智能网联汽车
数字证书应用技术要求
研究报告

汽标委智能网联汽车分标委

信息安全技术研究组

2021 年 6 月

目录

前言

智能网联汽车在给人们带来巨大的便利性、舒适性和高效性的同时，自身也将面临巨大的信息安全挑战，基于密码技术的数字证书应用体系可为智能网联汽车的发展提供安全保障，然而国内智能网联汽车数字证书应用相关标准相对缺失，因此有必要尽快形成统一的技术要求和管理规范。

本研究报告拟对智能网联汽车数字证书应用及标准发展情况进行综述，并提出智能网联汽车数字证书应用技术要求标准化建议，为后续制定相关标准和推动标准落地提供支撑和借鉴。全文框架如下：第一章节，基于对智能网联汽车通信场景的分析介绍，对目前车用数字证书应用现状及所面临的主要问题进行分析，进而发掘梳理出车用数字证书应用需求；第二章从国内外车用数字证书应用标准发展现状以及国内现有成熟行业数字证书应用相关标准的发展情况进行了综述分析，为智能网联汽车数字证书应用技术要求标准的内容定位提供参考；第三章针对智能网联汽车数字证书应用标准化进行研究分析，进一步明确标准的定位，并梳理标准撰写思路，最后对标准大纲规划给出建议；第四章，就研究过程中待讨论确认的问题进行梳理分析，并给出建议解决方案，并为后续标准编制做好充分准备。

在此衷心感谢参加研究报告编写的各单位、组织及个人。

组织指导：汽标委智能网联汽车分标委

牵头单位：中国汽车技术研究中心有限公司、中国信息通信研究院

参与单位：国汽（北京）智能网联汽车研究院有限公司、重庆长安汽车股份有限公司、东风汽车集团有限公司技术中心、泛亚汽车技术中心有限公司、吉利汽车研究院、上汽通用五菱汽车股份有限公司、安徽江淮汽车集团股份有限公司、上汽大通汽车有限公司、上海蔚来汽车有限公司、广州小鹏汽车科技有限公司、襄阳达安汽车检测中心有限公司、华为技术有限公司、上海智能网联汽车技术中心、国家 ITS 中心智能驾驶及智能交通产业研究院、惠州市德赛西威汽车电子股份有限公司、郑州信大捷安信息技术股份有限公司、福特汽车（中国）有限公司、北京汽车研究总院有限公司、高通无线通信技术（中国）有限公司、北京数字认证股份有限公司。

参与人员：张亚楠、于润东、李宝田、李岩、赵万里、张文翠、张宁、李慧娟、高鸿、刘建行、汪向阳、舒畅、冯海涛、周伟、邓宇、王林林、尹顺林、陈俊名、陈金凤、林凯、潘凯、李旭华、徐敏杰、郑旭明、刘为华、陈艺、牟洪雨、王江胜、李广超。

一、智能网联汽车数字证书应用技术研究

1.1 智能网联汽车通信场景简介

智能网联汽车（简称 ICV）是指搭载先进的车载传感器、控制器、执行器等装置，融合现代通信与网络技术，实现车与 X（车、路、人、云等）的智能信息交换与共享，具备复杂环境感知、智能决策、协同控制等功能，可实现“安全、高效、舒适、节能”行驶，并最终可实现无人驾驶。

如图 1 所示，智能网联汽车通信涵盖了车-云通信、车-车通信、车-路通信、车-人通信及车内通信。

图 1 智能网联汽车通信场景

车-云通信指车辆的车载设备通过网络与云平台连接，实现云平台与车辆之间的数据交互。车云通信主要应用于车辆导航、车辆远程监控、紧急救援、信息娱乐服务等。另外，汽车软件远程升级是典型的运用车云通信的新型业务，汽车软件升级包由企业云服务平台进行下发，车端在接收与识别到正确的软件升级包后进行软件包的更新。

车-车通信指车辆间通过车载终端进行的实时通信。最普遍的应用场景是在城市街道与高速公路中，车辆之间相互通信，实现信息和数据的共享。智能汽车计算平台可以通过发送或接收车辆的时速、相对位置、刹车、直行还是左拐等所有与行驶安全相关的数据，甚至包括拍摄周围事物的图片或者音视频等，分析和预判其他车辆的驾驶行为，从而实现主动的安全策略，提升行驶安全，为半自动驾驶、自动驾驶提供数据支撑。此外，车辆也可通过转发自身及前方的实时信息来预防事故的发生，实现改善交通环境、减少交通拥堵的目的。

车-路通信指车载设备与路边基础设施（红绿灯、交通摄像头、路侧单元等）进行通信，路边基础设施获取附近区域环境的信息并发布各种实时信息。车-路通信应用主要包括交叉路口安全管理、车辆限速控制、电子收费、运输安全管理以及道路施工和限高警示等。智能

汽车计算平台通过强大的 CPU 处理接收的信息，结合 GPU 处理通过摄像头识别的图像以及辅助高精地图和云端支持，建立协同式环境感知系统，便于整个智慧城市的搭建。

车-人通信指车辆中的车载设备和弱势交通群体（包括行人、骑行者等）使用用户设备（如智能手机、可穿戴式设备、自行车 GNSS 信号仪等）进行通信。车与人通信主要应用于交通安全、智能钥匙、位置信息服务、汽车共享等。智能汽车计算平台基于安全通信，通过智能钥匙，实现无钥匙进入和远程启动等功能，同时还要通过强大的计算能力，实时推算行人或者骑行者的行动轨迹，为驾驶员提供驾驶预判，避免发生交通事故。

车内通信是以车载终端、车内的传感器及电子控制装置为通信主体进行通信而形成车内通信网络，主要涉及 CAN/CANFD、FlexRay、车载以太网等通信协议。以汽车软件远程升级技术为例，车端的网关或 T-Box 在接收到软件升级包后通过车载以太网或 CAN 总线将升级包发送给对应的 ECU，同时还需要将升级进度等信息发送给 HMI 设备，向用户展示升级情况。

1.2 智能网联汽车通信安全威胁分析与防护

1.2.1 车云通信安全威胁分析与防护

车云通信安全威胁主要来源于通信链路及云服务平台。如表 1 所示，通信链路的安全威胁主要有身份伪造、无效的证书验证、明文传输等。目前主要通过使用 PKI 体系进行安全防护，具体措施包括：在服务器端部署 TLS 证书来实现传输通道加密，确保机密数据传输安全；各种代码（PC 代码和移动 APP 代码）都要有数字签名，来保证代码的真实可信，防止代码被恶意篡改；连网设备具备可信计算证书，用于证明设备可信身份和加密各种通信数据。

表 1 车云通信-通信链路安全威胁

通信协议	威胁与风险	防护措施
HTTP（超文本传输协议）	窃听/嗅探/篡改	**对数据使用密码加密算法进行加密；** **使用数字证书证明对方身份；** **使用 TLS/TLCP 加密传输。**
	身份伪造	
HTTPS（安全套接层超文本传输协议）	已知的 TLS 攻击	升级 TLS 版本至 1.2 及以上； **确保对 TLS 证书的有效性验证。**
	无效的证书验证	

MQTT(消息队列遥测传输)	明文传输	使用 TLS/TLCP 加密传输； **使用 X509 证书对设备进行认证。**
TCP(传输控制协议)	会话劫持	使用 IPSEC 加密协议传输
4/5G(移动蜂窝通信协议)	伪基站监听	对伪基站进行识别

另外，汽车软件远程升级功能（OTA）作为车云通信中最常见的应用，其面临的威胁一直普遍存在。汽车软件远程升级功能（OTA）不仅可以对车载娱乐、导航、人机交互等应用软件进行版本迭代，还可以对悬挂、转向、制动、车身控制、ADAS 辅助驾驶等系统进行升级。软件升级包的传输面临着被恶意篡改的风险，如汽车制动系统软件被篡改后成功刷写到 ECU，则会导致汽车无法正常行驶或行驶过程中刹车失灵到严重后果。

1.2.2 车-车/路/人通信安全威胁分析与防护

车与车、人、路的通信主要是为辅助驾驶、自动驾驶提供车辆、行人与道路设备的实时信息，黑客篡改消息可实现对车辆的欺骗，造成交通拥堵或安全事故等。车与车、人的通信消息多是用户的位置、行动轨迹、行驶习惯等敏感信息，若被黑客窃听，将导致用户隐私信息的泄露。车人通信的另一典型应用是远程控车功能，主要包括控制车辆启动、熄火、开锁、关锁、寻车等，对其进行伪基站监听，可获取用户位置等隐私信息，还可利用伪造身份非法控制或盗取车辆。

智能网联汽车通过 LTE-V2X 等技术与临近车辆和路基设施进行通信，通过 WiFi、蓝牙等技术与用户的移动智能终端进行信息传递。安全威胁主要来源于无线通信协议、移动智能终端的移动应用软件等。

（1）C-V2X 通信面临的安全威胁及防护

V2X 网络通信安全包含蜂窝通信接口通信安全和直连通信安全。蜂窝通信接入过程中，终端与服务网络之间应支持双向认证，确认对方身份的合法性。蜂窝通信过程中，终端与服务网络应对网络信令支持加密、完整性以及抗重放保护，对用户数据支持加密保护，确保传输过程信息中不被窃听、伪造、篡改、重放。直连通信过程中，系统应支持对消息来源的认证，保证消息的合法性，支持对消息的完整性及抗重放保护，确保消息在传输时不被伪造、篡改、重放。应根据需要支持对消息的机密性保护，确保消息在传输时不被窃听，防止用户敏感信息泄露。直连通信过程中，系统应支持对真实身份标识及位置信息的隐藏，防止用户

隐私泄露。

（2）WiFi 通信面临的安全威胁及防护

建立 WiFi 通信连接前，需进行通信双方进行身份认证，只有在身份认证成功后，才能进行相应的通信交互，以防止非法接入与访问。在车联网 WiFi 通信中，应采用加密认证方式防止被破解，且建议使用 WPA/WPA-PSK 等以上安全级别的加密认证方法，对具有 WiFi 功能的车联网设备或系统，应在设备或系统出厂时设置用户名和密码，且每个设备或系统出厂设置的用户名和密码不同，并且在初次使用 WiFi 功能时，应提示用户修改 WiFi 用户名和密码，以降低被人为恶意连接或发生误连接的可能。

（3）蓝牙通信面临的安全威胁及防护

针对蓝牙安全，蓝牙标准中规定了五项基本的安全服务：

认证：基于蓝牙设备地址，验证正在通信的设备的身份。蓝牙不提供原生的用户认证机制；

机密性：确保只有被授权的设备能够访问和查看传输的数据，并对数据进行加密保护，以防止窃听导致的信息泄露；

授权：通过确保设备在被允许使用一项服务之前是已经被授权的，来允许其对资源的控制；

消息完整性：验证在两个蓝牙设备之间发送的消息在传输过程中没有被更改；

配对/绑定：创建一个或多个共享密钥和存储这些密钥以用于后续连接，以便形成可信设备对。

在部署和维护蓝牙网络时宜关注以下事项，包括但不限于：

a)制定蓝牙网络安全策略；

b)在部署蓝牙网络前，掌握构成蓝牙网络设备的安全特性，如身份认证功能、数据加密功能等；

c)定期对蓝牙网络的安全状态进行评估；

d)记录接入蓝牙网络设备的信息，如蓝牙物理地址、蓝牙名称等；

e)设置连续请求之间的时间间隔数值为指数级方式增长，防止攻击者重复验证身份。

配置蓝牙的连接及通信链路时宜关注以下事项，包括但不限于：

a)设备之间的通信链路启用加密；

b)设备之间的连接采用双向认证；

c)设备需提示用户对蓝牙连接进行授权；

d)限制蓝牙传输功率大小至仅能满足蓝牙设备间的通信要求，降低受到侧信道攻击的风险。

1.2.3 车内通信安全威胁分析及防护

车载通信设备主要包括汽车网关、车载诊断系统接口（OBD）、车载 TBOX 及车载信息

娱乐系统（IVI）等。汽车网关是汽车内部通信局域网的核心，若利用其总线路由功能，向车身控制器、转向控制器等核心控制器发起中间人攻击，篡改控制消息，可导致无法控制车门、无法控制车灯、电动助力转向功能失灵或被非法控制等严重后果。车载诊断系统接口（OBD）是智能网联汽车外部设备接入 CAN 总线的重要接口，若利用 UDS 协议功能，向车内 ECU 进行配置变更、写入恶意代码、读取敏感信息，轻则导致用户隐私泄露，重则危及交通安全。另外一种以高速的传输效率为优势的 DoIP 诊断是通过以太网直接与车辆进行连接，因此以太网传输过程中面临的安全威胁同样也会通过 OBD 接口渗透到车内。车载 TBOX 及车载信息娱乐系统（IVI）面临的威胁主要是数据篡改，导致向用户显示错误或非法诱导信息。

