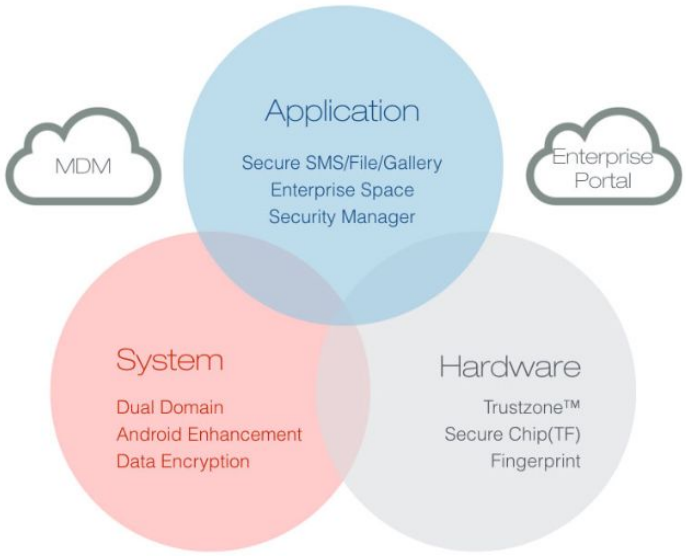
ThunderSec3.0 技术白皮书

面向行业的软硬一体安全办公解决方案

TS | 中科创达安全技术研究组 | 2016 年 4 月 16 日

一、整体介绍

ThunderSec3.0 是中科创达面向政府、金融、运营商、能源、制造等企业推出的新一代企业级软硬一体安全办公解决方案。为客户移动终端在使用企业资源时，提供从硬件、OS、应用、数据到链路等多层次的安全防护方案，确保企业数据和应用在移动终端上的安全性。



在硬件层面，中科创达作为全球最大的移动操作系统服务商，基于和芯片厂商和移动设备厂商的良好合作，充分发挥出移动终端的硬件安全保护能力，比如 CPU 芯片的 TrustZone 技术，指纹安全技术，智能安全 TF 卡技术等，保证为企业提供的终端都是定制了安全硬件保护方案的，确保设备的根可信，核心的密钥和算法的可信。

在操作系统层面，中科创达基于对操作系统的深厚积累，提供操作系统的层面的安全域隔离技术和加密技术，为企业应用提供隔离的运行环境，对企业敏感信息进行多层面的加密，同时提供多种切换方式，满足企业对隐藏安全域或者一键切换安全域的需求。同时从操作系统层面提供更加强大的设备管理功能，满足企业设备从发放到注销的完整生命周期以及各种使用场景的管理需求，对外提供 SDK 可支持任何三方 EMM 管理系统对设备进行管理。

在应用程序层面，中科创达的安全应用团队经过 3 年的积累，提供多种通用性安全应用以及满足企业办公需求的辅助办公类应用，解决了企业在移动终端上信息加密（文件，拍照，输入法等），通信加密（VPN，加密短信，加密网络电话，加密邮件等），安全办公（加密企业通讯录，统一认证等）这些常见的应用使用场景。同时提供 EMM 系统，支持部署到企业私有云以及直接提供公有云服务，满足安全应用推送，消息推送，内容推送等现代企业云管端的需求。

二、硬件安全介绍

硬件安全主要涉及到 TrustZone，指纹，安全智能 TF 卡等方面的安全技术。

a) TrustZone 技术

ARM TrustZone 技术本质上是一种虚拟化技术，通过将处理器状态分为安全和非安全状态，并且配合其他总线以及外设上的安全属性来实现遍布整个硬件系统的安全。ARM TrustZone 有自己的安全引导过程以及个性化的软件更新过程，也有自己的硬件随机数产生器，并且同应用处理器之间是通过中断驱动的 Monitor 模式以及共享内存来进行通信。

