

# 移动接入与监测 安全认证体系研究

北京信安世纪科技有限公司

张庆勇



移动互联网安全威胁与风险

移动互联网安全接入技术

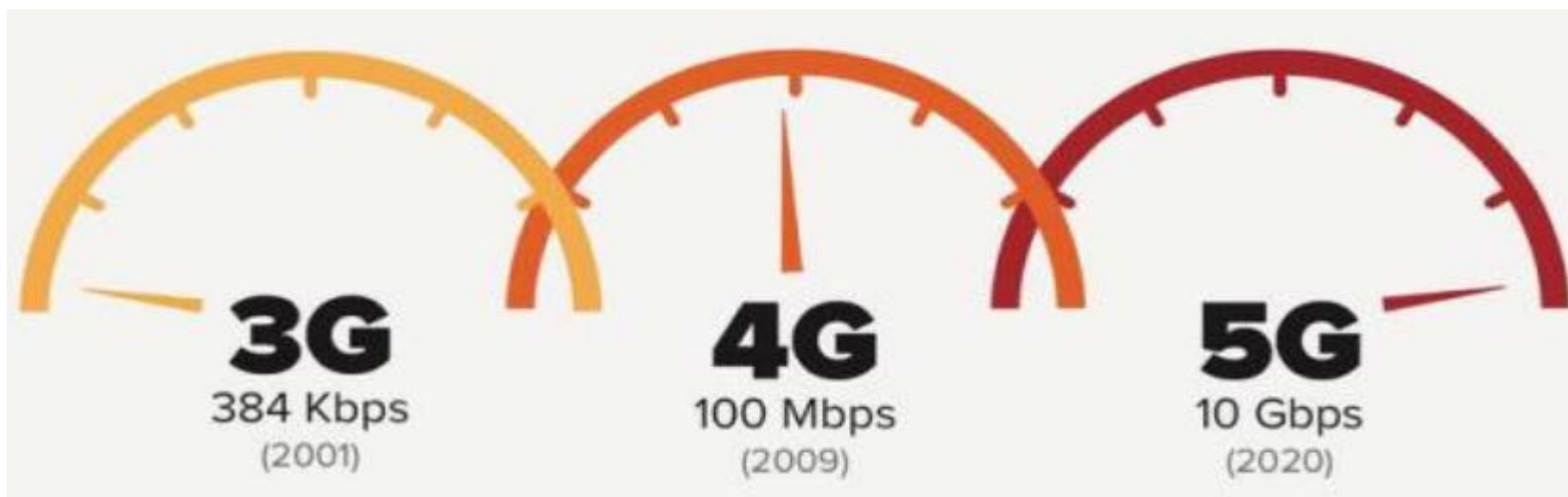
移动互联网安全风险监测

信安世纪移动安全领域应对

# 移动互联网发展 与安全风险

## 移动互联网发展

- 运营商将基础网络建设快速布局发展
- 智能移动终端产品的迅速普及
- App市场爆发式增长





## 存在安全威胁与风险

- 业务应用的安全威胁与风险
- 网络通讯的安全威胁与风险
- 终端设备的安全威胁与风险

系统漏洞  
SQL注入  
。 。 。 。

恶意WIFI  
非法数据截取  
。 。 。

病毒、木马  
远程控制  
。 。 。 。



# 移动互联网安全 接入技术研究

## 移动互联网安全接入技术

- PKI技术作为移动安全接入的基础安全技术保障
- 数字签名技术实现不可否认性
- VPN技术实现用户身份认证，建立安全隧道
- 基于移动虚拟化安全沙箱技术

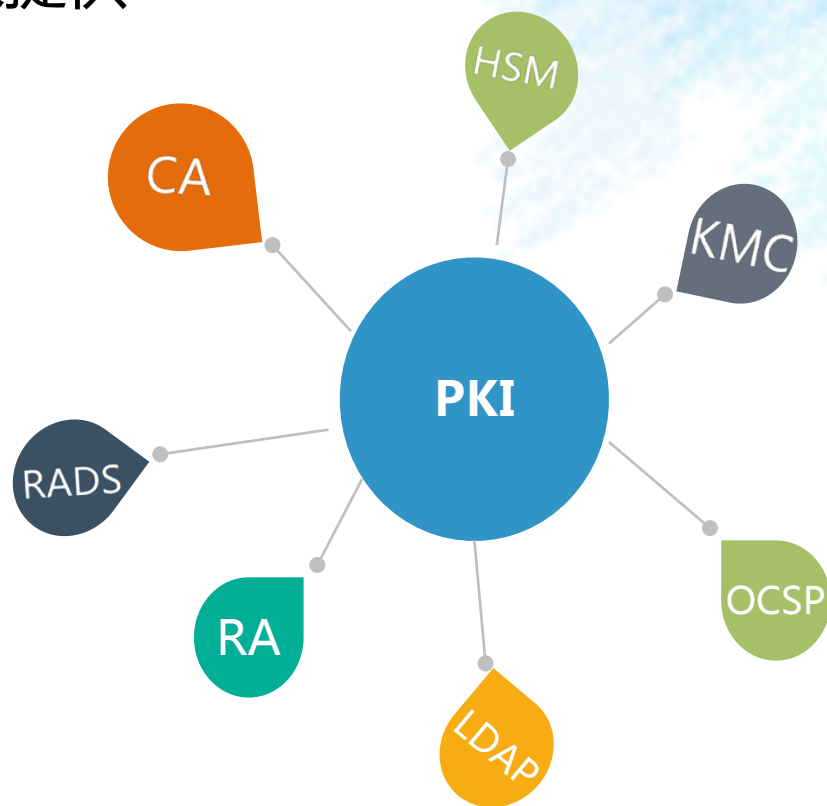
利用公钥理论和技术建立的提供网络信息安全服务的基础设施为终端接入提供安全底层技术支持；

