标识认证在网络安全的创新应用

刘鹏　　北京仁信证科技有限公司CTO

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China

目录

一、网络安全认证体系现状分析

万物互联，网络无界

万物互联的新时代

互联网　　移动互联网　　物联网

融合网络

泛在网络

无界网络

ZERO TRUST SECURITY

开放网络，攻击泛滥

Gmail、雅虎和账号泄露

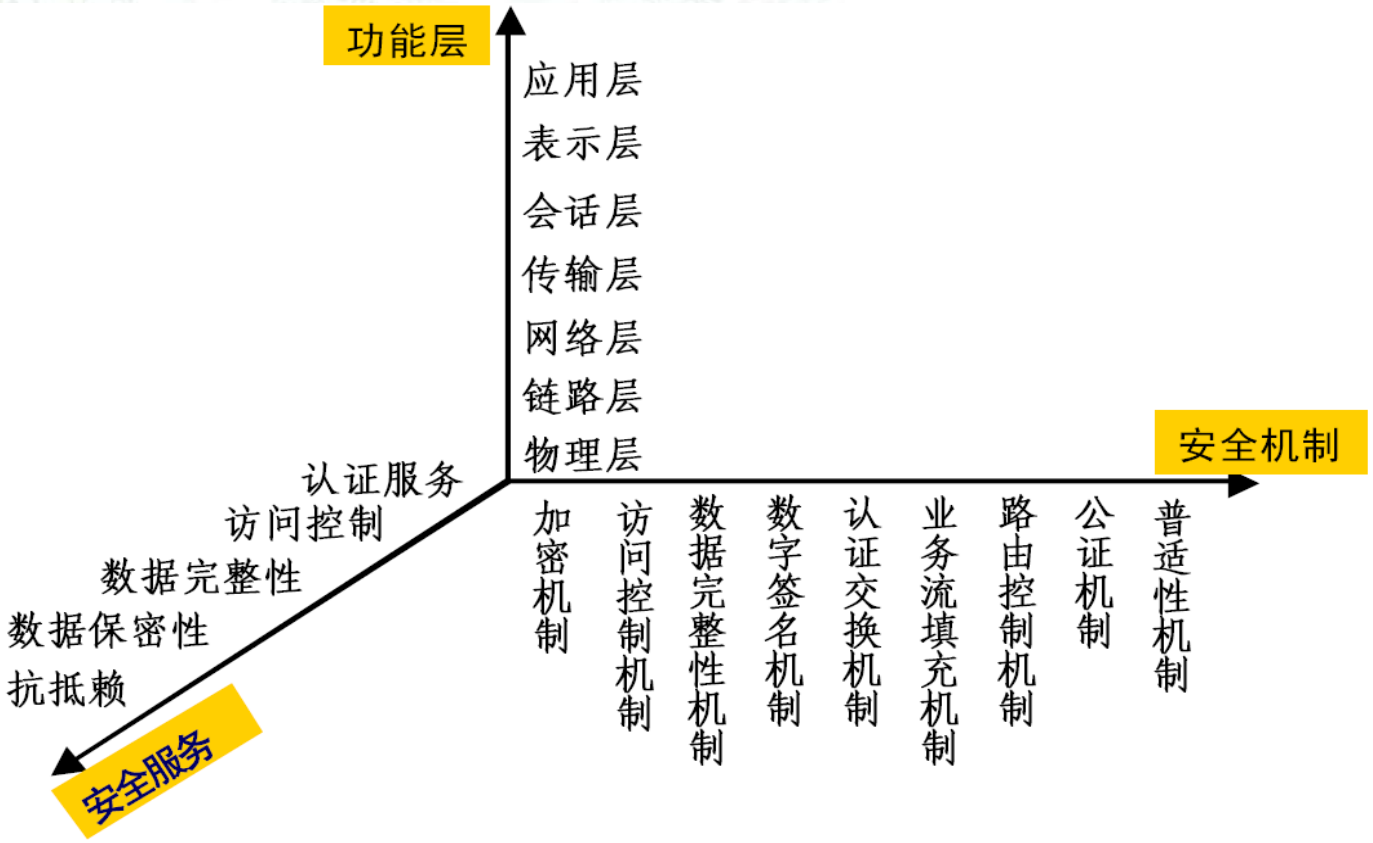
360公司破解特斯拉

“乌克兰电网”事件

1、网络攻击行为从以窃取用户信息、盗取用户资金为目的传统互联网和移动互联网攻击，演进为可危及工业设施安全、公共交通安全等的对工控网、车联网等泛在网络的攻击。

2、网络安全事件频发的大多数原因可归结于身份认证、访问控制的问题。

捍卫安全，认证为本



OSI安全体系架构

- **基于知识因素的身份认证**
  - 账号口令
- **基于拥有因素的身份认证**
  - 短信验证码
  - 对称密钥认证技术
  - PKI签名认证技术
  - 其他签名认证技术
- **基于固有因素的身份认证**
  - 人的声纹、指纹、面纹等
  - 设备的设备ID等信息