基于 TrustZone 之上有一个 Secure OS，业界通常所说的 TEE（Trust Execution Environment）就是指 Secure OS 执行环境，目前影响力比较大的 Secure OS 是高通公司的 QSEE（高通芯片代码预制，基本功能免费），Trustonic 公司的 Trustonic（MTK 芯片代码默认方案，需要 OEM 单独购买），以及华为的 TEE（华为芯片预制），同时目前还有一些三方 Secure OS，比如 Google 开源的 Trusty OS，韩国的 Solacia OS 以及国内的豆荚 OS 等。中科创达提供基于 QSEE，Trustonic 等主流 Secure OS 上的安全解决方案。

中科创达 ThunderSec3.0 安全方案解决方案涉及到 TEE 的功能有：

功能点	涉及到 TEE 的部分	TEE 技术点说明
安全启动（SecureBoot）	安全启动中，OS 的镜像一层层进行校验，校验通过后安全启动。	TEE 驱动 TEE 加解密
安全域认证	安全域初始化密钥存储在 TEE，支持 PIN，密码，图案等。 安全域认证在 TEE 执行。	TEE 安全文件存储 TEE 加解密
安全域一致性检查	安全域中域自身对象以及安全域安装的应用的认证过程定时在 TEE 执行，查杀非法应用。	TEE 安全文件存储 TEE 加解密
安全应用	企业通讯录，加密短信，加密邮件等用到的密钥和加解密过程在 TEE 中。 并且可以支持第三方 App 使用到 TEE 能力。	TEE 安全文件存储 TEE 加解密

指纹认证	通过指纹认证进入到安全域或者进入到安全应用，场景可定制。 指纹驱动，指纹的采集和认证等算法执行在 TEE 中。 注：和硬件相关，需要终端设备提供指纹模块。	TEE 驱动 TEE 安全文件存储 TEE 加解密

上述解决方案遵循 GP 规范，保证程序通用性和可移植性。

b) 指纹技术

指纹在手机上越来越普及，指纹不仅仅是一个密钥，更是一个人的身份，基于指纹，可以支持很多高安全要求的认证，比如支付认证，商业合同签署的身份认证等。所以指纹本身在设备上的安全性至关重要。核心的安全点在于，指纹数据仅能在 TEE 环境使用，并且永不出 TEE 环境。

虹膜的使用场景和技术要点和指纹类似。

在使用场景上，以 FIDO（快速在线身份认证）这样的技术为代表，通过生物特征仅在本地 TEE 环境采集和认证，以及标准化的认证协议，很好地解决了认证过程中生物特征安全和去密码化的需求。指纹/虹膜+TEE+FIDO 在支付，车载，企业 SSO（单点登录）等涉及到安全认证的地方都有很好的应用场景。

中科创达同时也是 FIDO 联盟中主要技术提供商 NNL（NokNokLab https://www.noknok.com/ ）的投资方，拥有充足的技术储备。

中科创达提供指纹，虹膜的 TEE 移植和应用开发服务，具体包括：

服务项目	内容	技术点说明
指纹驱动和算法往 TEE 中移植	支持 QSEE，Trustonic 的指纹 TEE 移植	TEE 驱动开发 TEE 应用开发
基于指纹的应用服务（支付，FIDO 认证等）	提供基于指纹+TEE 的应用服务 包括工厂工具支持	TEE 应用开发 工具开发

c) 安全智能 TF 卡技术

安全智能 TF 卡技术，是业界比较成熟的安全技术，被广泛应用于金融，保密等领域的密钥管理，数据加密，因为支持硬国产加密以及抗物理攻击，是目前能获得安全认证等级最高的安全技术。中科创达和业界领先安全智能 TF 卡供应商伙伴（国芯，航芯等公司）合作，把安全智能 TF 卡技术和安全手机相结合，提供了包括机卡绑定，域卡绑定，卡网绑定，以及安全域（参考后面双域功能介绍）+安全智能 TF 卡+行业定制应用等众多安全场景。

