

# 坚持自主可控，发展智能手机安全产业

中国电子科技网络信息安全有限公司

2016年10月

# 目 录

## CONTENTS

一

智能手机面临的安全威胁

二

智能手机安全技术分析

三

智能手机安全产业分析

四

发展自主可控智能手机安全产业

# 01

## 智能手机面临的安全威胁



## 1.1 智能手机应用广泛

根据eMarketer数据，2015年全球智能手机用户首次超过人口的十分之一，达19.1亿；预计2016年智能手机用户增长12.6%，达到21.6亿；到2018年，全球三分之一的消费者将成为智能手机的使用者。其中，**中国智能手机用户预计在2016年超过6亿**

智能手机的爆炸式普及，不仅带来通信领域的革命，也从生活、工作、社交、信息等多个渠道影响着人们，使**社会生活模式发生了巨大变化**。智能手机汇聚人们的各类信息和活动，俨然成为人类社会活动的缩影



## 1.2 智能手机安全问题日趋严峻



### 安全威胁

- 病毒、木马、恶意应用，窃取用户信息
- 利用操作系统漏洞和后门，非法访问、获取、篡改用户信息
- 无线攻击，窃取用户信息

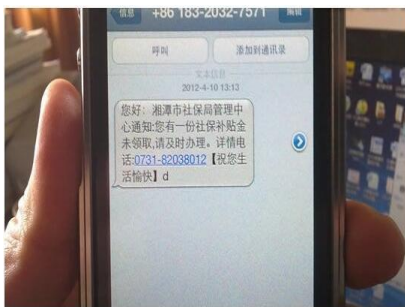
### 安全形势

- 每3个智能手机用户，就有1人曾遭受手机安全危害
- 2016年2季度，新增恶意程序样本426万个，累计监测智能手机用户感染恶意程序6180万人次
- 智能手机平均存在10-20个已知安全漏洞，后台消息、签名漏洞、短信欺诈、后台电话4类严重漏洞几乎存在于所有智能手机中





## 1.3 智能手机安全后果严重



### 账户被盗，财产损失严重

已发生多起手机中木马，银行卡被盗刷案件



### 个人隐私资料被窃取

国内、好莱坞多名明星手机内隐私资料被窃取



### 重要通信内容被窃听

希腊包括总理在内的100多名高官，手机被窃听长达一年



### 位置信息泄露

因手机暴露位置，“基地组织”二号人物被美军击毙

# 02

## 智能手机安全技术分析



## 2.1 智能手机安全技术

---

智能手机汇聚越来越多的敏感信息，任一安全事件经由智能手机都会被极大放大。智能手机安全已受到用户和业界的广泛关注，目前解决智能手机安全问题的措施主要分为以下几类：

- **操作系统安全防护**：TEE（可信执行环境）、安全APP、操作系统安全加固等
- **核心硬件防护**：SE（安全元件）、安全模块、处理器安全模式等
- **关键数据加密**：存储数据加密、通信数据加密等