如表 2 所示，车内通信的安全威胁主要包括录制重放风险、通讯数据篡改风险、数据明文传输风险、中间人攻击等，可通过基于数字证书的身份认证、密钥安全存储、增加加密机制等防护措施保障车内通信的安全。

表 2 车内通信安全威胁分析

通信协议	威胁与风险	防护措施
CAN/CANFD 协议	录制重放风险	ECU 使用 Autosar 架构下的 SecOC 机制，增加新鲜值管理（计数器）和**身份校验功能防重放攻击**。
	通讯数据篡改风险	
	数据明文传输风险	ECU 使用安全芯片或其他加密模块对其他 ECU 做**身份的合法识别和认证。**
	泛洪攻击风险	使用 OBD 隔离防火墙设置白名单机制，过滤无效和恶意报文数据。
	非正常安全访问风险	使用安全访问算法，提高算法复杂度和**密钥安全存储机制**。
FlexRay 协议	数据明文传输风险	ECU 使用安全芯片或其他加密模块对其他 ECU 做身份的合法识别和认证。
车载 Ethernet 协	以太网 Dos 攻击风险	VLAN 虚拟隔离通讯，过滤/丢弃数据包。
	网络嗅探风险	

议	中间人攻击	使用安全协议 TLS，**通过提供加密和认证机制**，保证通信数据的隐私和完整性。
	DoIP 协议服务风险	建立安全的 DoIP 诊断安全访问服务，提高访问认证算法机制

1.3 数字证书在智能网联汽车的应用现状

从以上对智能网联汽车通信过程中面临的安全威胁及防护措施来看，数字证书可以有效解决智能网联汽车通信过程中的身份认证、消息安全传输、代码安全等安全需求。按照数字证书体系架构，数字证书主要分为 X509 数字证书体系和 V2X 数字证书体系。两种证书体系构建标准不同，签发出来的数字证书无论从编码上还是格式上也都有明显差异，以下分别是两种证书的体系架构图。

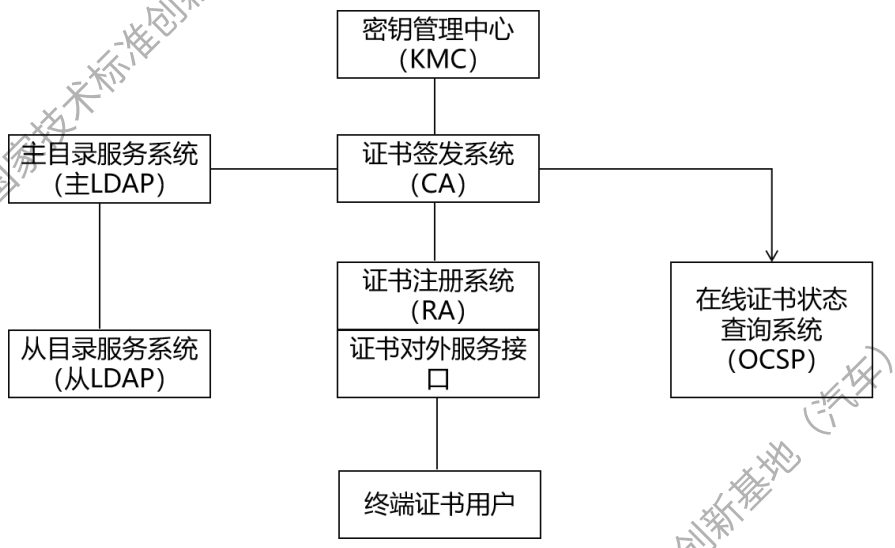

图 2 X509 CA 体系架构

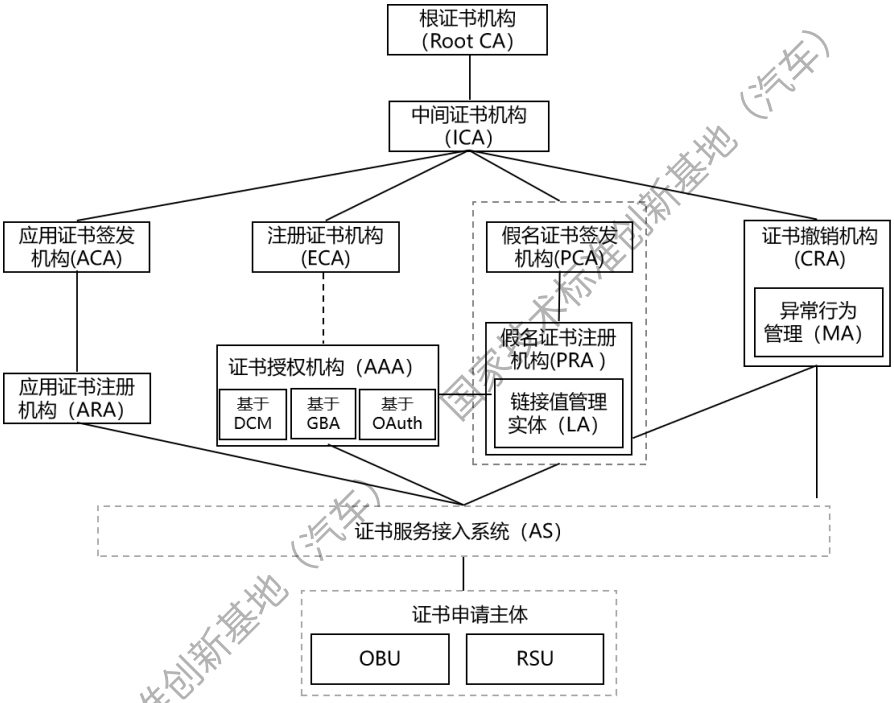

图 3 V2X CA 体系架构

X509 证书主要由 X509 CA 签发管理，X509 CA 通常包括证书签发系统、证书注册系统、密钥管理系统、目录服务器系统以及在线证书状态查询系统。证书的格式遵循 ITUT X.509 国际标准，证书编码是 DER 格式。证书包含一个公开密钥、名称以及证书授权中心的数字签名，一般情况下证书中还包括密钥的有效时间、发证机关的名称、证书的序列号等信息。广泛应用于互联网上的电子商务活动和电子政务活动，近些年也多用于车联网的车云通信。目前大部分车企已经或正在建设的数字证书体系以 X509CA 为主，面向企业内车辆、TSP 云平台服务器及平台系统管理员、车主 APP 等颁发 X509 证书，提供身份认证服务和证书应用支撑。

V2X 证书主要由 V2X CA 签发管理，V2X CA 架构体系和证书的格式主要参照 T/CCSA 307-2021《基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求》，证书编码是 OER 格式。与 X509 证书相比，V2X 证书中不包含证书 DN、证书自定义扩展项，但可针对证书应用的权限范围、地理范围等进行设置。V2X 证书是为适应车路协同 V2X 通信构建签发的一套数字证书，为车车、车路、车人直连通信提供高效率、低时延的安全认证，实现 V2X 通信中的身份认证、安全传输、数据完整性、有效性等安全特性，为智能网联汽车应用发展建立一个安全的网络运行环境。目前 V2X 数字证书体系和数字证书应用处于起步建设和试验测试阶段，尚未进入大规模商用。

以下将分别就数字证书在车联网各通信场景下的应用情况进行梳理分析。

1.3.1 数字证书在车云通信中的应用

数字证书在车云通信场景中主要用于实现车辆终端与云端业务系统在通信过程中双方的身份认证以及保证通信数据的安全传输，具体业务场景包括：车云数据交互、车端信息回传、服务端订阅内容推送、车端软件远程升级、车端故障远程诊断等。从目前的应用情况来看，车云通信过程中多以 X509 数字证书应用为主。

图 4 是基于 X509 数字证书的车云通信场景示例图，智能网联汽车和云平台分别向认证中心申请数字证书，智能网联汽车和云端的安全接入网关基于数字证书验证双方身份，确认双方身份合法性之后之后建立通信。针对敏感数据的传输，可采用安全通道的方式进行传输，或者使用对方证书公钥对数据安全加密后再进行传输，接收方收到密文消息后先使用己方私钥进行解密再做相应处理。

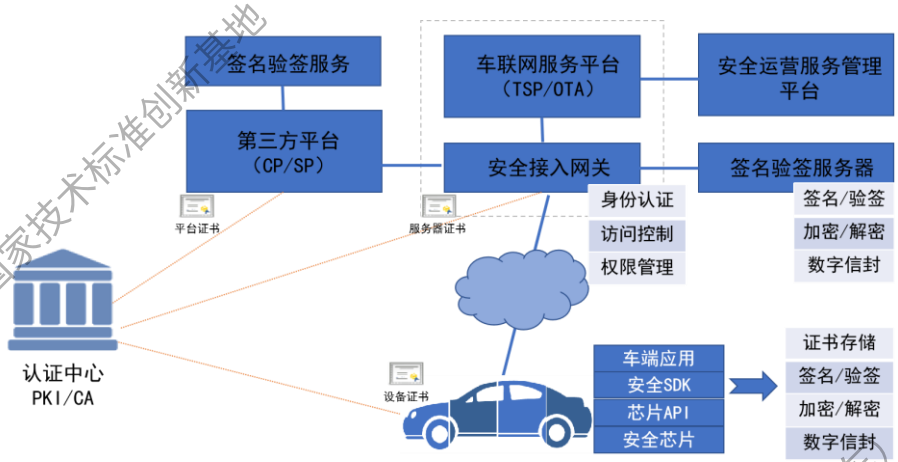

图 4 基于 X509 数字证书的车云通信示例

图 5 是 X509 数字证书在汽车软件远程升级过程中的应用，软件提供商、OTA 平台和智能网联汽车分别向认证中心申请数字证书，用于软件升级过程中的身份认证、安全传输等。软件供应商在提供升级包给 OTA 平台时，OTA 平台首先利用软件供应商的数字证书验证供应商身份的合法性，确认其身份合法后调用 PKI 服务对新版软件包进行数字签名，并将签名值和 OTA 平台自身的公钥证书保存到软件升级包中。车端的网关或 TBOX 在成功下载接收到升级包后，首先对软件包中的 OTA 平台证书合法性进行验证，然后对升级包进行验签，明确升级包来源的正确性以及升级包的完整性后，再执行升级包的刷写。

