线配置相关要求，对网络设备、安全设备、数据库、操作系统等设备进行基线安全配置。
- f) 应部署板卡、内存等相关硬件校验措施，防止插入恶意板卡读取内存信息、硬件被刷新恶意系统镜像等硬件篡改攻击。
- g) 设备应支持对敏感数据如口令、密码的加密存储，加密密钥支持分层密钥管理；支持证书管理（证书替换更新，证书过期前告警）；支持数字签名检查安装包、补丁包、升级包的完整性；认证凭据不需要还原的场景（例如认证服务端保存的用户登录口令），必须使用 PBKDF2 等单向 Hash 算法进行加密，而不是以明文或可逆加密的方式存储实际口令。
- h) UPF 应提供以下安全能力：具备上下行流量防地址欺骗检查及告警能力，若报文的源地址不是终端用户地址或目的地址与手机地址池不匹配，设备需丢弃该报文，并禁止将该报文转发出去；对没有匹配 PDP 上下文/承载的下行流量执行丢弃及告警；具备针对 GTP 协议恶意报文攻击的防御能力；具备 GTP 解封后的流量只流向内部数据网络的能力；支持 ACL 过滤功能；支持 L2TP 隧道、IPSec 隧道、安全启动技术等灵活的终端互访策略。

6.2.3.4 安全审计

本项要求包括：

- a) 应启用安全审计功能，审计范围覆盖设备上的每个用户。
- b) 审计内容应覆盖重要用户行为、系统资源的异常使用、重要系统命令的使用和重要安全事件。
- c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。
- d) 审计记录应按有关法律法规要求进行超过一定期限的留存，定期备份并采取安全保护措施，避免在有效期内受到非授权的访问、篡改、覆盖或删除等。
- e) 应支持按用户需求提供与其相关的审计信息及审计报告。
- f) 应确保对 MEC 平台用户应用、系统和数据等操作可被 MEC 平台用户审计。

6.2.3.5 资源安全管控

本项要求包括：

- a) 应限制单个用户或进程对系统资源的最大使用限度。
- b) 应能够屏蔽虚拟资源故障，确保某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机运行。
- c) 应保证虚拟机仅能使用为其分配的计算资源。

6.2.4 数据安全要求

6.2.4.1 数据保护

本项要求包括：

- a) 应保证重要数据在传输、虚拟机迁移等过程中的完整性，并在发现到完整性受到破坏时采取必要的恢复措施。
- b) 应采取技术措施保护业务相关数据安全，避免相关数据被泄露、篡改和破坏。
- c) 应具备数据加密存储、数据加密传输模块，采用加密等安全方式存储和传输用户口令等身份鉴别信息，防止用户鉴别认证信息泄露而造成身份冒用。
- d) 应对重要、敏感数据行分级分类处理，相关要求参考 2019-0216T-YD《基础电信企业数据分类分级方法》中的相关要求。
- e) 针对应用数据，应采取技术措施保证应用之间的数据隔离。

6.2.4.2 数据备份恢复

本项要求包括：

- a) MEC 平台建设部署方和用户应提供相应的重要业务及应用数据的本地数据备份与恢复功能，提供异地备份功能，可通过安全的通信网络将重要数据备份到异地。
- b) 应支持数据备份与恢复的云边协同配置，包括备份策略、备份数据一致性检验、备份位置查询等。

6.2.4.3 个人信息保护

本项要求包括：

- a) 应仅采集和保存业务必需的用户个人信息。
- b) 应禁止未经授权访问和非法使用用户个人信息。

6.2.4.4 剩余信息保护

本项要求包括：

- a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
- b) 应保证虚拟机所使用的内存和存储空间在回收时得到完全清除。
- c) MEC 平台用户删除业务应用数据时，MEC 平台应确保该业务应用数据的所有副本得到完全清除。

6.2.5 物理环境安全要求

本项要求包括：

- a) 应确保 MEC 平台基础设施位于中国境内。
- b) 对于部署在机房环境的 MEC 平台，在机房位置、电力供应、防火、防水、防静电、温湿度控制、机柜安装、监控、人员进出等方面应满足 YD/T 1754-2008《电信和互联网物理环境安全等级保护要求》中的第 2 级要求。
- c) 企业规范标准、企业具体操作维护规范等文档对相关物理环境安全有重复要求时，应采取从严原则，遵循更严格的安全要求。

