车联网安全数字证书应用解决方案

（V2.0）

中金金融认证中心

2018.10

目 录

一、 现状分析

随着移动互联、大数据、人工智能、云计算等新兴科技的快速发展，传统制造业将智能化、联网化作为产品转型升级的重要方向，“万物互联”已渗透至越来越多的细分领域，其中最具代表性的就是车联网。最近几年，全球的汽车厂商都在加快推出以网络互联、远程控制、自动驾驶为特点的智能网联汽车，汽车行业迎来重大的变革机遇和挑战。车联网赋予汽车更多的人车交互、车云交互业务场景，为车主提供更多的增值业务能力，已经成为车主在购车时愈加重要的评判标准。

而随着智能网联汽车从概念走向量产，越来越多的具备联网能力和远程控制功能的汽车出现在人们的日常生活中，伴随而来的车联网通信系统被黑客攻破，从而影响到车主人身安全、财产安全甚至国家公共安全的事件频频爆出，车联网安全已成为掣肘车联网创新的关键问题。

二、 安全需求分析

车联网安全问题主要是指由于车辆接入车联网而带来的开放网络安全问题，传统的开发式网络所面临的安全问题和安全需求对车联网来说同样存在和适用，包括可信身份、安全交互、授权认证和隐私保护这四个方面：

1. 可信身份

车端、云端、用户端在车联网中都需要有一个代表其身份的可信数字身份，可信数字身份是车联网云、管、端架构中各端通信互通的基础，相互之间交互信息的验证、加密都需要依托可信身份。

2. 安全交互

车端、云端、用户端在具体的业务流程中，如 OTA 固件升级、车辆信息采集传输至云平台、用户手机 APP 远程控车等，实现基于可信身份的业务层安全，避免非授权主体伪造

身份，获取、篡改、伪造业务信息和控制信息。

3. 授权认证

及为了达到安全交互的目的，业务系统基于各端的可信身份需设计一套安全的授权认证体系，有效标识不同身份主体之间的信任关系，并确保授权认证体系本身的安全性。

4. 隐私保护

即车辆的行车数据、位置数据、用户数据等均属于用户的隐私，这些数据在车辆本地存储、数据传输链路、云端存储中均应有加密机制和授权访问机制，确保用户的隐私不被恶意窃取

三、 PKI 数字证书体系介绍

3.1 互联网世界的安全基石

随着互联网、移动互联网在各行各业的快速渗透，线上业务的飞速发展也相应带来一系列安全问题。概括起来，网络用户所面临的安全问题有：保密性，如何保证互联网中涉及的大量保密信息在公开网络的传输过程中不被窃取；完整性，如何保证互联网中所传输的交易信息不被中途篡改及通过重复发送进行虚假交易；身份认证与授权，如何在互联网环境下对业务相关方进行身份认证，以保证业务相关方身份的正确性，抗抵赖，如何保证互联网业务的相关方无法否认已发生的交易。

为解决上述互联网安全问题，世界各国对其进行了多年的研究，形成了一套完整的网络安全解决方案， PKI 公钥基础设施采用数字证书管理公钥，通过认证中心 CA(Certificate Authority)，把主体的公钥和主体的其他标识信息（如名称、e-mail、身份证号、序列号等）进行绑定，结合主体的私钥和数字证书，在网络中验证主体身份，把传输的信息进行加密，保证信息传输的保密性、完整性，签名保证身份的真实性和抗抵赖。其中，信任服务主要是解决在茫茫网海中如何确认“你是你、我是我、他是他”的问题，PKI 是在网络上建立信任

体系最行之有效的技术。授权服务主要是解决在网络中“每个实体能干什么”的问题。在虚拟的网络中要想把现实模拟上去，必须建立这样一个适合网络环境的有效授权体系，而通过PKI 建立授权管理基础设施是在网络上建立有效授权的最佳选择。到目前为止，完善并正确实施的 PKI 系统是全面解决所有网络交易和通信安全问题的最佳途径，PKI/CA 体系已经在各行各业广泛应用，包括我们日常生活中切实能感受到的 HTTPS 网站，SSL VPN，IPsec VPN，网银 UKEY，税务 UKEY；还有无线通信基站、电表、国家安全等我们看不到的领域，都有 PKI/CA 安全体系在保证网络的安全，可以说 PKI/CA 体系构建了目前互联网世界的安全基石。