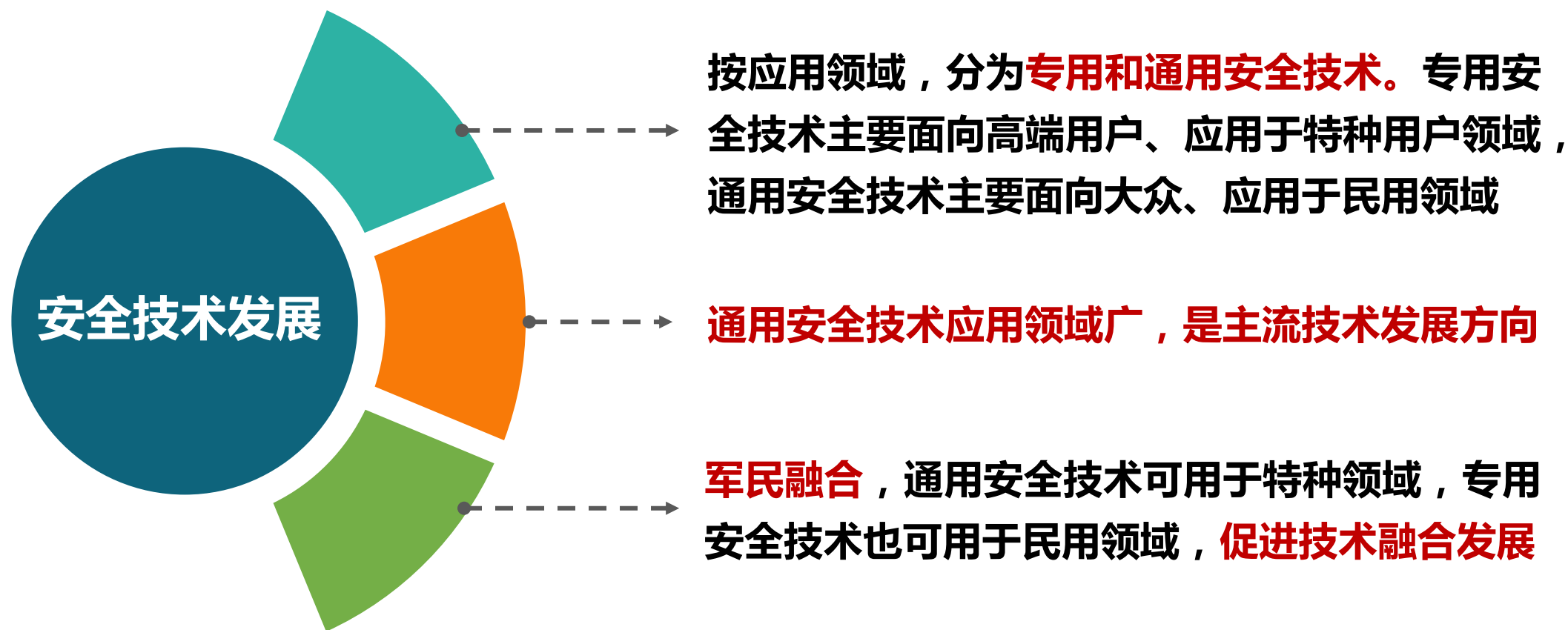


## 2.2 安全技术分析

目前主流的智能手机安全技术有SE、TEE、加密通信、安全APP等

| 安全技术            | 主要技术           | 应 用       | 特 点            |
|-----------------|----------------|-----------|----------------|
| SE<br>(安全元件)    | 密码芯片/模块，可信计算   | 移动支付/手机安全 | 安全性高；定制化安全应用   |
| TEE<br>(可信执行环境) | GP提出。“硬+软”安全   | 移动支付      | 标准、开放、通用；安全风险  |
| 加密通信            | 密码/芯片模块。专用基带芯片 | 特种及高端商务   | 应用受限（网络、终端、配对） |
| 安全APP           | 行为分析。操作系统安全    | 个人/企业/政府  | 应用层安全；应用广      |

## 2.3 安全技术发展



# 03

## 智能手机安全产业分析



## 3.1 产业基本情况

智能手机安全产业主要集中在安全手机、加密手机、安全移动支付、安全APP等领域



**安全手机**

应用广，厂家和产品多，竞争激烈，未形成著名品牌，TEE技术国外垄断局面正在被打破



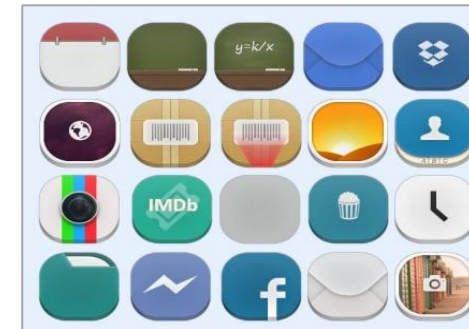
**加密手机**

市场需求相对较小，厂家和产品不多，尚未形成规模产业，重点关注通信安全，执行环境安全性不强



**安全移动支付**

应用广、规模大，核心的SE芯片被国外厂商垄断；2015年交易规模近10万亿元



**安全APP**

应用最广、规模最大；主要涉及应用安全。2015年活跃用户近5亿

## 3.2 安全手机基本情况

### 安全手机基本情况

#### 应 用

主要用于个人及商务领域，以敏感数据安全和应用安全为重点，如交易信息、财产信息、个人图片视频、通讯录、应用锁、防盗、防病毒木马等，支持通用性较强的IP化加密语音通信等功能