- d) 对于部署在非机房环境的 MEC 平台，应采取相应措施防范近端攻击，包括：应将设备或主要部件进行固定，并设置明显的不易除去的标记；应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。

6.2.6 管理安全要求

6.2.6.1 安全管理制度

本项要求包括：

- a) 应建立覆盖 MEC 平台安全管理活动中各类管理内容的安全管理制度，包括安全开发管理、机构设置和人员管理、运行维护管理、供应链管理、教育培训等，管理制度符合企业安全工作总体方针和安全策略。
- b) 应指定或授权专门的部门或人员负责安全管理制度的制定，通过正式、有效的方式发布安全管理制度，并进行版本控制和及时修订。
- c) 应对技术人员、安全管理人员、开发人员等执行的日常操作建立操作规程，对账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定。
- d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。
- e) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。
- f) 确保供应商的选择符合国家有关规定。

6.2.6.2 机构和人员

本项要求包括：

- a) 应设立安全管理工作的专门部门，指定专人承担系统管理员、网络管理员、安全管理员等岗位职责。
- b) 应建立相关方联系列表，包括 MEC 应用开发者、第三方服务提供商等外联单位名称、合作内容、联系人和联系方式等。
- c) 应指定或授权专门的部门或人员负责人员录用，对被录用人员的身份、背景、专业资格和资质等进行充分的审查。
- d) 应及时终止离岗员工的所有访问权限，并回收各类登录凭证、身份证件、标识卡、钥匙等软硬件访问凭据。
- e) 应定期对各类人员进行安全意识教育和安全知识培训，充分告知相关安全责任和惩戒措施，安全运维人员需进行上岗前培训。

6.2.6.3 安全运行

本项要求包括：

- a) 应在平台建设、业务开发等方案中明确网络安全保障具体措施，在新建、改建、扩建平台或引入新业务时，确保网络安全保障措施同步规划、同步验收、同步运行。
- b) 应确保开发环境与实际运行环境物理分离，测试数据和测试结果受到控制。
- c) 应确保在软件、系统等开发过程中，平台上线前对安全性进行充分测试，并出具安全测试报告，以在软硬件组件等安装前检测可能存在的恶意代码、安全漏洞等。
- d) 应定期进行常规安全检查，包括平台日常运行、数据备份等情况。
- e) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

- f) 对各类设备、线路等指定专门的部门或人员定期进行维护管理，并详细记录日常巡检工作、运行维护记录、参数设置和修改等运维操作日志。

6.2.6.4 安全评估

本项要求包括：

- a) 应定期进行安全风险评估（至少每两年一次），采取必要的措施识别安全漏洞和隐患，风险评估范围应与安全防护范围一致，并根据评估结果制定相应的风险处理计划，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
- b) 应对上线、升级的第三方应用开展安全评估，包括第三方应用的安全漏洞、安全隐患情况，第三方应用申请使用平台资源情况与业务匹配度等，对第三方应用自身的安全评估结果进行充分的审核。

6.2.6.5 应急和处置

本项要求包括：

- a) 应按照 YD/T 1731-2008 的相关要求，根据物理安全事件、网络安全事件、设备安全事件、数据安全事件、管理安全事件、应用安全事件、平台或系统漏洞事件等不同类别安全事件属性，制定针对性的应急预案，并定期组织应急预案的教育培训（至少每半年一次）和演练（至少每年一次）。
- b) 应根据与用户签订的 SLA 协议或合同等提供安全事件预警提示、安全响应等服务。
- c) 应维护安全事件的分类、分级报告和响应处置流程，及时报告所发现的安全弱点和可疑事件，分析鉴定事件产生原因，采取恢复措施。