3.2 物联网安全的最佳选择

- 安全性

PKI/CA 支持 RSA2048/4096、SHA256/512、ECC、SM2、SM3 等非对称加密算法和哈希算法，相比于单纯采用 HMAC 的安全方案和 DH 密钥分发的对称加密方案具有更高的安全性。

- 成熟度

PKI/CA 技术经历 20 余年的发展和行业应用落地，经受住了大规模应用的考验，相比于标识密钥 IBC 体系、组合公钥 CPK 体系等近几年新研发的方案成熟度更高，同时 CPK、IBC 安全体系为了效率牺牲了 PKI/CA 身份认证和不可否认性的特点，方案可行性仍在讨论过程中。

- 可落地性

随着终端设备 CPU/MCU 运算能力的提升和专用加密芯片的应用，物联网终端设备应用 PKI/CA 的性能问题已不再构成门槛，越来越多的物联网终端设备已具备了证书应用的硬件基础，PKI 数字证书认证体系在物联网场景下的应用需求和价值愈加体现。

- 通用性

PKI/CA 系统的建设作为物联网企业的基础安全平台，在企业其它业务系统如 OA 办公、系统登录等多个场景得到应用，系统具有良好的扩展性，避免重复投资。

- 合规性

PKI/CA 体系作为目前安全性和成熟度最高的解决方案，在物联网各细分领域已发布和制定中的国家标准和行业标准中被广泛推荐，在若干细分领域的国标中甚至作为强制要求执行。

3.3 建设方式

- 自建 PKI-CA 系统

自建型 CA 中心一般主要服务于各个企业或者大型的行业，由用户方自行投资建设、管理、运营，主要为自己内部的应用系统或者业务系统提供服务，通过自建 CA 中心签发的数字证书为企业内部或者行业内部应用提供安全支撑。自建型 CA 中心建设的规模没有限制，根据用户自己的情况定制，功能也可以根据用户自己的需求来定制，但是此类 CA 只能服务于企业或者行业内部，由于没有通过《电子签名法》的认证，不能作为第三方 CA 认证机构向社会公众提供服务，因此自建型 CA 中心在法律效力方面没有保障，仅作为信息安全系统用于提高企业内部应用系统安全性。

- 第三方 PKI-CA 系统

根据 2005 年国家正式颁布的《电子签名法》以及《电子认证服务管理办法》，其规范了第三方 CA 数字认证中心建设必须的资质，譬如注册资金 3000 万人民币、系统物理环境软件以及硬件体系必须通过国家密码管理局的系统安全性审查、30 人的专业运营人员等等的一系列的要求，只有同时满足上述要求才能获得由国家信息产业部颁布的《电子认证服务许可证》，获得第三方数字认证机构的运营资格。通过第三方数字认证机构签发的数字证书，

在电子商务、电子政务、电子交易等等一系列的活动中均受到法律保护。那么对于用户来说也可以采用第三方数字认证机构签发的数字证书完成内部应用系统的安全加固，证书的整体运营由第三方数字认证机构完成，但是可以根据用户的具体情况为用户定制符合自身需求的注册机构、证书模板等等一系列个性化的服务。

四、 车联网 PKI 数字证书应用方案

4.1 设计原则

- 可用性原则

车联网中基于数字证书的安全应用方案设计应符合车联网发展现状，安全功能的增加和安全交互的设计应充分考虑车辆现有电子控制系统和硬件的兼容度、各参与方的实施复杂度、成本和客户体验，确保安全方案的可用性。

