



车联网可信认证与安全连接

刘鹏

北京信长城技术研究院

北京信长城技术研究院成立于2010年，是一家以标识密码技术为核心，专注于信息安全领域的技术研发和产品开发的信息安全公司。

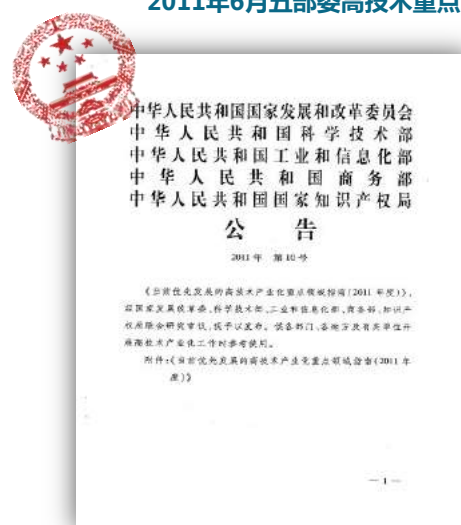
信长城致力于为用户提供**轻量化、高安全、低成本**、便捷可靠、无缝对接融合的安全体系构架。以基于标识认证的主要优势（离线身份认证、大规模密钥管理、去中心化、轻系统）为依托，在物联网、车联网、云安全等方向为用户提供安全产品和服务。

信长城——致力于为万物互联提供密钥基础设施！

标识密钥技术——中国完全自主知识产权的技术



2011年6月五部委高技术重点领域指南



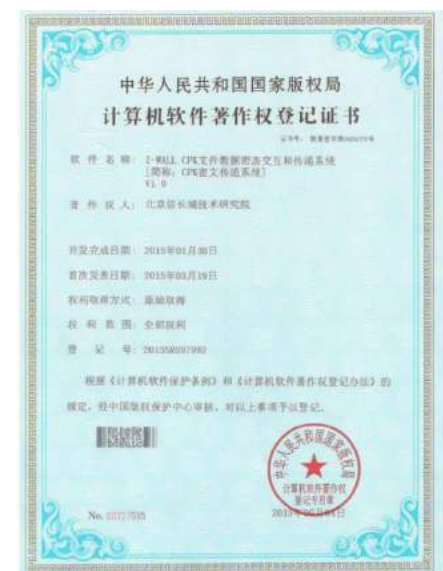
CPK作为新一代创新发展的可信安全技术，可嵌入到体系架构、系统和应用设计中，为中国信息安全产业构建生态基础。

件，重要行业的管理和应用软件。

8、信息安全产品与系统

适用于特殊领域的安全服务器，安全路由器，安全网络存储设备，计算机安全操作系统，安全数据库，操作系统与数据库安全管理系统防病毒和防攻击系统，入侵检测、防信息泄漏、后门发现和漏洞分析，加解密设备和芯片，安全协议，公钥基础设施(PKI)系统，**组合公钥(CPK)系统**，安全支付系统，**电子防伪系统以及网络安全监控系统**，虚拟专用网和无绳网络领域的安全监管系统，等级保护管理，可信计算技术与产品，**网络安全预警系统**，内容安全和网络容灾类产品，信息安全测评系统、**软件测评技术与系统**，**保障云计算、物联网、新一代信息网络以及面向三网融合的安全产品**，**多媒体内容监控系统**。