6.2.6.6 供应链安全管理

本项要求包括：

- a) 应按照 GB/T 36637-2018 的相关要求部署供应链安全风险控制措施，包括供应链相关人员管理、供应链生命周期管理，以及采购外包与供应商管理。
- b) 网络设备、安全产品、密码产品等相关产品与服务的采购和使用应符合国家对于供应链安全及国产化的有关规定。
- c) 应对供应商的安全保障能力、安全管理制度、持续性供货保障等情况进行综合评估，避免使用单一供货商的情况。
- d) 应与选定的供应商签订相关协议，明确供应链各方需履行的安全责任和义务。
- e) 应确保供应链安全事件信息或威胁信息能够及时传达到 MEC 平台用户。
- f) 应采用符合国家密码管理局要求的进行加密保护、安全认证的技术、产品和服务。

6.2.6.7 文档安全管理

本项要求包括：

应设立文档安全管理制度，根据文档的属性进行安全分级，并针对不同的文档采用不同的安全防护措施。

6.3 第 3 级要求

6.3.1 应用安全要求

6.3.1.1 应用清单管理

除满足第2级要求外，还应满足：

- a) 应建立安全态势感知系统，实现资产信息的可视化管理，为安全运维提供基础信息。
- b) 应根据 MEC 应用类型、能力开放程度等，对 MEC 应用资产清单进行分类分级管理。

6.3.1.2 身份鉴别

除满足第2级要求外，还应满足：

应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术来进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

6.3.1.3 访问控制

除满足第2级要求外，还应满足：

- a) 账户授权应遵循最小权限原则，避免过度授权和权限滥用。
- b) 访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级。
- c) 应控制主体对敏感信息资源的访问权限。

6.3.1.4 应用安全部署

除满足第2级要求外，还应满足：

应支持对 MEC 应用实例化的远程完整性校验。

6.3.1.5 攻击防范

除满足第2级要求外，还应满足：

应提供虚拟机逃逸攻击的检测机制，防止虚拟机对云平台的入侵攻击，防止 VM 获取云平台的控制权。

6.3.1.6 安全审计

除满足第2级要求外，还应满足：

- a) 应对审计进程进行保护，防止未经授权的中断。
- b) 应提供集中的安全管理平台，对收集的 MEC 各种运维日志、安全日志、安全产品告警信息，进行自动化的威胁检测，对多种异常操作、入侵行为等进行实时的检测和告警。

6.3.1.7 资源安全管控

同第2级要求。

6.3.2 网络安全要求

6.3.2.1 结构安全

除满足第2级要求外，还应满足：

- a) 应能够对网络拓扑结构图和资产清单进行实时更新。
- b) 应通过建立访问控制列表、划分安全域等方式，对 MEC 平台本身标识的正确识别和寻址进行保护。
- c) 应具有根据 MEC 平台用户业务需求自主设置安全策略集的能力，包括定义访问路径、选择安全组件、配置安全策略。
- d) 应保证 MEC 平台管理流量与用户业务流量分离。
- e) 应能识别、监测虚拟机之间、虚拟机与物理机之间的流量，发现异常流量应告警。

- f) 保证网络设备处理能力和带宽满足业务高峰期需求，并提供通信线路、关键网络设备、关键计算设备的硬件冗余。

6.3.2.2 访问控制

除满足第2级要求外，还应满足：
应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

6.3.2.3 安全审计

除满足第2级要求外，还应满足：

- a) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
- b) 应对 MEC 平台自身控制相关日志（包括网络资源管理信息、网络配置管理信息、网络性能管理信息、网络告警管理信息、运维管理信息等）进行及时备份，并提供异地实时备份功能。

6.3.2.4 攻击防范

除满足第2级要求外，还应满足：

- a) 应在关键网络节点处对从外部、内部发起的网络攻击行为进行监测和阻断，并根据攻击事件严重程度提供告警。
- b) 应制定 MEC 平台安全防护方案，部署 NTA 等流量监测分析、基于全流量的威胁分析溯源取证软件、平台或解决方案等。
- c) 应部署抗击多种攻击的安全防御能力，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。
- d) 应部署防止以 MEC 平台为跳板攻击 5G 核心网的安全隔离和流量监测能力。