安全智能 TF 卡一般可以支持硬 SM1、SM2、SM3、SM4、RSA、DES、AES 等加密算法，适合于有国密算法要求的场景。

从前面的介绍中，可以看到 TrustZone 和安全智能 TF 卡有一定的替代性，可以根据实际需要来选择用 TrustZone 还是安全智能 TF 卡，两者对比如下：

特性	TrustZone	安全智能 TF 卡

性能	优	一般
隔离性	优	优
加密强度	硬 RSA、DES、AES，软 SM1、SM2、SM3、SM4	硬 SM1、SM2、SM3、SM4、RSA、DES、AES
安全认证级别	高	超高（防物理攻击）
成本	无（CPU 支持即可）	有

以上硬件安全技术为 ThunderSec3.0 的终端安全打下坚实基础。

三、操作系统安全介绍

a) 双域隔离

针对政府、金融、运营商、能源、制造等企业的通用需求，目前 ThunderSec3.0 提供操作系统框架层隔离 + TrustZone 的双域隔离方案。中科创达从 Android4.3 开始提供双域隔离技术，已经发布了多款双域设备，目前 ThunderSec3.0 产品支持 Android4.4 到 Android6.0。其功能特点如下：

- 业务隔离：企业与个人的电话、通信录、短信、拍照等业务的隔离，保护用户隐私。安全域提供独立的应用生命周期管理，包括安装，运行，卸载，默认安全域内应用仅能通过安全应用商店提供，并支持应用推送，静默安装卸载。

- 数据隔离：不同业务工作时所产生的数据和文件均分开存储，不能互访。

- 网络隔离：针对不同的业务提供相互隔离的网络通信环境，保证通信安全，支持通过安全域级别的 VPN 和应用级别的 VPN。
- 双域间安全切换和认证：PIN，图案，密码，指纹、虹膜等，TEE 支持。同时支持多种切换入口，图标，通知栏，隐藏拨号等等。
- 安全域一致性检查：每 5 分钟对安全域自身和安全域内安装的应用进行一致性检查，检查是否有篡改行为发生，TEE 支持。
- 安全域内提供了一个独立的安全桌面，桌面程序是面向用户的门户，给用户提供区别于普通域可以显著标识的桌面体验，彻底清晰地分开个人和企业，不再混乱。
- 域卡绑定（可选），针对双 SIM 卡设备，支持一个域绑定一个卡槽，从 SIM 卡实体上分开个人和企业的电话短信通信数据。

b) 系统安全管理增强

自带设备办公(BYOD)引发了一场革新，企业如何启用安全而富有成效的移动性，这迫使以硬件为中心的移动设备管理(MDM)产品发展成为企业移动管理(EMM)套件。随着 BYOD 接受度的增强，安全移动性挑战以及 EMM 市场也在增长。根据技术研究公司 Radicati Group Inc.的研究，EMM 市场收入到 2018 年将超过 57 亿美元。

在 MDM 到 EMM 的演进过程中，需求究竟发生了什么样的变化？

MDM 的核心管理目标是设备：硬件资产管理、OS 配置（包括应用和应用配置）、以及远程发现和擦除功能，比较适用于企业配发的设备。

EMM 从保护设备转移到保护数据以及控制企业数据如何在应用间流动，从而保障数据处于静止和移动状态的安全。EMM 不仅能更好处理移动威胁，也使得 IT 部门可以只管理每部设备的企业业务部分。

中科创达搭建了 ThunderSec3.0 方案的移动设备，非常适用于从 MDM 到 EMM 对移动设备管理，并提供了众多系统安全管理增强功能，包括操作系统全局的增强以及安全域的增强。

ThunderSec3.0 软硬件一体化方案中支持的 API 如下：

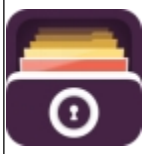
	分类	功能点	备注
Android 安全管控类 API（仅统计 Android4.0 及其以上）	动作类 API	擦出用户数据	
		锁屏	
		重新设置锁屏密码	
		安装 CA 证书	Android5.0 以及之后版本
	策略类 API	禁用摄像头	
		设置锁屏密码最低强度要求	
		设置锁屏密码规则要求	
		设置全盘加密要求	

