中国汽车技术研究中心有限公司

China Automotive Technology and Research Center Co., Ltd.

《智能网联汽车数字证书应用技术要求》

研究报告发布

项目组介绍

项目组成员

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，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

任务分工

第一章	智能网联汽车 车用数字证书应用技术研究背景	1.1 车用数字证书应用现状介绍		（国汽智联、信大捷安、小鹏汽车、上海智能网联（V2X））	国汽智联
		1.2车用数字证书应用面临问题		吉利，长安、天检中心、上汽大通、江淮汽车	
		1.3车用数字证书应用需求分析		国汽智联、信大捷安	
第二章	国内外汽车行业数字证书相关标准规范发展分析	2.1国外相关标准发展现状	2.1.1欧盟相关标准发展情况	蔚来汽车、戴姆勒	蔚来汽车
			2.1.2美国相关标准发展情况	福特	
		2.2国内相关标准发展现状	2.2.1国家标准及行业标准发展现状	华为、襄阳达安、德赛西威、江淮汽车	华为、ITS
			2.2.2交通部相关标准发展情况	ITS	
			2.2.3通标委相关标准发展情况	信通院	
			2.2.4密标委相关标准发展情况	软测中心	
			2.2.5 公安相关标准发展情况	华为	
		2.3其他行业数字证书相关标准体系分析		信大捷安	
		2.4总结分析	2.4.1分析所研究标准和其他标准关系	小鹏汽车	
			2.4.2 总结	华为、ITS	
第三章	智能网联汽车数字证书应用标准化需求分析	3.1标准范围界定		中汽中心、信通院、泛亚汽车、上汽通用五菱、东风汽车、襄阳达安、北汽研究总院	中汽中心、信通院
		3.2标准内容撰写思路			
		3.3标准研究主要内容			
第四章	后续工作建议	4.1整理待讨论确认问题		中汽中心、信通	中汽中心、信通院
		4.2后续标准编制和落实		中汽中心、信通	

研究进展介绍

首次提案

研究已有相关标准，收集车企需求，梳理标准范围，于汽车信息安全标准工作组第七次会议上完成标准提案。

2020.2-2020.4

企业调研

按照大会反馈函编写企业调研问卷，秘书处下发调研问卷，开展企业数字证书应用调研。

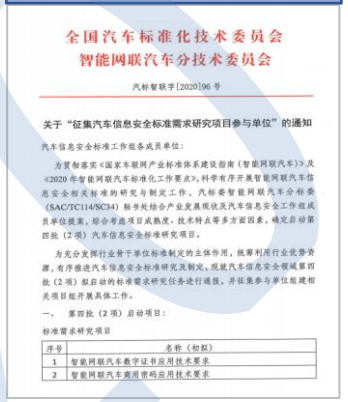
2020.5-2020.7

调研汇报

根据企业反馈，统计汇总调研数据，整理标准内容目录大纲，于汽车信安工作组第八次会议完成前期研究汇报。

2020.8-2020.10

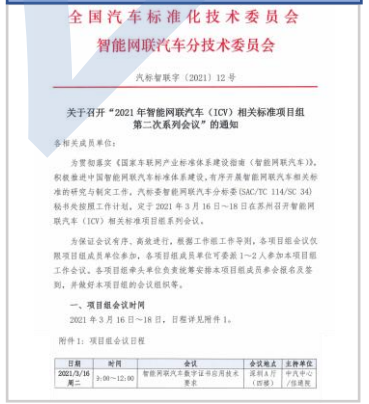
征集项目组



汽标委拟启动标准需求研究任务，智能网联汽车分技术委员会征集标准参与单位。

2020.11-2020.12

项目启动



汽标委秘书处确定标准需求研究项目参与单位，组织项目参与单位召开研究项目启动会。

2021.1-2021.3

项目成果发布

项目组完成智能网联汽车数字证书应用研究，编制并发布《智能网联汽车数字证书应用技术要求》研究报告。

2021.4-2021.7

目录

Contents

智能网联汽车通信场景与威胁分析

■ **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，主要面临通信数据被篡改、中间人攻击等安全威胁。**

智能网联汽车通信场景

安全威胁分析

车内通信安全威胁分析

- 汽车网关：黑客利用其总线路由功能对车身、转向等核心控制器发起攻击，可**导致车身、转向控制失灵等后果**。
- 车载诊断系统接口（OBD）：若黑客利用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。**
- TBOX、IVI：主要面临数据被篡改的威胁，**导致向用户显示错误或非法诱导信息。**

车-云通信安全威胁分析

- 远程控车：黑客利用伪造身份攻击技术可**非法控制或盗取车辆。**
- 汽车软件远程升级：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，将**导致汽车无法正常行驶或行驶过程中刹车失灵等严重后果。**