- 符合国家行业标准和政策的原则

目前车联网安全的国家标准和行业标准正在拟定中，车联网安全方案的设计思路应与国家的标准和政策思路保持一致，避免未来国家标准发布后安全体系面临重新设计的窘境。

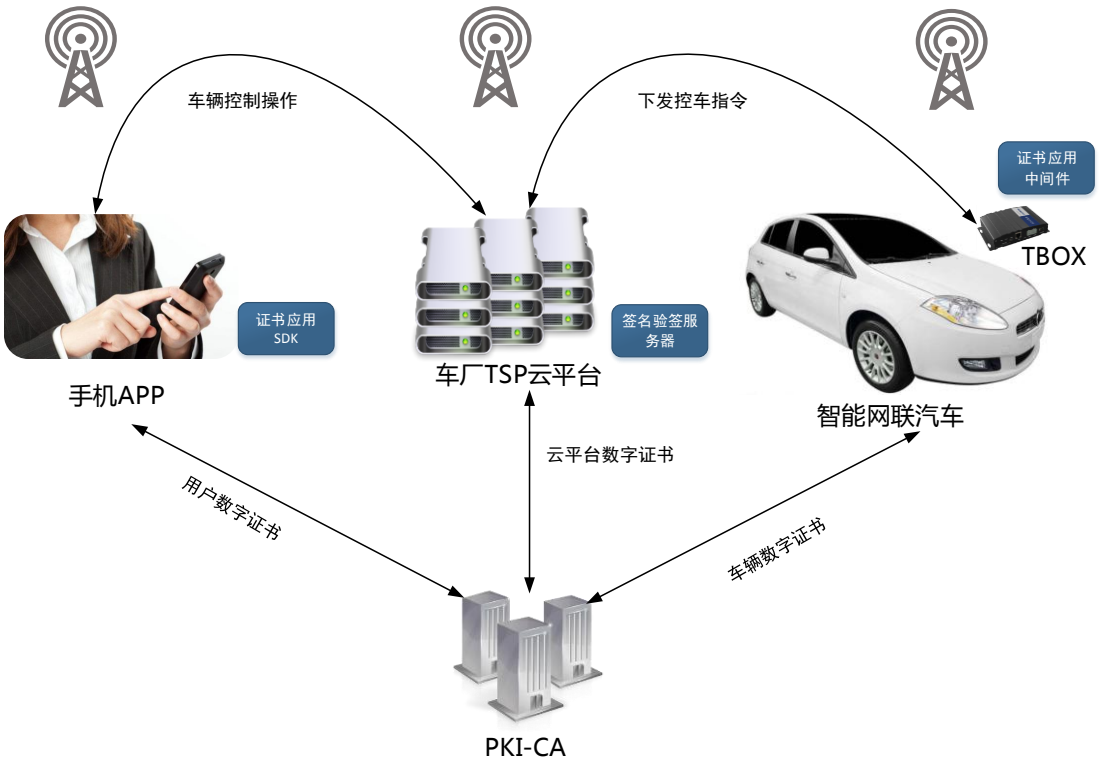
- 完整性原则

车联网的整体安全架构涉及车与车、车与人、车与云、人与云多个交互方式，安全方案的设计应完整考虑车端、云端、人端的一致性，确保每一端不存在安全短板。

- 可扩展性原则

车联网的数字证书安全方案设计应充分考虑后期应用规模及应用功能扩展能力，确保系统具有良好的扩展性，可以满足车联网今后较长时期业务发展的需求。

4.2 车联网通信安全架构



车联网通信安全架构中一般涉及车主 ,车厂 TSP 云平台和智能网联汽车这三个交互方：

a) 车厂业务系统以车架号 VIN 等车辆特征信息生成车辆公私钥对，并向 CA 系统批量申请车辆数字证书，车辆的私钥和数字证书文件分发至工厂相应批次的装车产线，在车辆下线前烧录至车辆相关的硬件模块（如 T-BOX、SIM 卡）中。车辆的私钥和数字证书在车联网中唯一标识车辆身份 ,TSP 云平台对智能网联汽车上报的行车数据通过车辆专属数字证书进行验证，确认数据的真实性和完整性。

b) 车主通过车厂官网或应用商店下载车联网 APP 到手机中，用于对归属自己的车辆进行信息交互和控制，用户在 APP 注册阶段完成实名身份认证和车辆归属认证后，对接 CA 系统申请一张代表用户身份的数字证书存储在手机中 ,后续人与车之间的信息交互均通过此数字证书进行验证，确保交互信息的正确性和真实性。

c) 车企 TSP 后台申请和部署服务器证书，TSP 后台向智能网联汽车发送信息和指令之前通过 TSP 服务器证书和车辆专属证书进行双向身份认证，身份认证后协商通信密钥对

后续的交互信息进行通信加密。

d) TSP 后台管理人员申请 USBKEY 数字证书，管理人员需插 KEY 登录 TSP 后台，在进行业务关键操作时使用 USBKEY 进行电子签名操作，确保操作行为可追溯。