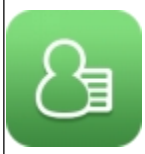
		设置屏幕固定	Android5.0 以及之后版本
		禁止卸载应用	Android5.0 以及之后版本
		禁用屏幕拷贝	Android5.0 以及之后版本
		禁用状态栏	Android6.0 以及之后版本
系统安全管控增强 API (以针对 EMM 的 API 形式提供）	安全域管理 API	激活安全域	
		擦除安全域	
		登出安全域	
		禁用安全域	
		安全域密码重置	
		安全域输入法策略配置	
	增强配置 API	VPN 配置	
		应用级 VPN 配置（VPN 池）	
		VPDN 配置	
		应用级 VPDN 配置	
		Wifi 配置	
		加密邮件配置	配合 ThunderSec3.0 提供的加密邮件应用
	增强管控 API （支持安全域和普通域配置不同的可用/禁用策略）	禁用外置 SD 卡	
		静默安装	
		设置摄像头策略	比 Android 原始策略更加底层实现，更加安全。
		设置 USB 策略	
		设置录音策略	
		设置剪切板策略	
		设置蓝牙策略	
		设置 NFC 策略	
		设置 Wifi 策略	
		设置 3G、4G 策略	
		设置截屏策略	比 Android 原始策略更加底层实现，更加安全。 Android4.0~Android6.0 均支持。
		设置共享策略	
		设置 GPS 策略	
		网络访问黑白名单	
		应用安装黑白名单	和静默安装配合
		应用禁用	（根据时间、地理围栏控制禁用策略）

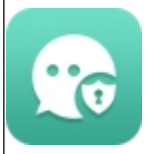
四、安全应用介绍

对企业客户而言，除了满足设备安全和设备，应用，数据的管理之外，最有价值的是切实能够给企业带来安全价值和效率价值的应用，满足企业移动办公需求和安全需求。中科创达的安全应用团队经过 3 年的积累，提供多种通用性安全应用以及满足企业办公需求的辅助办公类应用，解决了企业在移动终端上信息加密（文件，拍照，输入法等），通信加密（VPN，加密短信，加密网络电话，加密邮件等），安全办公（企业通讯录，统一认证等）这些常见的应用使用场景。同时提供 EMM 系统，接入到企业私有云，满足安全应用推送，消息推送，内容推送等现代企业云管端的需求。

附录：安全应用一览表

序号	分类	应用	主要功能	Icon
1	通用安全应用	文件保险箱	1，支持图片和文件的加密存储。 2，支持直接拍照加密存储或者导入照片、文件加密存储。 3，支持 PIN，图案，密码等多种认证方式。 4，支持 TEE 保护密钥。	
2		设备安保	1，支持绑定亲友号码来对设备进行管理。 2，支持短信通道。 3，支持远程锁屏，修改锁屏密码，发出报警声音，远程定位。 4，防恢复出厂设置和 SIM 卡更换，即使恢复出厂设置仍旧生效。（功能 4 需要和 ThunderSec3.0 定制设备配合）	