#### 市 场

需求量大，应用限制少（政策、网络、芯片、配对），便于推广

#### 技 术

通用安全技术，推广制约因素少（无特定网络和基带芯片）。技术封闭，标准化程度低，难以形成产业链。随着TEE的逐步普及，将为智能手机提供标准化、开放性的安全应用环境和平台

#### 研发生产

定制化，周期长，成本高；品种单一



## 3.3 加密手机基本情况

### 加密手机基本情况

#### 应 用

主要用于特种和高端商务领域，以通信安全为重点，如加密语音、加密短信、加密视频等，支持部分敏感数据安全和应用安全功能

#### 市 场

需求相对较小，应用制约因素较多（政策、网络、芯片、配对），推广受限

#### 技 术

采用专用安全技术，研发生产难度大，周期长，推广受限（需特定网络和基带芯片）；技术封闭，标准化程度低，难以形成产业

#### 研发生产

采用定制化研发生产模式，周期长，更新慢，成本高，品种单一

## 3.4 市场情况

随着手机安全事件的频繁发生，信息安全已成为智能手机的“刚需”



2016年手机安全活跃用户将超7亿



需要更安全、更可靠的措施保护支付等个人隐私信息，应对日益严重的高技术安全威胁



随着国家信息化发展战略的不断推进，政府和行业用户安全需求旺盛，急需解决以智能手机为代表的移动终端的应用安全问题

## 3.5 产业发展分析（1）



### 智能手机安全产业市场前景分析

据调查，随着5G时代的到来，智能手机将围绕个人工作、生活全场景展开，人们将感受智能手机带来的全联接体验，未来智能手机市场约在**3300亿美元**以上

层出不穷的智能手机安全事件，催生巨大的智能手机安全产业市场空间，这些市场有待信息安全企业前去开拓。智能手机安全产业**将是信息安全的重要方向**

## 3.5 产业发展分析（2）



**核心技术是产业发展的重要基础**

核心技术是产业发展的核心竞争力，是产业壮大的重要基础

智能手机安全产业发展**必须掌握SE、TEE等核心技术**，掌握竞争和发展的主动权，为满足公众的手机安全需求提供强大的技术支撑。