6.3.2.5 资源安全管控

除满足第2级要求外，还应满足：

- a) 应能够对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。
- b) 应能够根据运行状况、资源使用状况等监控结果，对相关安全状况进行统一分析，并根据分析结果对可能发生的安全事件进行告警。

6.3.2.6 通信安全

除满足第2级要求外，还应满足：

- a) 应采用校验码技术或密码技术保证通信过程中的数据完整性，采用密码技术保障通信中敏感信息字段或整个报文的保密性，包括相关网络功能上报的资源状态信息、业务信息，核心网下发的配置信息等。
- b) 应建立安全的控制传输通道，进行远程管理控制软件与网络功能间、核心网与 UPF 间、多个 MEC 平台间互联协作等通信，防止会话 ID 或 Token 等登录凭据被窃听，防范利用 MEC 控制通道的 MITM、DoS 等攻击。

6.3.2.7 安全能力开放

除满足第2级要求外，还应满足：
应支持在安全服务的统一控制下，对 MEC 平台安全能力进行按需的定制化配置和编排。

6.3.3 设备安全要求

6.3.3.1 身份鉴别

除满足第2级要求外，还应满足：

- a) 登录设备需要区分运营商和用户的不同管理通道，运营商设备需通过网管 EMS 系统进行登录管理。用户的设备登录时，需要通过堡垒机的等具备操作审计能力的系统进行接入。
- b) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术来进行身份鉴别。
- c) 应具备防范暴力破解等攻击的能力。
- d) 当远程管理相关设备时，对于设备和管理系统间的通信连接应采用数字证书进行双向身份验证，并能定期监控证书生命周期。

6.3.3.2 访问控制

除满足第2级要求外，还应满足：

- a) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。
- b) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。
- c) 应控制主体对敏感信息资源的访问权限。
- d) 应建立管理用户权限分离机制，为网络管理员、系统管理员、安全管理员等建立不同账户并分配相应的权限。

6.3.3.3 攻击防范

除满足第2级要求外，还应满足：

- a) 应具备主机入侵检测能力，检测针对主机的入侵行为，如进程异常、网络连接、文件读取等异常行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生入侵行为的严重程度提供告警。
- b) 应采取恶意代码防范、入侵防范、可信验证机制等技术措施对系统程序、应用程序和重要配置文件、配置参数等进行安全保护和可信执行验证，在检测到完整性受到破坏时采取恢复措施。
- c) 应能检测虚拟机之间的资源隔离失效、非授权虚拟资源使用行为、恶意代码在虚拟机间蔓延情况等，并及时告警。

6.3.3.4 安全审计

除满足第2级要求外，还应满足：

- a) 应对审计进程进行保护，防止未经授权或非预期的中断。
- b) 应能够根据记录数据进行安全状况分析，生成审计报表。
- c) 应能汇聚服务范围内的审计数据，并支持第三方审计。

6.3.3.5 资源安全管控

除满足第2级要求外，还应满足：

- a) 应建立物理资源和虚拟资源的管理机制，对相关资源实施统一管理调度与分配，包括资源管理、配置管理、性能管理和告警管理等。
- b) 应对关键设备的资源使用情况进行监测，包括 CPU、硬盘、内存等资源使用情况，并在相关资源使用情况超过一定水平，或导致关键设备的服务水平降低到一定程度时进行告警。

6.3.4 数据安全要求

6.3.4.1 数据保护

除满足第2级要求外，还应满足：

- a) 应采用校验技术或密码技术保证重要数据在传输、存储、虚拟机迁移等过程中的完整性和保密性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等。
- b) 应支持 MEC 平台用户部署密钥管理解决方案，支持 MEC 平台用户自行实现数据的加解密过程。
- c) 应根据业务需求，做好应用迁移或弹性扩缩过程中的数据保护，虚拟机的移动性应限制在特定的安全集群内，安全集群应能与虚拟系统安全架构的安全域相对应。
- d) 对于设备存储的重要敏感数据、信息，应进行加密存储保护，并采取保护措施对密钥进行保护。