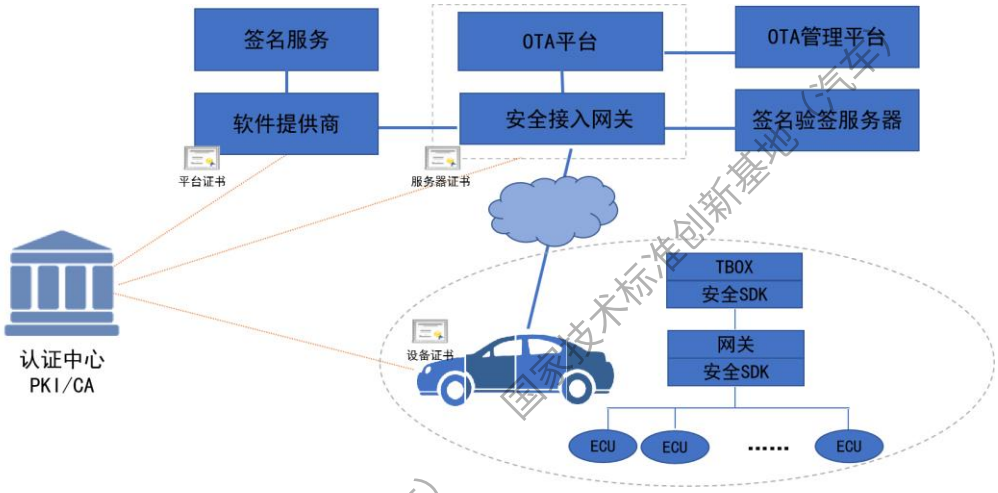

图 5 基于 X509 数字证书的汽车软件远程升级

1.3.2 数字证书在车车通信中的应用

为了满足 V2X 通信对低时延、高运算效率的需求，车车通信场景下对车端的数字证书编码格式、数字证书体量、基于数字证书的签名验签效率等都提出了更高要求。由于注册证书需要绑定车辆身份信息，相对较大，无法满足 V2X 低时延的需求，因此车车通信目前主要基于信息较少的假名证书实现车辆之间的身份验证。

以下以 V2X 假名证书应用为例，对车车通信场景下的数字证书应用进行分析说明。针对车辆行驶状态信息，需要使用假名 CA 签发给 OBU 的假名证书提供数字签名的保护，假名证书利用密码技术隐藏 OBU 或车辆的身份信息，以保护用户的隐私。发送方的 OBU 首先随机选用一张假名证书，并使用与假名证书对应的私钥对包含有其行驶状态信息的消息进行数字签名，再将该签名消息连同证书一起广播出去。周围接收到该消息的车辆首先验证消息中的签名证书是否有效，再利用通过验证的证书中的公钥验证签名消息中的签名是否正确，然后接收车辆利用通过验证的签名消息中的内容确定消息发送车辆的行驶状态。

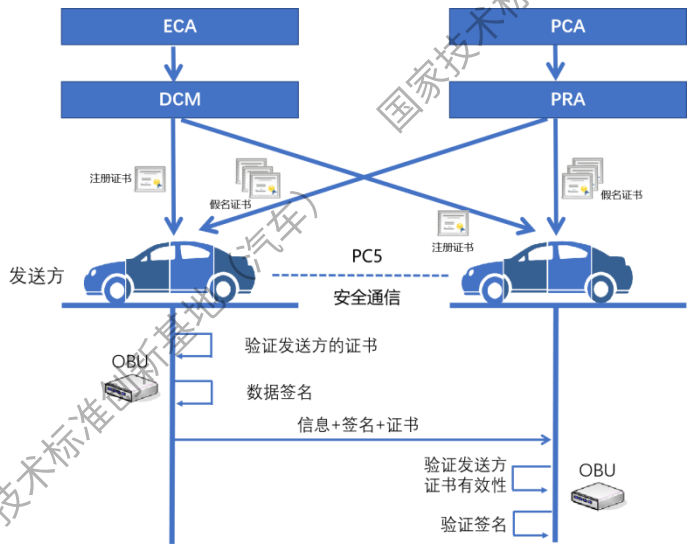

图 6 基于 V2X 数字证书的车车通信

1.3.3 数字证书在车路通信中的应用

基于 V2X 技术的车路通信指行驶车辆与道路侧的智能通信设备进行信息通信，以完成车端数据同步上传以及路侧端数据的广播下发及通知播报等业务。以下分别针对车路通信的四个典型场景的数字证书应用进行说明。

（1）车辆接收路侧设备的广播消息

车辆在行驶过程中，需要实时接收周围道路基础设施路侧设备 RSU 所广播的消息，道路设施管理机构需先向道路设施管理机构申请并下载应用证书，并利用应用证书对应的私钥对其播发的消息进行数字签名，并将其广播出去，该广播消息中还包含有应用证书。周围的车辆的车载 OBU 接收到该消息后，车载 OBU 首先验证该广播消息中的路侧设备 RSU 应用证书有效性，如果通过验证，继续利用该 RSU 证书中的公钥验证签名消息中的数字签名，若通过验证，则可以使用该广播消息携带的内容。

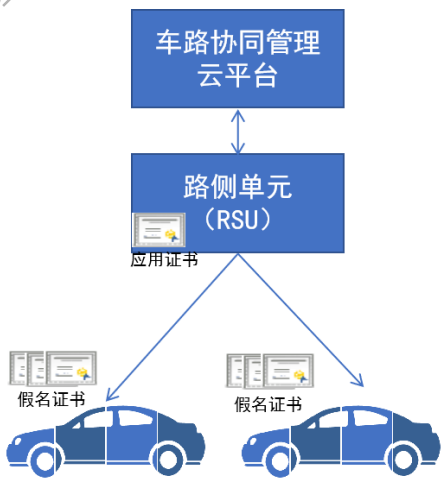

图 7 车辆接收路侧设备的广播消息

（2）特种车辆配置管理路侧设备

特种车辆（例如警车）需要控制一些道路基础设施的状态（例如交通信号灯）。道路基础设施 RSU 向道路设施管理机构申请应用证书，特种车辆车载 OBU 向道路设施管理机构申请身份证书。特种车辆上的车载 OBU 首先生成控制 RSU 状态的控制指令，并利用其身份证书对应的私钥对该控制指令进行数字签名，然后利用 RSU 的应用证书中的公钥对签名消息进行加密，生成签名加密消息，将签名加密消息和 OBU 身份证书广播出去。RSU 接收到该签名加密消息，首先利用与其公钥证书对应的私钥对消息进行解密，然后验证 OBU 的公钥证书，进而验证消息签名，最终获得控制指令，并执行该控制指令。

图 8 特种车辆配置管理路侧设备

（3）车辆 ETC 缴费

车辆在道路收费口需向道路管理部门结算并缴纳道路使用费用。路侧 RSU 和车辆的车载 OBU 分别向道路收费管理机构申请应用证书和用于道路缴费的身份证书。在道路收费入口，车载 OBU 获得入口处 RSU 的应用证书并使用其身份证书对应的私钥和入口 RSU 应用证书生成签名加密消息，并发送给入口 RSU，入口 RSU 解密并验证 OBU 的签名加密消息，确定 OBU 的起始位置。在道路收费出口，车载 OBU 获得出口 RSU 的应用证书，并使用其身份证书和出口 RSU 应用证书生成签名加密消息，并发送给出口 RSU。出口 RSU 解密并验证 OBU 的签名加密消息，确定 OBU 的结束位置。应用根据 OBU 的起始位置和结束位置，结合道路收费标准进行费用计算。

图 9 车辆 ETC 缴费

（4）电动汽车接入充电桩充电

目前电动汽车接入充电桩充电时，可以采用带外的方式进行通信，双方需互相验证对方

的合法性。在车辆与充电桩连接后，充电桩首先验证电动汽车的身份证书是否在黑名单中，如果不在黑名单中则进行身份认证，车辆对充电桩产生的随机数进行签名，充电桩对签名数据进行验证，验证通过后充电桩对电动汽车产生的随机数进行签名，电动汽车对签名数据进行验证，验证通过则完成充电桩和电动汽车的双向身份认证，这就保证了电动汽车与充电桩双方的合法受信身份，如果认证不通过则进行报警提示。下图是电动汽车接入充电桩充电时双方身份认证示意图。

图 10 电动汽车接入充电桩充电

1.3.4 数字证书在车内通信的安全应用

目前智能网联汽车内部对数字证书的应用主要体现在以下方面，一是用于车内网中各关联节点之间在通信过程中的身份认证，车内通信节点向 CA 认证中心申请身份证书，并利用证书对应的私钥签名、公钥验签技术实现对通信服务节点的合法性、真实性的确认，保证节点间传输的数据、信息、指令的真实性、完整性、不可篡改性。另外，诊断仪通过接入 OBD 接口实现对车内异常的诊断之前，OBD 接口与诊断仪分别向 CA 中心申请数字证书，在接入过程中完成双向身份认证，确保被授权的诊断仪才可访问车辆 OBD 接口。最后，车辆利用数字证书对应的私钥对 ECU 安全启动的固件或操作系统及应用软件进行代码签名保护，确保加载的软件未经篡改。以下是针对三种车内数字证书应用场景的示意图。

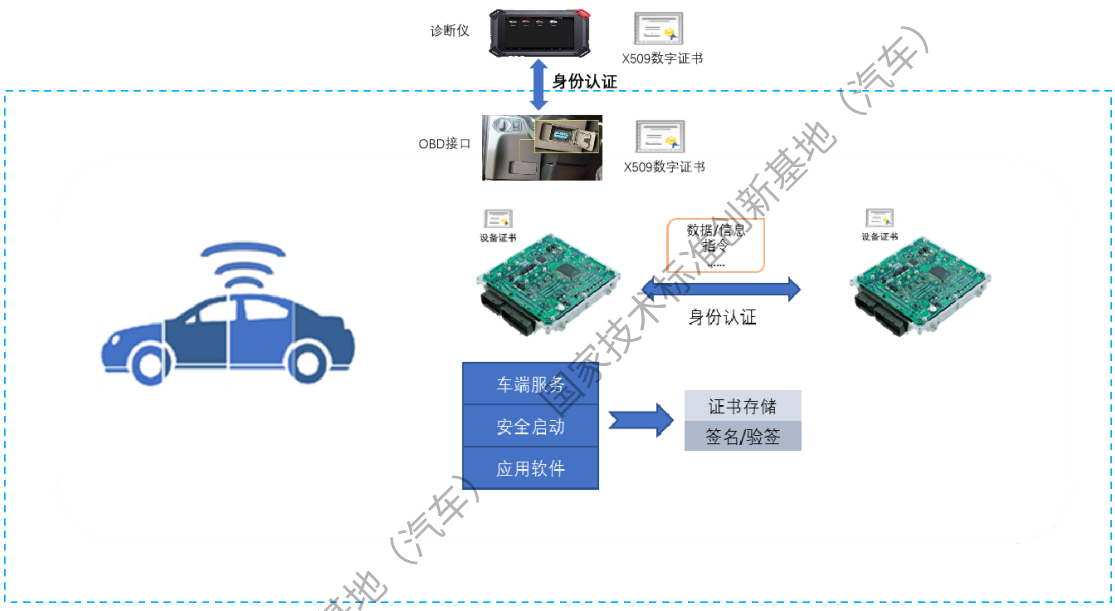

图 11 数字证书在车内通信中的应用

1.3.5 数字证书在车人通信中的应用

数字证书在车人通信中的典型应用场景是远程控车。远程控车依托于用户移动设备 APP，完成对关联车辆的远程开启、关闭、查看、钥匙分享等业务，移动设备 APP 发出的控车指令经由智能网联汽车服务平台转发到智能网联汽车终端，保证发送控车指令的移动设备 APP 的合法性和车辆收到的控车指令的完整性和保密性，是实现远程控车业务安全的关键所在。用户移动设备 APP、智能网联汽车服务平台和智能网联汽车均需向智能网联汽车认证中心申请数字证书，控车指令在用户移动设备 APP 发起端进行签名加密后发往服务平台，服务平台对收到的签名加密指令进行解密验签，验签通过后，再使用服务平台的数字证书对应的私钥和车辆的公钥证书，实现对控车指令的签名加密，并通过公共网络发放车辆终端，车辆终端针对收到的控车指令数据包分别进行解密和验签，确保控车指令的合法性和完整性。