CAServer

RA Server

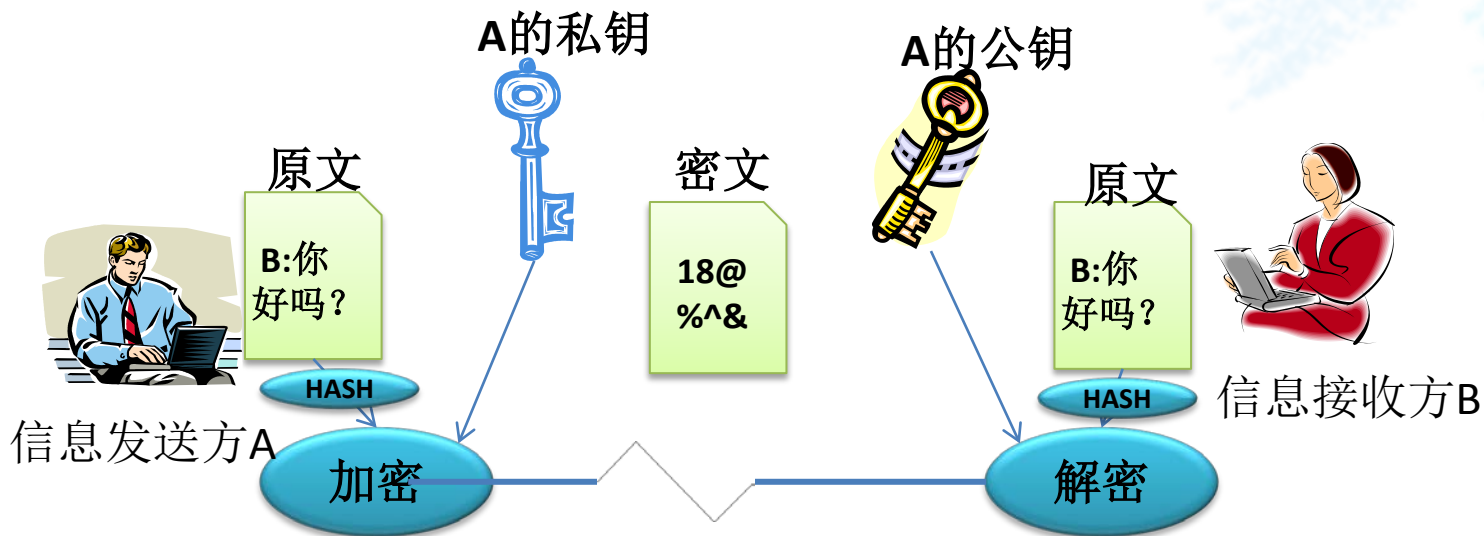
KMCServer

◦ ◦ ◦ ◦ ◦ ◦





使用数字证书的私钥对数据加密,以保证  
数据的完整性、真实性和不可抵赖;