6.3.4.2 数据备份恢复

除满足第2级要求外，还应满足：

- a) 应提供异地实时备份功能，可通过通信网络将重要数据实时备份到异地。
- b) 应为 MEC 平台用户将应用、业务系统和数据迁移到其他 MEC 平台和本地系统提供技术手段，并协助完成迁移过程。
- c) 应确保 MEC 平台用户数据存在若干可用的副本，各副本之间的内容应同步且保持一致。

6.3.4.3 个人信息保护

除满足第2级要求外，还应满足：

- a) 在开放网络能力过程中，仅开放必需的用户个人信息，对可能涉及的用户位置数据、行为偏好数据等用户个人信息应根据业务需求进行必要的脱敏。
- b) 在业务提供、控制与管理过程应保护用户隐私，未经用户同意，不能擅自收集、修改、泄露、共享用户相关敏感数据。

6.3.4.4 剩余信息保护

除满足第2级要求外，还应满足：

- a) 应保证敏感数据所在的存储空间被释放或重新分配前得到完全清除。
- b) 应确保在 MEC 平台计算迁移、数据迁移等场景下，残留在硬盘、内存、缓存等中的数据得到完全清除。

6.3.5 物理环境安全要求

本项要求包括：

- a) 部署于机房环境的 MEC 平台，在机房位置、电力供应、防火、防水、防静电、温湿度控制、机柜安装、监控等方面应满足 YD/T 1754-2008《电信和互联网物理环境安全等级保护要求》中的第 3.1 级和第 3.2 级要求。
- b) 应避免设在有窗户机房内，并配置强无线屏蔽技术手段。

6.3.6 管理安全要求

6.3.6.1 安全管理制度

除满足第2级要求外，还应满足：

- a) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
- b) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
- c) 应具备与第三方应用、第三方能力提供商的安全协作管理和安全责任划分策略。

6.3.6.2 机构和人员

除满足第2级要求外，还应满足：

- a) 应配备专职的安全管理员，不可兼任。
- b) 应针对不同岗位制定不同的培训计划，并定期对人员进行安全技能考核。

6.3.6.3 安全运行

除满足第2级要求外，还应满足：

- a) 应确保对当前发布的应用版本的修改、更新、发布进行授权和批注，并严格进行版本控制。
- b) 安全测试报告应包含密码应用安全性测试相关内容，包括“密码算法使用是否符合国家相关标准”等。
- c) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，并形成安全检查报告。
- d) 对于平台、第三方应用运维过程中可能引入的监控、调试等运维工具，应严格控制运维工具的使用、远程运维的开通，经审批后方可接入操作，在操作过程中因保留不可更改的操作日志，操作结束后应立即关闭接口或通道，删除相关工具中的敏感数据。
- e) 对于区县级或更低接入位置的无人值守的远程运维情况，应充分评估合作运维第三方的业务合作模式、服务模式合规性，合作企业资质等，可通过查看合作单位文档、人员访谈等方式，评估合作企业的网络安全保障能力（包括管理制度和技术手段）。

6.3.6.4 安全评估

除满足第2级要求外，还应满足：

- a) 定期对各类设备、系统进行安全风险评估（至少每年一次），形成安全评估报告，采取措施应对发现的安全问题。
- b) 应支持为用户提供安全评估结果等证明信息。

6.3.6.5 应急和处置

除满足第2级要求外，还应满足：

- a) 应规定统一的应急预案框架，定期组织所属各类平台、设备、系统灾难恢复预案的教育培训（至少每季度一次）和演练（至少每半年一次）。
- b) 应定期对原有应急预案进行重新评估和修订完善。

6.3.6.6 供应链安全管理

除满足第2级要求外，还应满足：

- a) 应定期监视、评审和审核供应商提供的服务，并对其变更服务内容加以控制。
- b) 应保证供应商的重要变更及时传达到 MEC 平台用户，并评估变更带来的安全风险，采取有关措施对风险进行控制。

6.3.6.7 文档安全管理

同第2级要求。

6.4 第4级要求

同第3级要求。

6.5 第5级要求

待补充。

行业标准信息平台

附录 A

(规范性)