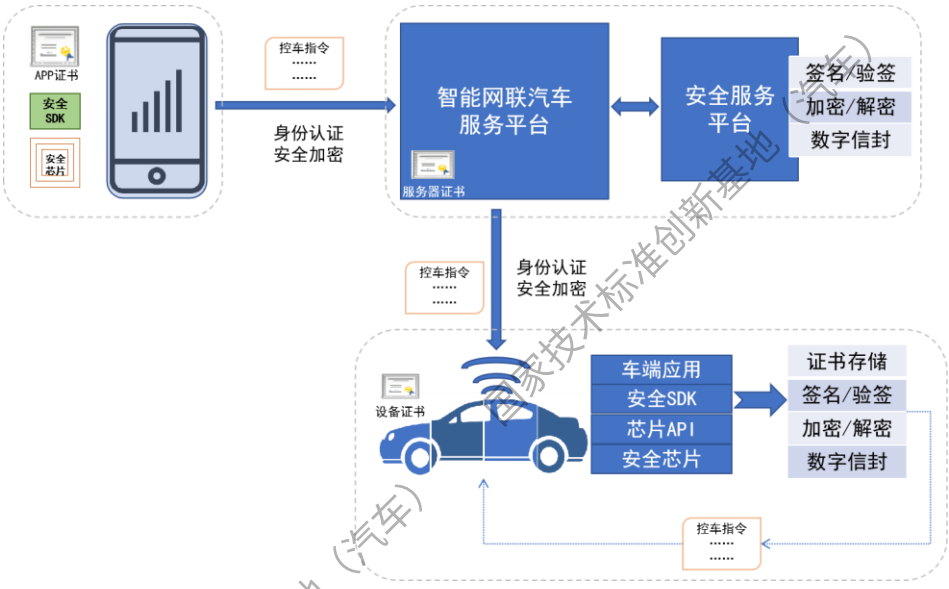

图 12 数字证书在远程控车中的应用

1.3.6 数字证书应用的检测

现阶段针对车用数字证书应用技术的检验工作，主要从以下几方面展开：

一是供应商内部检测，这个阶段的检验工作主要是针对证书应用软硬件产品的功能和证书应用对外接口的检验，此阶段的检验工作可参照相关部门已发布的证书应用产品的技术规范、管理要求、检测规范以及证书应用接口相关的标准规范。

二是车企基于证书应用业务的检验工作，包括集成应用证书之后，业务系统的可用性、稳定性和安全性等的检验，由于各车企业务内容和业务流程会有所不同，对于数字证书的集成方式和应用方式也会有所差异，此阶段目前尚无对应的检验标准可参考遵照，因此各车企检验范围、检验方法和检验结果判定标准也不尽相同。

三是在试验场地或开放式环境下基于场景的检验，多数车企现在还不具备大规模的开放式测试环境，因此会依托于第三方的测试平台开展一系列场景测试，第三方测试平台的测试依托于其测试场地基础设施的建设和配备情况，能够支持和模拟的测试场景也有所差异。

另外，政府、行业管理部门近几年也在持续开展多项应用示范工作，以推动具备安全身份认证的 V2X 通信应用尽快落地。IMT-2020（5G）推进组 C-V2X 工作组和中国智能网联汽车产业创新联盟于 2018 年开始逐年牵头组织了 C-V2X 的三跨、四跨和新四跨应用示范活动，主要针对 V2X 数字证书的安全初始配置及证书申请、通信过程中的签名验签、加解密等证书应用环节进行验证测试。2021 年上半年，工信部发文推动车联网身份认证与安全通信试点工作，重点面向智能汽车、路侧单元、云平台等车联网通信参与主体，针对车车、车路、车云、车人四类场景开展试点工作，其中数字证书在车联网各应用场景中的应用和管理作为一项重要的测试验证要求，各电信企业、互联网企业、汽车企业、安全企业、科研院所和示范区（基地）纷纷组队报名，参加示范试点。2021 年下半年，中汽中心将与信通院联合承

办 V2X 安全验证工作，依托天津（西青）国家级车联网先导区构建的 V2X 通信环境和场景，在开放道路上设计网络信任验证环境，设计 V2X 安全攻击场景，将验证车联网网络信任体系的安全保证能力以及验证测试数字证书在 V2X 通信过程中应用的可用性、合规性。

1.4 智能网联汽车数字证书应用面临的问题

通过对车用数字证书应用现状的研究，以及前期针对工作组成员单位数字证书应用现状的调研分析，梳理出车用数字证书在智能网联汽车领域的应用问题，包括：证书分类、内容、格式、证书申请灌装、根证书及信任链下载安装、证书有效期及更新、安全存储等通用问题，证书应用环境检查、身份认证、消息安全传输、代码保护等应用技术相关问题，以及数字证书应用的验证测试问题等。

1.4.1 数字证书应用面临的通用问题

1. 针对众多数字证书无分类要求及格式规范

由于智能网联汽车通信业务场景多样化，各场景对数字证书应用均有需求，且包含不同的证书应用实体，所申请使用的证书类型也不尽相同，因此目前各企业应用的数字证书类型较为多样化，如车云通信证书、注册证书、应用证书、身份证书、假名证书、车内节点证书、服务平台证书、移动 APP 证书等，但目前无统一的分类标准。另外，针对车联网的数字证书格式定义，虽然目前密标委、通标委和 ITS 标委都有各自的标准做了相应的规范，但是这些格式要求并未针对证书实际应用需求而定义，尤其对于特殊场景，如在 V2X 场景中，需考虑在有限通信带宽下如何定义证书格式才能更好地降低安全载荷的影响。因此，在实际的证书应用过程中，还需要结合证书应用场景、证书类型和应用需求进一步细化和统一规范数字证书分类及格式。

2. 数字证书内容存在较大差异

针对每种数字证书，由于证书用途有所差异，因此证书申请签发的数据项也有所差异，比如同是 X509 CA 签发的车云通信证书和车内节点证书，或者同是 V2X CA 签发的注册证书和假名证书，证书中所包含的数据项都有较明显的差异。这种由于在证书申请过程中存在大量企业自定义信息而导致的数字证书内容的差异性，也会影响证书应用的适用范围和证书应用技术实现，证书申请和管理都是为了证书应用做准备和支撑，因此，进一步确定数字证书的数据项、申请信息中包含的内容及关键数据结构定义也变得尤为重要。

3. 根证书、信任链、CRL 等初始化环节不规范

根 CA 是车联网安全体系中某个 PKI 系统中最高级别的 CA。根 CA 首先需要向自身签发一个自签名证书，该自签名证书又称为根证书，根证书是一个 PKI 系统中所有证书链的终结点，即该 PKI 系统的信任锚点。证书链是一个有序的证书列表，包含终端通信证书和证书颁发机构（CA）证书，使接收方能够验证发送方和所有 CA 是否值得信任。链或路径以终端通

信证书开头，链中的每个证书都由链中下一个证书标识的实体签名。CRL 证书吊销列表是 PKI 系统中的一个结构化数据文件，该文件包含了证书颁发机构 (CA) 已经吊销的证书的序列号及其吊销日期。以上三个文件是验证证书有效性的必须文件，需提前下载到验证者本地。目前针对车端根证书、信任链、CRL 文件的下载时机、下载流程、车端存储管理、更新检查验证的策略与流程尚不明确，需要明确相关的技术与管理要求，指导车企完成这些文件的下载安装，以便为证书应用做好准备。

4. 车用数字证书申请流程差异化明显且缺乏安全保障

目前车用数字证书的申请，根据车辆所处生命周期不同阶段和所属不同责任主体，可分别由零部件供应商申请、车企申请、车辆用户申请、4S 店售后申请。零部件供应商和车企主要在产线上完成数字证书的申请和下载安装，各企业在首次申请数字证书的流程差异较大，企业所选择的用于确认设备合法性的标识信息也各不相同，对于有些车企的证书密钥的生成和管理并未在车辆设备自身实现，不满足安全管理要求。由车辆用户申请数字证书主要是在车辆已经销售给实际用户之后，根据实际需要申请或更新车辆证书或者申请或更新车端应用 APP、车主移动设备 APP 的应用证书，如：基于出厂时车辆的注册证书申请或更新假名证书，基于车辆信息为移动 APP 申请用于控车的数字证书等。4S 店售后的证书管理多用于车辆硬件发生故障或证书本身出现问题时，主要涉及到车辆设备的证书注销、证书重申请、证书更新等操作管理。可见，数字证书申请时机和申请主体会根据实际情况不尽相同，目前由于缺乏统一的证书申请流程及操作规范，导致企业和用户在为车辆设备申请数字证书时的流程多样化，在设计实现上差异较大，且基本都缺乏与认证中心的安全认证机制，很可能为后续的证书应用埋下安全隐患。

5.针对数字证书有效期及更新缺乏统一管理

目前数字证书的有效期是由各车企的认证中心在签发数字证书时设定，各车企对于数字证书有效期的设置原则以及有效期长短取舍方面也存在一定的困惑，拿车云通信的 X509 证书为例，若企业采用数字证书在车辆下线前烧录进 TBOX 安全芯片，数字证书有效期过短，会导致车辆频繁需要重新部署证书，影响用户体验；若数字证书有效期过长，会导致证书因加密算法过时等原因不安全，因此车用数字证书的有效期需结合现实的可用性、易维护性和安全性等多方面综合考虑设定，并形成统一规范 。

另外，目前由于一些车企不清楚应如何监控检查证书有效期，不了解如何触发证书更新操作，以及对成功更新证书后应如何使用管理旧证书存有疑惑等，导致车企对证书有效期没有进行有效管理或识别，有些数字证书持有者或应用方在证书到期前未及时到认证中心更新证书，旧证书过期后，将被视为无效证书，继续使用会影响车辆的正常通信，若违规使用则会给整个车联网带来安全隐患。因此，在数字证书到期前的一段时间内，应完成数字证书的更新下载，以保证数字证书的有效性、安全性，从而保证车辆与云端系统、路侧设备、周边车辆及车辆内部的安全通信。

6.数字证书存储面临安全问题

随着数字证书被智能网联汽车越来越多的应用，有可能一辆车同时持有多张数字证书，由于车内核心零部件存储资源有限，再加上一些数字证书和对应的密钥本身体量较大，有可能不便于存储管理，有些企业的车用数字证书及密钥存储在车端系统和证书系统时，缺少必要的防护措施，可能会面临证书和密钥被恶意窃取或篡改的风险。还有些企业的数字证书是存放在系统软件内部的，更是增加了证书和对应的私钥被非法复制盗用的风险。对于配备数字证书的零部件，针对其信息安全相关的硬件配置要求，没有统一标准，整体安全性难以评估确认。因此，针对证书的安全存储，也需要有针对性的指导和规范说明。

1.4.2 数字证书应用技术面临的问题

1.数字证书与应用绑定管理要求不明确

数字证书的应用一方面解决了通信过程中的身份信任和信息安全的问题，另一方面也可以为企业的业务系统的权限管理提供解决思路，即将数字证书与业务系统的用户角色或操作权限进行绑定，为持有数字证书的实体赋予操作管理系统的权限，当业务系统基于数字证书的签名机制验证了请求实体身份的合法性之后，再验证该实体持有的证书是否具有访问操作业务系统的某一具体页面或功能及数据的权限。目前，车企基于数字证书实现系统用户权限管理的需求比较常见，但是真正实现应用的案例并不多，原因在于车企对于数字证书与应用系统的绑定管理流程以及相关的技术要求还不了解，因此，有必要针对数字证书与应用绑定的管理流程和技术要求进行规范说明。