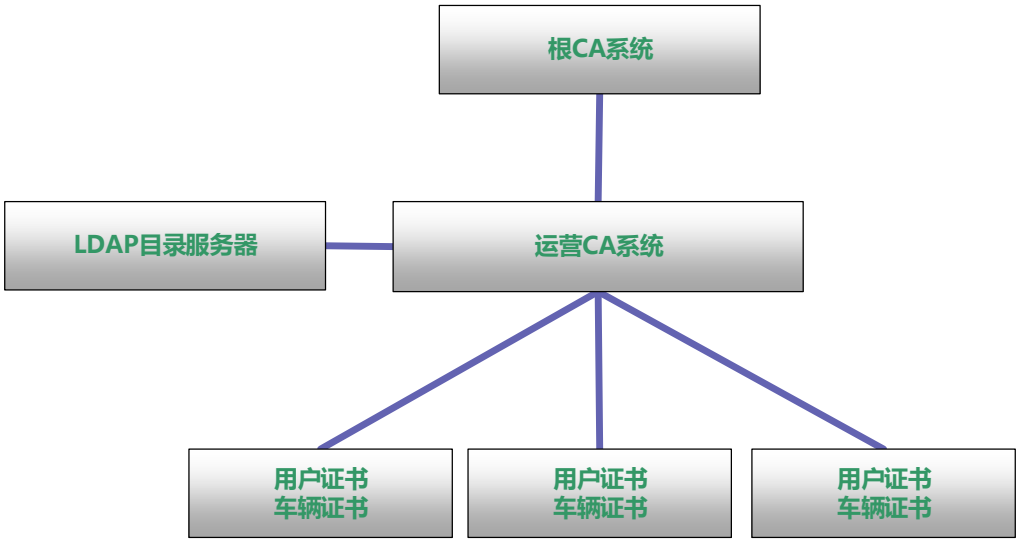
e) 通过数字证书全生命周期管理确保车联网各方身份的真实性、唯一性和黑名单机制，从而为车联网中的安全通信和安全应用打造一个可信的基础环境。

4.3 证书应用安全设计

4.3.1 自建 PKI-CA 建设

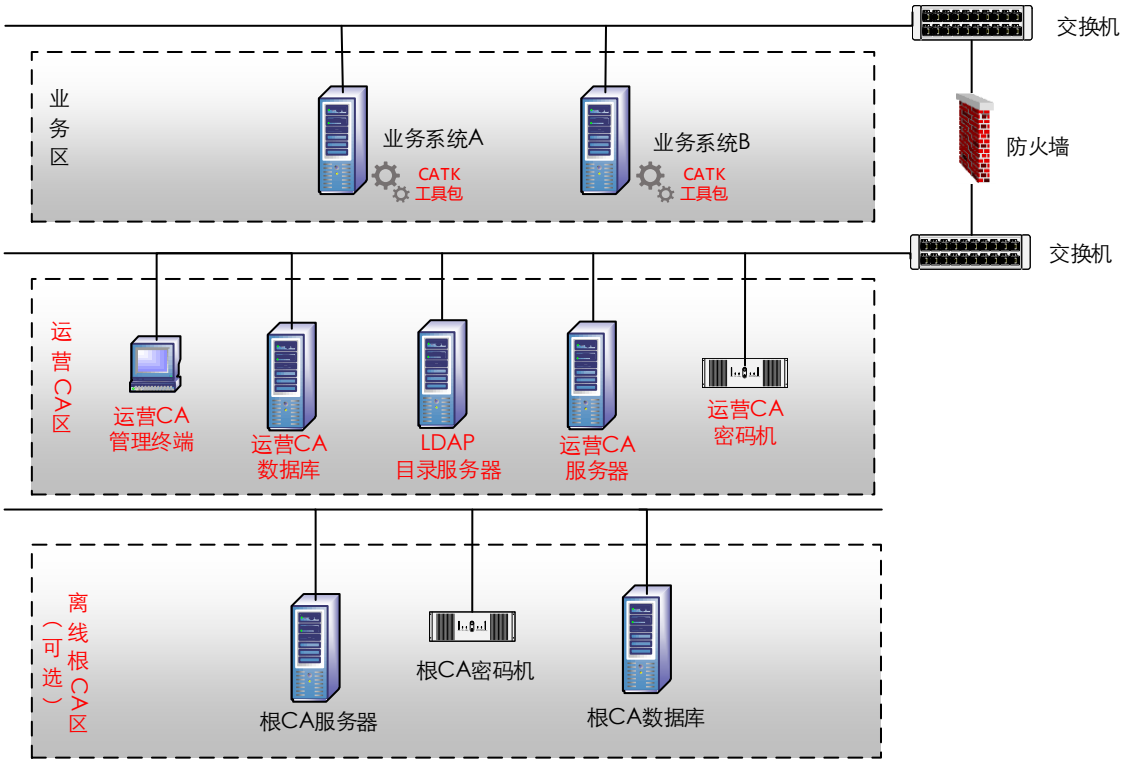
- 总体规划

CA 系统采取三层证书结构，分别是根 CA、运营 CA 和最终客户数字证书。根 CA 负责为运营 CA 签发 CA 公钥证书，运营 CA 的主要功能是签发和管理最终客户数字证书。我们设计的系统总体结构如下图所示。



