TD Tech

泛政务移动安全解决方案

移 动 安 全 鼎 力 相 助

CONTENT

目录

TD Tech

十年耕耘，实力雄厚

TD Tech
移动安全 鼎力相助

2017年中国通信业
企业第29名
2017年中国通信产业金紫竹奖

鼎桥是华为子公司，于2005年3月
成立北京、上海、成都三地设立研
发中心

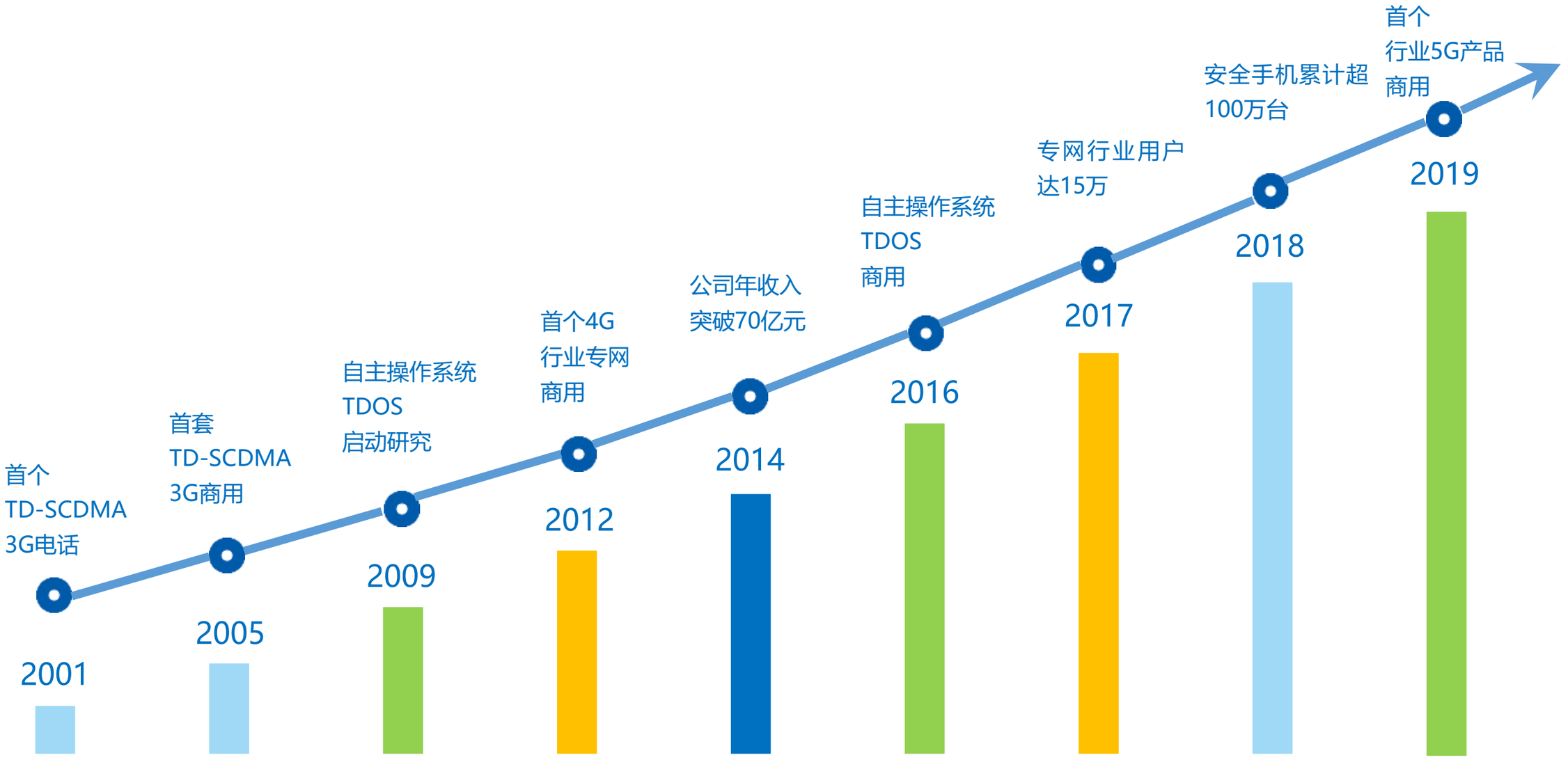
持续研发资金投入
累计超过60亿
纳税总额累计达
12亿人民币

2018年中国通信
标准化协会科学技术一等奖
2018年中国通信产业金紫竹奖
（年度安全终端领军企业）

员工超过1200人
平均年龄33岁
56%的员工拥有博士或硕士学位

砥砺前行 持续创新

TD Tech
移动安全 鼎力相助



客户认可 业绩骄人

TD Tech
移动安全 鼎力相助

公网（3G/4G）

60%
市场份额

300万
累计载频发货量

500亿+
累计销售额

专网

150个+
服务国家

500个+
建设专网

180亿+
累计销售额

安全终端

120万+
累计发货量

32个
覆盖省级行政区域

30亿+
累计销售额

技术领先，产业链贡献

TD Tech
移动安全 鼎力相助

业务覆盖公安、法院、检察院、监狱、戒毒、电力、企业多个行业领域

自主知识产权

规模应用的国产手机麒麟芯片
获得保密行业认可的自主操作系统

公安行业

公安部警务终端标准的主要撰写单位
首批通过公安部新部标检测的警务终端制造者