## 3.5 产业发展分析（3）



### 平台化是产业发展的重要保障

传统的定制化研发生产模式，周期长、更新慢、成本高、品种单一，是制约智能手机安全产业规模发展的重要瓶颈

**平台化模式**可大大缩短研发生产周期、降低成本，利于整合产业链、吸引上下游和第三方企业参与，**促进智能手机安全产业壮大**



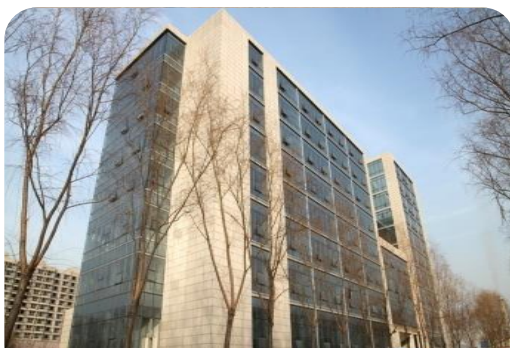
# 04

## 发展自主可控智能手机安全产业



## 4.1 中国网安相关情况（1）

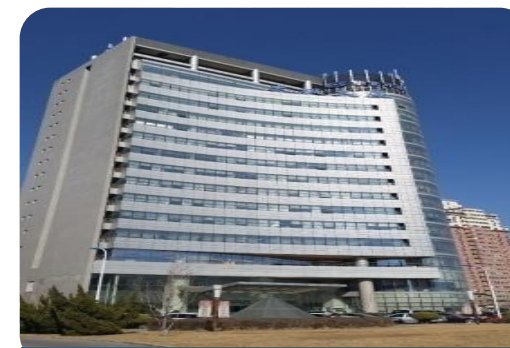
中国网安是中国电科集全集团之力，整合内外资源打造的国家级网络信息安全技术、人才和产业平台，是支撑国家网络空间安全战略、引领技术创新、推动产业发展、**唯一冠以中国字头的网络信息安全旗舰企业**



中国电科三十三所  
电磁防护、轨道交通安全



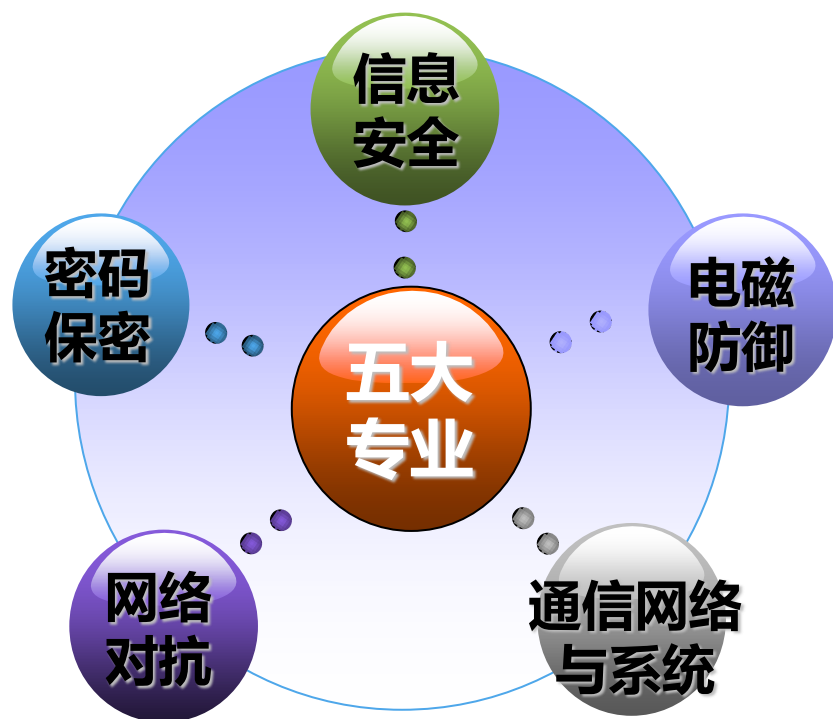
中国电科三十所  
网络信息安全核心资源



中电科技（北京）公司  
计算机可信固件

## 4.1 中国网安相关情况（2）

中国网安融合**密码保密**、**信息安全**、**通信网络与系统**、**网络对抗**、**电磁防御**五大核心专业，以网络空间安全研究院为创新平台，打造涵盖理论、算法、芯片、产品、系统、服务的完整信息安全产业链，引领国家及行业网络信息安全技术发展



- 拥有最完整的安全密码产品体系和相关资质
- 一流的信息安全产品、服务与整体解决方案提供商
- 战略和战术通信系统主要技术和产品提供商
- 网络对抗技术和产品主要提供商
- 国家国防电磁防御工程建设的中坚力量

## 4.1 中国网安相关情况（3）



### 加密手机与安全手机

自**1998年**以来，中国网安组建专门机构（瑞通公司、移动互联网事业部），整合内部优质资源，与国内多家知名手机厂商和运营商开展了广泛合作，在专用和通用领域先后推出**4代加密手机和安全手机**