根 CA 系统和运营 CA 系统支持签发 RSA 类型和 SM2 类型的数字证书，系统根据请求类型判断签发服务所使用的 CA 证书。CA 系统在 LDAP 目录服务器系统中发布 CRL，用户业务系统可以通过在线方式实现对 CRL 的查询。

- 体系架构



CA 系统

根 CA 系统：离线部署，用于签发下级在线 CA，如果只建设一个运营 CA 体系，根 CA 可以不进行建设部署。

运营 CA 系统：二级在线证书签发系统，负责证书的签发管理，所有证书的业务操作请求都提交到 CA 系统进行处理，包括证书签发、证书吊销、证书更新等。

CATK：连接 CA 系统的接口程序，是 CA 系统的应用开发接口，可以在业务系统中使用该接口提供证书的申请、下载等服务。

LDAP 目录服务系统

该系统对外提供发布公钥证书和证书注销列表（CRL）的查询服务。

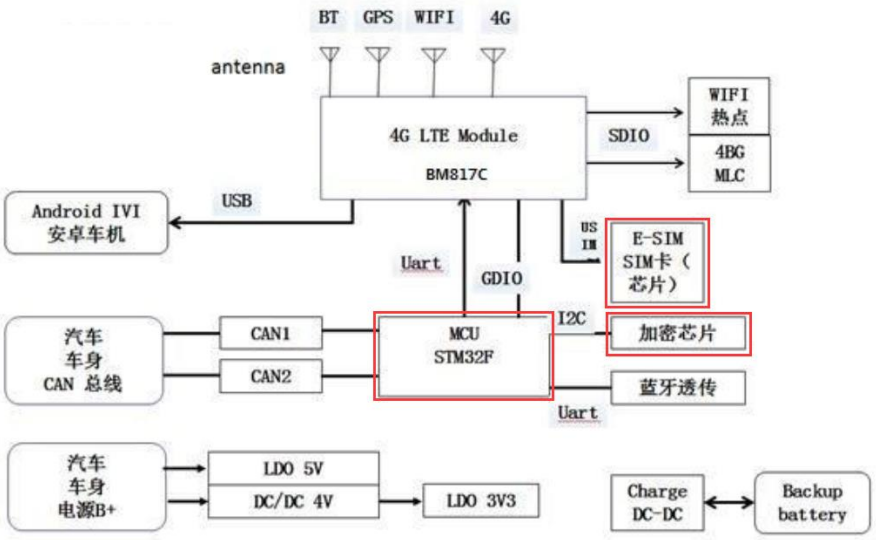
加密机

CA 系统的 CA 证书密钥和通讯密钥分别存放在各自的加密机中，负责提供密钥服务功

能，包括产生和存储密钥对，对 CA 系统提交的证书签发请求进行签发运算。为了保证根密钥的安全存储，建议另行购买一台加密机作为冷备负责将根、在线 CA 的密钥进行离线冷备，一旦主加密机出现故障或出现密钥损坏可快速从冷备设备中进行系统的恢复。

4.3.2 车端证书安全应用

TBOX 在车联网架构中处于连接智能网联汽车车内控制总线和车外网络的核心位置，是抵御车外开放网络安全攻击的关键安全设备，车端的数字证书安全应用将依托 TBOX 这一专用硬件设备落地实现，下图是典型的二代 TBOX 架构图如下所示：