对设备进行认证主要依托对称密钥认证技术以及签名认证技术。

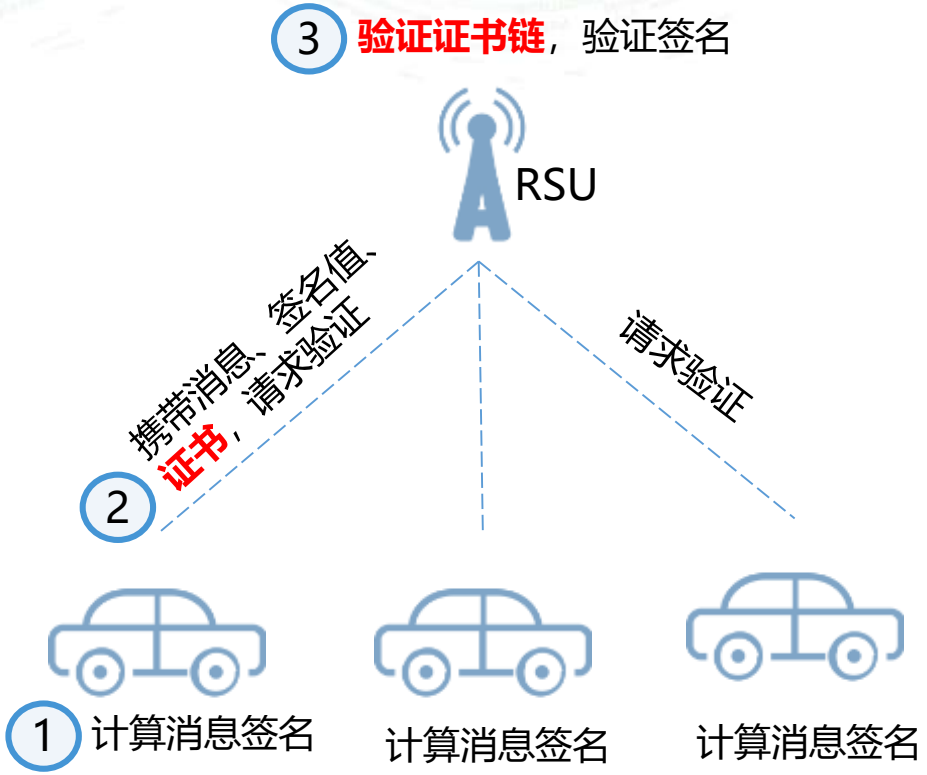
新的网络，新的挑战

新型网络条件下对认证技术提出的挑战：

融合网络中的短程通信网络带宽资源受限；多对多结构导致由中心认证方式转变为多节点交叉认证；拓扑快速变化要求在节点间可通信范围内完成认证；规模庞大的节点增加了并发计算的压力，节点计算能力不均衡需要轻量级的认证服务。

新的网络，新的挑战

万物互联时代，传统PKI能否独当泛在网络下的可信**身份**认证之大任?



PKI在车联网应用中的缺陷：

1、带宽占用量大，ETSI标准定义一个环境通知消息DENM数据包消息体长度约40Byte，而单个证书容量基本超过1K，将增加了传输报文20倍以上。在大用户量下，将会造成极大的通信拥堵。

2、RSU验证签名之前要验证证书链的合法性，大大增加了验证的时间，RSU需要集中处理众多车辆的消息，验证时间加长可能会导致RSU消息处理时间大于消息报文传输时间，将会导致大量的消息丢弃。

因此，PKI体系不适合在车联网很多场景下的应用。

车联网等新型网络场景下的可信身份认证技术何去何从

ZERO TRUST SECURITY

二、标识认证在网络安全的创新应用

标识密码技术

基于身份标识的密码系统（Identity-Based Cryptograph, 简称IBC），是一种公钥密码体系。标识密码最主要观点是系统中不需要证书，使用用户/设备的标识如电子邮箱地址、手机号码、设备ID等作为公钥。用户的私钥由密钥生成中心根据系统主密钥和用户标识计算得出。用户的公钥由用户标识唯一确定，从而用户不需要第三方来保证公钥的真实性。通过标识密码技术，无需证书的签发和交换，极大简化了公钥认证和加密的流程。IBC包含PBC和CPK两种技术体系。

IBC的提出 (1984)

- Shamir提出了基于标识的密码系统的概念；

IBE系统发现 (2001)

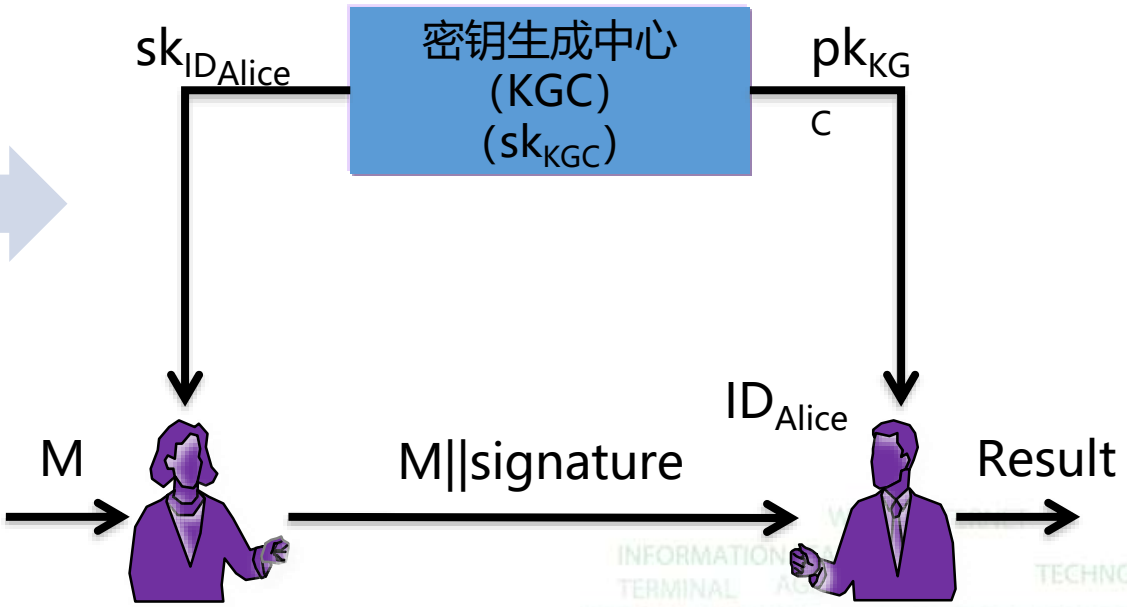
- Boneh和Franklin发明了基于Weil双线性对的IBE系统；

CPK体系提出 (2003)