### 4.1 中国网安相关情况（4）



1 数字前端设计能力

2 数字后端设计能力

3 模拟电路设计能力

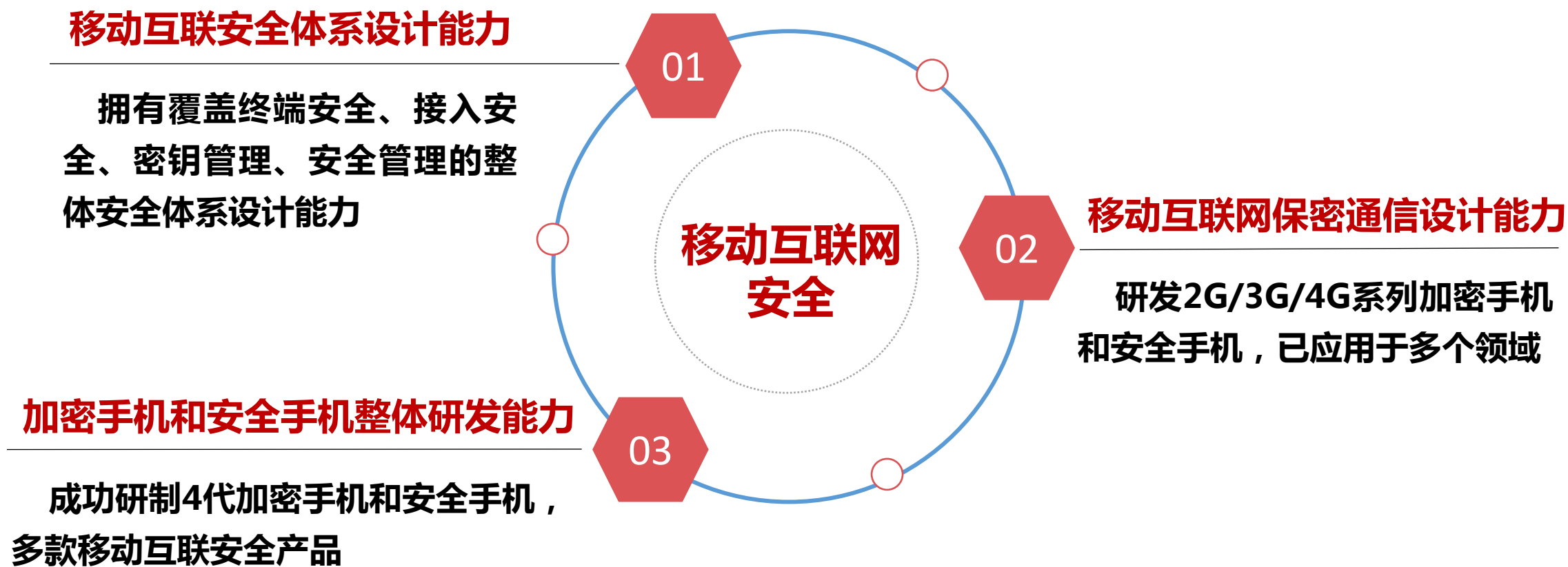
4 软件及应用方案设计能力

#### 安全芯片

中国网安组建专门机构（嘉微公司）从事安全芯片的开发、测试、销售与服务，具有全流程的自主开发能力。



## 4.1 中国网安相关情况（5）



## 4.2 自主可控智能手机安全产业

根据国家网络安全战略规划，结合产业发展需要和网安公司在相关领域的实践，我们认为，规模发展智能手机安全产业应具备以下两个条件：

- 1) 产业发展关键技术和产品必须**自主可控**
- 2) 安全技术和产品必须形成**通用、标准、开放的平台**



