ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35282—2017

信息安全技术　电子政务移动办公系统安全技术规范

**Information security technology—
Security technology specifications of mobile e-government system**

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

本标准按照 GB/T 1.1—2009 给出的规则起草。

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:国家信息中心、华为技术有限公司、深圳市雁联移动科技有限公司、青岛市经济发展研究院、新疆维吾尔自治区信息中心、广西壮族自治区经济信息中心、天津电子政务信息与网络中心、中国海洋石油总公司、中国交通建设股份有限公司、北京北信源软件股份有限公司、山东乾云启创信息科技有限公司、北京三未信安科技发展有限公司、中兴通讯股份有限公司。

本标准主要起草人:李新友、刘蓓、付宏燕、吴亚非、刘翊、周华东、曹道刚、杨兴义、温娜、马鸣、赵若平、赵俊、周鸣、靳芳、谈超洪、文静、徐长江、徐金宝、侯晓峰、周斌、冯雪、潘子翼、刘昕、钟力、刘晓东。

信息安全技术　电子政务移动办公系统安全技术规范

1　范围

本标准规定了电子政务移动办公系统的基本结构、安全框架，以及移动终端安全、信道安全、移动接入安全和服务端安全应满足的技术要求。

本标准适用于非涉密电子政务移动办公系统的安全设计、产品研发、工程实施和运行管理，也可作为对非涉密电子政务移动办公系统进行安全测评的依据。本标准中的增强要求适用于安全等级较高的移动办公系统，如安全保护等级第三级或以上信息系统。

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 30278—2013　信息安全技术　政务计算机终端核心配置规范

GB/T 30284—2013　移动通信智能终端操作系统安全技术要求(EAL2 级)

3　术语和定义

下列术语和定义适用于本文件。

3.1

移动终端　mobile terminal

便携式、可移动的计算设备。

注：移动终端包括智能手机、平板、笔记本电脑，具备无线上网功能。

3.2

电子政务移动办公系统　mobile e-government system

利用移动终端，随时随地通过无线网络访问电子政务办公系统进行网上办公的应用系统。

3.3

移动终端管理　mobile device management

针对移动终端，提供从注册、激活、使用到废弃等全生命周期的管理，如移动终端的配置管理、安全管理、资产管理等，简称 MDM。

3.4

移动应用管理　mobile application management

针对移动应用软件，提供从分发、安装、使用、升级和卸载等过程和行为的监控和管理，简称 MAM。

3.5

移动内容管理　mobile content management

针对移动终端访问、存储、传输或处理的数据内容，提供信息过滤、访问控制、数据加密、安全隔离、剩余信息清除等管理措施，简称 MCM。

4 缩略语

下列缩略语适用于本文件。

3G:第三代移动通信技术(3rd Generation Mobile Communication Technology)

4G:第四代移动通信技术(4th Generation Mobile Communication Technology)

API:应用程序编程接口(Application Programming Interface)

APP:应用(Application)

BMP:图像文件格式(Bitmap)

CA:认证中心(Certificate Authority)

CSV:逗号分隔值/字符分隔值(Comma-Separated Values)

GIF:图像互换格式(Graphics Interchange Format)

GPRS:通用分组无线电业务(General Packet Radio Service)

HTML:超文本标记语言(HyperText Mark-up Language)

IPSec:IP 安全协议(Internet Protocol Security protocol)

PNG:图像文件存储格式(Portable Network Graphic format)

PDF:可携式文件格式(Portable Document Format)

SD:安全数码卡(Secure Digital card)

SDHC:高容量安全数码卡(Secure Digital High Capacity card)

SM1:SM1 分组密码算法

SM2:SM2 椭圆曲线公钥密码算法

SM3:SM3 密码杂凑算法

SM4:SM4 分组密码算法

SSL:安全套接层(Secure Sockets Layer)

TF/Micro SD:微型 SD 卡(Trans-Flash/Micro SD)

TLS:安全传输层协议(Transport Layer Security)

UKey:USB 钥匙(USB Key)

URL:统一资源定位符(Uniform Resource Locator)

USB:通用串行总线(Universal Serial Bus)

VDI:虚拟桌面基础架构(Virtual Desktop Infrastructure)

VPN:虚拟专用网(Virtual Private Network)

WAP:无线应用协议(Wireless Application Protocol)

WAPI:无线局域网鉴别和保密基础架构(Wireless LAN Authentication and Privacy Infrastructure)

Wi-Fi:无线保真(Wireless-Fidelity)

WLAN:无线局域网(Wireless Local Area Network)

XSL:可扩展样式表语言(eXtensible Stylesheet Language)