2. 针对数字证书应用依赖的安全环境缺少检查机制

针对数字证书的操作和应用，很大程度上是对数字证书对应的公私钥的运算和使用，密钥运算需要有安全、可用的软硬件环境作为基础保障，同时由于证书应用主要体现在车辆通信的各场景中，那么自然也需要稳定的网络资源支撑。因此，在操作、应用或管理数字证书之前，应检查、验证证书应用所依赖的软件程序安全可用、硬件环境已上电且状态良好、网络状态稳定流畅，根证书、证书链及 CRL 注销列表已下载到本地且是最新版本，数字证书安全、有效、可用等，目前，这一系列相关的软硬件环境的安全检查无明确统一的范围和流程规范，缺少针对性的技术要求，因此，一些车企在证书应用环境的检查上有所忽略，缺少检查环节或者检查的内容覆盖不全，导致数字证书在应用过程中出现问题，影响了正常的业务运行。

3.数字证书有效性检查不全面

数字证书有效性是数字证书应用的基本前提，只有针对有效的证书，才可使用数字证书对应的公私钥进行签名验签运算，因此在应用数字证书之前需先检查证书有效性。目前大部分车企在数据签名验证之前基本都对签名证书的有效性进行了检查，但是在检查范围和颗粒度方面各有所侧重，或者说都存在不同程度的检查缺失；针对数据签名操作之前的证书有效性检查，很多车企并未涉及，而是直接调用证书对应的私钥进行运算，有可能会将无效证书和其对应的签名数据传播出去，直到接收方在验证签名证书有效性时才会发现此问题，如果

接收方对证书有效性验证不全面，未发现证书失效问题，会导致无效证书的滥用，从而引发安全问题。因此，针对证书有效性检查是保证证书有效应用的必要环节，需对检查范围、检查内容和相关技术要求进行规范化说明，指导车企全面有序的完成证书有效性检查。

4.数字证书应用技术要求不规范

目前智能网联汽车对于数字证书的应用主要体现在身份认证、消息加解密、代码签名等方面，如何将这些典型证书应用与业务需求结合并体现到实际的智能网联汽车通信场景中，以及这些典型应用涉及到的技术要求、实现流程以及注意事项有哪些，目前还没有相关的规范性的指导文件，因此若想统一智能网联汽车的数字证书应用，或减少各车企在证书应用过程中的问题，有必要规范化、标准化数字证书应用技术要求。

1.4.3 数字证书应用验证测试面临的问题

系统和车端集成应用数字证书之后，需经过测试验证无误后，方可投入生产运行，以避免由于数字证书的应用引起业务系统的功能、性能问题或给系统引入新的安全漏洞。目前测试工作基本都由各供应商或车企根据内部实际情况进行选择性测试，由于缺乏数字证书在智能网联汽车应用的测试经验，很多测试效果并不理想，一些问题会遗留到实际生产运营之后才暴露出来，这就增加了车企追踪、定位和解决问题的难度，也会给车企带来额外的投入和成本消耗。近两年，国家和行业也在牵头组织各种规模的示范验证测试活动，但是更多的是体现整体效果，针对数字证书的应用测试仍不够全面，也并非所有的车企都会报名参加活动。因此，有必要针对智能网联汽车的数字证书应用验证测试方法进行统一要求，其验证测试应至少应包括对数字证书通用性要求的符合性测试，以及数字证书应用技术要求符合性的测试。

1.4.4 数字证书应用的其他问题

1. 部分车企对证书应用场景及对应的证书应用仍不清晰

数字证书应用场景尚不统一，部分车企对其应用场景及对应流程仍不明确，目前用于智能网联汽车的数字证书包含了通用的 X.509 证书、交通专用证书、V2X 数字证书，这三类证书又根据实际业务需求和证书用途细分出更多类型的证书，如何在既定的场景中使用合适的证书是亟需解决的问题。

2.证书应用的互联互通还有待提升

由于企业在智能网联汽车数字证书应用过程中遵循标准差异较大，甚至存在部分企业无标准可依的情况，例如：不同 PKI 厂商签发的 X.509 证书，在根证书，信任链，算法，证书大小等都有所不同，没有统一标准，也无法实现不同车企间的证书互认。在实际工作中，当涉及切换到不同 PKI 厂商系统或不同车厂的项目时，车端数字证书 SDK 都需做对应的重新开发或移植适配。另外，在 V2X 通信场景里，涉及到车辆与车辆、人、道路、基站、云平台

等之间的通信过程，所以车辆与附近车辆、道路设施、便携式电子产品、电信运营商等之间都要能够验证发送方的真实性和完整性，这就要求数字证书能支持多种通信场景，适配各系统接口要求。

1.5 小结

本章先对智能网联汽车通信场景进行间接，进而对智能网联汽车网络安全面临的安全威胁进行了分析，针对安全威胁，分析总结目前的安全防护策略、选取的防护产品、引入的安全技术，得出基于密码技术的数字证书在增强智能网联汽车网络安全防护能力方面所能发挥的作用，并列举了数字证书在车联网通信过程中全应用情况。数字证书在被广泛应用于车联网解决通信安全问题的同时，数字证书在应用过程中也面临着不可忽略的问题，其中很大一部分问题可通过形成数字证书应用标准化并尽快推动证书应用标准的试点落地来验证解决。因此，我们有必要对目前国内外车联网数字证书相关标准化进展情况进行梳理分析，从而针对数字证书应用标准化体系的构建以及标准的定位、主要内容和编写思路等给出建议。

二、国内外数字证书相关标准分析

全国智能运输系统标准化技术委员会、全国信息安全标准化技术委员会、全国通信标准化技术委员会及国外的 ETSI、IEEE 等组织已开始着手数字证书标准化相关的工作，在数字证书接口、格式等方面提出了相应的标准。本章将在研究汽车行业数字证书相关标准与分析其他行业数字证书标准体系的基础上，探索汽车行业的数字证书标准体系建设思路。

2.1 汽车行业数字证书相关标准分析

2.1.1 国外相关标准发展现状

国外数字证书相关的标准多是由 ETSI（European Telecommunications Standards Institute）和 IEEE（Institute of Electrical and Electronics Engineers）两大组织提出的，如表 3 所示，主要从隐私保护与通信安全的角度规范了数字证书的正确应用。

表 3 国外相关标准发展现状

标准组织	标准名称	标准内容	说明
ETSI	ETSI TS 102 731 ITS; Security; Security Services and Architecture	规定了用于 ITS 环境中的安全和隐私保护通信机制，包含凭证和身份管理、隐私和匿名性、完整性保护、身份验证和授权功能；描述了 ETSI ITS 第 2 阶段安全体系结构，通过将安全服务及其功能组件映射到 ITS 体系结构，将第 2 阶段的安全体系结构和安全服务用作进一步开发 ITS 安全体系结构的基础。	由于欧洲涉及多个欧盟成员国，不同成员国可能使用来自不同PKI签发的证书，为此 ETSI 智能运输系统（ITS）技术委员会针对ITS发
	ETSI TS 102 940 ITS; Security; ITS communications security architecture and security management	规定了用于 ITS 通信的安全体系结构；标识了在 ITS 环境中支持安全性所需的功能实体，以及实体本身与 ETSI EN 302 665 中定义的 ITS 参考架构元素之间存在的关系；确定了一系列安全服务的作用和位置，以保护传输的信息和管理基本安全参数，其中包括标识和证书管理、PKI 流程和接口以及建立信任的基本策略和准则。	
	ETSI TS 102 941 ITS; Security; Trust and Privacy Management	规定了 ITS 通信的信任和隐私管理，基于 ETSI TS 102 731 中定义的安全服务和 ETSI TS 102 940 中定义的安全体系结构，确定了支持 ITS 环境中的安全性所需的信任建立和隐私管理以及之间存在的关系；指定了用于在 ITS 中建立和维护身份和加密密钥的安全服	

		务，目的是提供可以在 ITS 中建立信任和隐私系统的功能。	布了多项规范和标准。
	ETSI TS 102 942 ITS; Security; Access Control	规定了身份验证和授权服务，以避免未经授权访问 ITS 服务；指定了确保 ITS 消息通信所需的安全性和隐私级别的措施。	
	ETSI TS 102 943 ITS; Security; Confidentiality services	规定了一些服务，以确保发送到 ITS 终端和从 ITS 终端发送的信息的机密性可以保持在该终端的用户可以接受的水平上。	
	ETSI TS 103 097 ITS; Security; Security header and certificate formats	规定了 ITS 的安全头和证书格式，这些格式是专门为保护 G5 通信而定义的。	
IEEE	IEEE 车载无线通信标准 1609.2	该标准为密码安全服务相关的标准，定义了 WAVE 装置使用安全讯息封包格式及其处理程序，包含 WAVE 管理信息与应用信息安全保护方式；WAVE 标准定义了一种体系结构以及一组补充的标准化服务和接口，可共同实现安全的车对车（V2V）和车对基础设施（V2I）无线通信；描述了必要的管理功能以提供核心安全性功能。	解决了不同汽车制造商之间没有同类通信接口的问题。

2.1.2 国内相关标准发展现状

国内数字证书相关标准分国家标准、行业标准、国密标准及公共安全标准，如表 4 所示，主要涉及数字证书接口规范、数字证书格式、数字证书管理、认证系统等方面。

表 4 国内相关标准发展现状

标准类型	归口单位	标准名称	标准内容
国家标准（GB/T）	全国智能运输系统标准化技术委员会	《智能交通数字证书应用接口规范》	规定了智能运输系统中的数字证书应用接口和安全消息语法。
		《交通运输数字证书格式》	规定了交通运输信息系统中数字证书分类和数字证书格式。在国家对数字证书分类的基础上，结合交通运输信息系统各类应用场景，重点考虑了智能交通系

			统应用中，各类数据安全服务对数字证书长度、运算效率等方面的要求，对 ITS 设备证书的格式进行了规范化定义。
	全国汽车标准化技术委员会	《基于 LTE-V2X 直连通信的车载信息交互系统技术要求》	规定了基于 LTE-V2X 直连通信的车载信息交互系统的一般要求、系统功能要求、系统通信性能要求、定位定时要求以及测试方法等内容。
		《电动汽车充电系统信息安全技术要求》	规定了电动汽车充电系统车内系统信息安全技术要求和测试评价方法。
	全国信息安全标准化技术委员会	《数字证书策略分类分级规范》	通过分类分级的方式，规范了用于商业交易、设备和公众服务领域的电子认证服务中的 8 种数字证书策略。
		《车载网络设备信息安全技术要求》	对车载网络设备提出了信息安全要求，提出了应对直连通信消息进行签名，支持对接受的消息进行验签等内容。
行业标准（YD/T）	中国通信标准化协会	《基于 LTE 的车联网无线通信技术-安全证书管理系统技术要求》	规定了基于 LTE 的车联网无线通信技术安全证书管理系统技术要求，包括用于 LTE V2X 安全证书管理技术要求、安全证书管理系统架构和相关的显式证书格式及交互流程。
		《基于 LTE 的车联网无线通信技术-安全认证测试方法》	规定了基于 LTE 的车联网无线通信技术的安全认证检测方法，对基于 LTE 的车联网无线通信技术的安全认证测试方法的检测参数与指标、检测方法、检测规则进行了规范。
		《公众 IP 网络安全要求——基于数字证书的访问控制》	规定了根据用户所持有的数字证书对普通用户访问网络资源及有偿信息资源的访问控制要