利用公共网络建设的专用私有网络

IPSec VPN、SSL VPN

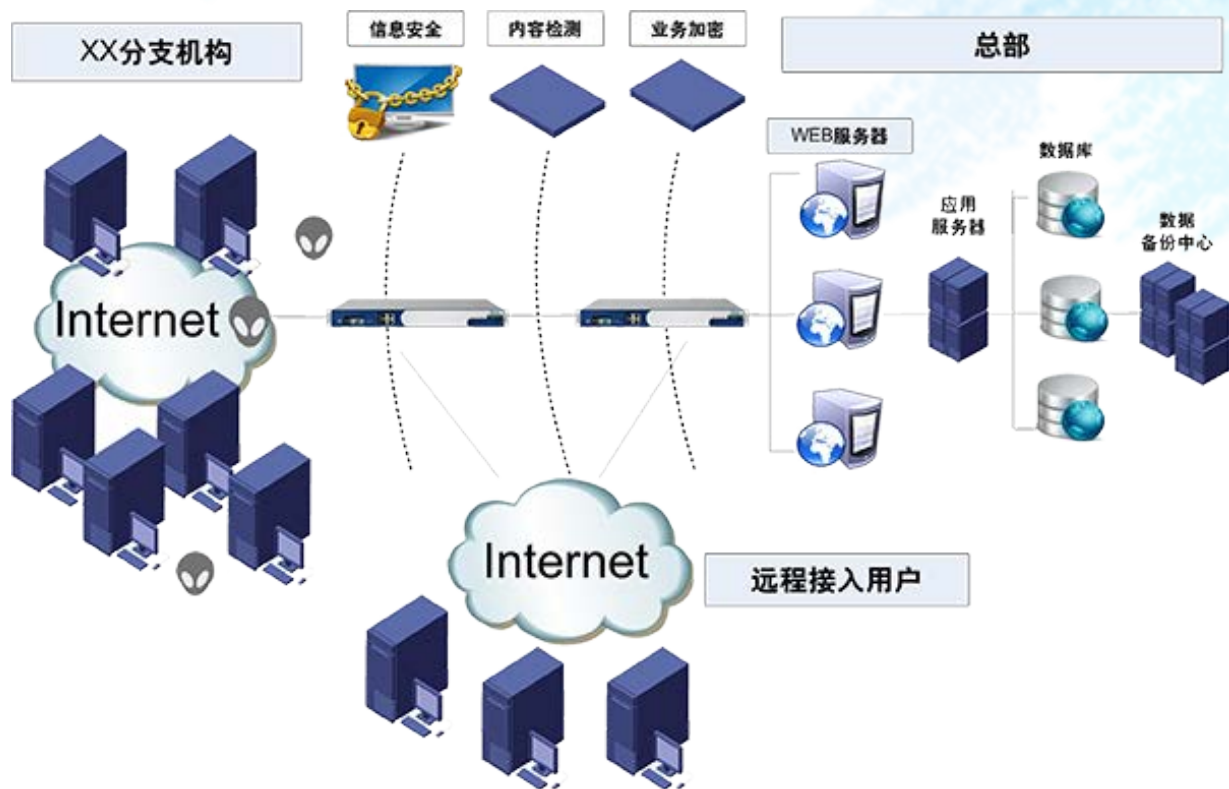
隧道技术

加解密技术

密钥管理技术

身份认证技术

。 。 。 。 。 。



安全沙箱是一种程序的隔离运行机制，其目的是限制不可信进程或不可信代码运行时的访问权限；移动虚拟化是移动设备实现外部隔离的基础技术；

虚拟化级沙箱

应用级沙箱





## APP安全 接入方案

- 移植较快速
- 支持国密算法安全通道
- 少量开发
- 易用性稍差
- 采用无私钥方式进行应用签名



## 中间件 SDK方案

- 移植最慢
- 支持国密算法安全通道
- 开发量较大
- 易用性最好
- 可采用签名加密



## VPN 接入方案

- 移植快速
- 支持国密算法安全通道
- 无须开发
- 易用性差
- 无法实现应用签名加密