- 2003年我国密码专家南湘浩提出了基于组合公钥CPK技术的IBC体

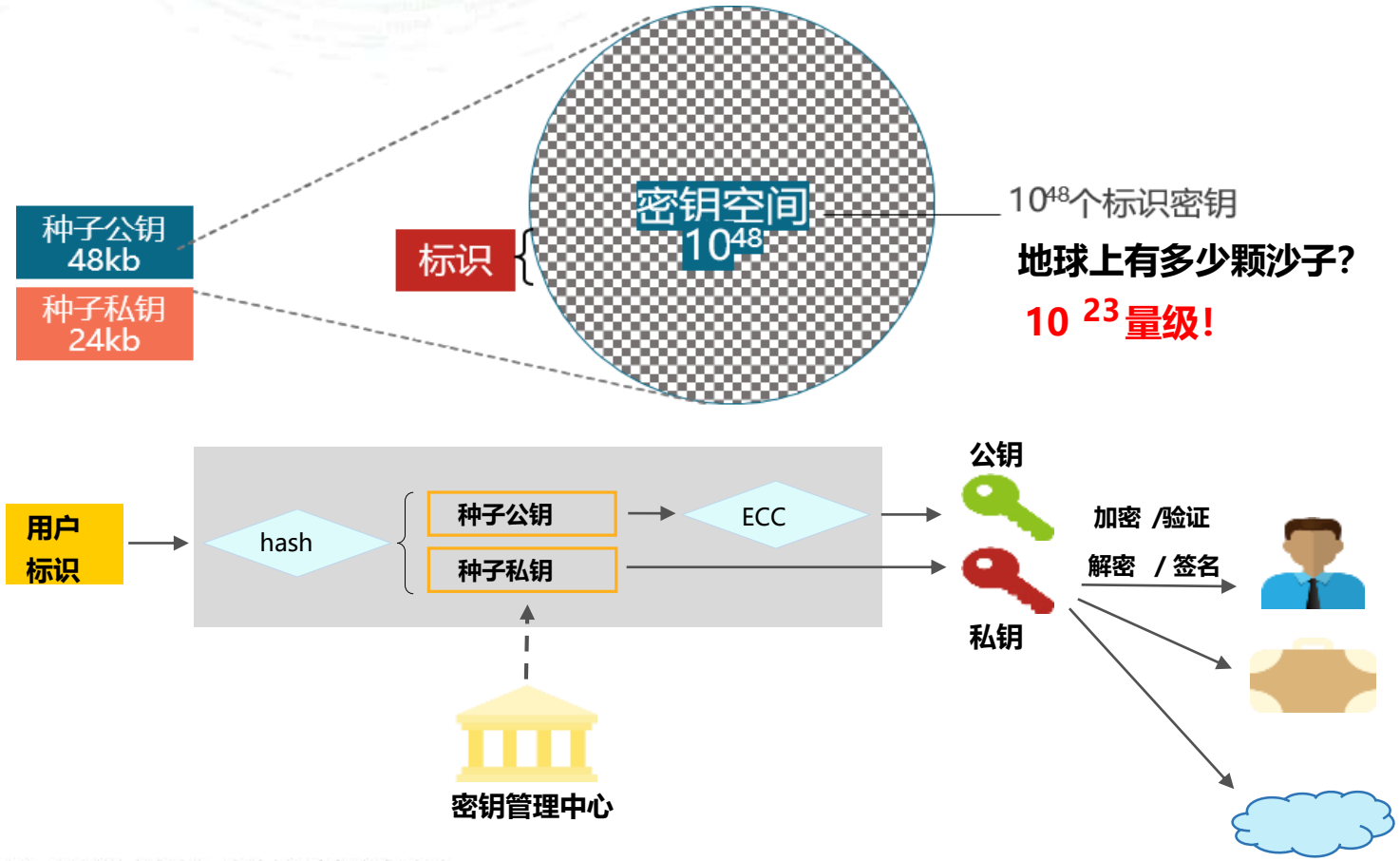
SM9标准发布 (2016)

- 中国于2016年发布了基于双线性对技术的“SM9标识密码算法标



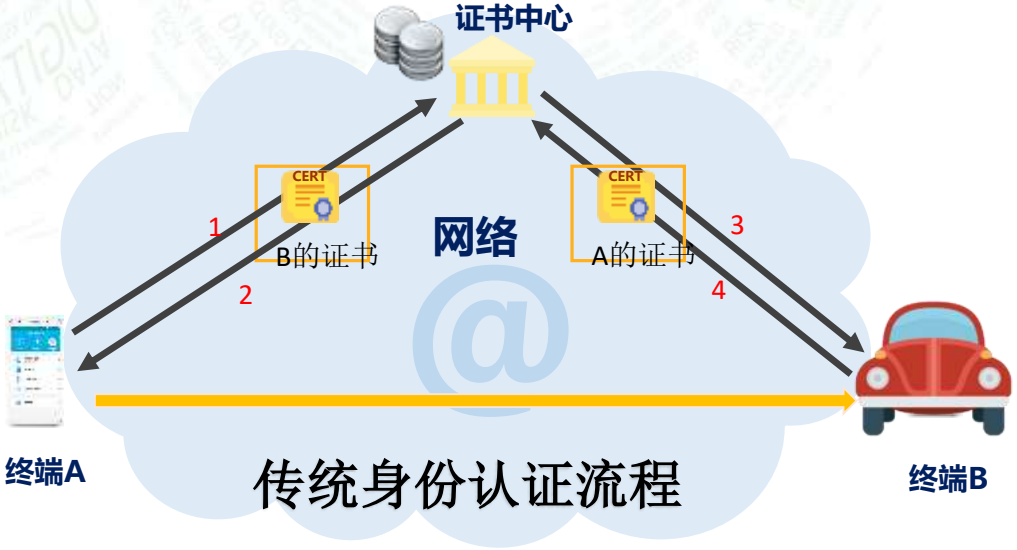
标识认证技术——CPK密码体制

CPK即组合公钥体制，将密钥生产和管理结合，能够实现数字签名和密钥交换，可以满足超大规模的标识鉴别、实体鉴别、数据保密需求。**密钥生产管理集中、使用去中心化、可离线认证的特性，尤其适用于物联网（车联网）场景。**