## 4.3 产业发展需满足的条件

### 智能手机安全产业发展的必要条件

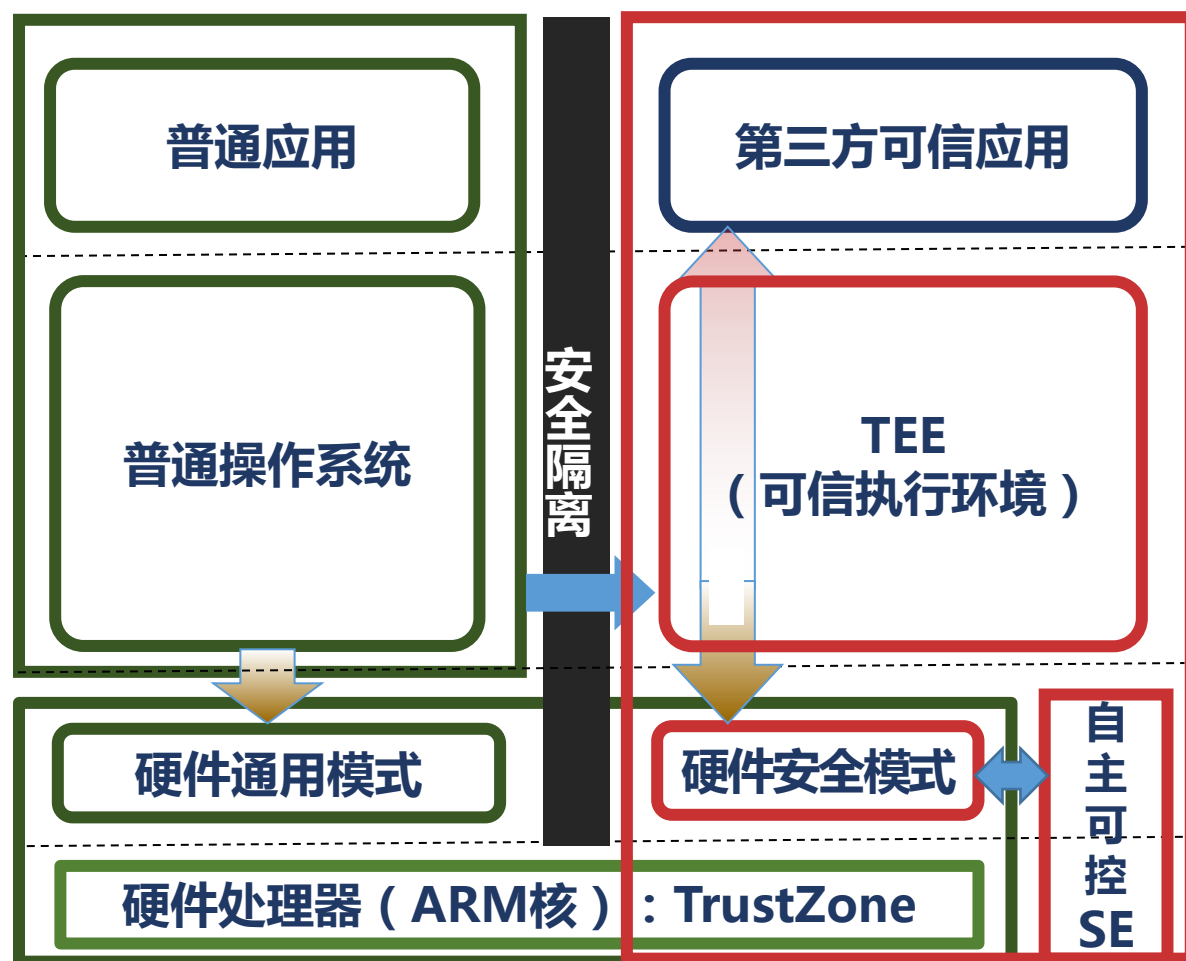


## 4.4 自主可控安全元件



立足国内骨干科研院所和安全企业，整合优质资源，着力提升在智能手机安全元件芯片设计、流片等关键环节的自主可控能力，研发满足大多数用户多样化安全需求、性价比高、**自主可控**、高安全的**安全元件芯片**，为智能手机提供执行环境和各种应用的高可信支撑，为智能手机安全产业的规模发展**提供基础保障**

## 4.5 自主可控可信执行环境



立足国内骨干科研院所和安全企业，整合优质资源，着力提升智能手机操作系统安全技术能力，研发**自主可控**、通用、标准、开放的**可信执行环境**产品，为智能手机各类应用提供较安全的执行环境，为智能手机安全产业的规模发展**提供支撑**