9、集成电路



目录



车联网信息安全需求



基于标识的车联网安全解决方案



标识认证方案优势

Part 1 车联网信息安全需求



需求来自安全挑战



2015年7月，两位美国黑客远程破解并控制了克莱斯勒的JEEP汽车，克莱斯勒因此召回了140万辆汽车；



2015年8月，国内某汽车厂商的云服务也曾被曝存在漏洞，可导致车主信息泄露和汽车被远程控制；



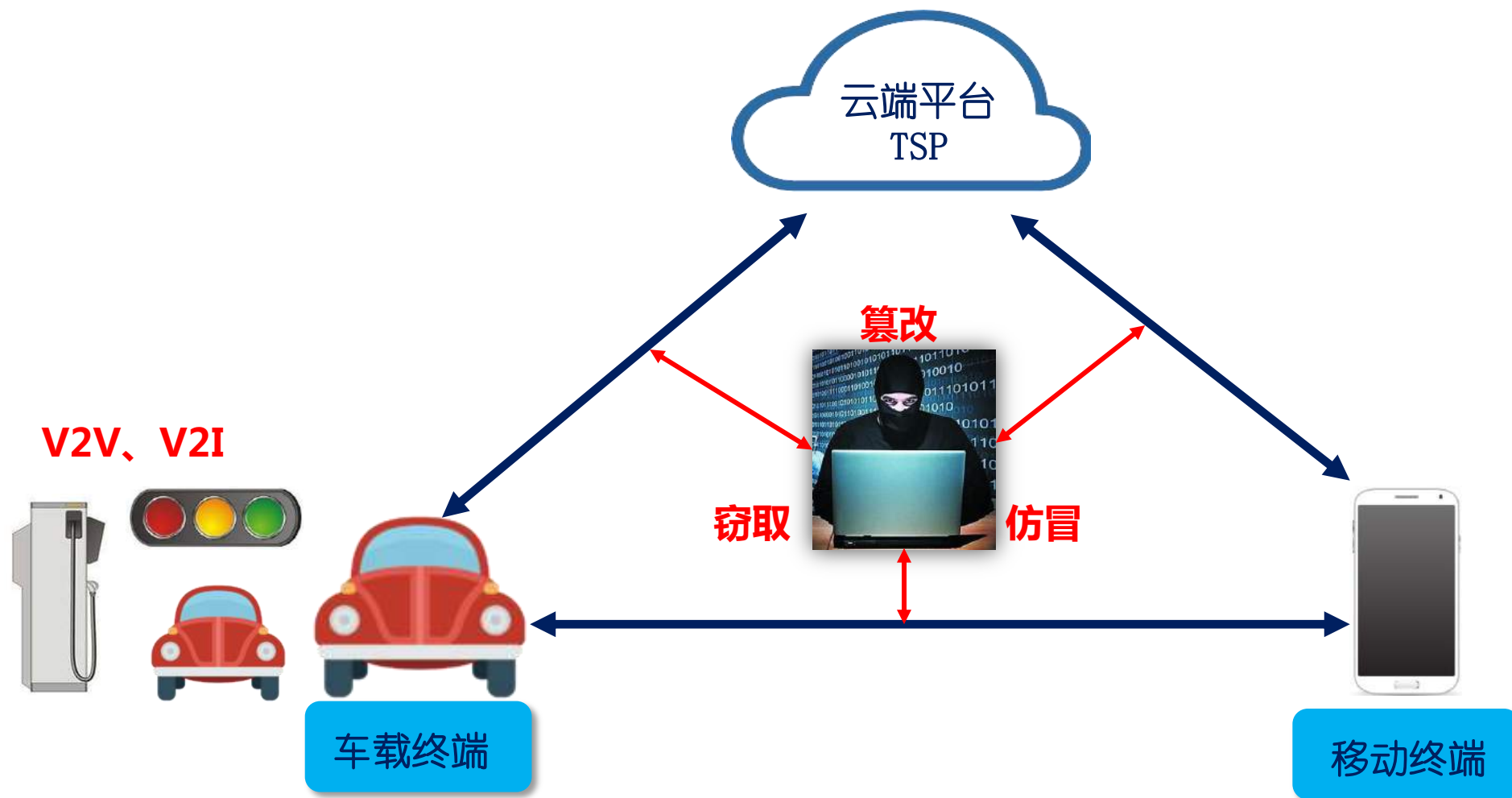
2015年，欧洲两所大学的研究人员表示，通过无线模块和天线，可以跟踪一个小城市里的所有车辆，跟踪成本不足50万美元；



