电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0028-V1.0.0:2018

移动政企终端安全管理技术要求

Technical Requirements for Government and Enterprise Mobile Terminal Security Management

2018－09－03 发布　　2018－09－03 实施

电信终端产业协会　　发 布

目　　次

前　言

本标准是为了保障移动政企终端的良性可持续发展，对移动终端设备安全、移动应用安全、移动内容安全等维度制定安全管理技术要求。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院华东分院、中国信息通信研究院。

本标准主要起草人：杨伟利、潘娟、郑忠斌、刘建泉、傅山、魏凡星、董雯、曹远晶、严三霞。

引　　言

随着云计算、移动等新兴的IT趋势的逐步成熟，移动终端也走进了企事业单位，员工可以在任何时候、任何场所便捷地访问公司内网，运行内部应用，这提升了办公效率并且促进了员工之间的协同合作，然而却给企业信息安全带来了严峻的挑战。移动办公环境主要存在三个方面的安全隐患：首先是通过移动网络链路接入，天然处在一个开放的网络，而传统重要的信息系统都是通过企业内网接入；其次，使用的环境与传统信息化模式不一样，传统的大部分时间都在固定的办公场所，设备丢失可能性很小，而移动智能终端更加容易丢失；第三，移动办公设备上往往同时安装很多个人的APP，而个人APP市场上的恶意软件多如牛毛，这就将企业数据置于安全隐患之中。保护用户个人信息已成为业界及用户非常关注的问题。

为了保障移动政企终端的良性可持续发展，制定移动政企终端安全管理技术要求，确保移动终端上信息的安全流动、存储和管理，帮助政企在移动办公的高效率与信息安全之间找到最佳平衡点。

移动政企终端安全管理技术要求

1 范围

本标准针对移动政企终端在移动办公的系统架构下，制定移动设备安全管理、移动应用安全管理、以及移动内容安全管理的各项技术要求。

本标准适用于移动办公环境下的移动政企终端。

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，仅所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。

3 术语、定义和缩略语

3.1 术语和定义

3.1.1 移动智能终端 Smart Mobile 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，并能够安装和运行第三方应用软件的移动终端。

3.1.2 移动政企终端 Government and Enterprise Industry Mobile Terminal

由企业根据自身业务特点定制并仅限内部员工办公使用的的移动智能终端。

3.1.3 移动设备管理 Mobile Device Management

保护、监控和管理移动政企终端。包括提供移动设备生命周期管理，从设备注册、激活、使用、淘汰各个环节进行全面管理。具体能实现用户管理、远程控制、通信安全、设备自检、资产管理等功能。

3.1.4 移动应用管理 Mobile Application Management

针对移动政企终端应用的安全保护、分发、访问、配置、更新、删除等策略和流程。通过政企应用商店控制和推送应用，能集中监控应用的使用情况，对应用设置相应策略以满足政企的规范。

3.1.5 移动内容管理 Mobile Content Management

提供隔离环境，实现安全传输及安全存储，确保政企数据安全无忧。

3.2 缩略语

BYOD	携带自己的设备	Bring Your Own Device
COPE	企业拥有、个人使用	Corporate Owned, Personally Enabled

MAM	移动应用管理	Mobile Application Management
MCM	移动内容管理	Mobile Content Management
MDM	移动设备管理	Mobile Device Management

4 系统架构

移动办公系统参考架构如图1所示，移动设备通过无线网络，运用HTTPS协议对服务器进行访问。政企移动业务区域、移动设备和移动设备上的相关的应用由政企直接控制。政企核心业务区域也是在其控制范围内，但该区域不在本规范描述范围内。

移动设备需保证移动计算以及接入到政企资源的安全，政企移动业务区域包括移动设备管理（MDM）、移动应用管理（MAM）和移动应用商店；MDM是集中对移动设备的功能、安全进行管理和优化；MAM为装载在移动设备上的政企应用提供分发、配置、数据控制以及应用生命周期管理的功能，它还可以提供应用诊断的功能；移动应用商店提供了政企应用的下载渠道，这些已经获得许可的应用需下载并安装到经政企许可的移动设备上。