司法行业

司法部行政移动执法标准的主要
起草单位

CONTENT

目录

TD Tech

01 鼎桥概况

02 行业现状

03 解决方案

04 案例分享

移动政务政策

TD Tech
移动安全 鼎力相助

中华人民共和国中央人民政府
www.gov.cn

2018年国务院办公厅关于印发进一步
深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案

“拓展**政务服务移动应用**：推动政务服务向“两微一端”等延伸拓展，为群众提供多样性、多渠道、便利化服务。结合国家政务服务平台建设，加强和规范政务服务移动应用建设管理，推动更多政务服务事项提供移动端服务。”

中共中央办公厅 国务院办公厅印发
《关于促进移动互联网健康有序发展的意见》

“依托**移动互联网加强电子政务建设**，完善国家电子政务顶层设计，加快推进“互联网+政务服务” ”

背景概述 – 泛政务领域的挑战和诉求

TD Tech
移动安全 鼎力相助

- 移动终端接入办公网络的合规问题；
- 移动终端管控的合规问题；
- 移动应用管控的合规问题；
- 密码应用情况的合规问题；

《网络安全法》
《等保2.0》
《电子政务移动办公系统安全技术规范》

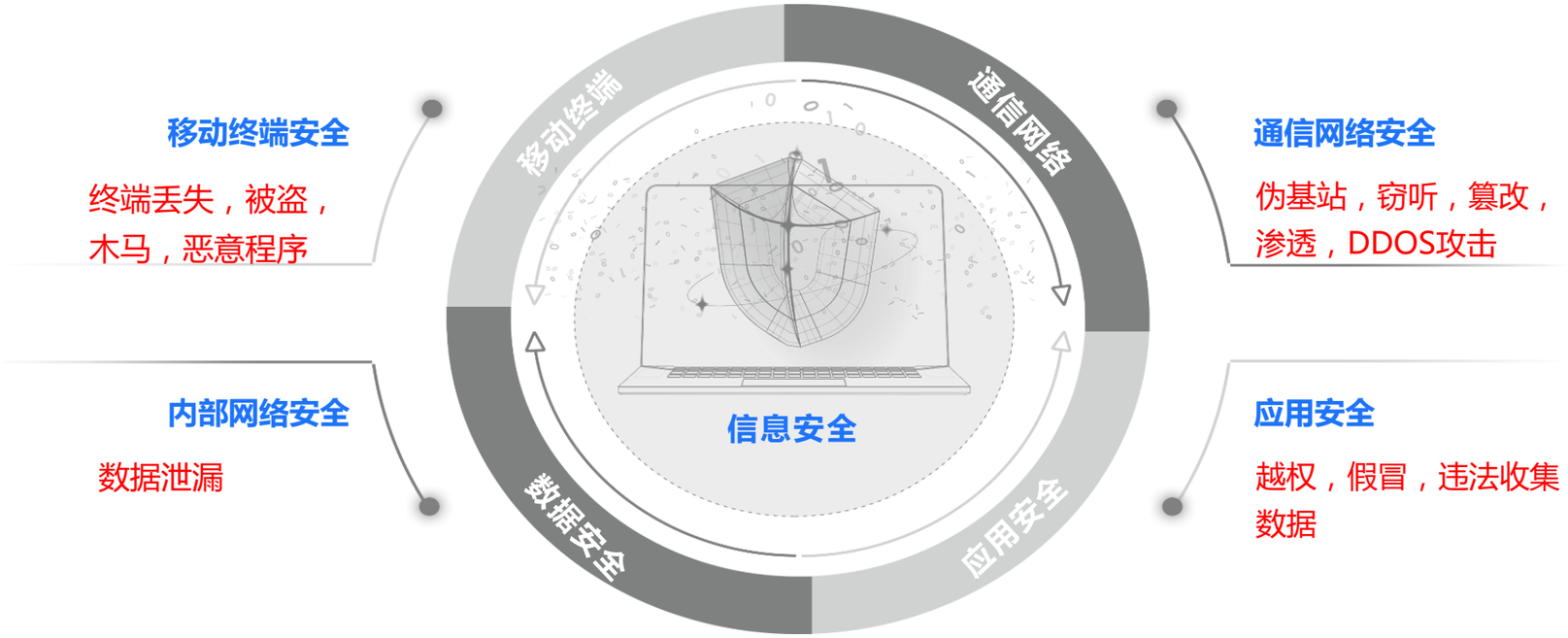
- “棱镜门”等海外势力的监听客观存在；
- Android系统漏洞及未披露后门攻击频发；
- 终端敏感数据泄密风险越来越严重；
- 假冒、恶意应用违法搜集敏感信息；