3		安全中心	1，提供电池优化管理方案，包括电量显示、系统耗电显示、各场景省电方案设置、低电量省电模式自动切换方案等，让手机更省电，拥有更长续航时间。 2，提供网络使用情况统计分析和网络优化方案，网络流量管理、手机联网管理、数据流量查询和设置等。 3，管理三方应用的通知是否弹出，包括通知中心，状态栏和锁屏 3 部分。 4，管理三方应用的是否可以自启动。	
4	辅助办公类应用（Client + Web）	安管中心	由云端和客户端程序构成，支持组织结构-用户-设备-设备中的应用和数据等整体的管控。 包括： 组织结构管理；用户和权限管理； 设备全生命周期管理；设备检测和远程控制；设备安全策略和配置推送管理； 远程推送应用程序，通知消息（短信和系统通知形式）； 信息审计。	
5		VPN 池	1、在 EMM 服务器端维护 VPN 配置，Token（分配的字符串，给使用 VPN 的应用使用，每个 Token 绑定一个 VPN 配置，VPN 配置和 token 是多对一关系），以及两者的映射关系； 2、某个应用需要使用 VPN，根据提供的 SDK 来实现 VPN 配置和连接，交给 VPN Pool 应用去执行； 3，VPN Pool 根据 token 去 EMM 服务器获得对应的 VPN 配置（支持 Android 系统支持的几种类型，包括证书类型），切换到对应的 VPN，连接过的 VPN 配置都会保存下来。	
6		统一账户	1，辅助办公包支撑应用。 2，账户管理，可以支持和客户的账户系统对接。 3，为加密短信，邮件，企业通讯录用到密钥提供身份标识。 4，为企业通讯录数据同步提供身份标识。 5，为安全应用推送提供身份标识。	

7		加密企业通讯录	1，支持云端同步企业联系人，支持搜索和字母排序 2，支持公司组织结构，可以看到各组织结构和人员 3，支持基于账户的自动同步 4，数据加密传输和存储，使用的时候解密，隐藏手机号码的直接显示。 5，在 ThunderSec3.0 定制终端上，系统拨号界面也对企业通讯录中的电话号码隐藏显示。 6，采用基于身份的非对称加密算法，在收发流程中不需要访问密钥服务器，更加安全。	
8		加密短信	1，支持中英文短信 2，同时支持明文和密文的短信，并支持混合使用。 3，采用基于身份的非对称加密算法，在收发流程中不需要访问密钥服务器，更加安全。	
9		加密邮件	1，支持 POP3，IMAP，Exchange 多种主流邮件； 2，支持自动及手动邮箱配置功能，支持 EMM 进行远程配置； 3，支持搜索，分类合并，自定义文件夹，支持单个或批量的移动，删除，标记等操作。 4，支持普通邮件和加密邮件同时显示，并指出混合使用。 5，采用基于身份的非对称加密算法，在收发流程中不需要访问密钥服务器，更加安全。	
10		安全应用推送	1，支持访问所属企业的应用，显示应用信息，类似于常见的应用商店； 2，支持应用搜索； 3，支持单个更新和全体更新； 4，支持管理员从云端后台强制静默安装，升级应用。	
11		加密网络电话	1，基于 SIP 协议的加密网络电话； 2，网络条件良好的情况下，延迟低于 1 秒； 3，可负载千人规模的企业。	
12		加密输入法	1，支持中文/英文输入。 2，通用密钥。需要和统一账户结合做密钥管理。	