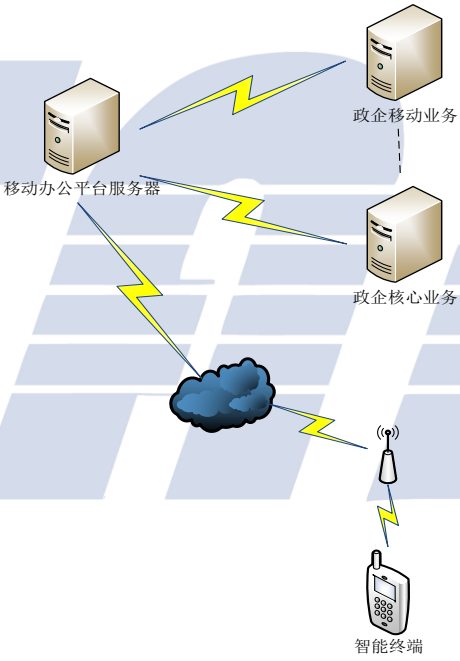

图1 政企移动办公框架图

5 安全目标

5.1 概述

为了解决政企办公人员在工作中使用移动政企终端存在的安全风险，需要对移动设备、移动应用、移动内容进行安全管理，以保证政企办公数据在存储、处理、传输过程中没有被盗，以此来改善员工和政企办公风险问题。

5.2 移动设备管理安全目标

5.2.1 用户管理

为解决用户有意或无意安装不符规定的软件，或者附录B中所提到的员工有意或无意泄密问题，安全功能应对用户进行相应的权限管理。

在访问受保护的功能和数据前，需要用户发起向设备的鉴权申请。一些非敏感功能（如拨打紧急电话，文字提示）可以无需鉴权直接访问。

用户反复尝试鉴权的行为应被限制或阻止，应保证未成功的尝试间间隔足够长时间。

5.2.2 远程控制

为解决附录B中提到的设备丢失所带来的数据丢失，移动设备应提供数据保护，移动设备应该能够具备远程保护的能力，且终端的远程控制功能也应具备非授权访问的安全设置，确保终端仅处在有安全隐患的情况下才能被启用。

5.2.3 通信安全

为解决附录B中提到的网络窃听和网络攻击的威胁，移动设备和远程网元间应使用可信通信传输方式。

5.2.4 设备自检

为保证移动设备的完整性，移动设备应能自检其关键功能、软件、固件和数据的完整性，自检失败的信息应能提示给用户。

为解决应用程序漏洞和恶意软件攻击，对软件和固件版本升级也应在安装运行前进行完整性检测。

5.2.5 资产管理

如果终端为企业所有、个人使用，则需要对终端进行资产管理，确保资产在使用过程中的安全可控。

5.3 移动应用管理安全目标

政企实施移动办公，移动应用是重要的软件资产，需要通过移动应用管理能力来提供移动应用全生命周期管理，保障移动应用的安全高效使用。

5.4 移动内容数据加密安全目标

政企办公数据的内容管理既要确保内容的安全性，确保用户数据不被非法篡改、获取，同时能够通过备份保证有效恢复，还需要具备擦除内容的能力。

6 安全管理

6.1 移动设备安全管理

6.1.1 概述

根据5.2节的安全目标，移动设备的安全管理包括用户管理、远程控制、通信安全、设备自检和资产管理等功能。

6.1.2 用户管理

移动设备能够在用户访问受保护的功能和数据前发起鉴权申请，以及对不同领域的用户进行相应的权限配置，即通过分权分域的方式来配置用户的不同权限。用户管理要求包括：

(1) 对用户的认证和授权通过移动设备与授权服务之间的可信通道建立；

(2) 用户在解密敏感数据时，应提供相应的鉴权机制，例如PIN码、指纹等；

(3) 针对身份认证口令，安全功能应支持以下功能：

1. 口令应可以由大写英文字母、小写英文字母、数字、特殊字符任意组合而成。

2. 口令长度不低于6位。

(4) 限制用户在认证前尝试，用户认证尝试连续失败次数不超过10次，两次尝试间隔应不小于500毫秒；

(5) 当用户修改身份认证因子口令时，应要求用户先输入正确的口令；

(6) 在设备进行口令输入认证过程中，设备应只提供隐式显示或提示，如显示*号，不允许明文显示和提示。（最多允许短暂（不大于1秒）显示输入各个字符，方便用户确认自己的输入字符）

