



# 中华人民共和国国家标准

GB/T 35281—2017

---

## 信息安全技术 移动互联网 应用服务器安全技术要求

Information security technology—  
Security technique requirements for application servers in mobile internet

2017-12-29 发布

2018-07-01 实施

---

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会 发布

# 目 次

前言 .....	I
引言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义、缩略语 .....	1
4 资产分类 .....	2
4.1 设备资产 .....	2
4.2 系统资产 .....	2
4.3 业务资产 .....	2
4.4 用户数据资产 .....	2
5 安全框架 .....	3
6 数据安全 .....	3
6.1 数据自身安全 .....	3
6.2 数据防护安全 .....	3
7 业务安全 .....	4
7.1 业务安全构成 .....	4
7.2 一般业务安全 .....	4
7.3 特定业务安全 .....	4
8 系统安全 .....	5
8.1 操作系统安全 .....	5
8.2 中间件安全 .....	5
8.3 数据库安全 .....	6
9 设备安全 .....	6
10 协议安全 .....	6
10.1 标准协议安全 .....	6
10.2 私有协议安全 .....	6
11 运维安全 .....	6
11.1 安全配置 .....	6
11.2 安全监控 .....	6
11.3 安全审计 .....	7
11.4 恶意代码防护 .....	7
11.5 备份与故障恢复 .....	7
附录 A (资料性附录) 安全风险分析 .....	8
参考文献 .....	10

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国信息通信研究院、浙江蚂蚁小微金融服务集团股份有限公司、中国移动通信集团公司、中国电信股份有限公司广东研究院、北京邮电大学。

本标准主要起草人:潘娟、宁华、陈泓汲、刘陶、翟世俊、落红卫、张滨、金华敏、徐国爱、邱勤。

## 引 言

移动互联网应用服务器承载着各类移动应用业务,涉及众多有价值的敏感信息资源,因此易成为被攻击的目标。随着移动互联网应用对在线服务的依赖程度逐渐加深,应用服务器的重要程度也与日俱增,如果其中存在安全问题,轻则致使大量用户无法正常使用移动互联网应用提供的各类业务,重则可能导致用户信息遭到大规模泄露等安全风险。

本标准主要针对移动互联网应用服务器提出安全技术要求,通过规范应用服务器安全实现和运维,强化服务器端技术和管理安全水平,完善整个移动互联网的安全架构,确保用户权益不受损害,维护产业有序健康发展。

# 信息安全技术 移动互联网 应用服务器安全技术要求

## 1 范围

本标准规定了移动互联网应用服务器的安全技术要求,包括数据安全、业务安全、系统安全、设备安全、协议安全和运维安全等。

本标准适用于支持承载各类移动互联网应用业务的计算机系统,可用于指导移动互联网应用服务器开发、部署、管理运维和测试评估,也适用于相关产品的测试和服务等。

## 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 20271—2006 信息安全技术 信息系统通用安全技术要求  
GB/T 20272—2006 信息安全技术 操作系统安全技术要求  
GB/T 21028—2007 信息安全技术 服务器安全技术要求  
GB/T 25069—2010 信息安全技术 术语  
GB/T 31168—2014 信息安全技术 云计算服务安全能力要求  
JR/T 0095—2012 中国金融移动支付 应用安全规范

## 3 术语和定义、缩略语

### 3.1 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

#### 3.1.1

##### **移动互联网 mobile internet**

用户使用移动终端(包括手机、上网本、平板电脑、智能本等)通过移动网络获取移动通信网络服务和互联网服务的开放式基础电信网络。

#### 3.1.2

##### **移动互联网应用服务器 mobile internet application servers**

为移动终端提供移动互联网服务的计算机系统,由支撑系统(如硬件、操作系统、中间件、数据库管理系统、WEB服务等)和业务应用系统组成。

#### 3.1.3

##### **移动智能终端 mobile smart terminal**

能够接入移动通信网,具有能够提供应用程序开发接口的开放操作系统,并能够安装和运行应用程序的移动终端。

### 3.2 缩略语

下列缩略语适用于本文件。