网络泄密案占政府泄密案总数的**70%**
通过网络泄密的文件资料达**70多万份**
——国家信息中心统计

- 移动政务；
- 移动执法；
- 移动办公；
- 移动作业；

合规、安全是效率提升的**必要条件**

泛政务移动办公/执法面临的安全威胁



- 终端敏感数据或信息泄漏
- 移动应用中的恶意软件利用程序后门或漏洞实现提权控制、勒索病毒等
- 无线接入被窃听、篡改或伪基站攻击
- 终端系统漏洞未及时更新
- 终端设备遗失或被盗

Source: Study on Mobile Security, DHS USA, April 2017

“合规、安全、高效”的一体化方案是移动政务的最佳选择

TD Tech
移动安全 鼎力相助

高效便捷

- 公文流转
- 日常办公
- 通信协同
- 行政执法
- . . .
- 远程会议

合规&安全

安全接入平台（VPN、APN/VPDN...）

安全合规
- 国密认证
- 符合等保三级
- 完善的安全资质

高安全性
- 国密芯片
- 双系统隔离
- 安全增强

加密通信
- 加密电话
- 加密即时通讯
- 加密邮件

深度定制
- 外设接口策略
- 应用权限策略
- 个性化定制

TD Tech

01

鼎桥概况

02

行业现状

- *政策要求*
- *挑战与诉求*
- *传统方案的问题*
- *行业趋势*

03

解决方案

- *总体方案*
- *部署模式*
- *资质证书*

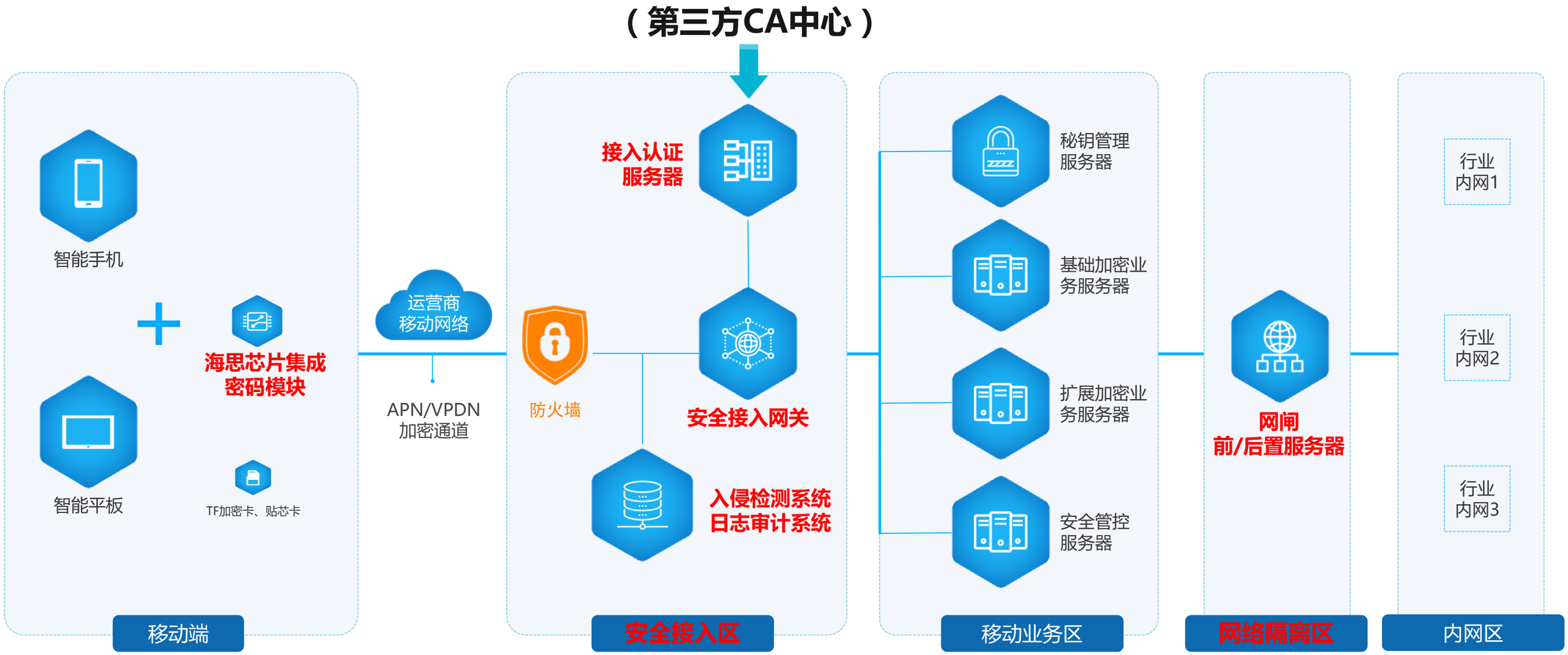
04

案例分享

- *项目背景及客户诉求*
- *客户价值*
- *交付模式*

满足合规要求 – 安全接入解决方案

TD Tech
移动安全 鼎力相助



- ✓ 通过安全传输链路，移动设备安全接入客户内网区
- ✓ 采用数字证书机制，移动终端与网关双向身份认证
- ✓ 支持接入认证服务器发证或对接第三方CA中心
- ✓ 端到端完整方案可**满足等保2.0要求**，满足政府部门相关合规要求