- 大规模
- 轻体量
- 去中心
- 高效率
- 更简洁
- 抗量子
- 更安全

标识认证技术——CPK密码体制

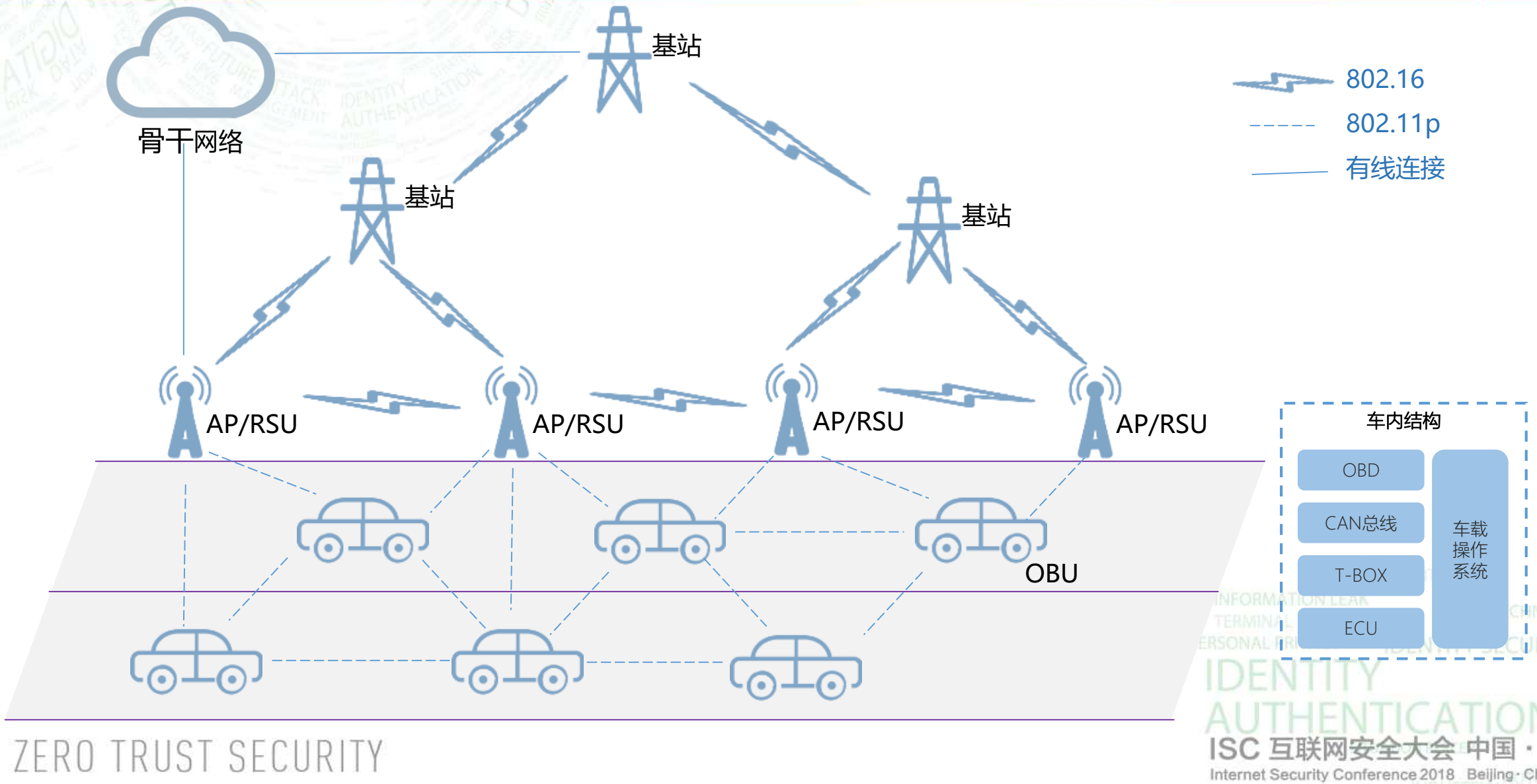


- 有证书传递过程，对网络环境敏感度高
- 认证流程复杂，对接和开发成本高
- 系统间依赖程度高，故障易传导
- 信任传递使安全性脆弱，存在中间人攻击

- 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

CPK基于椭圆曲线运算，而SM9基于双线性对运算，双线性对计算复杂，因此CPK相比于SM9具有更快的运算速度!