			求，同时规定了基于 IPSec 的 VPN 中对等体之间利用数字证书进行认证的技术要求。
		《移动应用身份认证总体技术要求》	描述了移动互联网时代移动应用对用户进行身份认证的技术原理，规定了移动应用身份认证（MAA）体系结构，制定了移动应用身份认证（MAA）所需要支持的组件功能、消息流程、接口协议等方面的业务能力总体技术要求。
		《移动互联网应用程序开发者数字证书管理平台技术要求》	规定了移动互联网应用程序开发者数字证书管理平台关于证书申请、审核、发放、使用等方面的内容和具体要求。
		《移动互联网应用程序开发者数字证书管理平台接口规范》	规定了移动应用程序开发者、数字认证机构、移动应用商店及移动应用程序用户间数据接口的定义。
	中国通信标准化协会	《电子商务技术要求 第 3 部分：证书及认证系统》	规定了在进行电子商务交易过程中需要使用的数字证书及对数字证书进行认证的认证系统的技术要求，还规定了认证系统的结构、提供的服务、证书及 CRL、支持的算法、操作协议和管理协议的相关技术要求。
		《互联网码号资源公钥基础设施（RPKI）安全运行技术要求 证书策略与认证业务框架》	规范了互联网码号资源公钥基础设施（RPKI）系统安全运行设计的证书策略与认证业务框架。
		《移动通信网络域安全认证框架》	适用于使用网络安全域/网际互连协议（NDS/IP）或者传输层安全（TLS）的网元的认证。
		《基于安卓系统的移	规定了基于安卓操作系统的移

		动应用程序第三方数字签名技术要求》	动应用程序第三方数字签名架构、语法类型、签名流程，以及对移动终端的要求和签名接口要求。
		《移动应用程序代码签名技术要求》	规定了移动代码签名体系的技术要求，包括移动代码签名的定义、流程以及功能要求。
国密标准（GM/T）	国家密码管理局	《数字证书认证系统密码协议规范》	适用于基于密码技术的数字证书认证系统的设计、建设、检测、运营及管理，规范数字证书认证系统中密码协议的标准化应用，推动数字证书认证系统密码协议的互连互通和相互认证。对于组织或机构内部使用的数字证书认证系统密码协议的建设、运营及管理，可参考使用。
		《基于 SM2 密码算法的数字证书格式》	规定了数字证书和证书撤销列表的基本结构，并对数字证书和证书撤销列表中的各数据项内容进行了描述。本标准适用于数字证书认证系统的研发、数字证书认证机构的运营以及基于数字证书的安全应用。
		《证书应用综合服务接口规范》	规定了面向证书应用的统一服务接口。本标准适用于公钥密码应用技术体系下密码应用服务产品的开发，密码应用支撑平台的研制及检测，也可用于指导直接使用密码设备和密码服务的应用系统的集成和开发。
		《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》	规定了基于 SM2 密码算法的数字证书认证系统的密码及相关安全的技术要求，包括证书认证中心、密钥管理中心、密码算法、密码设备及接口等。

		《证书认证密钥管理系统检测规范》	规定了证书认证密钥管理系统的检测内容与检测方法。
	密码行业标准化技术委员会	《证书认证系统检测规范》	规定了证书认证系统的检测内容与检测方法。
		《数字证书互操作检测规范》	依据 GM/T 0015 和 GM/T 0034 的要求规定了数字证书互操作的检测内容与检测方法。
		《基于数字证书的身份鉴别接口规范》	规定了公钥密码基础设施体系上层应用中基于数字证书的身份鉴别接口。
公共安全标准（GA/T）	公安部计算机与信息处理标准化技术委员会	《公安数字证书硬件介质存储空间划分规则》	规定了公安数字证书硬件介质存储空间的划分规则，适用于公安数字证书的制作和使用。
		《取证与鉴定文书电子签名》	规定了取证与鉴定文书电子文档中的电子签名，适用于基于 PKI 的取证与鉴定文书的电子文档的电子签名。

2.2 其他行业标准体系分析

目前关于电子认证服务的基础法规有《电子签名法》《电子认证服务管理办法》，工信部可以依据以上法规对电子认证服务机构以及电子认证服务实施监督管理。基于法规和管理措施，各行业还制定了对应的管理办法和标准。

为更好地规划和制定智能网联汽车数字证书相关的标准，本章节分析与总结了金融、政务、卫生行业数字证书标准的经验，在标准规划和制定实施方面借鉴这些行业先进经验。

2.2.1 金融行业相关标准

表 5 为金融行业数字证书相关的标准。金融行业在标准体系的建设中，不仅善于借鉴国际已有的成熟标准，积极对国际已有标准的等同采用进行转化，还按照行业内具体的业务需要，制定对应业务实施匹配的数字证书和密码技术应用的行业标准，指导行业业务过程中技术落地实施工作。

表 5 金融行业数字证书相关标准

标准分类	归口单位	标准名称	标准内容
国家标准		《用于金融服务的	规定了通过证书策略和认证业务

（GB/T）		公钥基础设施 实施和策略框架》	说明对 PKI 进行管理，以及将公钥证书用于金融服务行业的要求框架。定义了风险管理的控制目标和控制程序。
		《金融业务 证书管理 第 1 部分：公钥证书》	定义了用于法人和自然人的金融业务证书管理系统，包括：凭证和证书内容；证书授权系统，包括用于数字签名和加密密钥管理的证书；证书的生成、分发、验证、更新；鉴别结构和认证路径；撤销和回复程序。
	全国金融标准化技术委员会	《银行业务 证书管理 第 2 部分: 证书扩展项》	规定了证书扩展项由金融服务行业使用证书扩展项的附加需求
行业标准（JR/T）		《金融电子认证规范》	规定了金融电子认证机构以及自建电子认证系统的机构所应遵循的要求，明确了金融电子认证管理和认证应用等内容。
		《保险电子签名技术应用规范》	规范了电子签名在保险业应用的技术要求和发生法律纠纷时应该采取的建议性措施
		《中国金融集成电路（IC）卡规范 第 17 部分：借记贷记应用安全增强规范》	描述了基于 SM2、SM3、SM4 算法的借记/贷记应用安全功能方面的要求以及为实现这些安全功能所涉及的安全机制和获准使用的加密算法，包括：基于 SM2、SM3 的 IC 卡脱机数据认证方法，基于 SM4 的 IC 卡和发卡行之间的通讯安全以及为实现这些安全功能所涉及的安全机制和加密算法的规范。

2.2.2 政务行业相关标准

表 6 为政务行业数字证书相关标准。政务行业的标准建设是以国密局制定电子政务电子

认证系列管理办法和要求作为建设依据和指导。由于政务场景比较复杂，需要更细化的标准支撑，有一些地方标准更具本地实施落地的接口规范，保证不同业务、不同系统间的互联互通。

表 6 政务行业数字证书相关标准

标准类型	归口单位	标准名称	标准内容
国家标准（GB/T）	国家信息安全标准化技术委员会	《信息安全技术 电子政务移动办公系统安全技术规范》	基于电子政务移动办公系统的安全风险，提出了电子政务移动办公系统的整体安全框架，规定了移动终端安全、信道安全、移动接入安全、服务端安全应满足的技术要求。对移动终端数字证书的使用也明确了相关要求，指导移动办公系统安全实施。
地方标准（DB11/T）	北京市经济和信息化委员会	《政务数字证书规范 第 1 部分：格式》	规定了电子政务外网中政务数字证书的格式，并给出了政务个人证书、政务机构证书、政务设备证书的模板，适用于数字证书认证机构、数字证书认证系统的开发商、电子政务应用部门以及基于数字证书的安全应用开发商，来设计和处理各类政务数字证书。
		《政务数字证书规范 第 2 部分：应用接口》	规定了电子政务外网中数字证书应用接口体系结构，各个接口函数的接口原型、功能、参数和返回值以及政务数字证书应用接口所需的宏定义、错误代码和调用示例，适用于数字证书认证机构、数字证书认证系统的开发商、电子政务应用部门以及基于数字证书的安全应用开发商进行信息系统建设。

2.2.3 卫生行业相关标准

表 7 为卫生行业数字证书相关标准。卫生行业管理体系整体比较完备，统一组织制定卫生行业系列管理规范，明确建设依据和指导。按照行业内具体的业务需要，制定更多对应业务实施匹配的数字证书和密码技术应用的标准，指导行业业务过程中技术落地实施工作。

表 7 卫生行业数字证书相关标准

标准类型	归口单位	标准名称	标准内容
国家标准（GB/Z）	中国标准化研究院	《健康信息学 公钥基础设施（PKI）第 1 部分：数字证书服务综述》	本部分定义了医疗保健数字证书的基本概念，给出了使用数字证书进行健康信息安全通信所需的互操作方案。本部分还给出了进行健康信息通信的主要利益相关方以及使用数字证书进行健康信息通信所需的主要安全服务。本部分简述了配置医疗保健数字证书所需的公钥密码算法和基本构建，并进一步介绍了不同类型的数字证书（包括标识证书、用于可依赖方的关联属性证书、自签名认证机构（CA）证书）以及 CA 等级体系与桥接结构。
		《健康信息学 公钥基础设施（PKI）第 2 部分: 证书轮廓》	本部分规定了在单独组织内部、不同组织之间和跨越管辖界限时医疗保健信息交换所需要的证书轮廓。本部分还详述了公钥基础设施（PKI）数字证书在医疗行业中形成的应用，并侧重描述了其中与证书轮廓相关的医疗保健问题。
		《健康信息学 公钥基础设施（PKI）第 3 部分: 认证机构的策略管理》	本部分为在医疗保健过程中包括配置使用数字证书在内的证书管理问题提供了指南。它规定了证书策略的结构和最低要求，包括认证实施生命的结构等。它还给出了为实现跨国界通信所需的医疗保健安全策略的基本原则，以及专门针对医疗保健方面的安全要求的最小级别。

2.3 小结

通过对现有标准的分析总结，目前我国缺乏智能网联汽车数字证书相关标准，无可遵循的统一规范，特别是证书格式、证书内容、安全存储等通用要求以及数字证书应用技术要求等相关标准的缺失将影响数字证书在智能网联汽车的应用与推广。

按照《国家车联网产业标准体系建设指南（智能网联汽车）》对智能网联汽车网络与信息安全标准建设的要求，以及《车联网（智能网联汽车）网络安全标准体系框架》对智能网联汽车安全、身份认证安全相关标准建设的要求，应借鉴其他行业细化业务需求、积极转化

国际标准的发展经验，尽快完善智能网联汽车数字证书标准体系，为数字证书在智能网联汽车的应用落地提供指导。

三、智能网联汽车数字证书应用标准化建议

智能网联汽车数字证书应用的标准化不仅需要符合行业标准体系的规划，还应更好的服务于企业。因此，项目组积极收集企业对数字证书应用标准化的需求和建议，结合前期对数字证书应用问题及现有标准的梳理，对智能网联汽车数字证书应用标准化提出具体建议。

3.1 数字证书应用标准化的企业调研分析

为了更有针对性的了解和获取各车企针对《智能网联汽车数字证书应用技术要求》标准编制的建议和需求，项目组在汽标委秘书处的支持和协助下，对企业针对数字证书应用相关标准需求和编制建议进行了调研，通过调研问卷方式搜集到部分车企针对该标准的编制建议，具体内容如下：

1. 建议标准中识别梳理车用数字证书应用场景，并针对数字证书应用场景、应用流程进行规范化；
2. 建议明确数字证书存储规范，明确数字证书管理技术要求；
3. 建议明确初次申请证书流程和技术要求；
4. 针对车企的数字证书申请模板进行规范化，明确对数字证书申请内容的具体要求；
5. 建议针对证书链、CRL 下发流程进行规范化，并明确技术要求；
6. 针对证书应用场景规范证书应用类型并定义证书有效期，并建议针对证书更新过程的安全技术要求进行规范化；
7. 建议制定基于数字证书安全通信过程中的技术要求，即在车联网业务应用中，如何基于数字证书技术提高通信双方的安全性；
8. 建议规范手机 APP 证书的下发和应用管理的技术要求，比如在一些手机控车、数字钥匙等安全应用过程中，如何进行移动终端数字证书应用和管理；
9. 规范车企自建平台包含的证书应用系统及功能，并针对证书的集成应用技术要求进行定义；
10. 建议国内外车企共同参与标准定制，以便于标准的国际化，增强对国外车企证书应用落地实施的指导；
11. 建议标准满足未来 10 年以内应用场景、业务流程和技术要求，尤其针对车路协同、互联互通的证书应用标准化的升级和扩展留出空间。