增强安全特性 – 系列化终端和安全特性

TD Tech
移动安全 鼎力相助

高中低档系列化手机和平板

Mate系列

Nova系列

畅享系列

MatePad Pro

M6

终端可独立支持配置的安全特性

序号	特性分类	特性描述
1	终端操作系统安全增强基本软件	防刷机
		防root
		安全启动
		内核安全保护
		全程水印（默认水印内容为空白）
		禁止用户截屏、录屏（默认不禁用）
		防止操作系统境外非受控IP访问
		客户化开机动画预置、客户化桌面预置、客户化铃声预置
		客户化专用APN预置，并提供APN的防删除、防增加、防修改功能
		客户化的应用预置和应用裁剪，并提供所预置应用的应用保活、应用防删除、进程防冻结
		第三方应用适配和调测的配合
		第三方应用权限提升，默认赋予第三方应用权限
2	终端双系统特性软件	一套硬件上运行两个系统，两个系统同时在线，相互隔离，一键切换
3	终端隐私三防特性软件	实现防跟踪防窃听功能特性，支持隐私模式下关闭听筒、摄像头等输入接口和位置服务，避免用户在不知情的情况下被窃听、偷拍和定位
4	可信度量模块	系统可信度量及签名验签功能

增强安全特性 – 终端整体安全方案

TD Tech
移动安全 鼎力相助

终端安全方案

数据安全
Dat
全盘/文件夹加密 | 安全擦除 | 全程水印 | 防窃听、防跟踪、防定位

应用安全
APP
应用可信度量 | 应用权限管控 | 应用防杀保活

操作系统安全
OS
双系统安全隔离 | 系统安全裁剪 | 内核完整性保护 | 安全启动
MDM设备管控 | 可信安全机制 | 安全升级
TUI可信服务 | 芯片加密代理 | 证书管理服务 | 安全存储服务

硬件安全
Kirin
CPU | Modem
硬件RoT: eFuse电路 | 硬件密钥
芯片集成密码模块: 警务通加密 | 麒麟芯片加密

通信安全
VoIP 加密通话
VoLTE 加密通话
VPN 加密传送
跨设备 安全互联

通信
- 客户专用APN预置及VPN通信机制，确保通信链路的机密性和完整性
- 可选的语音加密通信机制（VoIP/VoLTE等）

数据
- 数据及文件加密存储，确保数据机密性和完整性
- 安全擦除和远程擦除，确保手机意外丢失后的数据有效清除
- 全程水印和禁止用户截屏/录屏，防止敏感信息泄露