移动  
互联网  
安全  
未来  
发展

- 移动单点登录 Mobile single-sign on
- 移动语音保护 Mobile voice protection
- 安全短信/彩信 Secure texting
- 虚拟移动基础设施 Virtual mobile infrastructure
- Arm TrustZone构建TEE
- 密码算法移动端推广和应用



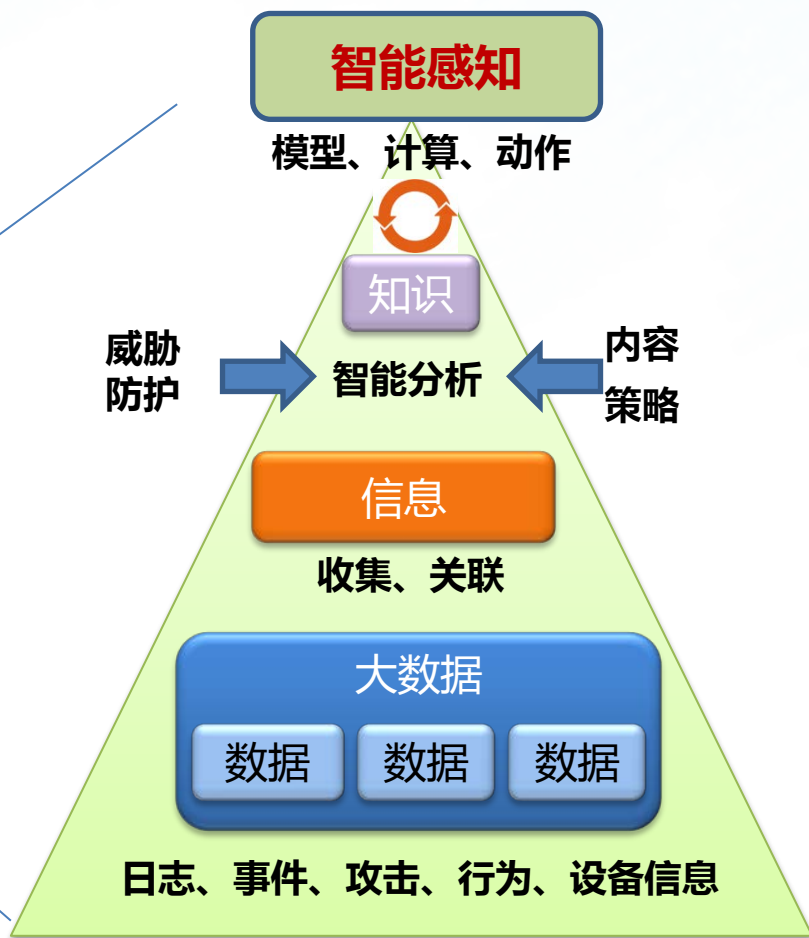
# 移动互联网 安全风险监测

## 移动互联网安全风险监测平台

- 终端数据快速收集
  - 网络情况
  - 设备情况
  - 使用习惯
  - 配合应用获取异常信息
  - 性能要求实时参数
  - 全部SDK模块独立
- 终端环境的快速检测
  - 病毒木马预警查杀
  - 性能预警
  - 环境风险提示