5 电子政务移动办公系统基本结构

电子政务移动办公系统主要由移动终端、通信网络、移动接入区和服务端四部分构成,其基本结构如图 1 所示。

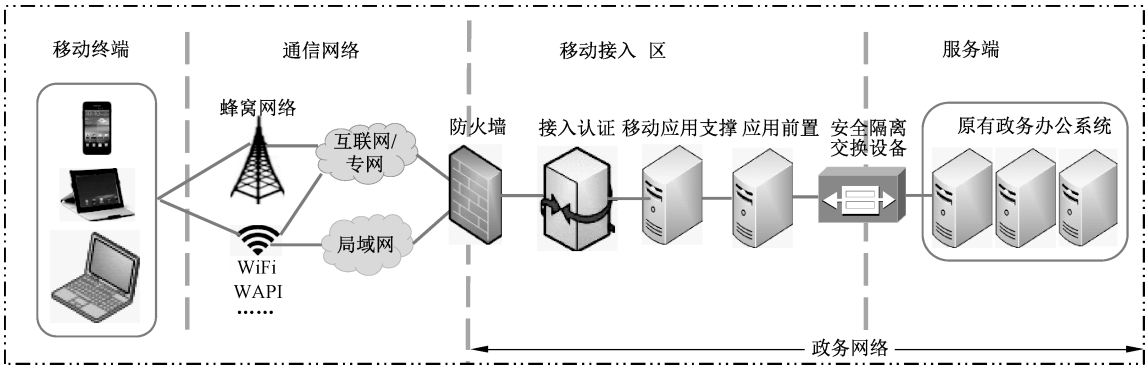

图 1 电子政务移动办公系统基本结构

电子政务移动办公系统的基本结构包括：

a) 移动终端：处于电子政务移动办公系统的用户侧，多在组织办公场所外部使用，也支持组织办公场所内部使用。

b) 通信网络：位于移动终端与政务网络之间，以移动蜂窝网络、Wi-Fi 或 WAPI 等公共无线网络连接移动终端，以互联网/专网或局域网等方式接入政务网络。

c) 移动接入区：处于政务网络边界侧，一般包括互联网边界防护设备，如防火墙、接入认证网关、移动应用支撑平台(用于实现政务系统 Web 页面向 WAP 或移动应用 APP 的转化和显示适配)，应用前置系统(用于接入区与服务区进行政务应用或数据同步)，以及安全隔离与交换设备，如网闸等。

d) 服务端：指政务网络的核心服务区域，包括组织原有的政务办公系统，以及对移动应用和移动内容进行管理的移动应用系统。

6 电子政务移动办公系统安全框架

6.1 系统主要安全风险

电子政务移动办公系统的安全风险存在于移动终端、通信网络、移动接入和服务端四个方面。系统面临的主要安全风险见表 1。

表 1 电子政务移动办公系统面临的主要安全风险

组成部分	面临安全风险的要素	主要安全风险
移动终端	硬件、操作系统、应用软件及数据	a) 非授权用户访问 b) 授权用户恶意访问 c) 恶意软件访问 d) 互联网非授权实体的访问 e) 移动终端丢失或被盗
通信网络	通信网络自身、信息传输过程	a) 意外中断 b) 传输信息被非法窃听、截获或者修改 c) 恶意攻击破坏
移动接入区	网络接入设备、移动应用支撑系统、应用前置系统	a) 非授权用户访问 b) 授权用户恶意访问 c) 恶意软件访问

表 1（续）

组成部分	面临安全风险的要素	主要安全风险
服务端	业务应用系统和信息数据	a） 非授权用户访问 b） 授权用户恶意访问 c） 恶意软件访问 d） 信息泄漏

6.2 系统安全技术框架

基于对电子政务移动办公系统的安全风险分析，电子政务移动办公系统的安全技术框架应包括移动终端安全、信道安全、接入安全和服务端安全四部分，涵盖了对移动终端、信道、接入和服务端的具体安全技术要求，如图 2 所示。图 1 中的基础设施，如边界防护或安全隔离交换设备不包含在图 2 范围。