5G 多接入边缘计算平台各个主体的责任范围

本附录指导5G多接入边缘计算平台的安全防护中，各个主体应承担的责任范围。

其中：建设部署方责任范围如表A.1所示。

表A.1 建设部署方责任范围

层面	安全要求	相关组件
物理环境安全	物理位置选择，以及部署所在的机房环境和开放环境安全防护	MEC平台物理设施
网络安全	网络结构、访问控制、远程访问、入侵防范、安全审计	物理网络及附属设备、虚拟网络管理平台、虚拟网络安全域
应用和数据安全	应用安全性验证和评估、API接口安全、安全审计、应用使用平台资源情况监控、应用间安全隔离、数据完整性、数据保密性、数据备份恢复	管理平台、应用系统及相关软件组件
设备安全	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、供应链安全风险防护	物理网络及附属设备、虚拟网络管理平台、物理宿主机及附属设备、虚拟机管理平台、镜像、虚拟机、虚拟网络设备、虚拟安全设备，以及设备运输过程等
管理安全	平台安全管理制度、灾难恢复预案	MEC平台
	对第三方应用开发商的安全评估和审核、多用户MEC应用区分用户的业务运维和安全管理、设备供应商的安全管理	第三方应用开发商、多用户MEC应用、设备供应商

第三方合作商责任范围如表A.2所示。

表A.2 第三方合作商责任范围

层面	安全要求	相关组件
设备安全	恶意代码防范、供应链安全风险防护	物理网络及附属设备、虚拟网络管理平台、物理宿主机及附属设备、虚拟机管理平台、镜像、虚拟机、虚拟网络设备、虚拟安全设备的关键芯片、核心部件、软件功能，以及设备研发、生产、组装、运输过程等
应用和数据安全	消除安全漏洞风险隐患、API接口安全、对平台和用户数据的使	MEC应用、API接口、serverless、service mesh、微服务框架、监控工具、调试工具等组件

层面	安全要求	相关组件
	用、传输、存储、共享等进行授权管理和安全保护	
安全功能、产品、解决方案	依据建设部署方委托要求，为平台提供相应安全功能、产品、解决方案等	物理环境安全、网络安全、应用和数据安全、设备安全、管理安全等

MEC平台用户责任范围如表A.3所示。

表A. 3 MEC 平台用户责任范围

层面	安全要求	相关组件
应用安全	应用清单管理、身份鉴别、访问控制、应用安全部署、攻击防范、安全审计	用户使用的对应虚拟机、应用系统及相关软件组件
数据安全	安全审计、资源控制、数据完整性、数据保密性、数据备份恢复	MEC平台服务用户应用系统配置、MEC平台服务用户业务相关数据等
管理安全	MEC平台建设部署方选择及测试验收、安全管理机构、安全管理制度及管理人员配置等	MEC平台建设部署方、管理流程、人员等

行业标准信息服务平台

附录 B
(资料性)

5G 多接入边缘计算平台风险分析

本附录指导5G多接入边缘计算平台风险分析过程中的资产、威胁、脆弱性分析。

5G多接入边缘计算平台的资产应至少包括：通用/专用设备、软件、数据、文档和资料、人员、物理环境，如表B.1所示。

表B.1 资产列表

类别	主要资产
通用/专用设备	包括定制化服务器（OTII等）、通用服务器等服务器设备，MEC智能网关（CPE等）、交换机、路由器、负载均衡等基础网络设备，入侵防范、安全防护等安全设备（安全过滤、入侵检测和防护设备），物理通信链路、硬件加速卡等
软件	包括虚拟化网络功能、封装的边缘计算能力、边缘应用、数据库软件、第三方SDK组件、监控工具、调试工具、管理控制软件等
数据	用户数据、网络信息、平台运行数据、运维管理信息等
文档和资料	纸质以及保存在存储介质中的各种文件资料（如，设计文档、技术要求、管理规定、工作计划、技术报告、用户手册等）
人员	相关管理、维护、开发人员等
物理环境	平台相关系统和设备所处的物理环境，机房、电力、防火、防水、防静电、温湿度控制等相关设施