## 移动互联网安全风险监测

- 统计方法
- 推理建模
- 及其学习
- 聚类分析



# 信安世纪移动 安全领域应对



## 成立

成立于  
1998年1月

服务金融、政府  
行业超过14年

## 技术底蕴

中科院信息安全  
国家重点实验室

资深应用安全  
技术人才

## 发展

总部设在  
北京

上海、成都、深圳、西安、沈阳  
和武汉设有分支机构



国家信息安全标准化委员会WG3、WG4工作组成员

国家密码管理局电子交易应用安全体系专项组成员

国家密码管理局知识产权专项组成员

国家密码管理局金融领域国产密码应用推进实施过渡策略组组长成员

中国密码协会会员单位



## 主持制定的国家标准及行业标准

- 《XML签名语法与处理规范》
- 《烟草行业数字证书应用接口规范》
- 《烟草行业互联网接入安全规范》
- 《人力资源和社会保障电子认证体系证书应用管理规范》
- 《交通运输行业数字证书格式规范》
- 《交通运输行业数字证书应用接口规范》
- 《智能交通 信息安全 应用系统安全建设规范》
- 《智能交通 信息安全 车载单元信息安全规范》
- 《智能交通 信息安全 固定点单元信息安全规范》

## 国家密码局相关规范

- 《证书认证系统和密钥管理系统检测规范》
- 《证书认证系统密码技术及其协议规范》
- 《数字证书认证中心和密钥管理中心的技术标准》



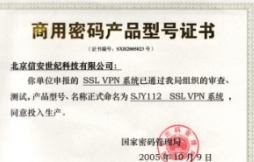
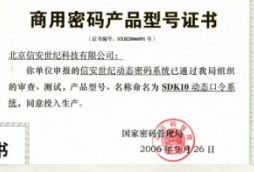
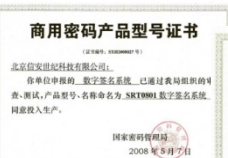
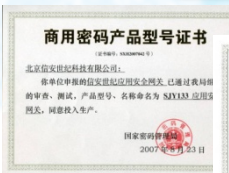
## 安全行业资质

公司

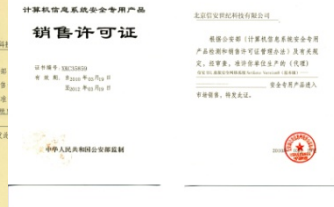
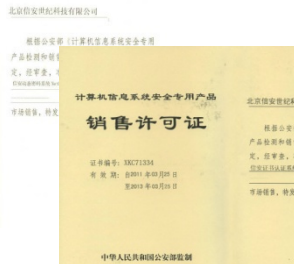
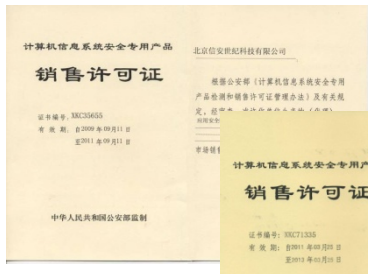
## 各项产品

# 质量管理

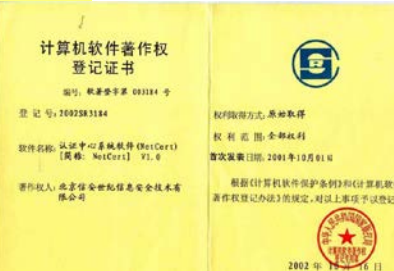
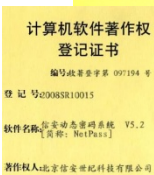
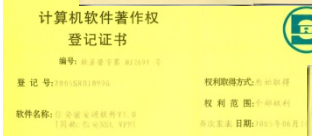
国密局