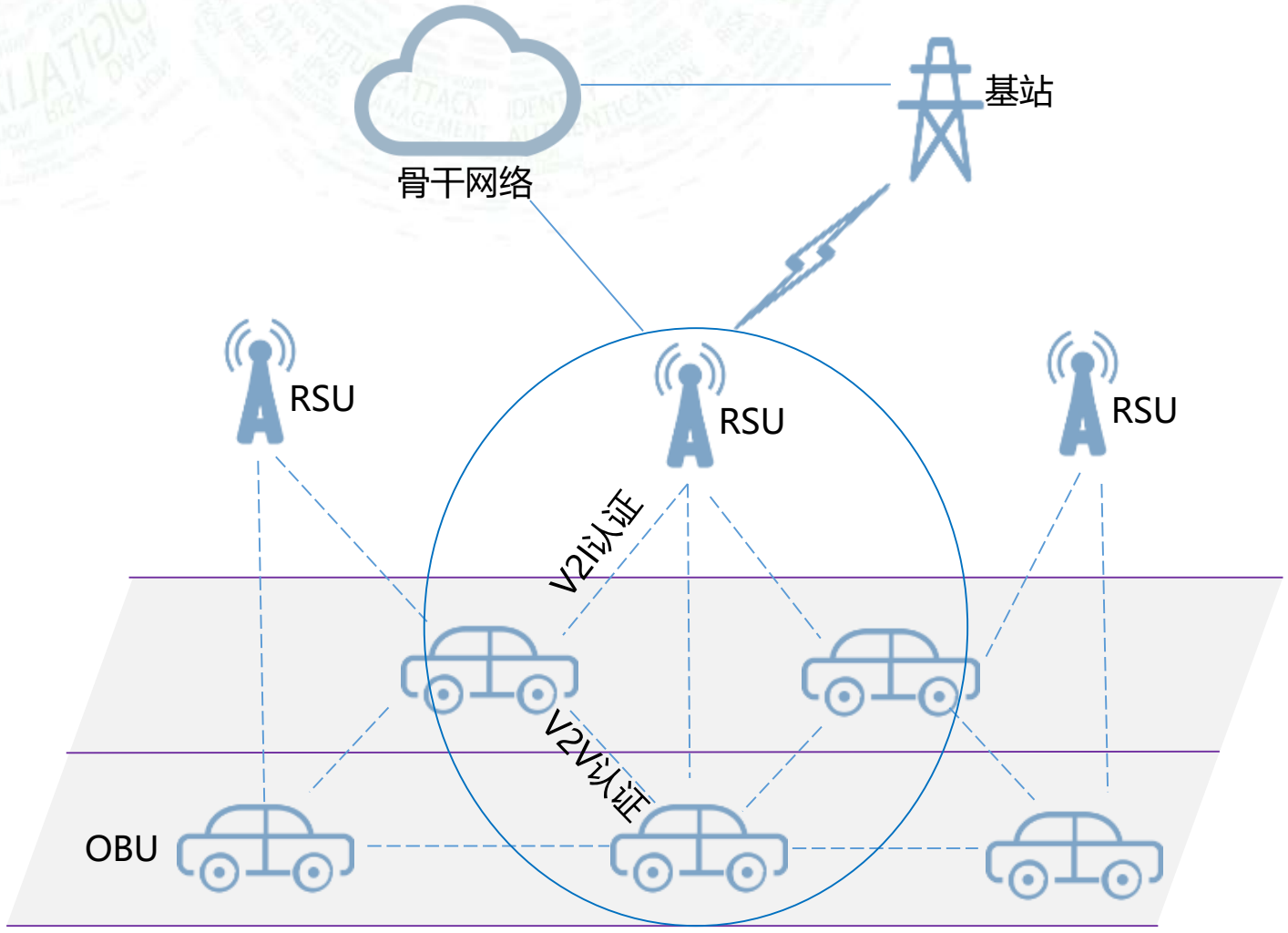
标识密码保障车联网安全——车联网架构



标识密码保障车联网安全——车联网安全威胁

序号	攻击目的	攻击手段	安全诉求
1	享受更好的道路资源	通过软件定义无线电等冒充RSU或者篡改合法RSU向其他车辆发布虚假的交通拥堵、事故等信息，以达到享受更好的道路资源目的。	RSU消息的认证性、完整性（车辆对RSU消息的认证）
2	非授权互联网接入服务	分析AP接入认证的漏洞，达到非授权的AP接入目的，享受免费的互联网接入服务。	车辆消息的认证性（AP对车辆的认证）
3	犯罪或交通事故逃避责任	通过在篡改车辆传输过程中的消息或篡改已保存的消息（如位置、时间等信息），制造不在场等证据，已达到逃避责任的目的	车辆消息的认证性、完整性、不可否认性（RSU对车辆、车辆对车辆的认证）
4	扰乱交通	可通过冒充RSU等多种手段发布虚假信息以扰乱交通秩序或制造事故	车辆、RSU消息的认证性、完整性、不可否认性。