2016年8月，360汽车安全实验室首次通过传感器漏洞破解了特斯拉自动驾驶系统。



需求来自安全挑战





身份认证

车与云之间的认证
APP与云间的认证
车与车间的认证
车与APP间的认证
车与基础设施认证



存储保护

车载数据存储保护
云端数据存储保护
APP数据存储保护
关键密钥的保护



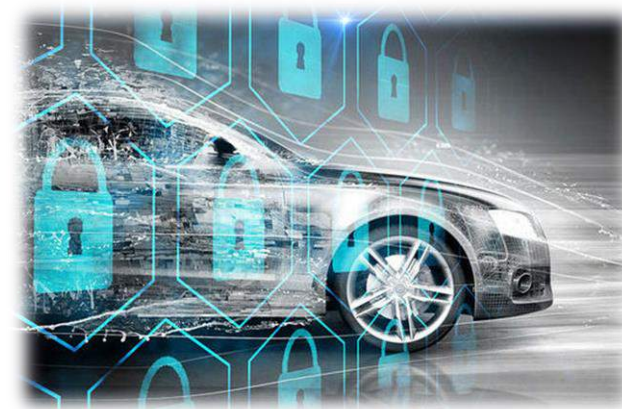
数据交互

数据防窃取
数据防伪造
数据防篡改
安全升级