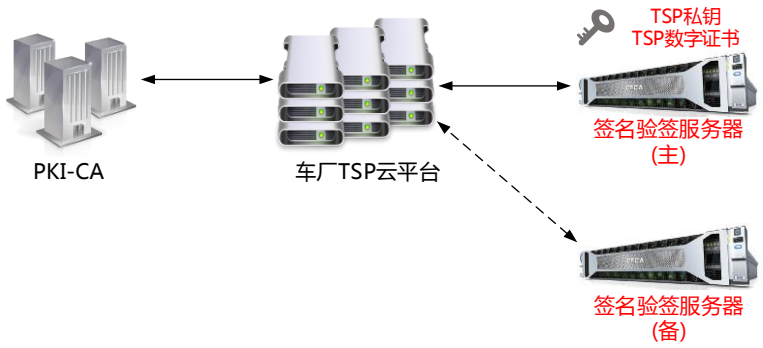


SIM 卡芯片和加密芯片（如有）均可作为数字证书安全应用的载体：

- 车厂后台业务系统根据 TBOX 终端的 IMSI 号或车架号 VIN 批量生成车辆公私钥对并对接 CA 批量申请车辆专属数字证书；
- 业务系统将某一批次的车辆对应的私钥、专属数字证书和可信证书链以文件形式发送至工厂产线，在汽车下线前烧录至 TBOX 的加密芯片中；
- 对于 TSP 发送的控制指令，TBOX 调用验签接口使用加密芯片中信任证书链进行验签，验签成功后通过 CAN 总线控制对应车身控制单元；
- 对于车辆相关上报信息，TBOX 调用签名接口使用加密芯片中私钥进行消息签名后

发送至 TSP 云平台，TSP 对上报数据进行验签确保信息无误后进行存储和大数据分析等增值业务应用。

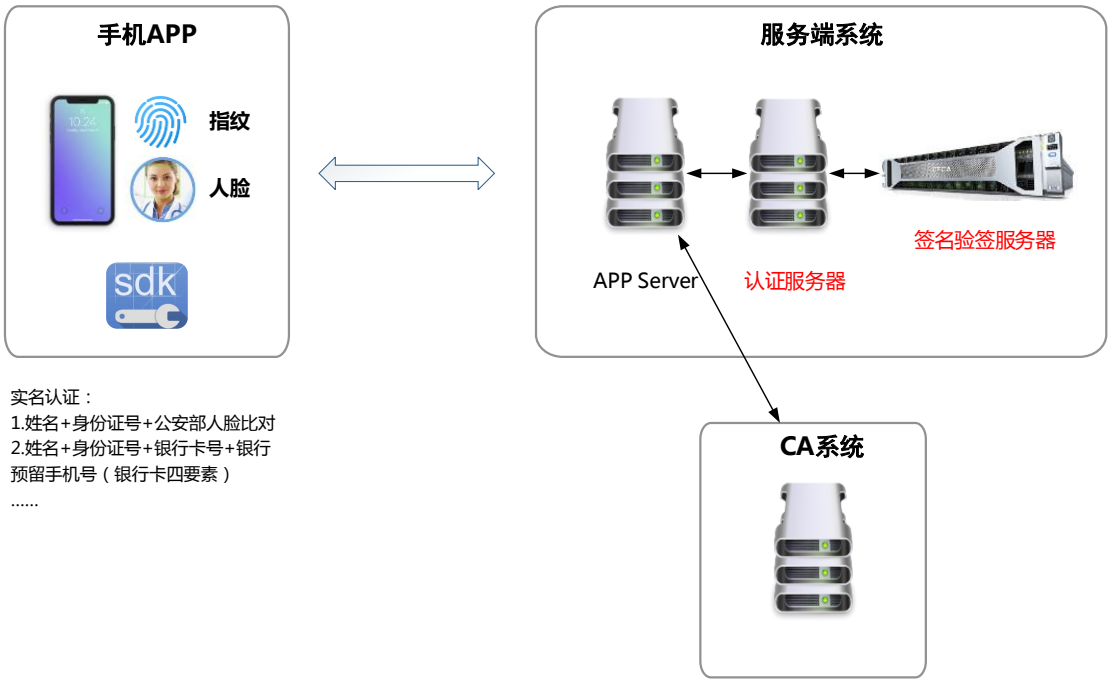
4.3.3 云端证书安全应用



车厂 TSP 云平台作为网联汽车、用户 APP、应用系统之间通信连接、信息传输、身份认证和业务鉴权的控制中心，是整个车联网架构的“大脑”，其安全性是整个车联网云、管、端的安全基石。

在 TSP 云平台的 PKI 数字证书应用方案中，需使用专用密码硬件设备（签名验签服务器）产生和存储 TSP 的公私钥对和数字证书，签名验签服务器中代表 TSP 云平台身份的私钥物理不可导出，确保云平台身份凭证的绝对安全性，同时采用主、备方式对签名验签服务器硬件进行备份。TSP 云平台和智能网联汽车、用户手机 APP 之间业务交互中涉及的签名、验签、加密、解密等密码运算由 TSP 平台调用签名验签服务器 API 接口实现，签名验签服务器作为专用密码硬件设备，对密码运算处理效率高，可以支撑 TSP 云平台高并发、高 TPS 的智能网联汽车管理需求。