标识密码保障车联网安全——V2V、V2I快速认证



V2V认证：

车辆A向车辆B发送的认证数据

车辆A的ID	消息数据	时间戳	签名值

车辆B向车辆A发送的认证数据

车辆B的ID	消息数据	时间戳	签名值

V2I认证：

车辆A向RSU发送的认证数据

车辆A的ID	消息数据	时间戳	签名值

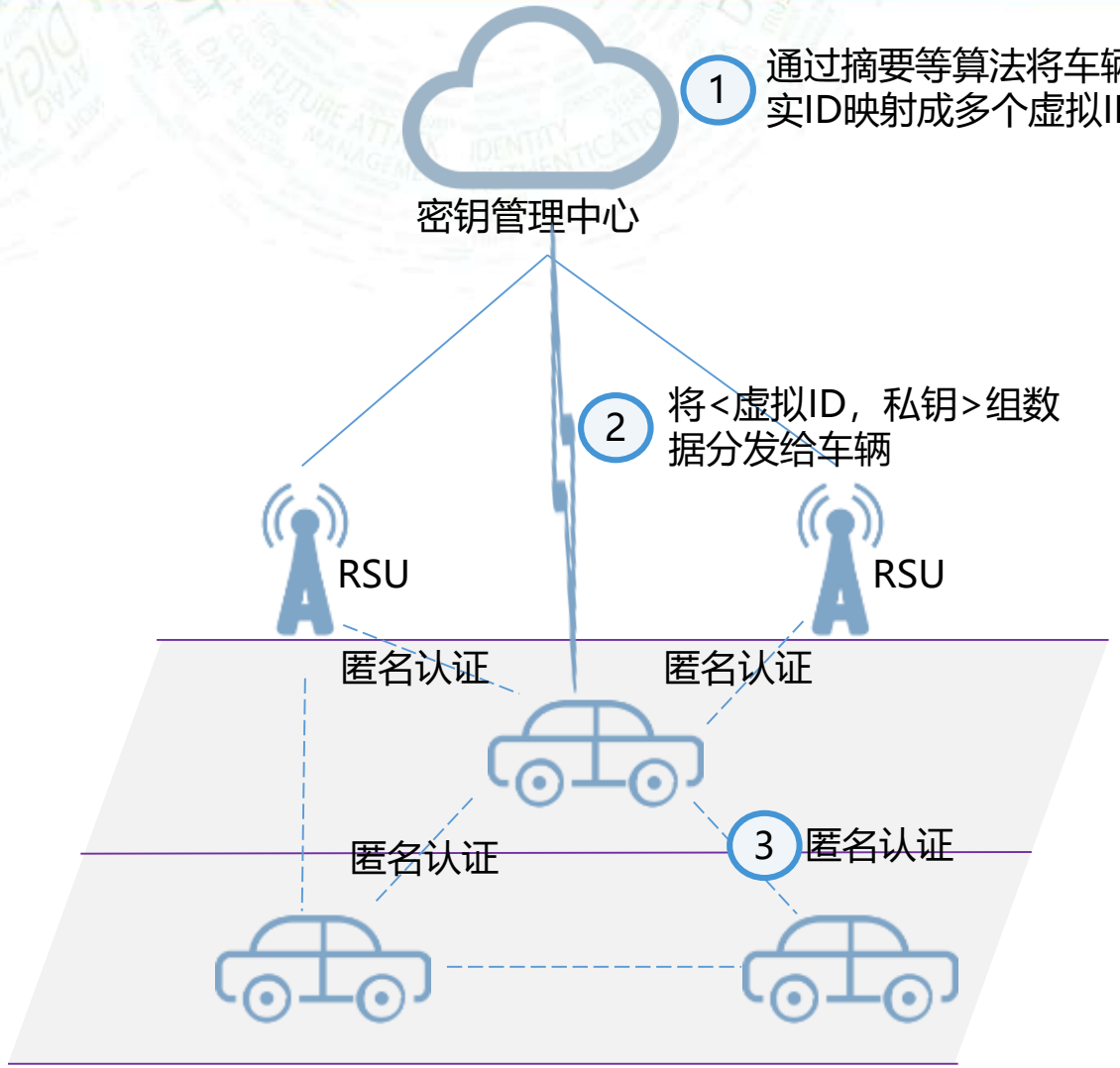
RSU向车辆A发送的认证数据

RSU的ID	消息数据	时间戳	签名值

基于ID的快速认证，认证速度快（无需验证书链），网络负载低（无需传输证书），解决了车辆和RSU发送消息的认证性、完整性和不可抵赖性。

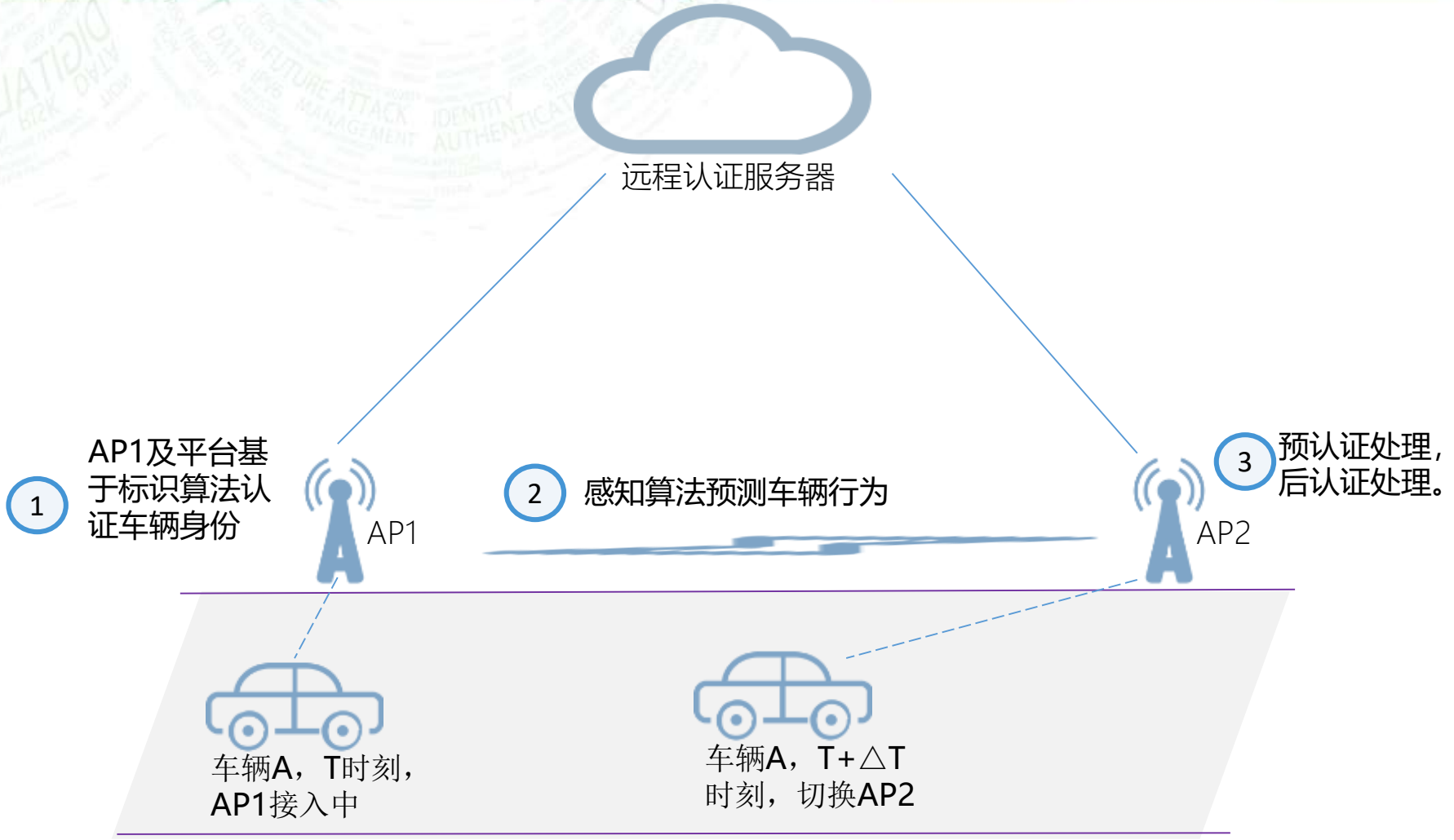
ZERO TRUST SECURITY

标识密码保障车联网安全——匿名认证



虚拟ID映射	• 将真实的VIN号等映射成虚拟ID，通过虚拟ID对应的私钥签名，保障了发送消息的匿名性