应用
- 客户化的应用预置及应用裁剪，提供应用保活、防删除、防冻结机制
- 应用签名验签和白名单机制，确保合法应用才能安装和运行

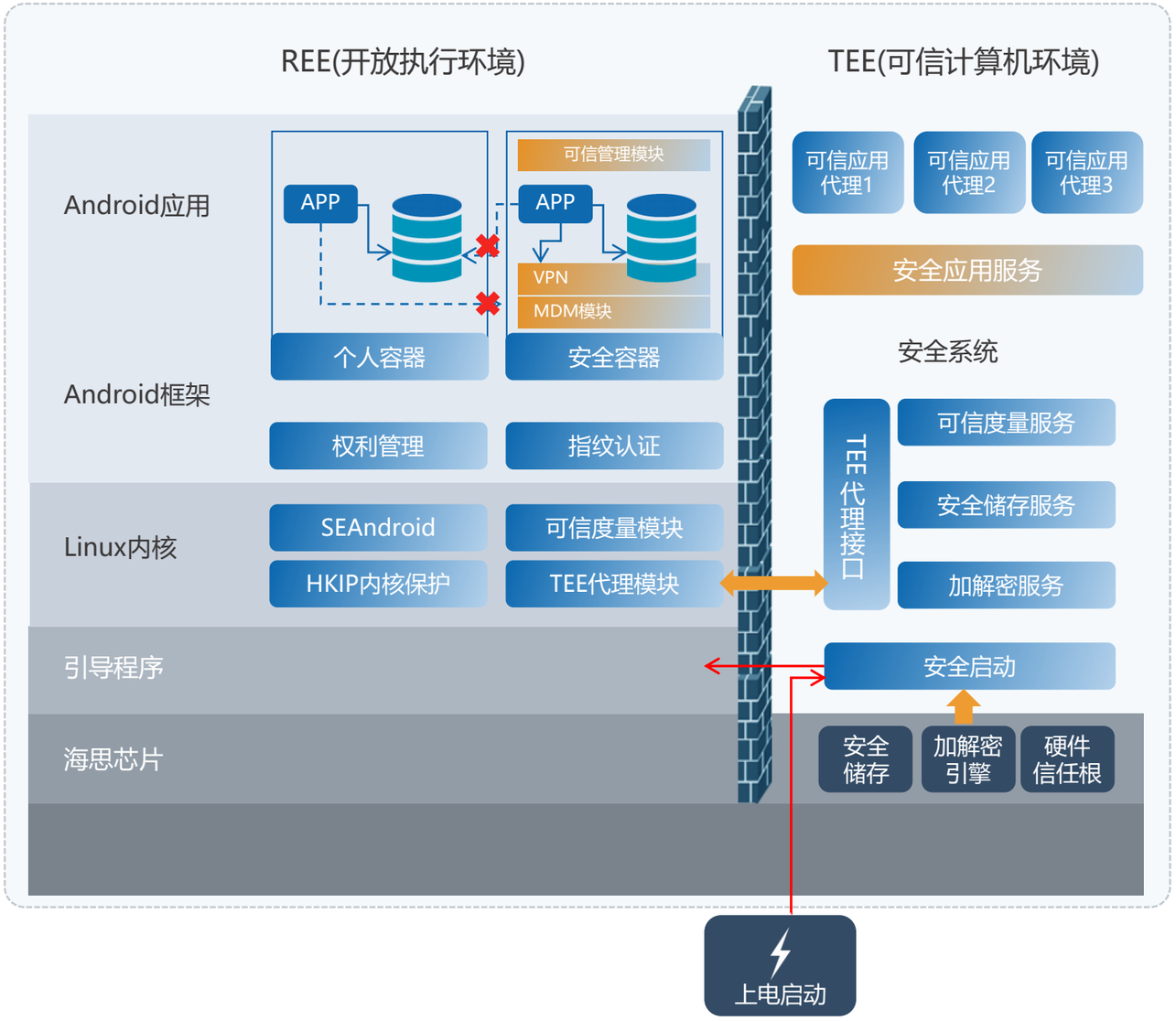
管控
- MDM管控框架和接口（GA/T1466.2部标，国内行业事实标准）
- 典型外设接口的远程管控措施

操作系统
- 基于自主芯片的安全启动机制，实现信任链完整覆盖
- 采用完整性保护、安全加固和可信度量等措施保证操作系统安全
- 可选双系统架构，一套硬件同时运行两个Android系统，兼顾互联网工作区和内网工作区，互相隔离、一键切换
- 操作系统定制裁剪，非受控海外IP地址自动发包禁止
- 防刷机、防Root、专用OTA升级

硬件
- 基于海思芯片硬件密钥和eFuse电路，构建芯片唯一、不可篡改的信任根（RoT）
- 芯片集成密码模块和TEE可信执行环境，提供密码和证书服务

增强安全特性 – 终端操作系统安全机制

TD Tech
移动安全 鼎力相助



- 基于海思芯片硬件密钥和eFuse电路，构建芯片唯一、不可篡改的信任根（RoT）
- 安全启动机制，从上电开始，覆盖引导程序、启动镜像、系统内核、应用程序，信任链覆盖全流程
- 采用包括内核地址随机化、内核模块签名和校验、内核完整性保护等多项技术保护操作系统
- 通过可信度量机制实现对内核、驱动和应用的完整性度量、保护与审计
- 操作系统定制裁剪，非受控海外IP地址自动发包禁止