公安部



版权局



北京信安世纪科技有限公司

## 信安世纪移动安全统一认证平台

- 后台系统
- 前端APP/SDK

## 信安世纪安全监测平台

- 后台系统
- 前端SDK

## 信安世纪移动安全服务平台

- 后台系统
- 前端SDK



## 产品组成：

- 认证平台后台系统
- 客户端APP/SDK

## 主要功能

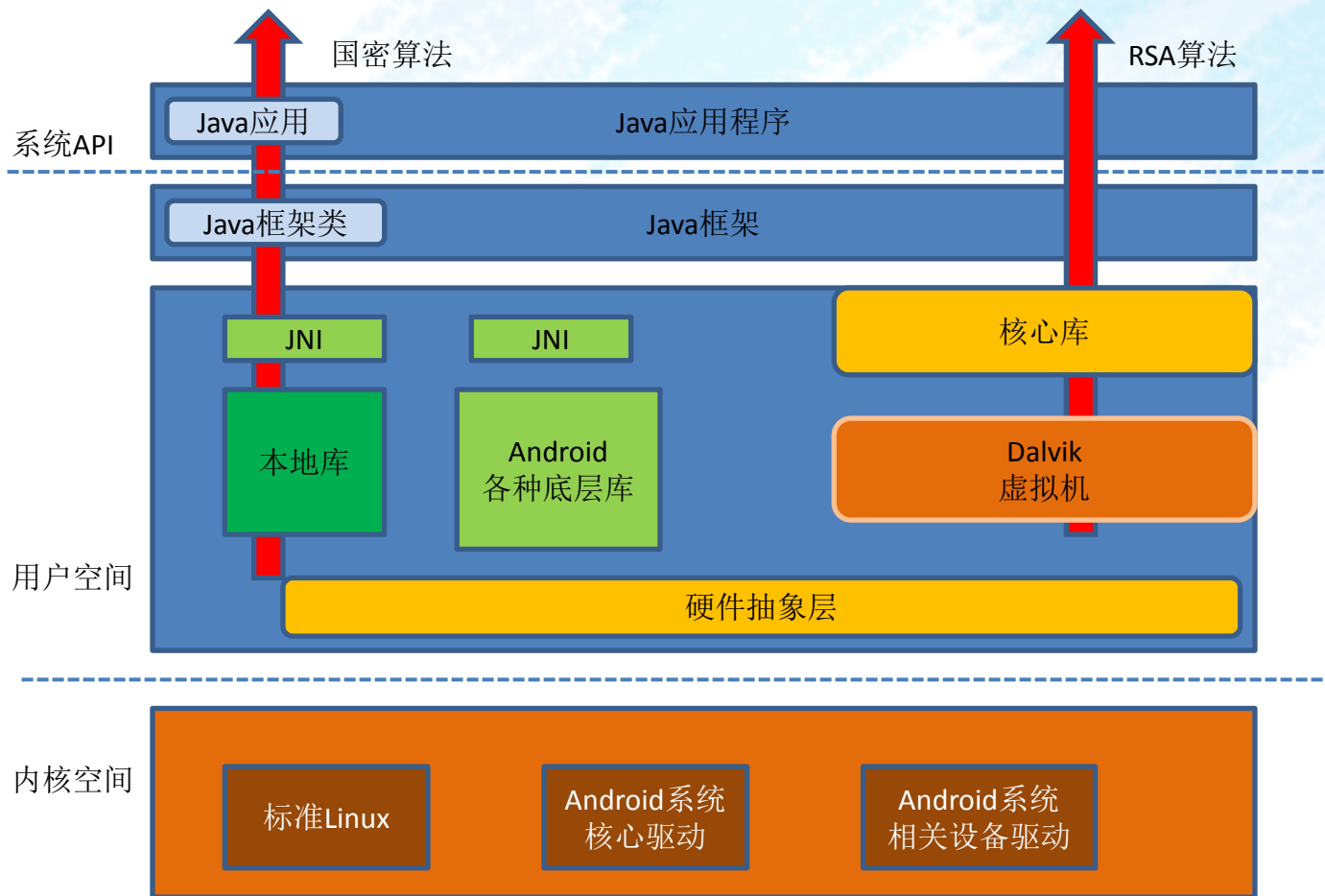
- 数字证书管理
- 动态口令管理
- 应用市场
- 地理围栏

• • • • •

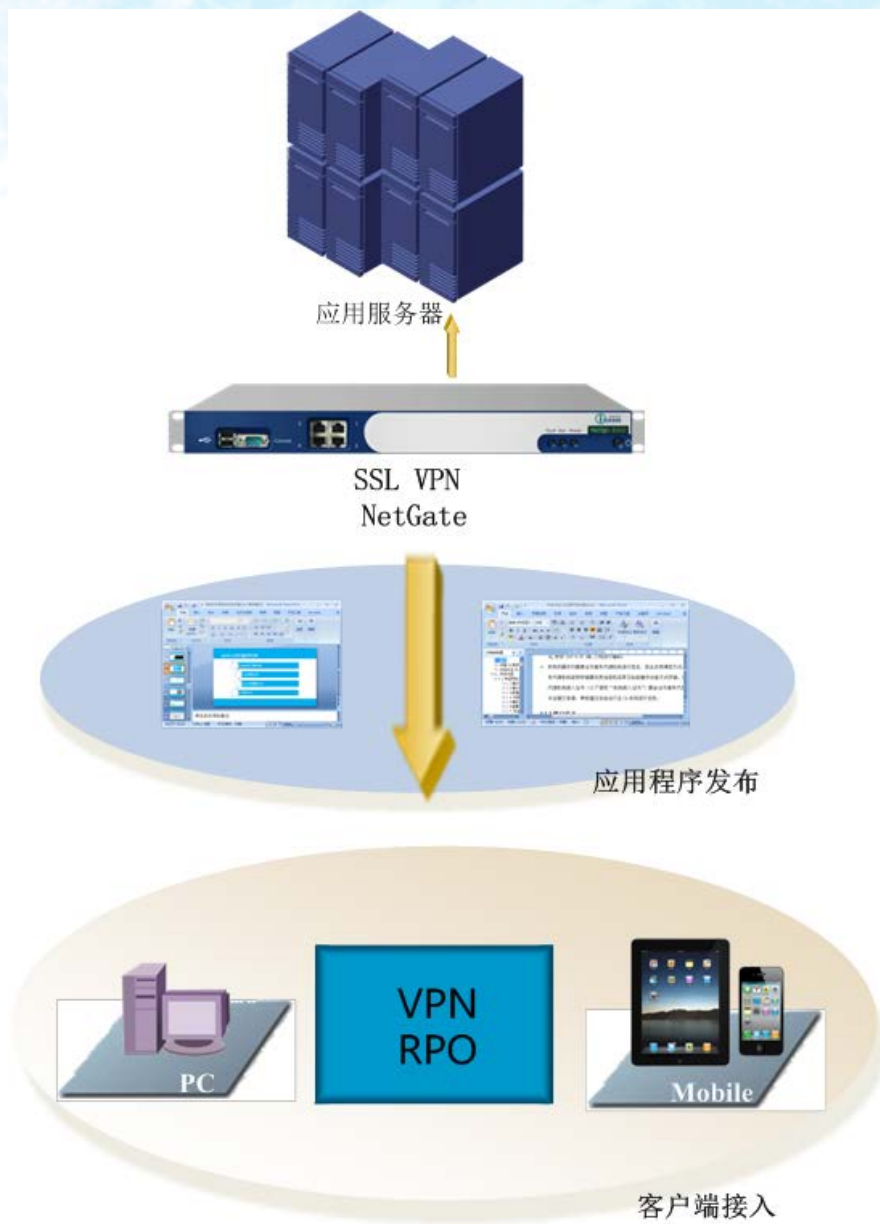