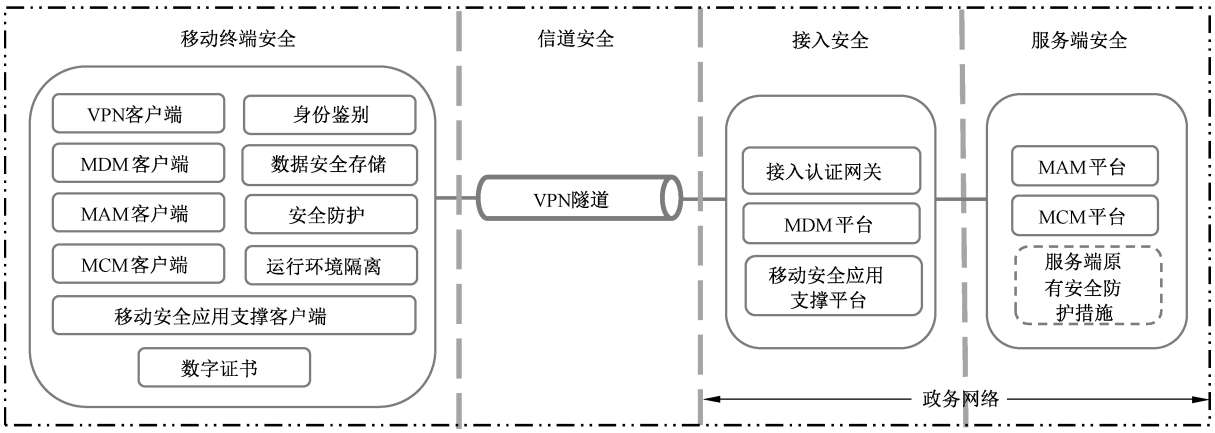

图 2 电子政务移动办公系统安全技术框架

电子政务移动办公系统的安全技术框架包括：

a） 移动终端安全：移动终端在基本配置上应支持如下安全客户端的安装和运行，包括 VPN 客户端、MDM 客户端、MAM 客户端、MCM 客户端和移动安全应用支撑客户端等，支持数字证书的安装与使用，具备身份鉴别、数据安全存储、安全防护、运行环境隔离等安全功能。

b） 信道安全：应通过构建 VPN 隧道满足移动终端从公共无线网接入政务网络的传输安全要求。

c） 接入安全：应在政务网络边界侧构建接入区，以满足移动终端安全接入要求，以及与政务网络核心服务区的安全隔离，包括接入认证网关和 MDM 平台，支持移动终端设备的接入认证和安全管理等。

d） 服务端安全：在保持服务端原有安全措施的基础上，需配备 MAM 平台和 MCM 平台，分别对移动应用和移动内容实施安全控制管理。

7 移动终端安全

7.1 通用配置

移动终端的通用配置要求包括：

a） 应支持数字证书的安装和运行；
b） 应支持 VPN 客户端的安装和运行，以及在线升级；
c） 应支持 MDM 客户端的安装和运行，以及在线升级；
d） 应支持 MAM 客户端的安装和运行，以及在线升级；
e） 应支持移动安全应用支撑客户端的安装和运行，以及在线升级。

增强要求为：

a） 应支持硬介质形式的数字证书；
b） 应支持 MCM 客户端的安装和运行，以及在线升级。

7.2 数字证书

移动终端应支持使用软件形式或硬介质形式的数字证书，支持国家密码主管部门认可的密码算法。

7.3 VPN 客户端

VPN 客户端与 VPN 服务端通讯，在公共无线网络上构建政务数据传输的安全信道，VPN 客户端启动时，应作为网络通信的唯一通道。

7.4 MDM 客户端

MDM 客户端与 MDM 平台通讯，实现移动政务办公时对移动终端的安全管理，具体要求包括：

a） 应开机自动运行，保持移动政务应用访问过程中对移动终端的实时监测；
b） 应支持移动终端的注册和登录管理；
c） 应支持移动终端运行状态的收集上报，如终端标识、位置信息、固件版本、系统版本、网络类型、用户信息等；
d） 应支持 MDM 服务端管理策略执行，包括终端锁定、整机远程擦除、出厂设置恢复、数据擦除、ROOT 检测、策略更新、SD 卡检测等；
e） 应支持将移动终端本地的政务办公数据远程备份至服务端；
f） 应具备防卸载机制，当 MDM 客户端被卸载时，政务应用客户端及本地办公数据将被自动擦除。

7.5 MAM 客户端

MAM 客户端与 MAM 平台通讯，实现对移动政务应用的安全管理，具体要求包括：

a） 应在移动政务应用开启时自动运行，保持对移动政务应用的实时监测；
b） 应支持移动政务应用及第三方应用信息收集上报，如程序标识、名称、版本、平台、开发商等；
c） 应支持 MAM 服务端管理策略执行，包括移动应用分发、安装、卸载、应用黑白名单设置等；
d） 具备防卸载机制，可与 MDM 客户端联动，当 MAM 客户端被卸载时，执行终端锁定或信息擦除策略。