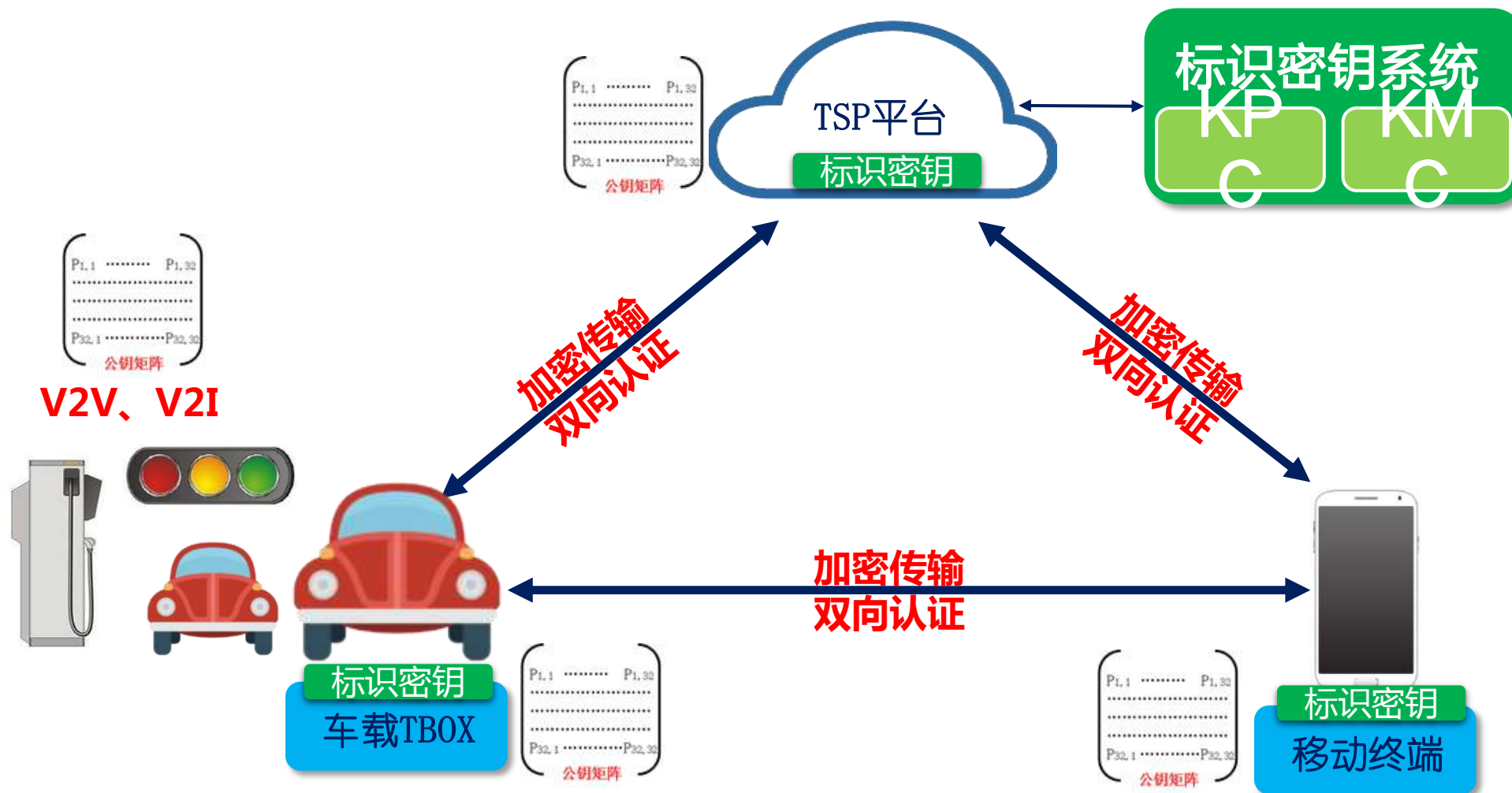
轻量！

高效！

Part 2 基于标识的车联网 安全解决方案

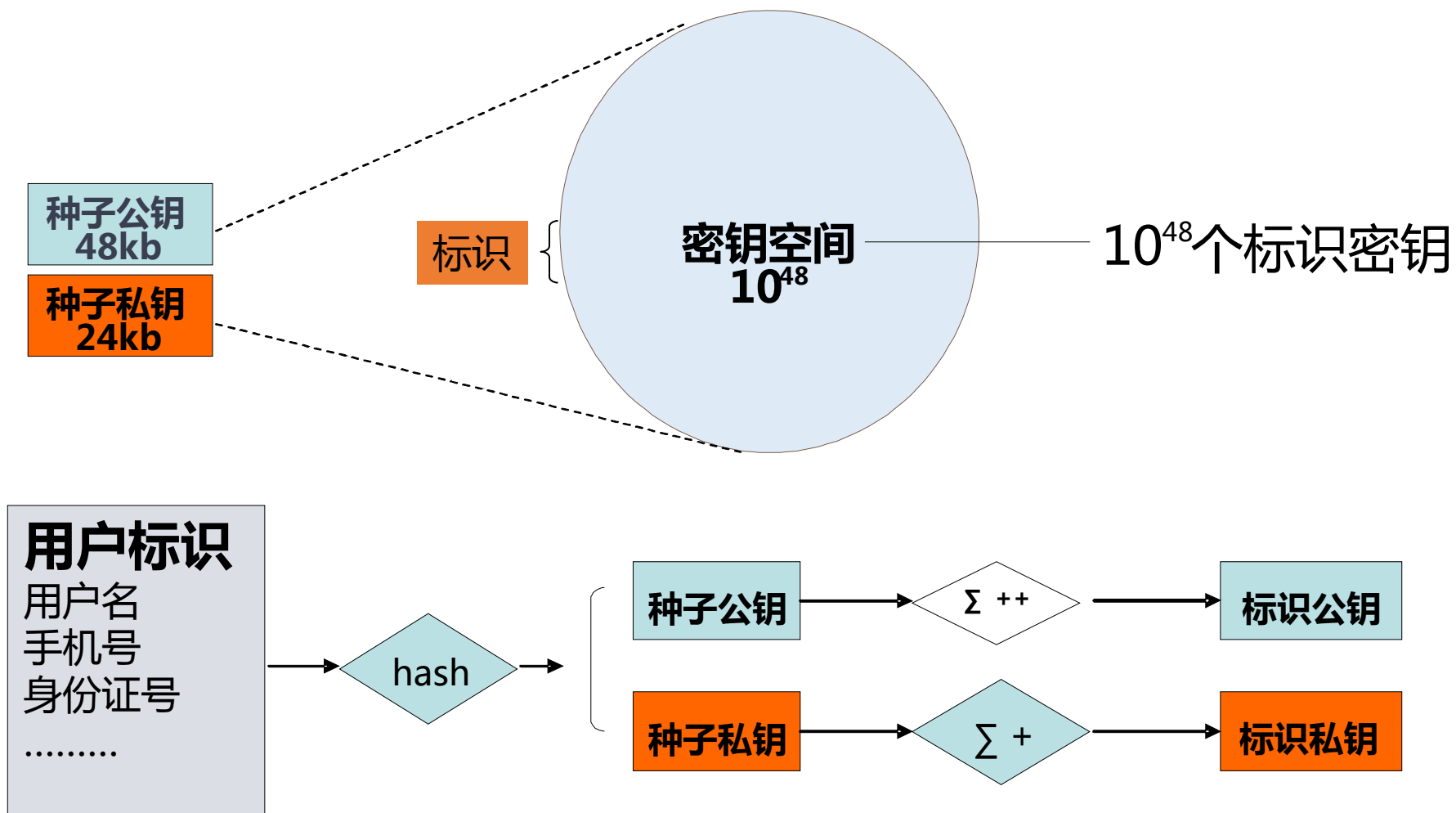


一、车联网安全——标识密钥系统架构

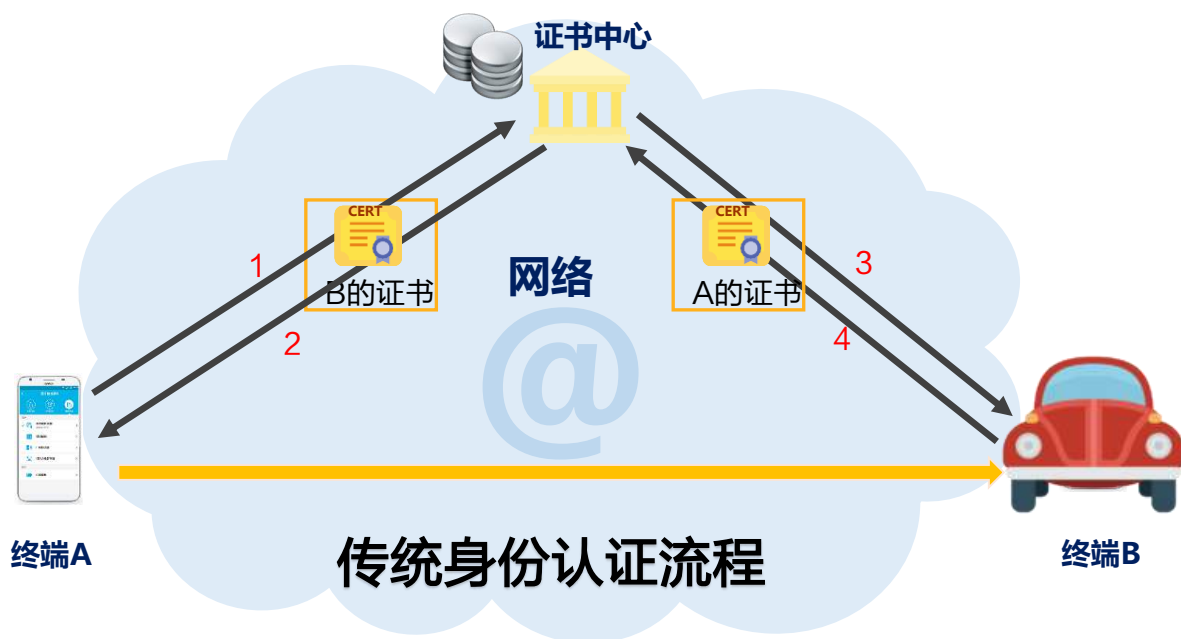


轻量级密钥系统——标识密钥简介

问题：地球上有多少颗沙子？ 10^{23} 量级！