4.3.4 手机端证书安全应用



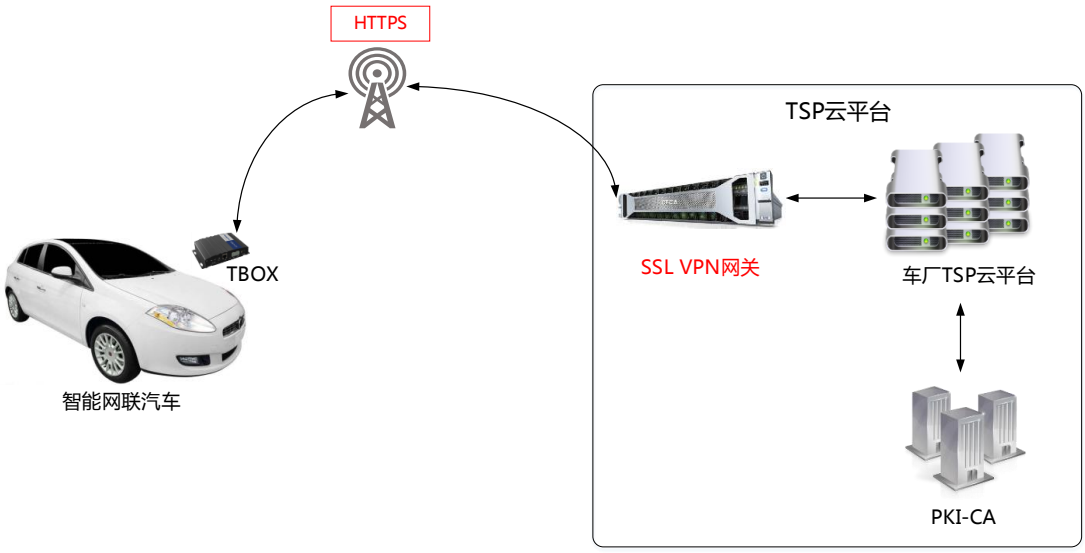
实名认证：
1.姓名+身份证号+公安部人脸比对
2.姓名+身份证号+银行卡号+银行预留手机号（银行卡四要素）
……

车厂提供的手机 APP 主要为车主提供诸如车辆信息查看、远程开启车门、打开空调、加热座椅等车辆远程控制类服务 ,在此基础上也可提供诸如面向车主的抵押贷款等金融增值服务。手机 APP 的使用需对车主的身份、行为进行有效识别和认证，对传输的数据进行严格的加密保护，同时 APP 的操作应实现高效便捷的用户体验：

- 车主在手机 APP 初次注册登录时，通过身份证+人脸识别、银行卡三、四要素等实名认证手段确保车主身份的真实性后为车主发放代表其线上身份的数字证书；
- 通过在手机 APP 中集成 FIDO+数字证书安全方案，用户可通过预存的指纹和人脸信息进行生物识别，避免后续使用过程中用户在 APP 登录和操作行为确认时的用户名、密码、短信验证码、PIN 码等繁琐的传统验证方式，大幅提升用户体验；通过密码技术和数字证书技术对用户行为的主体进行有效鉴定和追溯。

4.3.5 网络协议层安全应用

智能网联汽车 TSP 业务系统和车端 TBOX 之间的通信链路需采用安全网络协议（如 HTTPS）进行加固，确保接入双方的身份验证和交互数据加密。



智能网联汽车通过 TBOX 与远端 TSP 云平台建立连接，为保证 TBOX 与 TSP 之间通信链路的安全性，通过 HTTPS 协议基于两端的数字证书进行 TLS 握手，其中 TBOX 中 HTTPS 协议栈可以在 MCU 中或安全芯片中实现；TSP 云平台因为要与大量的智能网联汽车建立 HTTPS 连接，建议通过部署 SSL VPN 网关设备对智能网联汽车的 HTTPS 接入请求进行细粒度验证鉴权。

4.4 车联网典型安全应用场景

4.4.1 固件远程升级（FOTA）

- 前置条件：

  车载 T-BOX 中安全设置已在下线前正确设置；

  TSP 云平台正确配置 HTTPS；

- 操作流程

  1) TSP 云平台向需要固件升级的车辆批次的 TBOX 发送固件升级地址（HTTPS 地址）；

  2) TBOX 主动发起与 TSP 的 HTTPS 连接；

  3) TSP 对 TBOX 进行细粒度身份验证后建立 HTTPS 连接，发送固件升级包文件；

4) 固件升级包接收完毕，TBOX 进行升级包代码签名验证，验证无误后进行固件升级。

4.4.2 车辆无钥匙进入

- 前置条件：

  手机 APP 已注册认证并证书下载完毕；

  车载 T-BOX 中安全设置已在下线前正确设置；

- 操作流程：

  1) 手机 APP 开启蓝牙后与车载 T-BOX 配对成功，手机 APP 将开门信息使用其私钥进行数字签名。

  2) 签名信息通过蓝牙通信链路传输至车载 T-BOX ,车载 T-BOX 使用可信证书区的车主公钥证书对开门信息进行验签，验签成功通过 CAN 总线向相应控制单元发送控制指令，打开车门。