7.6 MCM 客户端

MCM 客户端与 MCM 平台通讯，实现对移动政务数据文件的安全管理，具体要求包括：

a） 应在移动政务应用开启时自动运行，支持自动更新升级；
b） 应支持 MCM 服务端对移动政务数据文件信息的统计采集，如文件名称、格式、大小、时间等；
c） 应支持 MCM 服务端管理策略执行，对 PNG、JPG、GIF、BMP、PDF、DOC、DOCX、XSL、CSV、TXT、HTML 等格式数据文件进行加解密和安全展现，如按页加载、按页清除等；

d） 具备防卸载机制，可与 MDM 客户端联动，当 MAM 客户端被卸载时，执行终端锁定或信息擦除策略。

7.7 移动安全应用支撑客户端

移动安全应用支撑客户端与移动安全应用支撑平台通讯，实现移动应用的安全展现和安全运行，具体要求包括：

a） 应支持移动应用安装及运行环境的安全隔离；

b） 应支持应用页面安全加载显示，应用运行时禁止截屏操作；

c） 应支持移动应用临时文件加密存储；

d） 应支持移动应用退出及时清除缓存页面、临时文件等剩余信息。

增强要求为：

应采用动态加载、虚拟化或其他技术实现客户端仅显示用户界面和传输用户交互数据，办公数据不在移动终端留存。

7.8 身份鉴别

移动终端在身份鉴别方面的要求包括：

a） 应支持设置开机口令或利用生物特征识别等，开启移动终端时进行身份鉴别；

b） 应支持屏幕锁定口令，移动终端空闲时间达到设定阈值时锁定屏幕；解锁时应重新进行身份鉴别；

c） 访问政务应用和本地政务数据之前应采用数字证书进行身份验证；

d） 在限定时间段内多次连续尝试身份验证失败，应锁定系统。

7.9 数据安全存储

移动终端数据存储方面的要求包括：

a） 政务数据应与个人数据隔离存储；

b） 政务数据应加密存储，采用的加密算法应符合国家密码主管部门的相关规定。

增强要求为：

政务数据不应存储在移动终端上。

7.10 安全防护

移动终端的安全防护要求包括：

a） 应支持对病毒、木马的查杀，拦截恶意软件的攻击；

b） 应支持对系统漏洞的修复；

c） 应支持系统补丁的升级；

d） 应支持移动办公应用关闭时及时清理缓存页面等临时文件。

此外，手持式移动终端（如手机、PAD）的操作系统安全应符合 GB/T 30284—2013 规定的技术要求；

笔记本电脑在安全防护方面应符合 GB/T 30278—2013 第 7 章规定的核心配置基本要求。

7.11 运行环境隔离

移动终端的运行环境隔离要求包括：

a） 应采用沙箱等隔离技术保证移动政务应用与个人应用运行环境的有效隔离；

b） 应在移动应用关闭时及时清除临时文件等剩余信息。

8 信道安全

信道安全的具体要求包括：

a） 移动终端通过移动蜂窝网络或公共无线网络接入政务网络时，应采用 VPN 方式接入；

b） 应支持系统级或应用级 VPN，在移动政务应用启动时自动启动 VPN。通过应用专属的安全隧道，实现多政务应用之间的安全隔离。

9 接入安全

9.1 接入认证网关

接入认证网关的要求包括：

a） 应支持国家密码主管部门认可的密码算法；

b） 密钥协商数据的加密保护应采用非对称密码算法（如 SM2），报文数据的加密保护应采用对称密码算法（如 SM1 或 SM4）；

c） 应支持 SSL/TLS 或 IPSec 等网络安全协议；

d） 应支持基于用户账户和权限分配的细粒度访问控制，支持仅授权用户才能访问特定资源；

e） 应支持网关运行情况的集中监控。

9.2 MDM 平台

9.2.1 设备管理

MDM 平台对已授权的移动终端的设备管理要求包括：

a） 应支持移动终端首次访问移动政务应用前注册到 MDM 平台，支持建立设备序列号、证书序列号、人员和手机号码信息等绑定关系；

b） 应支持移动终端设备信息统计，包括硬件、网络、系统、应用、位置及用户信息等；

c） 应支持远程对发生异常（如丢失）或废弃的移动终端进行注销、禁用和锁定管理；

d） 应支持基于用户进行管理，支持一个用户绑定多个移动终端或者一个移动终端绑定多个用户，支持通过用户分组和关联角色进行管理控制；

e） 应支持限制或者禁用移动终端硬件模块功能，如摄像头、录音、蓝牙、麦克风等。

9.2.2 安全管控

MDM 平台对已授权的移动终端的安全管控要求包括：

a） 应支持对移动终端的安全准入检查，不合规的移动终端不应注册；

b） 应支持与接入认证网关联动，不合规的移动终端不应接入；

c） 应支持对移动终端的软硬件环境、运行状态及安全事件的持续监控、安全审计及预警；

d） 应支持针对移动终端违规行为采取有效控制措施，包括限制访问、警告、锁定、禁用、系统还原、数据擦除等；