增强安全特性 – 终端双系统架构特性

同时兼顾内网和互联网工作业务

双系统，双APN同时在线

后台系统收到消息会通知前台系统

内网工作区和互联网工作区各自的存储文件相互不可见

安全系统可对文件/文件夹进行加密安全保护

安全系统可对硬件驱动限制，防止数据泄露

支持一键切换，独立指纹识别切换，NFC感应切换

增强安全特性 – 终端防止操作系统境外非受控IP访问

TD Tech
移动安全 鼎力相助

内网工作区彻底清理google服务及残余代码

内网工作区清理原有预置的程序及代码，只预置客户需要的程序

内网工作区预制专用APN，该专用APN是运营商特别为用户分配的，运营商网络根据该APN信息，只会将内网工作区的信息路由到用户内网，不会路由到其他任何地方

不允许用户增加、修改或删除APN，这样就确保了内网工作区只能和用户内网进行信息交换

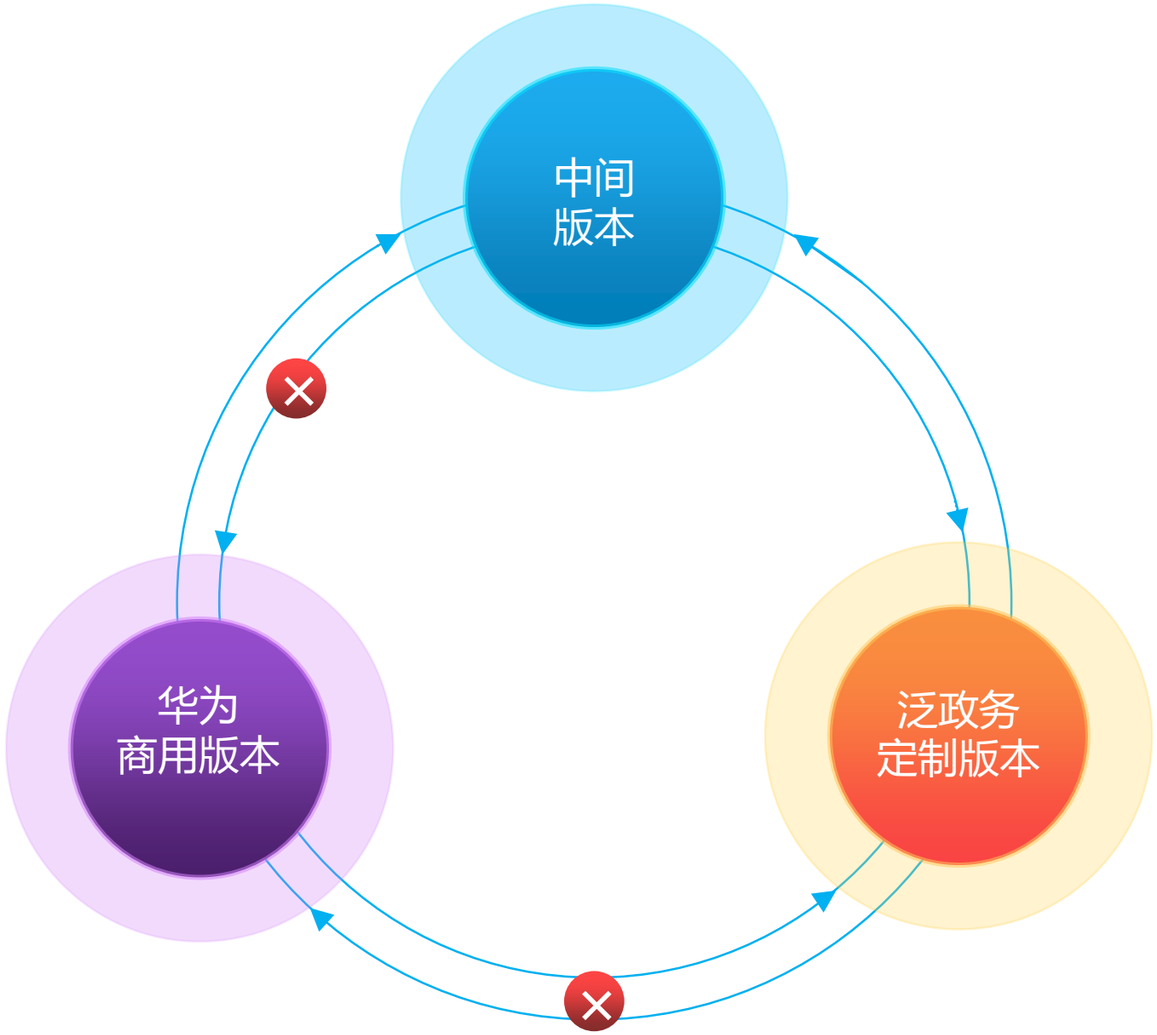
APN探测机制，系统会主动探测所采用的APN，如果非法，则自动中断网络连接，进一步防止用户通过非法APN上互联网