## 4.6 自主可控智能安全手机（1）

安全元件SE安全性好、性价比高，存在资源有限、应用受限等问题；可信执行环境TEE通用性好，具有较高的安全性。但由于缺乏硬件可信根的支撑，存在一定安全风险，在部分应用领域受到限制

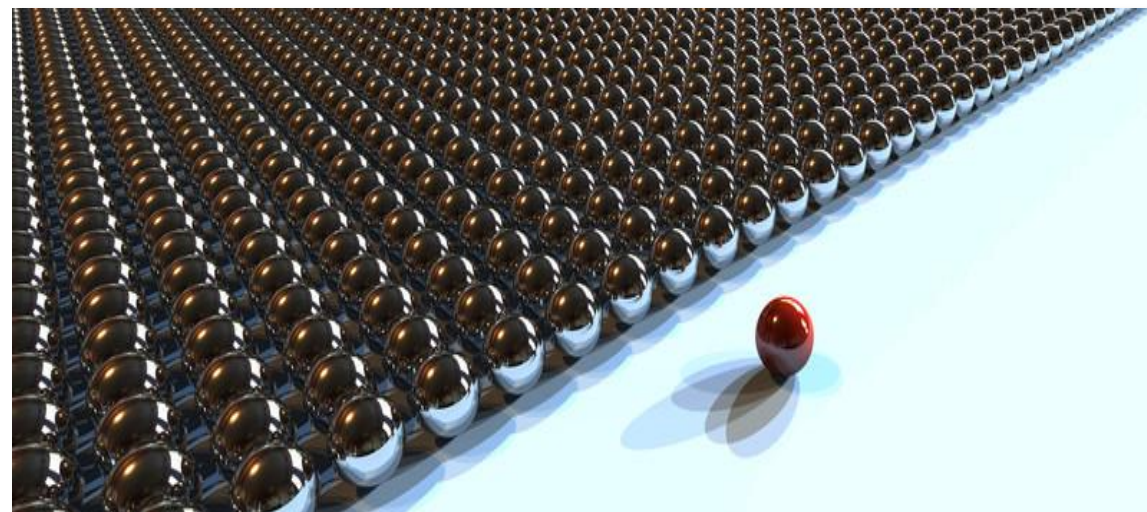
融合国产自主可控的SE芯片和TEE软件，打造平台化的智能手机安全平台（**国产化+SE+TEE**），可广泛应用于各种智能安全手机的研发和生产，具有安全性好、性价比高、通用性强、研发周期短等特点，满足大多数用户的多样化安全需求，是**发展自主可控智能手机安全产业的有效途径**



## 4.6 自主可控智能安全手机（2）

### 安全平台应具备的能力

- 1) 支持不同厂家硬件平台（ARM核）和富操作系统（Android等）
- 2) 保护数据安全，如移动支付、隐私保护、内容管理、企业应用等多类型安全应用
- 3) 提供第三方应用安全开发标准接口



### 安全平台应具有的特点

- 1) 通用化设计，适用于各种智能手机平台（除苹果）
- 2) 平台化设计，符合国际标准，效率高，功能较强
- 3) 开放性设计，支持各类第三方应用安全开发
- 4) 重点保护数据安全和应用安全，需求大，易推广