- 安全访问控制
- 安全保护机制
- 支持多种应用
- 瘦客户端系统



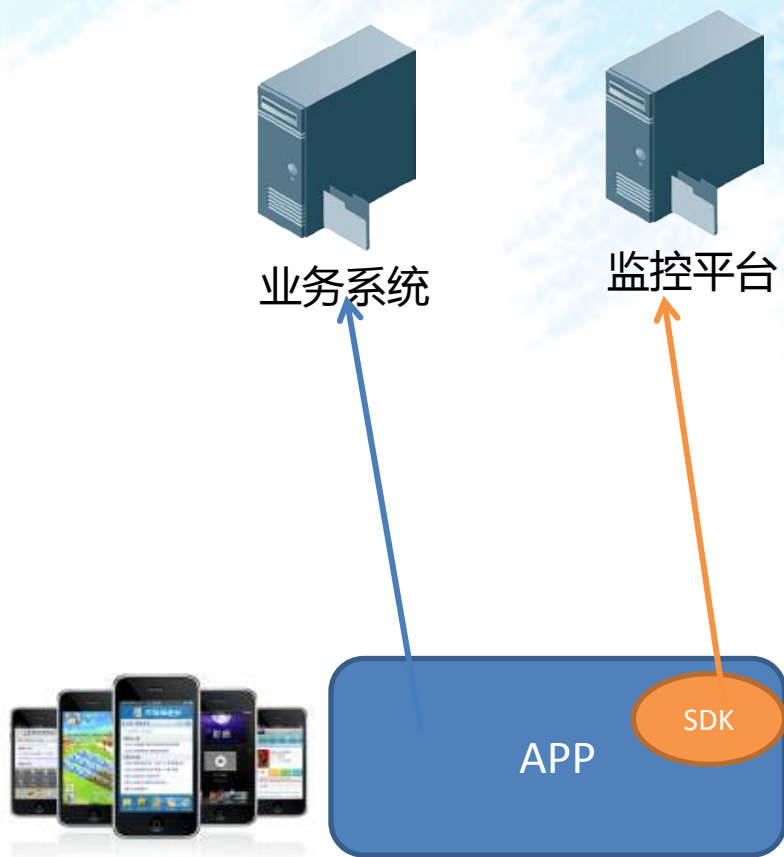
## 产品组成：

- 监测平台后台系统
- 客户端SDK

## 主要功能

- 系统检测
- 数据收集分析
- 业务预警
- 业务信息收集

。 。 。 。 。 。



## 应用运行环境：模拟器设备占比

App运行在模拟器设备中，容易受到逆向破解、抓包分析等攻击，同时增加业务风险，不同的模拟器的占比将会引发不同程度攻击和业务风险

20%

将导致风险提升

2.14% ↑ 恶意注册风险    5.35% ↑ 垃圾消息风险    5.51% ↑ 账号被盗风险    2.30% ↑ 作弊行为风险

[查看详情](#)

杀毒软件

1

TOP5应用软件：

日历存储

Live Wallpaper Picker

### 调试扫描

开启调试设备： 7个

未开启调试设备： 3个

### WLAN开启数

我的WLAN设备数： 7个

未开启WLAN设备数： 3个

### NFC开启数

我的NFC设备数： 2个

### 模拟器检测

模拟器设备： 2个

非模拟器设备： 8个

### ROOT设备

我的ROOT设备数： 2个

非ROOT设备数： 8个

### 可疑框架



二维码key



蓝牙key



谢谢！