身份认证流程及对比



- 有证书传递过程，对网络环境敏感度高
- 认证流程复杂，对接和开发成本高
- 系统间依赖程度高，故障易传导
- 信任传递使安全性脆弱，存在中间人攻击

- 基于标识直接认证，对网络环境容忍度高
- 认证流程简洁高效，对接和开发成本低
- 系统一手掌握，故障率低
- 不存在信任传递，没有中间人攻击



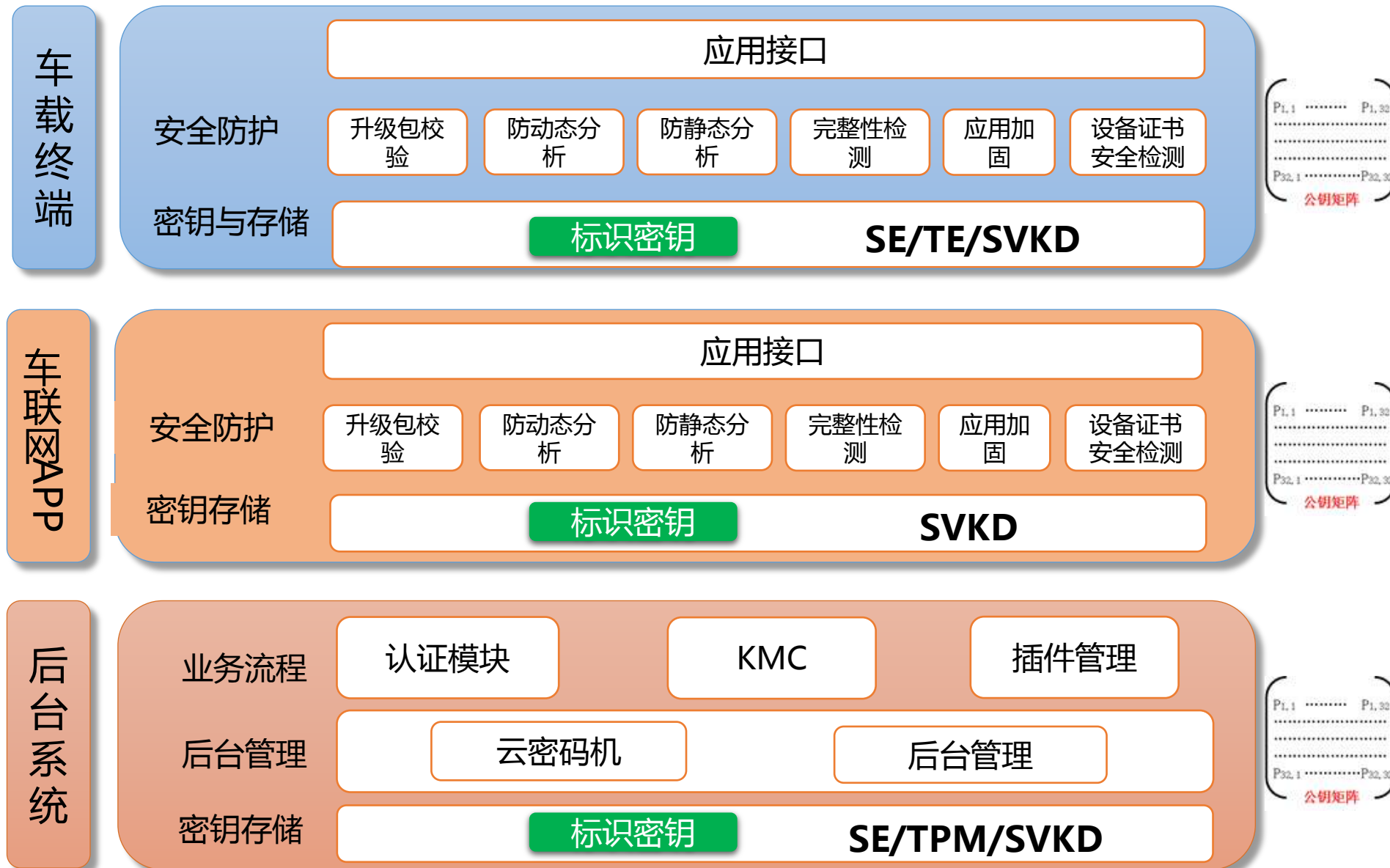
标识认证是基于区块链技术吗？

NO!