(7) 移动设备应在一定的时间间隔无操作后转入锁定模式；

(8) 在移动设备转入锁定模式时应将之前显示的内容清除或覆盖设备显示；

(9) 移动设备在使用仅充电模式下且处于锁定状态，移动设备应不支持数据存取功能；

(10) 移动设备应有用户权限管理，每个通过认证的用户只能操作其授权的功能。

6.1.3 远程控制

移动设备支持远程控制功能，应具备一下条件：

(1) 应在移动设备与远程控制设备之间建立可信链路，用于保证远程控制的控制安全。

(2) 控制设备与被控设备之间应建立强认证机制，确保非授权设备控制移动设备。

移动设备能够可执行的远程操作如下：

(1) 用户的数据的远程擦除，保证被删除用户数据不可再恢复，远程擦除数据可以提供多项选择，例如：擦除SD卡数据、恢复出厂设置和应用的权限配置等；

(2) 移动设备的远程锁定，若使用者由于疏忽暂时无法找到终端时，终端应支持远程锁定终端，保证信息安全；

(3) 移动设备的远程备份，备份系统应具备安全性、可管理性和可扩展性，且移动设备的数据备份系统的数据加密最好使用数字信封的方式，保证高效的完成数据加密。

6.1.4 通信安全

移动政企终端通过移动网络接入远程接入区，移动终端应满足一下要求：

(1) 移动终端与远程接入区应具备双向身份认证机制，确保移动终端与远程接入区的身份可信。

(2) 移动政企终端应安全接入区建立可信加密通讯链路（例如VPN）

移动设备的通信安全要求包括：

(1) 使用HTTPS等安全传输协议进行安全通信；

(2) 应提供VPN客户端接口，或数据流直接通过VPN客户端的方式传输，如IPsec VPN或者SSL VPN；

(3) 与外部蓝牙设备配对前，应要求用户进行显式的认证；

(4) 使用TLS版本应限于TLS 1.2版本或更高版本，如TLS1.3版本，应限制使用自身不安全的版本，如TLS 1.0版本等；

(5) 安全功能应提供适当方法，可以在某应用使用安全通信前，检查其认证证书的合法性；

(6) 当移动设备无法建立网络连接来决定认证证书的合法性时，安全功能应运行管理员或用户来选择是否认可该认证证书合法。

(7) 安全功能应为应用提供认证证书合法性验证服务，验证结果应告知该应用。

6.1.5 设备自检

移动设备的自检要求包括：

(1) 在开机初始化过程中运行自测套件来测试所有安全功能正常运行；
(2) 对完整性验证值进行加密签名；
(3) 为自身使用提供可靠的时间戳；
(4) 通过应用处理器OS内核和在互斥媒介中存储的所有可执行代码验证启动链的完整性，该代码在用数字签名、硬件保护非对称密钥、或硬件保护哈希运行前在互斥媒介中存储；
(5) 使用更新前厂商提供的数字签名来验证对应用处理器系统软件和其他处理器系统软件的软件更新；
(6) 不更新或仅由被验证过的软件更新其根完整性保护密钥或哈希；
(7) 验证在更新中使用的数字签名验证密钥的合法性，验证方法可以是通过信任锚数据库公共密钥验证其合法性或通过硬件保护的公共密钥验证其符合性；
(8) 使用非对称算法管理根密钥，持续不定期的更新根密钥；
(9) 将设备软件完整性验证值计入日志或提供给管理员。

6.1.6 资产管理

对于企业所有、个人使用的终端，其资产管理要求包括：

(1) 应具备资产注册及注销的功能；
(2) 对终端的位置信息、使用账户信息要进行记录。
(3) 智能终端应具备唯一标识该设备的硬件标识。

6.2 移动应用安全管理

6.2.1 移动应用分发管理

(1) 通过建立政企移动应用商店进行私有的、安全的管理移动应用；
(2) 政企移动应用商店不面向大众公开，终端访问应用商店以及下载应用时需要通过身份认证；
(3) 政企应用商店需要支持企业自行开发的移动应用和第三方应用市场的公共应用上架、下架管理；
(4) 可以基于员工的组织结构信息、设备的归属（BYOD、COPE）定向控制每个应用的分发和可视范围；
(5) 可以快速将移动应用定向推送到员工的移动设备上；
(6) 应用商店能够进行应用版本更新，并快速将新版本应用推送到对应的员工移动设备上；
(7) 在新版本应用上架后，支持移动应用的部分设备试点升级；
(8) 支持应用黑名单和白名单，能够进行黑白名单的检查。

6.2.2 应用层面的数据丢失保护

(1) 基于应用的，而不是基于整个设备的数据加密；
(2) 防止恶意软件和欺骗应用访问数据；
(3) 基于应用，防止非授权的对数据的拷贝和粘贴；
(4) 保证附件或者文件在安全的打包应用间传输（仅适用于安卓系统）。