根据实际调研分析得出的数字证书在应用过程中存在的问题和实际需求，以及车企针对标准编制的诉求和建议，我们考虑按如下思路进行《智能网联汽车数字证书应用技术要求》标准的编制。

3.2 标准定位

2021 年 6 月 21 日工业和信息化部公布了组织编制的《车联网（智能网联汽车）网络安全标准体系建设指南》（征求意见稿），如图 13 所示，车联网（智能网联汽车）网络安全标准体系框架包括总体与基础共性、终端与设施安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等六个部分，其中密码应用标准主要规范车联网（智能网联汽车）密码应用通用要求，明确数字证书格式、数字证书应用、设备密码应用等方面要求，与本次智能网联汽车数字证书应用标准化研究的目标相符。

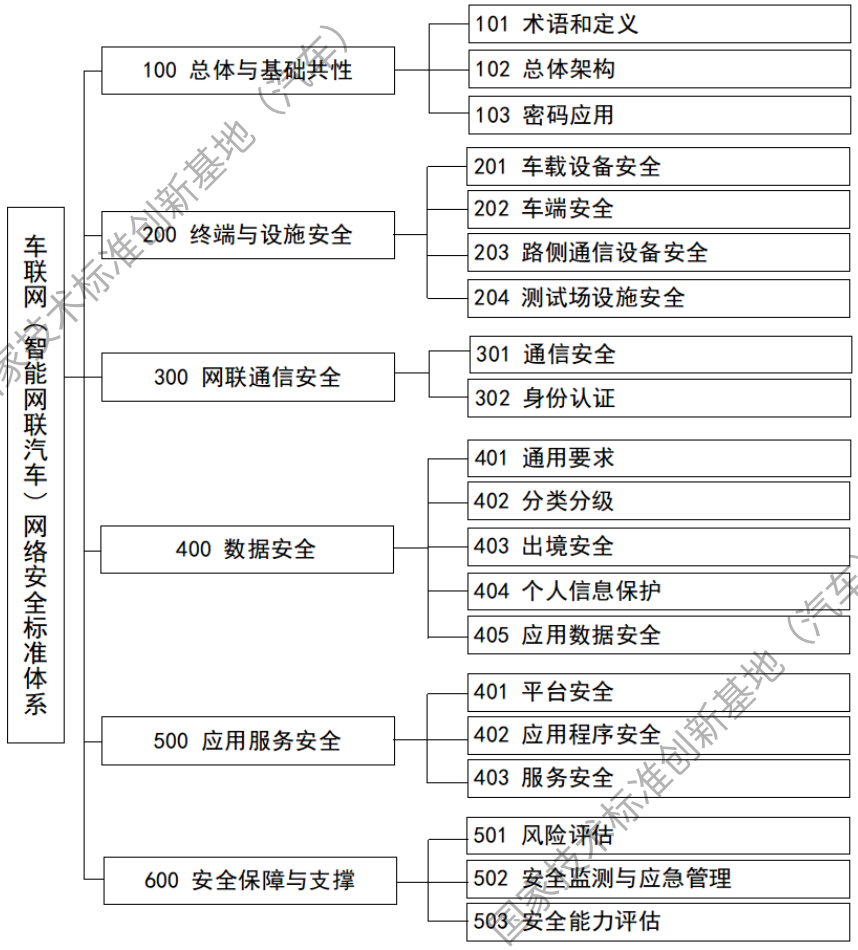

图 13 车联网（智能网联汽车）网络安全标准体系框架图

经项目组研究分析，建议从智能网联汽车数字证书通用要求、初始化要求、应用技术要求及试验方法等方面进行规则定义，针对证书应用流程进行梳理，制定数字证书应用的标准，用于指导整车厂、零部件供应商、软件供应商等汽车产业链企业，在汽车整个生命周期中开展数字证书安全应用的设计实现和验证评估。

3.3 标准撰写思路

3.3.1 识别数字证书应用场景

智能网联汽车 V2X 通信场景主要包括车云通信、车车通信、车路通信和车人通信，同时汽车内零部件和控制单元之间也需要时时高频次的进行数据和指令等信息传输，无论是针对汽车与外部实体之间的通信，还是针对车内各节点之间的通信，都需要保证通信各方的合法身份，保障所传输数据的完整性和保密性，数字证书在智能网联汽车领域的应用很大程度上能满足这些安全需求，提升智能网联汽车的安全性。通过调研梳理目前数字证书在智能网联汽车的应用情况，以及分析未来数字证书在车联网安全通信领域所能发挥的作用，已经明确的数字证书应用场景包括：

（1）基于数字证书的车云通信场景，如远程诊断、远程升级、车端数据上传。

（2）基于数字证书的车车通信场景，如车辆之间运行状态、行驶轨迹交互。

（3）基于数字证书的车路通信场景，如行驶车辆与交通路侧之间的信息广播。

（4）基于数字证书的车人通信场景，如远程控车、数字钥匙。

（5）基于数字证书的车内安全通信场景，如车内安全节点之间的数据通信。

3.3.2 梳理车用数字证书应用通用要求

车用数字证书通用要求从数字证书分类及格式、数字证书基本的信息内容，根证书、信任链的初始化要求，数字证书申请、灌装要求，数字证书有效期及更新要求，以及数字证书安全存储等方面进行分析考虑。

1. 数字证书分类及格式要求

从数字证书应用场景分析，以及各场景中数字证书应用的作用来看，标准所涉及到的车用数字证书主要包括设备证书、注册证书、假名证书、身份证书、APP 证书、车内节点证书，其中，设备证书主要用于车云通信时的身份认证，注册证书作为申请假名证书的凭证，假名证书用于 V2X 通信数据的消息签名，身份证书多用于特种车监控道路设施时的身份认证和指令加密，APP 证书用于鉴别移动终端的合法性。每种类型数字证书应遵照的证书格式，标准会给以规范定义，如果现有标准中对证书格式已有定义或要求，标准中将明确具体参照的标准文件及出处。

2. 数字证书基本内容要求

针对数字证书在智能网联汽车业务应用中的不同用途，数字证书申请实体应在数字证书申请请求信息中明确申请证书所包含的内容和取值，明确哪些内容是通用内容，哪些内容是根据证书类别和证书用途而有所区别的，各类证书标识内容的取值要求应清晰明确，以便于证书与实体一一对应，为后续证书的查找、识别和应用做好准备，以下针对不同证书类型申

请标识取值要求进行定义。

表 8 证书标识及取值要求

证书类别	证书标识内容	取值要求
车云通信证书	CN=设备 ID,OU=业务标识,O=公司名,C=CN，OU/O/CN 项下同	符合设备 ID 的定义
APP 证书	CN=证书所属应用主体的标识，如车辆 VIN、手机 IMEI	由证书所属应用定义
云服务器证书	CN=服务器的域名或 IP 或证书所属应用主体的标识	符合域名或 IP 的定义，或由证书所属应用定义
注册证书	OBU 设备 ID 或 RSU 设备 ID	符合 OBU 设备 ID 或 RSU 设备 ID 定义
假名证书	链接值或空	若为链接值，符合链接值定义
应用证书	证书所属应用主体的标识，如路边站点标识符	由证书所属应用定义
身份证书	证书所属应用主体的标识，如车牌号	由证书所属应用定义，不允许暴露用户隐私
车内节点证书	车内服务节点的标识，如设备 SN	符合设备 ID 的定义

3.根证书、信任链的初始化要求

车用数字证书包括 X509 证书和 V2X 证书，这两种证书分别由 X509 CA 和 V2X CA 签发，X509 CA 和 V2X CA 都只有一张根证书，但是企业可根据证书管理需要和实际证书应用情况建立多个子 CA，这些子 CA 的根证书都由根 CA 签发，如此便会产生多个信任链，如 V2X 根 CA 可签发 ICA、ECA、PCA、ACA 等不同的 CA 机构，因此，车端要在业务系统使用证书之前完成根证书和信任链的初始化，主要包括根证书和信任链的下载和存储，以及对新版本根证书和信任链的检测更新，建议标准对根证书和信任链的下载、存储以及管理过程中所涉及的相关技术要求进行规范定义。

4.数字证书申请、灌装要求

此处的数字证书，即指车辆终端从车联网 PKI 证书签发系统申请下载的车用数字证书，根据证书类别和用途不同，相应的证书申请和灌装流程随之不同，在申请和灌装过程中所涉及的技术要求也不同，需分别加以规范定义。另外，车辆在证书申请过程中，至少应确保以下操作环节的安全性：

(1) 车企应对提交证书申请的车辆终端进行合法性认证，即必须是经过车企认证授权的车辆才能申请数字证书；

(2) 车辆终端在接入 CA 系统服务之前，应验证 CA 服务身份，确保接入系统是授信的证书签发机构；

(3) 车辆终端在本地生成证书申请请求，证书私钥在安全环境中产生，并存储到安全介质中，且私钥不可导出，对私钥的访问加入权限管理；

(4) 车辆终端应对证书申请信息进行加密后，再传输提交到 CA 系统，以避免申请信息中的敏感信息泄密；

(5) 车辆终端收到 CA 系统签发返回的数字证书后，要先验证证书有效性，再进行证书的导入存储。

5.数字证书有效期与更新要求

应根据数字证书的类型、使用频度和业务场景，在满足其安全需求的前提下，选择设定合适的证书有效期。数字证书在到期前需提前完成证书更新操作，由证书所有者自行检测证书到期时间，并自行触发证书更新操作，确保新证书下载保存成功后，旧证书做失效或注销处理。证书更新针对不同的证书类型，证书有效期及证书更新提前时间要求见下表。

表 9 数字证书有效期参照表

证书类别	证书有效期	证书更新提前时间
车云通信证书	15 年	180 天
APP 证书	1 年	90 天
云服务器证书	6 年	180 天
注册证书	6 年	180 天
假名证书	7 天	1 天
应用证书	3 年	90 天
身份证书	30 天	7 天
车内节点证书	3 年	90 天

6.数字证书安全存储要求

标准将针对数字证书及其密钥对的安全存储提出具体要求，密钥应存储在车端安全芯片、其他安全硬件介质中或符合安全等级要求的其他介质中，具体要求可参照 GM/T0039-2015《密码模块安全检测要求》的相关内容。标准也会对存储介质的技术指标进行规范，如算法支持、存储容量、可读写次数、性能指标、安全防护等，同时对证书和密钥的访问权限进行阐述说明。

3.3.3 规范车用数字证书应用技术要求

1.数字证书关联应用要求

车端获取数字证书后，各机构应将证书信息注册到业务应用系统中，并与业务应用中的账户信息进行关联。应用系统中所注册的证书信息应是证书的唯一识别信息，一张数字证书应只与一个用户关联。

2.数字证书应用环境初始化技术要求

在基于数字证书的业务操作运行之前，应先完成证书应用所依赖的软硬件环境初始化，包括硬件已上电，且运行状态良好，网络状况良好，根证书和证书链都已下载且均有效，数字证书合法性和有效期的检查，数字证书可用性检查，数字证书密码运算环境安全性检查。