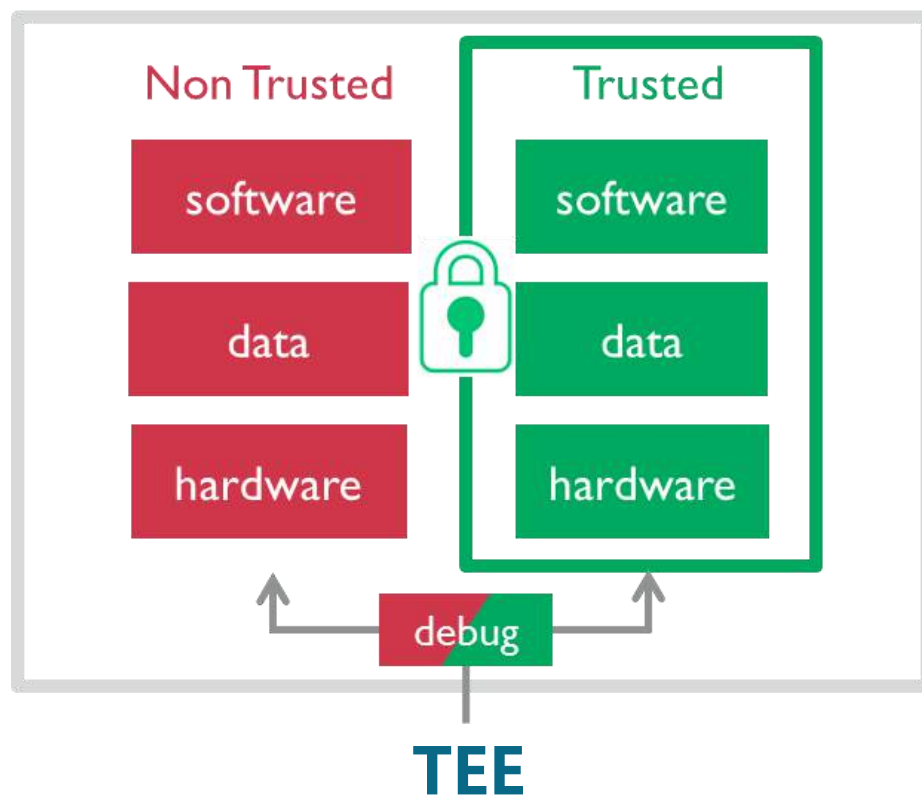
区块链：**账本**的分布式

标识认证：**证书**的分布式

车联网安全——终端保护架构



标识密钥技术和SVKD可以与TEE技术深度融合，保护密钥和数据相关的敏感操作，具有安全度高、应用灵活的优点。

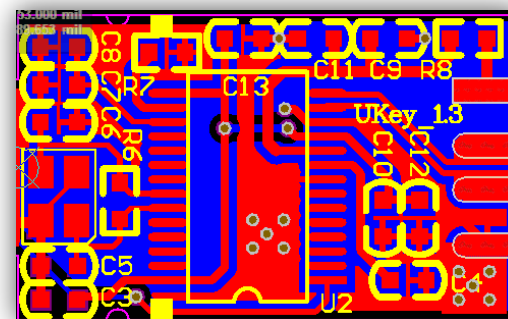


支持多款国际和国内算法芯片，可以支持国际通用加密算法（AES、3DES、ECC、RSA、SHA）和国密算法（SM1/2/3/4），我们根据多年经验，对COS进行安全加固，有效防止侧信道攻击。