6.2.3 应用级别的接入控制

(1) 在允许用户接入到政企特定的应用前，应验证用户身份的合法性；
(2) 把应用授权给用户、角色或部门，保障应用使用安全；
(3) 在政企规定的尝试次数认证失败后，企业应具有相应的措施使应用无法被使用；

(4) 在几次尝试认证失败后，应丢弃或拒绝应用数据的恢复。

6.2.4 应用级使用控制

(1) 当设备被越狱或者ROOT后，应具有相应的措施使应用无法被使用；
(2) 为每个应用设置超期时间来生成时间限制的接入。

6.2.5 数据保护

(1) 受保护的存储数据仅仅由相应授权的应用访问；
(2) 为每一个应用和应用服务器建立一个安全的传输通道；
(3) 在装载应用的过程中要验证设备的完整性。

6.3 移动内容数据加密安全管理

移动内容安全管理的要求包括：

(1) 对企业数据和用户数据使用数据加密密钥(DEK)，通过特定的密码算法进行加密/解密；
(2) 要求用户在解密受保护数据和加密DEK、KEK和其他长效密码材料、软件密码存储开始前，输入身份认证因子口令；
(3) 在擦除受保护数据时，
EEPROM： 销毁应进行单向随机数覆盖，覆盖后应进行读取验证；
闪存：销毁应进行单向全零覆盖或块擦除，覆盖或擦除后应进行读取验证；
其他非易失存储器：销毁应进行三次或三次以上随机数覆盖，每次覆盖使用的随机数不同。
(4) 在擦除操作完成后移动设备应进行重新启动；
(5) 对缓存文件进行加密；
(6) 在擦除加密密钥时，
对易失性存储器：销毁应进行单向随机数覆盖，覆盖后应进行读取验证；
EEPROM： 销毁应进行单向随机数覆盖，覆盖后应进行读取验证；
闪存：销毁应进行单向全零覆盖或块擦除，覆盖或擦除后应进行读取验证；
其他非易失存储器：销毁应进行三次或三次以上随机数覆盖，每次覆盖使用的随机数不同；
(7) 可将移动设备分为企业工作区域和用户个人区域；
(8) 不允许用户或未授权的应用将企业数据发往移动设备的个人区域和其他区域；
(9) 可以提供方法在IT管理员授权情况下将联系人、日历事件信息在用户个人区域和企业工作区域共享。

6.4 安全审计要求

(1) 实现安全审计管理，收集、记录、管理用户与系统安全有关的活动，数据访问和关键操作行为记录；
(2) 对接口的所有请求和响应都要有详细的日志记录，便于后期的分析和审计；
(3) 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；
(4) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

附 录 A
（规范性附录）
标准修订历史

修订时间	修订后版本号	修订内容
2018.7	V1.0.0	范围，全文格式

附 录 B
（资料性附录）
附录

B.1 由于设备的丢失所带来的数据丢失

移动设备被盗或者丢失后，攻击者可通过对这些设备的物理接入获得终端设备上的数据。通常的接入点包括：外部硬件端口、用户接口，或者直接进行破坏性接入到终端的存储介质。除此之外，无密码或者弱密码强度、无加密或者弱加密能导致设备上的数据泄露。

B.2 网络窃听和网络攻击

攻击者位于无线通信信道或者在网络中的任何一点处，监听或者截取移动设备与另外一个端点进行的交互数据。另外一方面，攻击者也可以借助发起和移动终端的通信对其进行攻击，将一些恶意软件、恶意网页或者邮件通过网络发送到终端。

随着 WIFI 在公共区域的广泛部署，越来越多的人开始使用 WIFI 网络实现移动和数据业务。由于 WIFI 的安全性的缺失，导致连接到 WIFI 的移动设备面临着广泛的被攻击的可能。

B.3 员工有意或无意泄密

在数据泄露威胁方面来看，任何没有理解企业移动办公安全立场的员工都可能带来风险，如果企业未能解释清楚企业的政策，或者未能教授员工最佳的安全做法，这都会使员工有意或者无意地泄露敏感信息，从而造成严重的后果。

B.4 应用程序漏洞导致数据丢失和泄露

应用程序通常申请很多权限接入或收集用户数据，这些用户数据可能是他们需要的，也有可能是他们根本就不需要的。

参 考 文 献