多虚拟ID机制	• 通过给车辆生成多个虚拟ID，车辆签名时可随机选择使用哪个虚拟ID私钥进行验签，避免使用同一ID被追踪路径
短时效的匿名ID	• 可将有效期作为匿名ID的一部分构成，验证方直接判断匿名ID是否失效
可追溯责任	• 车辆发生消息对其他车辆和RSU是匿名的，但密钥管理中心保存着真实ID的匹配关系，能够对签名主体进行追责。

标识密码保障车联网安全——基于移动预测的快速认证切换

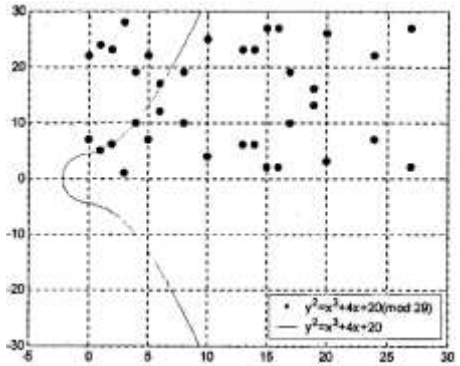


- 车辆请求AP或平台认证时，只携带标识、签名值等信息，无需携带证书，数据量小，极大减少了DSRC的带宽资源和传输速率的压力；
- AP或平台对车辆身份认证时，只需根据ID计算公钥，再对签名进行验证，而无需验证证书链，极大加快了验证的效率；
- 基于感知网络的预测，可提前进行预认证处理，加快了车辆在不同AP切换时的认证速度。