e） 若检测到移动终端有 ROOT 行为，应立即锁定终端；

f） 应支持对移动终端允许使用的地理区域进行限制；

g） 支持远程禁用或重新启用移动终端。

9.2.3 安全审计

MDM 平台对已授权的移动终端的安全审计要求包括：

a） 应支持对移动终端的政务应用访问操作进行审计；

b） 应支持对移动终端的状态变化及用户违规行为等安全事件进行审计；

c） 审计日志记录应包含如下字段：日期、时间、发起者信息、类型、描述和结果等。

9.3 移动安全应用支撑平台

移动安全应用支撑平台的要求包括：

a） 应支持政务办公系统 WEB 应用到移动应用的安全转换，包括页面适配、文件解析、格式转换等；

b） 应支持政务办公应用的访问控制和授权管理；

c） 应支持对用户访问请求和移动应用内容的安全过滤。

增强要求为：

应采用动态加载、虚拟化或其他技术，支持政务应用和政务数据仅在服务端运行和存储，办公数据不在移动终端设备留存。

10 服务端安全

10.1 MAM 平台

10.1.1 资源分类管理

MAM 平台的资源分类管理要求包括：

a） 应支持远程推送安装移动政务应用到指定的移动终端；

b） 应支持对移动政务应用的安装、使用情况进行统计；

c） 应支持对移动政务应用的版本管理，并可回退至指定历史版本；

d） 可通过建立企业移动应用商店实现对移动政务应用的统一发布、更新和管理。

10.1.2 应用访问控制

MAM 平台的应用访问控制要求包括：

a） 应支持移动应用黑白名单策略，并设置移动政务应用的用户访问权限；

b） 应支持远程监控和管理移动终端上安装的政务应用，包括应用安装、更新和删除等；

c） 删除移动政务应用时应同时擦除应用数据；

d） 移动政务应用不应在未认证的移动终端中安装和运行；

e） 应支持将沙箱等安全容器推送至移动终端默认安装，增加应用访问的安全性。

10.1.3 政务应用客户端（APP）安全管理

对政务应用客户端的安全管理要求包括：

a） 可设置专门应用商店提供政务应用客户端发布、下载及更新服务；

b） 支持对移动政务应用客户端进行安全扫描，阻止含恶意代码和严重漏洞的应用发布至应用商店；

c） 支持对移动政务应用客户端进行安全防护和加固，防止受到恶意程序的破坏、破解和篡改。

10.2 MCM 平台

MCM 平台的要求包括：

a） 应支持 JPG、GIF、BMP、PDF、DOC、DOCX、XSL、CSV、TXT、HTML 等多种格式文件的识别、导入、发布和下载；

b） 应支持政务文档的分级分类管理，并设置用户访问权限，如读写、拷贝、下载等；

c） 应支持向已授权的移动终端分发或推送政务文档；

d） 应支持对移动政务文档内容展现时按页加载和按页清除；

e） 应支持对用户下载、查阅文档的统计记录。

增强要求为：

a） 应支持对移动政务文档内容的加解密；

b） 应支持移动政务文档内容不在移动终端留存并及时清除缓存。

参 考 文 献

[1] GB 15629.11—2003 信息技术 系统间远程通信和信息交换局域网和城域网 特定要求 第11部分:无线局域网媒体访问控制和物理层规范

[2] GB 17859—1999 计算机信息系统 安全保护等级划分准则

[3] GB/T 18336(所有部分) 信息技术 安全技术 信息技术安全评估准则

[4] GB/T 20269—2006 信息安全技术 信息系统安全管理要求

[5] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[6] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

[7] GB/T 25068.4—2010 信息技术 安全技术 IT网络安全 第4部分:远程接入的安全保护

[8] GB/T 25068.5—2010 信息技术 安全技术 IT网络安全 第5部分:使用虚拟专用网的跨网通信安全保护

[9] GB/T 25070—2010 信息安全技术 信息系统等级保护安全设计技术要求

[10] GA/T 671—2006 信息安全技术 终端计算机系统安全等级技术要求

[11] GM/T 0022—2014 IPSec VPN技术规范

[12] GM/T 0024—2014 SSL VPN技术规范

[13] GM/T 0026—2014 安全认证网关产品规范

[14] GM/T 0027—2014 智能密码钥匙技术规范

[15] NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise, 2013