五、在售设备&成功案例

当前在售旗舰设备：2015 年 TCL 旗舰设备 + ThunderSec 完整方案+EMM 管理系统

主屏尺寸：5.5 英寸

网络类型：双卡，全网通

操作系统：Android 5.0

CPU 型号：高通 骁龙 615（MSM8939）

核心数：真八核

内存：2GB

电池容量：2910mAh

后置摄像头：1300 万像素

前置摄像头：800 万像素

除了安全功能外，该手机还有如下亮点：

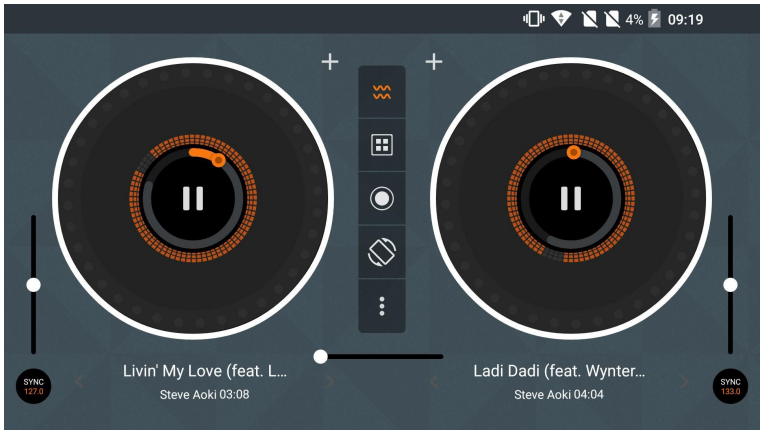
一、创新反转接听设计

正反接听的手机，通过感应重力等智能传感判断并调整手机正反位置，支持 180 度反转通话，为消费者带来特色的使用体验，从口袋拿出来后无论是正还是反，都可以随意接听。正面采用对称设计，顶部与底部都内置了双扬声器与双听筒。

二、融入精致工艺

和全球知名手机厂商 TCL 合作，在工艺上采用复杂的二次镭雕退镀工艺，让整个机身都不失金属质感。磨砂质感的后盖有效避免了指纹的残留，而且重量仅为 140g，不仅带来了美观的视觉感受，在握持手感和单手体验方面都获得了很大的提升，远看还是上手都突显出高端商务的金属质感。

三、JBL 认证 Hi-Fi 体验



通过与 JBL 的深度合作，在上下两端都设置了独立扬声器，融入 JBL 最新的音频解决方案，并有独立 DAC 的支持，使得用户在聆听音乐时达到真正 的 HI-FI 音乐体验和 IMAX 影院效果。配合媲美专业的 DJ 混音软件，自己上手制作混音音乐，一旦喜欢上真的根本停不下来。

四、1080p 悬浮阳光屏

屏幕是直接悬浮于机身之上，5.5 英寸 1080p 超高清显示屏，表面覆盖大猩猩玻璃，还加入了独特的阳光屏特性，经过强化的对比显示，超过 660nit 的亮度即使是在户外阳光充足的情况下依然可以清晰的看到屏幕上的内容。

五、NFC 与 4G 全网通

消费者对全网通功能的需求日益剧增，采用高通极速智能基带芯片，支持移动、联通、电信三大运营商 2/3/4G 网络以及全球漫游功能，提供最高 50M 上行和 150M 下行速率，看电影、玩游戏无需等待。支持 NFC，刷公交卡、移动支付就是这么方便快捷。

该设备对行业客户的定制支持：

手机后盖背壳

开关机动画

桌面壁纸及应用布局

预装应用

历史上的成功案例：

从 2014 年下半年开始，中科创达联合 OEM 合作伙伴一起为行业定制了多款安全终端，如下：

联想 Lenovo

4G 网络： 移动 4G、FDD-LTE、TD-LTE

主屏尺寸： 6 英寸

屏幕分辨率： 2560*1440 像素

系统： Android 4.4

电池容量： 4000mAH

CPU： MSM8974AC 2.5GHz（4 核） 3GB RAM

运行内存： 3GB RAM

内置容量： 32GB

酷派 Coolpad

4G 网络： 电信 4G、TD-LTE、FDD-LTE

主屏尺寸： 5.5 英寸

屏幕分辨率： 1280*720 像素（720P）

系统： Android 4.4

电池容量： 2500mAH

CPU： MSM8926 1.2GHz（4 核）

运行内存： 1GB RAM

内置容量： 8GB

TCL

4G 网络： 电信 4G、FDD-LTE

主屏尺寸： 5.5 英寸

屏幕分辨率： 540*960 像素（qHD）

系统： Android 4.3

电池容量： 3300mAH

CPU： MSM8926 1.2GHz（4 核）

运行内存： 1GB RAM

内置容量： 4GB

富可视 InFocus

4G 网络： 电信 4G、TD-LTE、FDD-LTE

主屏尺寸： 5.5 英寸

屏幕分辨率： 1920*1080 像素（FHD）

系统： Android 4.4

电池容量： 2600mAH

CPU： MSM8974AC 2.5GHz（4 核）

运行内存： 2GB RAM

内置容量： 16GB