IP地址黑/白名单

可配置（一般是通过MDM系统，从网络侧下发配置到手机生效）内网工作区操作系统所能访问的IP地址池

可配置内网工作区操作系统所不能访问的IP地址池

增强安全特性 – 终端安全升级，防止私自刷机



签名认证的机制

确保只有合法的版本才能被升级，也就是除了专用的泛政务定制版本外，其它任何非法版本都无法通过签名认证；

版本树校验

从普通商用版本到泛政务定制版本，过程不可逆的，防止工作用机改为私人用机；

可选内网专用OTA升级（选购）

增强安全特性 – 终端全程水印 安全个性

在国防涉密单位和保密部门、重点行业、企业单位的保密及信息泄露管理工作中，屏幕偷拍泄密成为失泄密管控的防范重点。

全程水印功能:是在手机屏幕上显示可以定制的内容（图片或者是文字），只要亮屏，该水印图案就会显示在手机屏幕的最顶层，不会被任何其他应用遮挡。

安全性：手机的屏幕被拍照了，可以根据水印信息找到对应的组织或者人，做到有据可查。

个性化：提供专属定制，企事业logo，个人信息等

增强安全特性 – 终端隐私三防特性

TD Tech
移动安全 鼎力相助

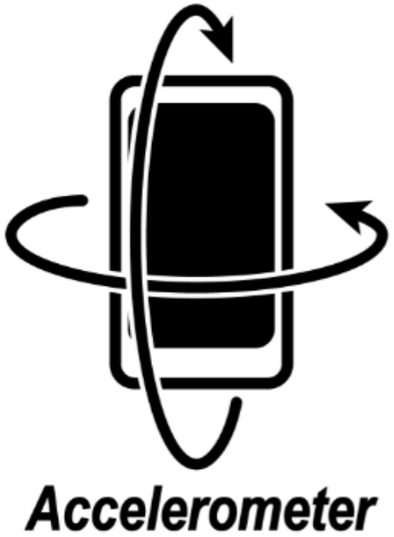
隐私模式

正常模式

通过系统安全定制，实现隐私模式下关闭听筒、摄像头等输入接口和GPS位置，实现防窃听、防定位，确保隐私安全

增强安全特性 – 加速度传感器防窃听特性

TD Tech
移动安全 鼎力相助



手机加速器用途

- 功能包括运动检测，失重检测，姿势识别，用于用户测速、记录步数和游戏等应用

被证实窃听漏洞

- 近日，浙江大学网络空间学院院长任奎团队、加拿大麦吉尔大学、多伦多大学研究团队共同发表了一项聚焦智能手机窃听攻击的研究成果：智能手机App可在用户毫不知情时，利用手机内置的加速度传感器实现对用户语音的窃听，且准确率达到90%。
- 上述研究发现，在无需系统特别授权的情况下，智能手机App通过加速度传感器采集手机扬声器所发出声音的振动信号，就可实现窃听。

鼎桥通过系统安全定制，实现加速度传感器防窃听特性，确保隐私安全

增强安全特性 – 终端按需定制能力

TD Tech
移动安全 鼎力相助

鼎桥拥有华为授权的产品源代码，除提供具备身份标识能力的轻度定制外，
还可以根据客户需求提供系统级深度定制。

个性化定制

- 可定制开机动画、开机logo、铃声、桌面壁纸、锁屏壁纸
- 可根据用户需求定制特殊按键功能，如长按音量下键可报警

应用预置

- 可进行应用预制及保活，保障应用不被系统冷冻、杀死
- 可给予预制应用开机自启动、关联启动及其他系统权限
- 可删除系统原生应用，保持纯净应用桌面
- 可设置应用安装策略，防止用户非法安装应用

外设管控

- 可使能或禁用Bluetooth、WiFi USB、NFC、GPS对外连接功能
- 可使能或禁用通话、短信、相机录音机、截屏、录屏功能

部标规范

- 支持公安监控组件接口规范，配合统一的后台管理系统，实现全生命周期安全管理
- 境外IP访问控制，防止手机底层服务向境外Google服务器发送信息

增强安全特性 – 端到端安全管控解决方案

TD Tech
移动安全 鼎力相助

设备管理

提供激活、外设接口、设备安全、合规性、锁定/解锁、数据擦除、淘汰等的终端设备的安全管理

机卡绑定

机卡绑定， 杜绝私自删除或关闭管控功能

权限控制

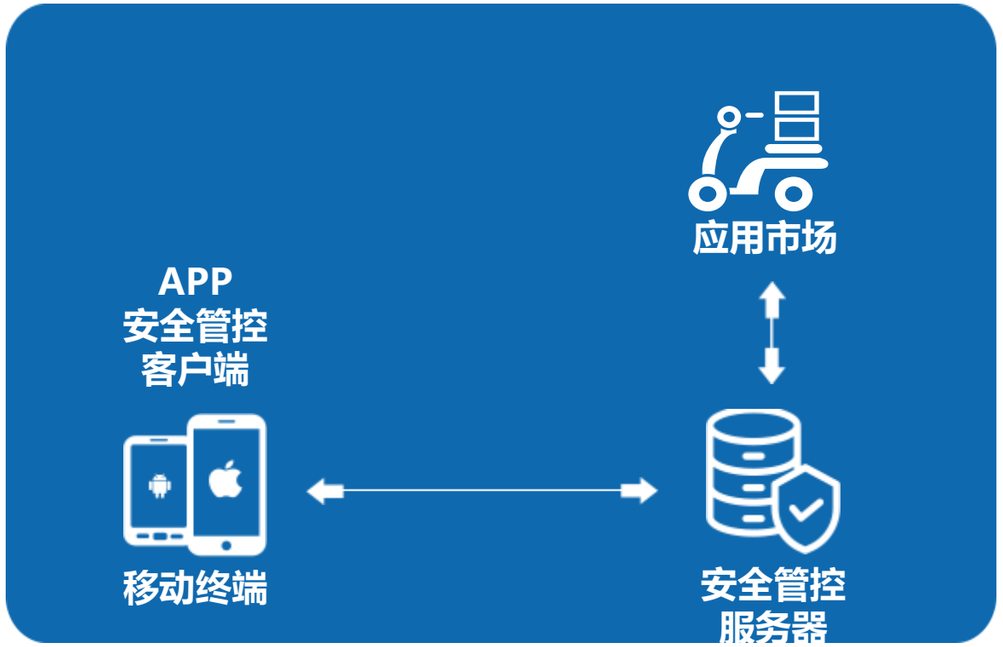
禁止卸载、禁止安装、禁止运行、黑白名单、权限管理、数据防泄露...