为了集成和测试方便，我们还制作了专用加密模块，尺寸为30*20mm或20*20mm，模块上有UART、SPI、USB等接口插针，可以很方便的和各种TBOX集成。

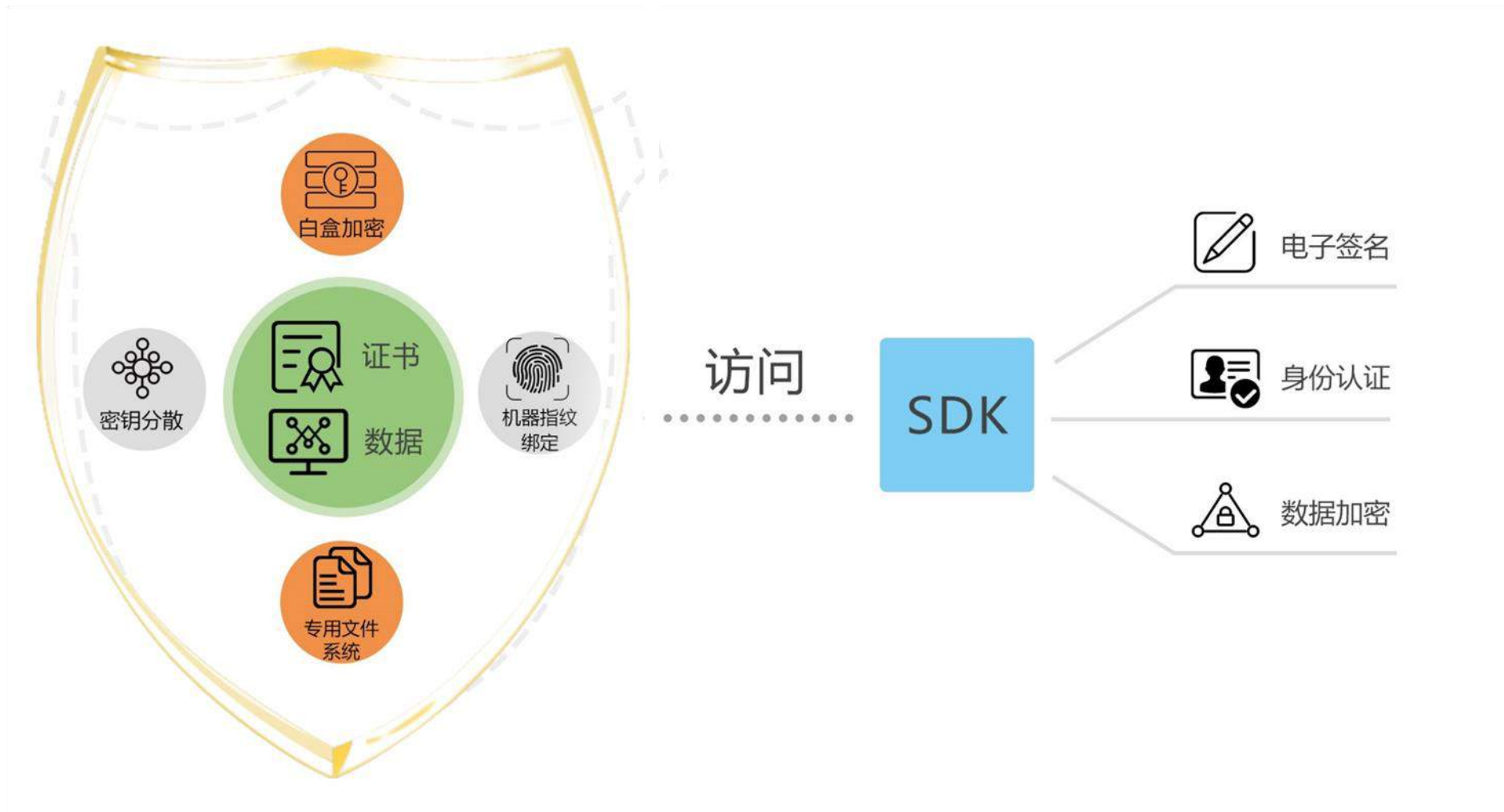


算法芯片

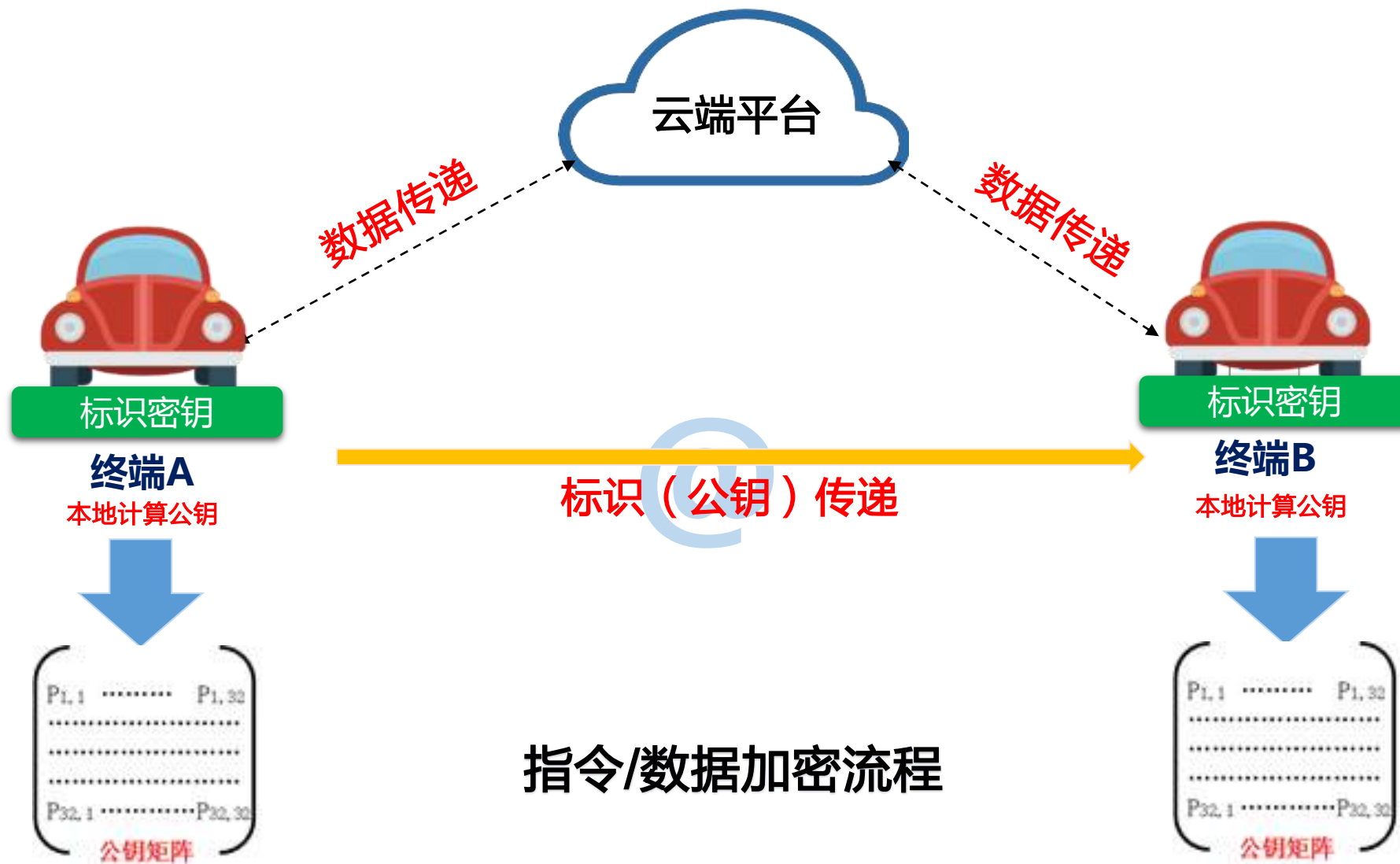


加密模块

终端密钥保护——SVKD（软盾）



安全场景——车辆间数据传输安全



Part 3 标识认证方案优势



本安全方案优势

自主可控

- 我国自主知识产权技术，支持国际、国密算法

身份认证更安全

- 基于标识分布式身份认证，认证更加直接高效

数据传输更安全

- 端到端数据加密，有效防止中间人攻击

系统负载低

- 离线密钥交换，降低对系统的负载，认证效率高

可支撑规模大

- 分布式密钥系统，可支撑大规模用户，扩展性强

使用成本低

- 服务器低压力运行，建设和运行成本低

维护成本低

- 系统复杂度低，不易出故障，维护成本低



标识密钥技术应用的市场潜力



网络世界从形成始，一直呈无序性，一边创造财富，提供方便，一边隐藏假冒伪劣，滋生犯罪，制造麻烦。

为了主动迎接这种基础性、方向性、体制性变迁，把先进的理念、理论、技术变为现实，我们还需要继续努力！

- ✓ 标识密钥技术打通信息网络与非信息网络（包括物联网）之间的壁垒，为建立网络安全集中化管理提供了有效技术保障，由于这一技术具有认证的海量性和验证的简便性，可从源头净化市场环境，建立可信网络世界。
- ✓ 组合公钥体制顺应时代锐势拓展，正在迅猛冲破传统的信息安全观念和发展模式，并孕育着新的巨大的创新空间和商机，催生新的研究课题和产业链。
- ✓ 推广并应用标识密钥技术，包括国际合作，使其成为国际标准，有利于我国抢占未来全球信息化建设先机。推动标识密钥技术应用，可使我国在人类建设有序和谐的网络世界中作出贡献。



THANKS
谢 谢 聆 听

电话：010-58341334

邮箱：liupeng@i-wall.cn

地址：北京市西城区西直门西环广场9层