3.数字证书有效性检查技术要求

业务系统在应用数字证书之前，需对数字证书的有效性进行检查，只有确认有效的证书才能在业务系统中得以应用。数字证书有效性检查技术要求从以下几个方面进行规范定义：

（1）数字证书合法性检查：即验证证书是由合法签发机构颁发。

（2）证书状态检查：即确认证书正处于正常使用状态，未被吊销或禁用。

（3）数字证书有效期检查：验证证书在有效期内，通常指证书未过期。

（4）证书的密钥用法检查：检查基于数字证书的密钥运算符合证书的密钥用法要求。

（5）数字证书应用权限检查：此项检查要求主要针对 V2X 数字证书，检查数字证书的密钥用法或权限描述，确定所应用范围未超出权限描述。

（6）数字证书适用地理区域检查：此项检查要求主要针对 V2X 数字证书，应保证在数字证书所允许使用的地理区域范围内应用数字证书。

4.基于数字证书的身份认证技术要求

在车-云、车-车、车-路、车-人通信过程中，均需使用数字证书来验证所声明身份的合法性，对通信实体身份进行鉴别。

5.基于数字证书的消息安全传输技术要求

在车联网业务数据的存储或应用消息的传输过程中，对敏感信息在保存前或传输前应进行数字签名，并在信息使用前或接收后对其签名数据进行验签，以保证数据信息的完整性和抗抵赖性，各实体可根据业务需求针对数据内容进行加密或基于数字证书的 TLS/TLCP 安全通道实现数据的机密性保护。

6.基于数字证书的代码保护技术要求

对来自外部的软件代码需进行数据签名，同时针对车内关键固件或系统软件进行代码签名保护，在车端安装运行之前完成验签，以保证软件代码的完整性、真实性。

3.3.4 统一车用数字证书应用验证方法

标准将针对车用数字证书应用场景以及标准涵盖的车用数字证书通用技术要求、数字证书初始化要求和应用技术要求等，研究梳理对应的测试环境要求、验证对象、验证内容、测试流程、测试依据和测试结果判定标准等。

1. 车用数字证书通用要求符合性验证

（1）验证确认数字证书属于标准要求范围内的证书；

（2）检查数字证书格式和相关内容符合相关标准要求；

（3）验证车辆终端已经成功下载了根证书、信任链，且根证书、信任链均有效；

（4）验证车辆终端证书申请流程符合标准要求，验证证书申请过程中，安全保护措施高于标准要求；

（5）验证数字证书有效期符合标准规定，验证车端应用启动了数字证书有效期检查和提醒机制，并在证书到期前的规定时间内完成了证书更新操作；

（6）验证数字证书存储介质和存储环境的安全性符合标准要求；

2. 车用数字证书应用技术要求符合性验证

结合实际数字证书应用场景，验证智能网联汽车在通信过程中是否应用数字证书以增强系统的安全性，具体如下：

（1）验证车联网业务系统对所应用的数字证书已按照标准中要求进行关联；

（2）验证车辆终端证书在启用之前，其依赖的软硬件环境的可用性和安全性；

（3）验证数字证书应用程序在基于数字证书的公私密钥进行密码运算已完成对证书有效性的检查，确保证书合法可用；

（4）验证在车-云通信过程中，车端基于数字证书实现身份认证，且对发往业务服务端的信息，车端均使用数字证书对应的私钥进行签名，针对敏感信息，车端采用保密措施来保证数据保密性；

（5）验证在车-车通信过程中，车端针对对外广播的消息，均使用假名证书实现数据签名，并对接收到的来自他车的签名消息进行验签，以保证通信双方身份合法性和消息完整性；

（6）验证车-路通信过程中，车端针对收到的路侧端的签名消息进行验签以保证路侧设备合法性以及所收到消息的完整性；

（7）验证车-人通信过程中，终端基于数字证书实现身份认证，并对发出的消息指令进行签名或加密，车端针对直接来自 APP 或经由业务系统转发的消息指令进行验签和解密，以保证消息源的合法性和指令的保密性；

（8）验证车联网业务应用消息传输过程中，对敏感信息应进行数字签名，并对签名数据进行验签，以保证数据信息的完整性、机密性；验证在车端下载安装使用第三方软件过程中，对其来源可靠性进行验证，对软件包本身进行验签，以保证软件包的合法性、完整性。

3.4 与现有相关标准比对分析

在前期对智能网联汽车数字证书应用现状的调研以及对数字证书在智能网联汽车应用过程中存在的问题梳理分析的基础上，项目组总结得出了《智能网联汽车数字证书应用技术要求》标准编制的必要性。为了避免与现有相关标准在内容上的重复编制，项目组也对国内外及国内各行业与证书相关的标准进行了汇总分析。与所研究建议编制标准关联性较强的标准包括 T/CCSA 307-2021 《基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求》、

国标《基于 LTE-V2X 直连通信的车载信息交互性系统技术要求》、国标 GB/T 37374-2019《智能交通 证书应用接口规范》、GB/T 37376-2019《交通运输 数字证书格式》、《C-V2X 车联网系统认证授权系统技术要求》、《C-V2X 车辆异常行为管理技术要求》，以下是这几个标准的比对分析。

表 10 相关标准比对分析表

序号	标准名称	标准归口	标准类型	标准内容	适用范围	证书应用相关	标准状态
1	《基于 LTE 的车联网无线通信技术安全证书管理系统技术要求》	CCSA	团标	规定了基于 LTE 的车联网安全证书管理系统技术要求，主要内容包括安全证书管理系统架构和相关的显式证书格式及交互流程	适用于 LTE-V2X 设备和安全证书管理系统	“4.2.2 通信安全协议数据单元”、“4.2.5 通信安全过程”等章节提到消息中可包含数字证书或对消息进行非对称运算，但未提及具体证书应用	发布
2	《基于 LTE-V2X 直连通信的车载信息交互系统技术要求》	SAC/TC114	GB/T	规定了基于LTE的车联网无线通信技术（LTE-V2X）支持直连通信的车载信息交互系统的环境评价要求、系统功能要求、系统通信性能要求、定位定时要求以及试验方法等内容	适用于安装有基于 LTE-V2X 直连通信方式的车载信息交互系统的 M 类、N 类汽车，其他类型车辆可参照执行	“6.4 通信安全要求”章节中的“安全层消息发送要求”的内容，指出发送消息中应包含假名证书或摘要，并说明假名证书使用条件，“隐私保护要求”包含了假名证书改变的要求和时机	报批
3	GBT37374-2019《智能交通证书应用接口规范》	SAC/TC268	GB/T	规定了交通运输信息系统中数字证书应用接口和安全消息语法	适用于交通运输信息系统中与数字证书应用相关的软硬件系统设计、	标准仅规定了数字证书应用接口和安全消息语法，并未涉及证书应用，更未涉及到智能网联汽	现行

					研发及测试	车的数字证书应用	
4	GBT37376-2019《交通运输数字证书格式》	SAC/TC268	GB/T	规定了交通运输信息系统中数字证书分类和数字证书格式	适用于交通运输信息系统中与数字证书应用相关的软硬件系统设计、研发及测试	标准仅包含了交通运输信息系统中数字证书应用接口及相关数据结构以及安全消息签名示例，并未涉及具体的证书应用相关内容	现行
5	《C-V2X车联网系统认证授权系统技术要求》	CCSA	YD/T	规范认证授权机构功能的系统架构、管理流程和接口的技术规范；以及认证授权机构与其他系统或功能实体的交互流程和接口	适用于指导整车企业、零部件供应商、软件供应商等汽车产业链企业，开展车联网证书体系中认证授权系统的建设	标准所涉及证书遵循 T/CCSA 307-2021《基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求》规范的车联网专用短证书要求，不涉及其他类型证书应用	已立项
6	《C-V2X车辆异常行为管理技术要求》	CCSA	YD/T	规范了 V2X 消息的安全性检查、正确性检查、一致性检查、语义连续性检查、合理性检查等内容；定义了异常行为上报的流程及报告的数据格式	适用于指导整车企业、零部件供应商、软件供应商等汽车产业链企业开展 C-V2X 车辆异常行为管理	异常行为上报中使用 T/CCSA 307-2021《基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求》规范的车联网专用短证书进行车辆身份认证，不涉及其他类型证书应用	已立项
7	《智能网联汽车数	SAC/TC11	GB/T	从智能网联汽车车用数字证书应	适用于指导整车厂、零	包括智能网联汽车数字证书应用	研究

	字证书应用技术要求》	4		用通用要求、数字证书应用技术要求和数字证书应用试验方法等方面进行梳理定义	部件供应商、软件供应商等汽车产业链企业开展数字证书安全应用的设计实现和验证评估工作	场景、数字证书应用通用要求、数字证书应用技术要求以及数字证书应用技术试验方法，也会对数字证书应用场景进行指导说明	

3.5 标准框架

经过前期的研究分析和梳理总结，按照本章梳理出的标准撰写思路，工作组对标准的主要内容进行了初步探讨规划，建议标准大纲如下。

目录

以下是针对标准各章节内容编制的规划说明：

第一章用来说明标准的定位和适用范围。

第二章列出了标准中引用的其他规范性引用文件。

第三章针对本章所用到的术语进行定义说明。

第四章针对标准中使用的缩略语进行定义说明。

第五章描述了标准编制的背景和意义。

第六章针对智能网联汽车的应用场景进行简单的总结概述。

第七章从车用数字证书的分类、格式、证书内容，数字证书应用所需的根证书、信任链下载安装，数字证书首次申请、灌装，数字证书有效期及更新、安全存储等方面规范车用数字证书的通用要求。

第八章针对数字证书应用技术要求进行规范定义，主要包括数字证书应用关联技术要求、数字证书应用环境检查技术要求、数字证书有效性检查技术要求、身份认证技术要求、消息安全传输技术要求和代码保护技术要求等方面。

第九章是对车用数字证书验证方法的规范定义，验证内容对应于第七章、第八章所涉及到的数字证书应用相关的通用要求和技术要求。针对每一个技术要求，分析明确验证对象、验证内容、测试环境要求、测试流程、测试依据和测试结果判定标准等。

附录章节会针对目前常用通用的车用数字证书应用场景进行展开描述，详细描述数字证书在这些场景中的应用流程和所起作用。

四、后续工作展望

4.1 处理和其余标准的关系

一方面，当前已经能识别到一些标准与本研究报告建议的标准内容产生一些交集，潜在可能会产生一些技术要求上的冲突，基于此，后续标准在编写过程中应尽量兼容当前已有标准的内容，标准计划编制内容如果已在其他标准中有所规定和提及，则不再重复定义编制，标准中会注明需参照遵循的标准名称及具体章节的内容，标准在编制过程中也尽量做到抽象化描述，不涉及具体技术细节。实际应用中，此标准仍可作为厂商设计开发、应用集成和验证测试的参考。

另一方面，未来也会有其他新增数字证书应用场景，或者在现有场景基础上更细分的应用环节，针对于此，标准的编制应尽量基于当前可预见的未来趋势，将相关证书应用技术要求体现在标准内容中，未来，根据数字证书应用的实际情况酌情调整标准的内容，以适应新的应用场景和技术要求。

4.2 整理待讨论确认问题

基于研究项目组前期的讨论内容，在后续正式开展标准的起草编写工作之后，将对如下问题开展针对性的研讨和讨论。

1. 针对车端 X509 数字证书的生命周期管理，是否考虑纳入到标准中，或者是否可根据实际需要归纳总结通用的管理要求纳入标准？

2. 考虑在各种异常情况或突发情况下的数字证书应用场景及技术要求，并在标准中明确如何规范应对处理；

3. 梳理现行或制定中的可能与此标准具有潜在关联的标准，处理好此标准与这些标准的关系；

4. 国内外已经开始使用隐式证书格式及算法，我国并没有类似的用于汽车的隐式证书的标准要求，关于隐式证书管理和应用相关的技术，后续应继续研究并根据实际应用情况补充完善。

5. 讨论未来智能网联汽车数字证书应用技术发现趋势，在标准内容上进行兼容性考虑。