## 4.7 安全平台目标用户与应用

### 安全平台用户

- 智能手机安全厂商



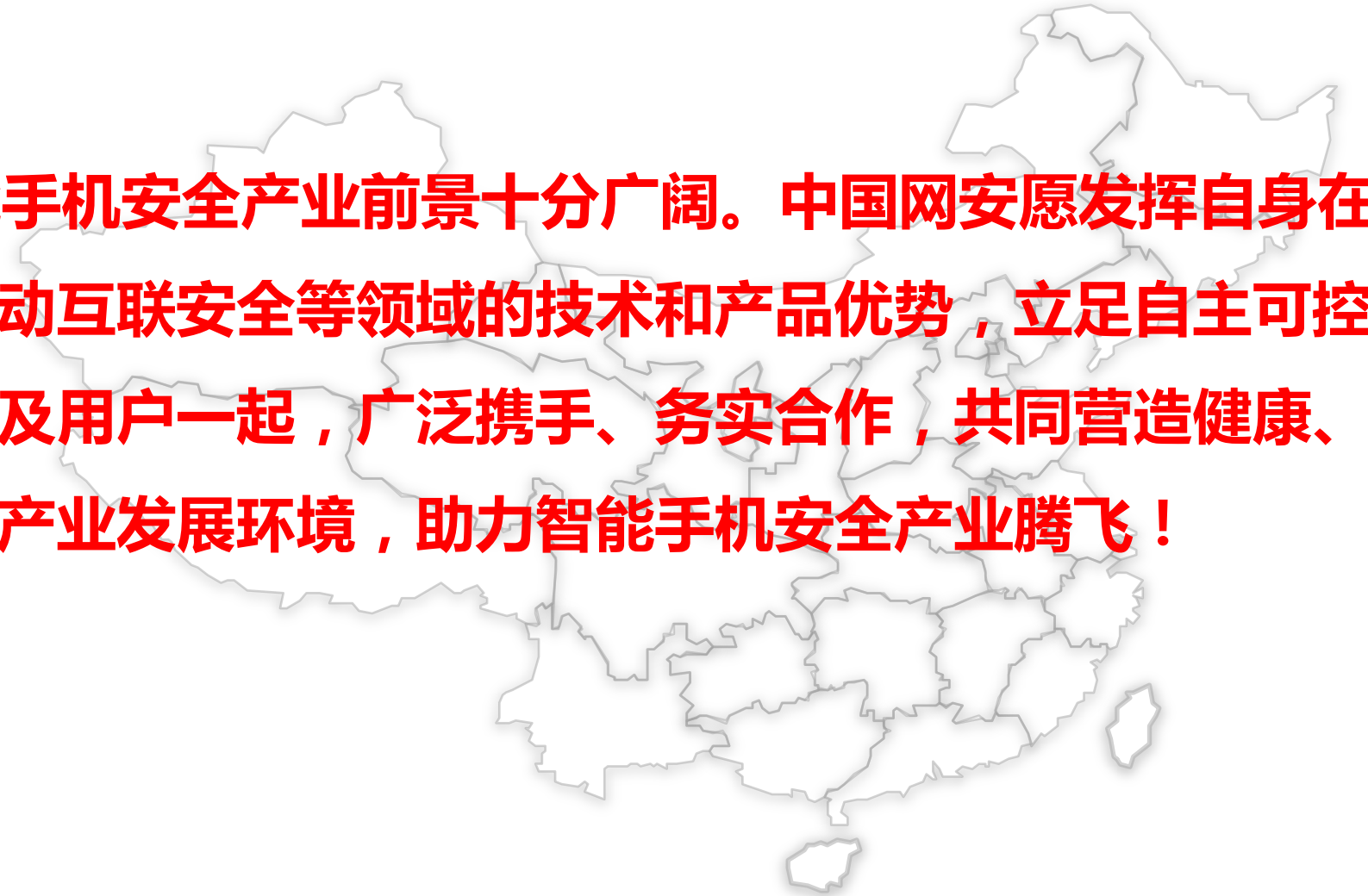
### 安全平台应用

- 公众：移动支付、服务发布、隐私保护、内容管理等各类安全需求
- 行业：行业安全应用
- 政府：政府治理



## 结束语

---



**智能手机安全产业前景十分广阔。中国网安愿发挥自身在安全芯片和移动互联安全等领域的技术和产品优势，立足自主可控，与行业伙伴及用户一起，广泛携手、务实合作，共同营造健康、安全、有序的产业发展环境，助力智能手机安全产业腾飞！**



CETC

中国网安 网安天下