表B.2列举出5G多接入边缘计算平台主要的脆弱性识别内容。其中，技术脆弱性包括设备配置错误、应用和协议安全漏洞、非授权访问、虚拟化环境隔离不规范、数据丢失和泄露、网络攻击威胁等；管理脆弱性包括管理制度不完善、供应链安全管理不规范等。

表B.2 脆弱性分析表

类别	对象	主要脆弱性
技术脆弱性	通用/专用设备	设备存在配置错误、基线配置不合规； 设备硬件隐患或质量问题，相关设备超过使用年限或核心部件老化； 相关设备的操作系统存在安全隐患，设备防攻击手段部署不足； 相关设备密码设置不合理、复杂度不够或没有经常更新； 设备重要部件未进行合理备份； 设备缺乏安全漏洞自动或手动更新机制； 相关设备发生故障后未及时告警；
	软件	相关应用、协议等存在漏洞、后门； 缺乏对应用的病毒扫描、资产清单管理、安全评估等； 相关功能网元配置不合理，平台管理策略配置不合理，访问控制策略设置不合理，虚拟化环境隔离不规范等； 相关应用日志功能没有启用或不够详细； 网络和系统规划、设备部署、链路部署、资源配置、业务保护和恢复能力、安全技术措施和策略等方面的设计缺陷；
	数据	数据未进行分级分类处理、重要数据未及时进行备份、敏感数据未加密或脱敏、数据开放共享不合规等；

类别	对象	主要脆弱性
	物理环境	机房场地选择不合理； 防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范； 通信线路、相关服务器、主机等设备的保护不符合规范；
	管理脆弱性	安全管理机构方面：安全管理人员、运维管理人员等配置过少、职责不清，授权和审批程序简化、沟通和合作未执行、审核和检查未执行等； 安全管理制度方面：内部安全管理制度不完善、风险管理制度评审和修订不及时、缺乏软件升级或补丁更新管理机制、缺乏标准化实施程序、安全管理文档资料不完备等； 人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续、人员未进行安全培训、对于第三方人员未进行限制访问等； 建设管理方面：安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等； 运维管理方面：物理环境管理措施简单、存储介质使用不受限、设备没有定期维护、厂家支持力度不够、关键性能指标没有定期监控、无恶意代码防范措施、无数据备份和恢复策略、访问控制不严格、操作管理不规范等，应急保障措施不到位，灾难恢复预案不完善； 供应链管理方面：供应商安全开发能力评估不到位、供应商设备安全审查不规范、采购流程缺乏安全规范、供应链可持续性评估不合格等。

5G多接入边缘计算平台威胁可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其它物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。表B.3列举出5G多接入边缘计算主要面临的威胁。

表B.3 威胁来源列表

类别	主要威胁
技术威胁	相关主机和服务、及系统网络设备使用时间过长或质量问题等导致硬件故障； 系统链路发生故障； 相关设备的操作系统软件、应用软件运行故障； 相关设备数据丢失或系统运行中断； 存储介质老化或质量问题等导致不可用；
环境威胁	断电、静电、灰尘、潮湿、温湿度异常、电磁干扰等； 意外事故或通讯线路方面的故障；

类别		主要威胁
	自然灾害	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷击；
人为威胁	恶意人员	不满的或有预谋的内部人员滥用权限进行恶意破坏； 攻击者利用非法手段进入机房内部盗窃、破坏等，攻击者非法物理访问相关设备、存储介质等； 攻击者利用网络协议、操作系统、应用系统漏洞，越权访问相关设备的文件、数据或其他资源； 攻击者利用各种工具获取相关设备身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问应用系统，或非法使用相关文件和数据； 攻击者利用应用系统扩散病毒、蠕虫、木马、垃圾电子邮件，利用相关攻击工具恶意消耗应用系统资源，导致系统能力下降或瘫痪、无法正常提供应用服务； 攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失；
	非恶意人员	内部人员由于缺乏责任心或者无作为而应该执行而没有执行相应的操作、或无意地执行了错误或危险的操作导致安全事件； 内部人员没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致故障或攻击； 安全管理制度不完善、落实不到位造成安全管理不规范或者管理混乱导致安全事件。

行业标准信息平台