标识密码保障车联网安全——安全性分析

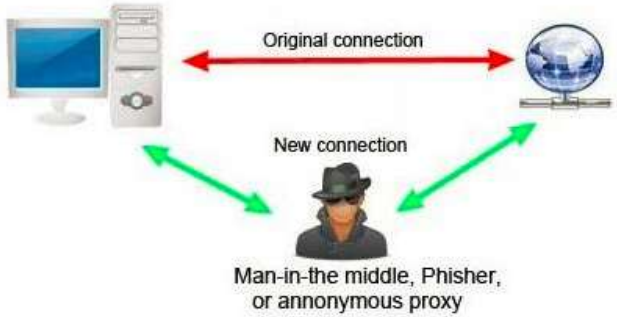
1 算法强度

- CPK算法是基于ECC/SM2算法根据ID组合出公钥，本质上是利用ECC的签名验签原理，因此其算法强度是等价于ECC/SM2算法的强度。



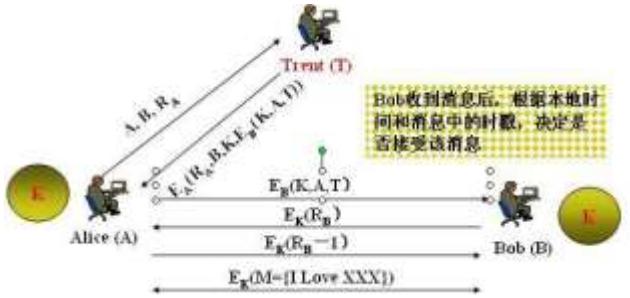
2 无中间人攻击

- CPK算法直接以用户ID绑定用户的公钥，无需第三方保证公钥的合法性，无需传递证书，不存在信任的传递，因此无中间人攻击。

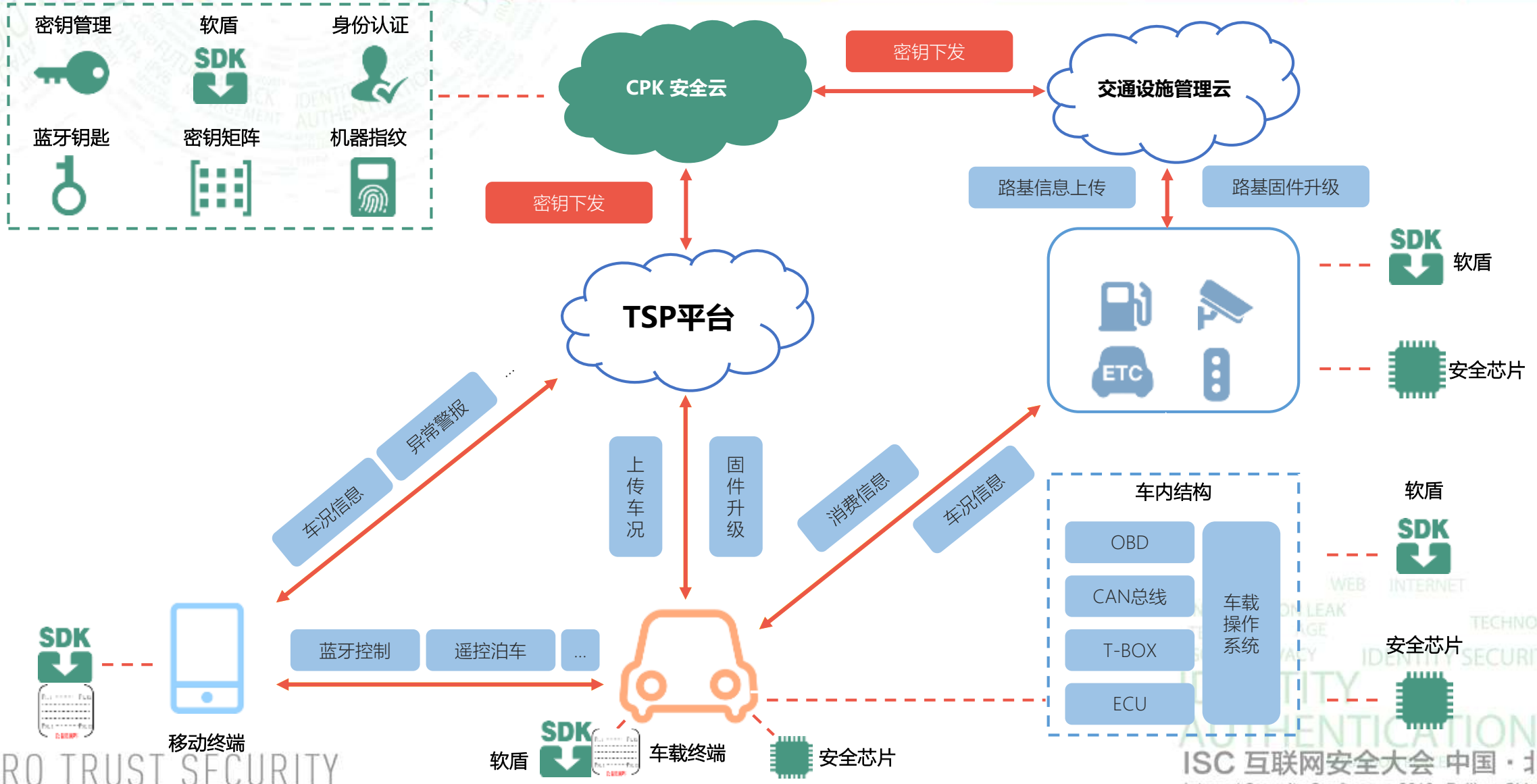


3 抗重放攻击

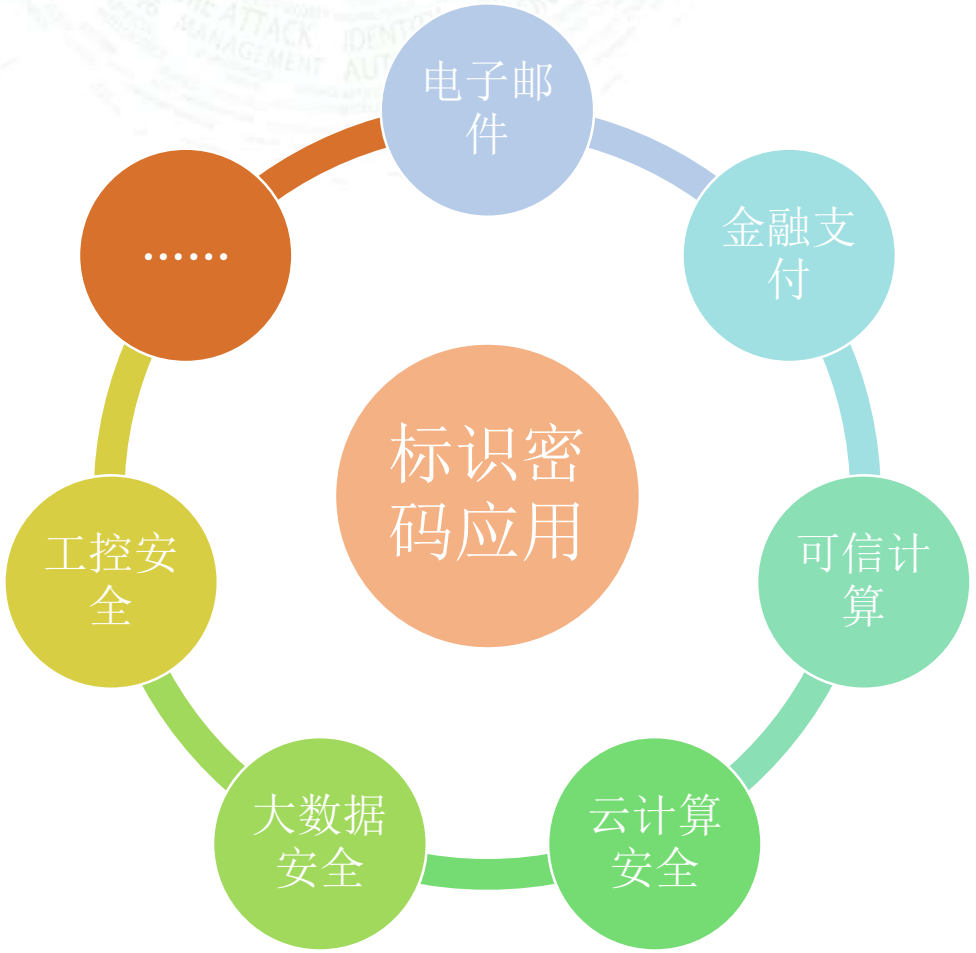
- V2X通信本身是高速运动状态下的认证，并且通信距离相对较短，重放攻击的实施条件较难具备；
- 认证报文中加入时间戳，有效抵抗重放攻击。



标识密码保障车联网安全——其他应用场景



标识密码其他创新应用场景



- 传统PKI的应用领域均可使用标识密码技术进行代替。
- 非对称加密业务场景中，标识密码相比于PKI始终是最优选择。
- 在多对多认证、通信带宽小、效率要求高等认证场景下，标识密码技术尤为适用。

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China