应用商店

应用发布、定时推送、静默安装、替换/升级、应用下架、禁用使用、远程清除数据、远程卸载...

应用统计

支持对应用进行监控，应用安装分析、应用策略分析



数据防泄漏

- 防复制
- 防截屏
- 数据加密
- 数据删除

提供终端设备全生命周期管理，提供一揽子安全应用管理方案

提升工作效率 – 基础加密业务解决方案

TD Tech
移动安全 鼎力相助

密码方案：麒麟集成密码模块（国密SM2 /3 /4）

加密输入法

支持**微信加密**以及钉钉、Whats App等国内外各类即时通信工具的加密

加密通话

支持VoIP加密通话或VoLTE加密通话端到端加密，一话一密，有效防止监听和窃密

加密储存

支持手机中的图片、视频、音频文件和拍照、录像、录音加密保存，保护您的隐私不被窥视

加密IM

专用加密即时通信工具，信息加密传输，自动解密显示

提升工作效率 – 扩展加密业务解决方案 – 既有业务加密

TD Tech
移动安全 鼎力相助

终端侧

既有办公系统

安全增强SDK

手机

平板

平台侧

终端授权管理

密钥管理

远程销毁密钥
和擦除数据

即时通信加密

音视频通话加密

邮件加密

文件存储加密

办公流加密

方案介绍 – 产品资质

TD Tech
移动安全 鼎力相助

资质证书

获得公安部，工信部，
中国信息安全认证中心
的权威认证

公安部手持式移动警务双模式终端认证 | 可信移动办公终端认证 | 工信部5级安全认证 | IT产品信息安全认证 | 安全加固双系统测试

密码证书

获得国家密码管理局的商用密码证书：

- 终端芯片麒麟990的商用密码证书
- 手机数据传输和存储加密模块密码证书
- 贴片IC卡加密证书

CONTENT

目录

TD Tech

01 鼎桥概况

02 行业现状

03 解决方案

04 案例分享

方案介绍 – 上海电信政务手机项目

TD Tech
移动安全 鼎力相助

项目背景

上海电信政企部通过加密手机拓展了15万政府部门用户，由于需要在手机上进行更多的工作相关数据的处理，用户在合约到期换机时提出了更高的手机安全性要求， 由于是公司重点保障的VIP用户，上海电信希望通过合规、安全的方案提高客户工作效率。

客户诉求

减少数据泄露风险，放心使用移动终端业务

解决方案

搭建安全管控平台，统一管理终端并进行策略下发
支持文件加密，密码安全增强，手机和SIM对应的机卡绑定，远程数据销毁，远程手机锁定/解锁

客户价值

提高手机使用安全性，防止用户数据泄露
手机安全性提升后，提高了使用手机处理工作业务的频次，提升了工作效率

提升手机安全性手段

远程锁定

手机临时丢失，锁定手机防止其他人使用，还可以在手机找回后解锁手机，正常使用

数据销毁

手机永久丢失后，远程销毁手机上的用户数据，避免数据泄露

密码增强

设定锁屏密码输入失败次数和锁定时间，避免其他人尝试手工解锁手机

文件加密

所有用户数据进行文件加密，防止拆卸存储芯片读取用户数据

安全终端管控平台

案例分享 – 湖南省纪委移动监务

TD Tech
移动安全 鼎力相助

合规、安全、高效

项目背景及规模

- 之前省内没有统一的移动终端接入平台，各级单位的移动办公、办案普及率及效率不高；
- 根据可需求，鼎桥参照等保三级要求，为省纪委提供统一安全接入方案，并配备双系统安全增强终端设备，适配业务应用，打造了全省范围内的统一办公、办案平台。
- 项目于一期交付省委直属机关620台Mate30双系统安全终端、全省统一接入平台1套，二期各地市将会基于此方案进行建设，总量预测在2~3万台。
- 鼎桥泛政务方案解决了客户的全省统一接入、业务隔离、加密通信的痛点诉求，获得了客户的高度好评。

客户价值

- 合规合法：整套方案遵循“等保2.0”三级要求进行建设，保证合规问题。
- 保安全：方案建设从终端安全、接入安全、数据安全、通信安全、应用安全等体系化安全的角度出发，保证了移动办公、办案整套业务的信息安全。
- 提效率：在合规和安全的前提下，为客户提供了全省统一的整套“监务通”应用的移动化适配移植，让客户可以随时随地的进行移动办公、办案，大大提升客户的工作效率；


THANKS
TD Tech®
移 动 安 全 鼎 力 相 助