4.4.3 车辆数据回传云平台

车辆的运行数据和状态数据通过回传 TSP 云平台、大数据分析平台和第三方应用接入平台来进行数据的展现、分析和增值服务，其数据的真实性十分重要。

- 前置条件：

  车载 T-BOX 中安全设置已在下线前正确设置；

  TSP 云平台正确配置 HTTPS；

- 操作流程

  1) 车辆关键数据通过 TBOX 进行数据签名和加密后传输至 TSP，使用 TSP 公钥做数字信封；

  2) TSP 用自身公钥解开数字信封得到对称密钥对密文进行解密，查找对应 TBOX

的公钥证书对签名数据进行验签；解密验签无误，接受 TBOX 回传的车辆数据。

4.4.4 APP 远程控车

- 前置条件：

  手机 APP 已注册认证并证书下载完毕；

  车载 T-BOX 中安全设置已在下线前正确设置；

  TSP 云平台正确维护手机用户和智能网联汽车 TBOX 的对应关系。

- 操作流程：

  1) 手机用户登录车企 APP，进入绑定车辆，远程开启座椅加热；

  2) 手机 APP 使用私钥对控车指令进行电子签名后传递至 TSP；

  3) TSP 使用手机用户的公钥证书对指令签名信息进行验签，查询用户身份，确认用户与车辆的绑定授权关系；

  4) TSP 通过安全通信链路将控车指令传递至指定车辆；

  5) T-BOX 可根据信任证书的设置对控车指令进行验签，验签成功通过 CAN 总线向相应控制单元发送控制指令，打开座椅加热。

4.5 证书全生命周期管理

方案中涉及的车联网各方的数字证书应用，TSP 和手机 APP 的数字证书全生命周期管理可对接 CA 系统通过接口方式直接在线完成（包括证书申请、证书更新、证书吊销等），车载 T-BOX 的证书全生命周期管理考虑实际情况，可以采用两种方式，一种方式是在车辆下线前即提前申请并部署到 T-BOX 中，证书有效期可以设置为一个较长的时间（如 15 年）确保车辆在报废前无需更新数字证书。另外一种方式是车辆在首次初始化时自动产生公私钥对并在线申请和下载数字证书到 T-BOX 中，证书有效期设置为常见的 1-5 年，当证书到期

后自动在线进行密钥更新和证书更新。

五、 方案优势

1. 成熟完善的 PKI 数字证书应用体系

PKI 数字证书应用体系目前是唯一经过大规模实践验证的集网络身份验证和数据传输加密为一体的技术体系，日常生活中像 HTTPS 网站、网银 U 盾，报税盘，银行卡等均采用了 PKI 数字证书体系来保证安全，而且越来越显示出强大的生命力。相比于传统验证密码验证、MAC 验证、标识密钥体系等技术在安全级别、健壮性等方便有明显优势；

2. 安全的密钥管理

在车联网中代表各方身份的私钥以及预置的可信证书是整个车联网安全的基础，一旦代表身份的证书私钥被窃取，或者可信证书被恶意替换，第三方可毫不费力破译车辆与外界通信信息，给车辆及个人带来巨大的安全风险，本方案中车端的公私钥对均在 TBOX 安全芯片中产生，私钥不出芯片，可信根证书在车辆下线前即烧录在 TBOX 安全芯片中；同时云端的私钥和证书存放在加密机、签名验签服务器等专用硬件设备中；APP 端的私钥存储在手机的安全存储区，有效确保私钥的安全性。

3. 覆盖车端、云端、APP 端的整体安全设计

本方案对车联网中“云、管、端”架构体系的各个部分的安全保护体系进行了整体统一的设计，确保车端、云端、APP 端不留安全短板，同时整体安全方案的设计充分考虑了实施复杂度、用户体验和未来的扩展性。

4. 满足国内外政策导向和行业标准趋势

车联网数字证书安全解决方案的设计完全依照了国内网物联网、车联网领域的行业标准和政策导向，确保方案的合规性和前瞻性。