



中华人民共和国公共安全行业标准

GA/T 1538—2018

信息安全技术 企业移动终端安全管理产品 测评准则

Information security technology Testing and evaluation criteria for enterprise mobile
terminal security management products

2018 - 12 - 27 发布

2018 - 12 - 27 实施

中华人民共和国公安部 发布

目 次

前言	II
引言	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	1
5 受检要求	2
5.1 检验周期	2
5.2 测试用例要求	2
5.3 资料要求	2
6 功能要求	2
6.1 自服务式部署功能	2
6.2 安全接入功能	2
6.3 策略管理功能	2
6.4 审计功能	3
6.5 远程定位功能	3
6.6 远程数据备份功能	3
6.7 产品自身安全	3
7 测试方法	3
8 报告格式	3
9 评级方法	4

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：国家计算机病毒应急处理中心、公安部十一局七处、天津市公安局网络安全保卫总队、恒安嘉新（北京）科技股份有限公司、迈克菲（上海）软件有限公司、北京启明星辰信息安全技术有限公司、北京天融信科技有限公司。

本标准主要起草人：陈建民、黄一斌、祝国邦、陆磊、曹鹏、袁江涛、张雷生、张鑫、李冬、孟彬、李菊、舒心、孙波、崔婷婷、徐雨晴、王龔。

引 言

本标准详细描述了与企业移动终端安全管理产品相关的受检要求、功能要求、测试方法、报告格式及评级方法。

本标准仅给出了企业移动终端安全管理产品应满足的功能要求,但对企业移动终端安全管理产品的具体技术实现方式、方法等不做要求。

信息安全技术 企业移动终端安全管理产品测评准则

1 范围

本标准规定了企业移动终端安全管理产品的受检要求、功能要求、测试方法、报告格式及评级方法。本标准适用于企业移动终端安全管理产品的开发和检测。

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。

- GA 243-2000 计算机病毒防治产品评级准则
- GA/T 757-2008 程序功能检验方法
- GA 849-2009 移动终端病毒防治产品评级准则

3 术语和定义

GA 243-2000、GA/T 757-2008、GA 849-2009 界定的以及下列术语和定义适用于本文件。

3.1

企业移动终端 **enterprise mobile terminal**

企业员工在企业移动计算环境中使用的便携式电子设备，包括智能手机、平板电脑等。

3.2

企业移动计算 **enterprise mobile computing**

企业为提高生产力而采取的一种新的生产方式，使企业员工可以通过移动终端方便快捷地处理企业事务。

3.3

企业移动终端安全管理产品 **enterprise mobile terminal security management product**

用于管理企业移动终端，保护企业计算环境安全的产品。

3.4

移动终端合规性 **mobile terminal compliance**

移动终端应符合企业制定的安全策略。

4 缩略语

下列缩略语适用于本文件。

IrDA: 红外 (Infrared Data Association)

MMS: 彩信 (Multimedia Messaging Service)

WiFi: 无线保真技术 (Wireless Fidelity)

5 受检要求

5.1 检验周期

检验机构对程序版本发生重大升级或名称发生改变的企业移动终端安全管理产品应进行检验；同时，可以根据安全威胁的发展情况对企业移动终端安全管理产品进行专项检验。

5.2 测试用例要求

受检企业应提交其产品检验用的测试用例。

5.3 资料要求

受检企业应提交的资料如下：

- a) 受检企业应提交产品研发人员的个人简历；
- b) 受检企业应提交产品的中文使用说明书；
- c) 受检企业应提交核封完整的正式产品。

6 功能要求

6.1 自服务式部署功能

企业移动终端安全管理产品应提供自动设置安全策略、配置网络连接等功能。

6.2 安全接入功能

6.2.1 总体要求

企业移动终端安全管理产品应提供保证移动终端安全接入到企业移动计算环境中的功能并记录接入情况。

6.2.2 认证功能

企业移动终端安全管理产品应在移动终端要求接入企业移动计算环境前，对移动终端进行身份认证并对认证结果进行记录。

6.2.3 合规检查功能

企业移动终端安全管理产品应在移动终端接入企业移动计算环境前，对移动设备的合规性进行检查并记录检查结果。

6.3 策略管理功能

6.3.1 推送安全策略功能

企业移动终端安全管理产品应提供向移动终端推送安全策略和配置更新的功能。

6.3.2 数据保护功能

企业移动终端安全管理产品应提供远程擦除数据和远程锁定移动终端的功能；擦除数据方式应支持全部擦除和部分擦除。

6.3.3 设备控制功能

企业移动终端安全管理产品应对设备的摄像、WiFi、蓝牙、红外、录音、短信、彩信、安装应用程

序等功能能够控制。

6.4 审计功能

企业移动终端安全管理产品应对所管理的移动终端的状况进行审计，并可生成报告。

6.5 远程定位功能

企业移动终端安全管理产品应能远程定位移动终端。

6.6 远程数据备份功能

企业移动终端安全管理产品应能远程备份移动终端的数据。

6.7 产品自身安全

企业移动终端安全管理产品应能抵御已知手段攻击，保证其正常运行不受影响。

7 测试方法

测试方法按 GA/T 757-2008 的规定。

8 报告格式

产品检验结果及评分表格式见表 1。

表 1 产品检验结果及评分表

检验项目		检验结果	分数	备注	
自服务式部署 (10分)	能否支持以自服务部署方式设置安全策略		5		
	能否支持以自服务部署方式配置网络连接		5		
安全接入 (18分)	能否对移动终端进行身份认证		9		
	能否对移动设备的合规性进行检查		9		
策略管理 (50分)	能否向移动终端推送安全策略和配置更新		8		
	能否支持全部擦除数据		5		
	能否支持部分擦除数据		5		
	能否远程锁定终端		8		
	能否对设备功能进行控制	摄像头		3	
		WiFi		3	
		蓝牙		3	
		红外		3	
录音			3		
	短信		3		
	彩信		3		

		安装/卸载应用程序		3	
审计 (8分)		能否对移动终端的状况进行审计		8	
远程定位 (5分)		能否支持远程定位		5	
远程备份 (5分)		能否支持远程数据备份		5	
产品自身 安全(4分)		能否抵御已知手段攻击		4	
总分				100	

9 评级方法

按照产品测试所得分数进行级别划分：

- a) 按表 1 规定的检验项目对受检产品进行评分。
- b) 受检产品未满足检验项目要求，则该项分值为零，满足检验项目要求，则该项分值按表 1 计算。
- c) 按受检产品所得总分数确定产品的级别，级别划分见表 2。

表 2 级别划分

分值	级别
71-80 分	一级
81-90 分	二级
90 分以上	三级