车-车/人/路通信安全威胁分析

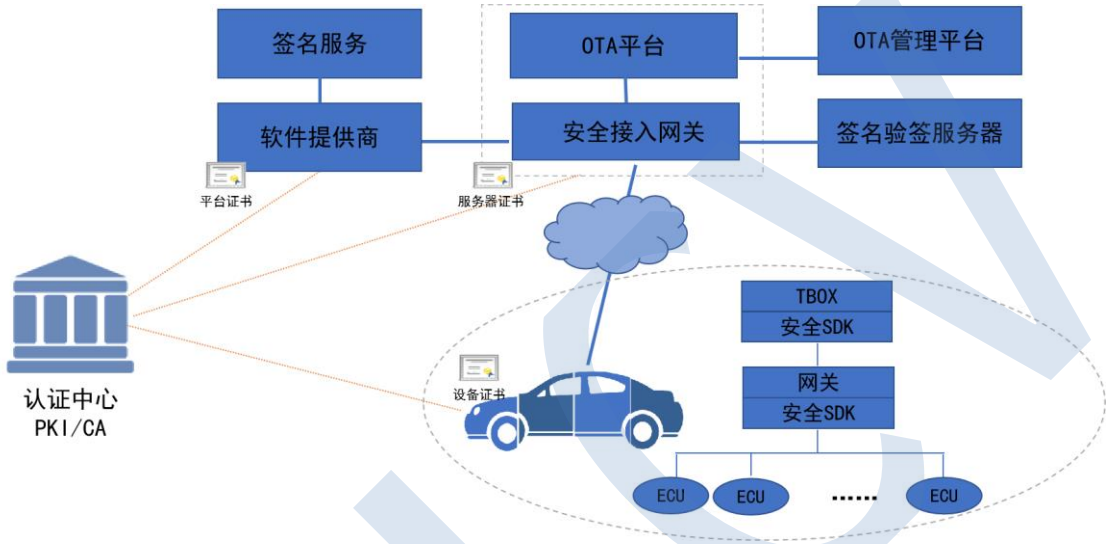
- 车与车、人、路的通信消息主要是车辆、行人与道路设备的位置、行动轨迹、交通设施实时信息等，若被黑客窃听，将**导致用户隐私信息的泄露；**若黑客篡改消息可实现对车辆的欺骗，**造成交通拥堵或安全事故。**

数字证书在智能网联汽车的应用现状-车云通信

■ 数字证书在车云、车人通信中的典型应用分别是汽车软件远程升级与远程控制功能。

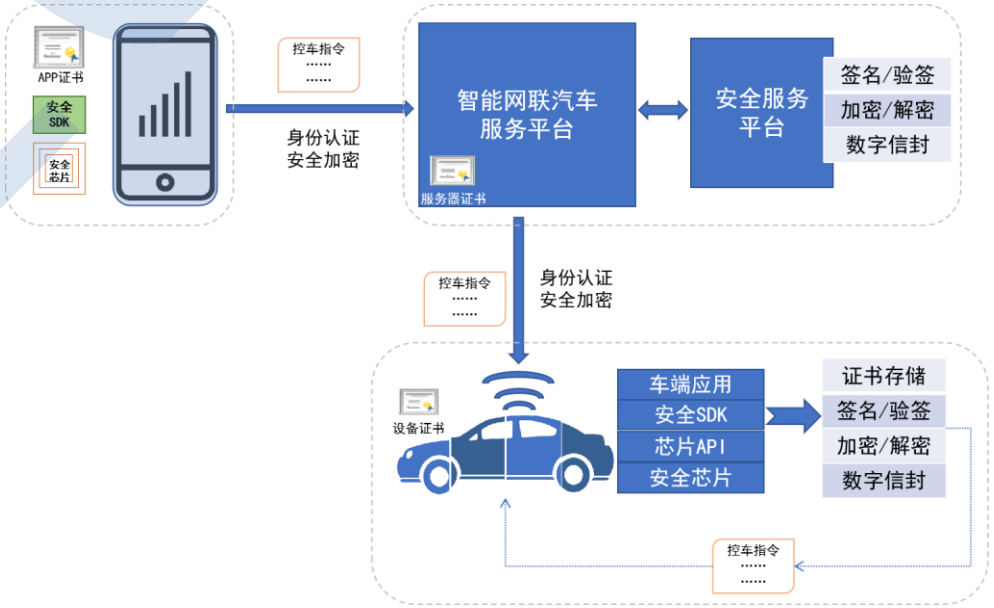
基于X509数字证书的汽车软件远程升级

软件提供商、OTA平台与智能网联汽车均向CA中心申请数字证书，OTA平台在验证软件提供商的身份合法后对软件升级包进行数字签名，并将服务器证书与软件升级包一起发送到车端，车端进行身份识别及验签后执行软件升级包的刷写。



数字证书在远程控车中的应用

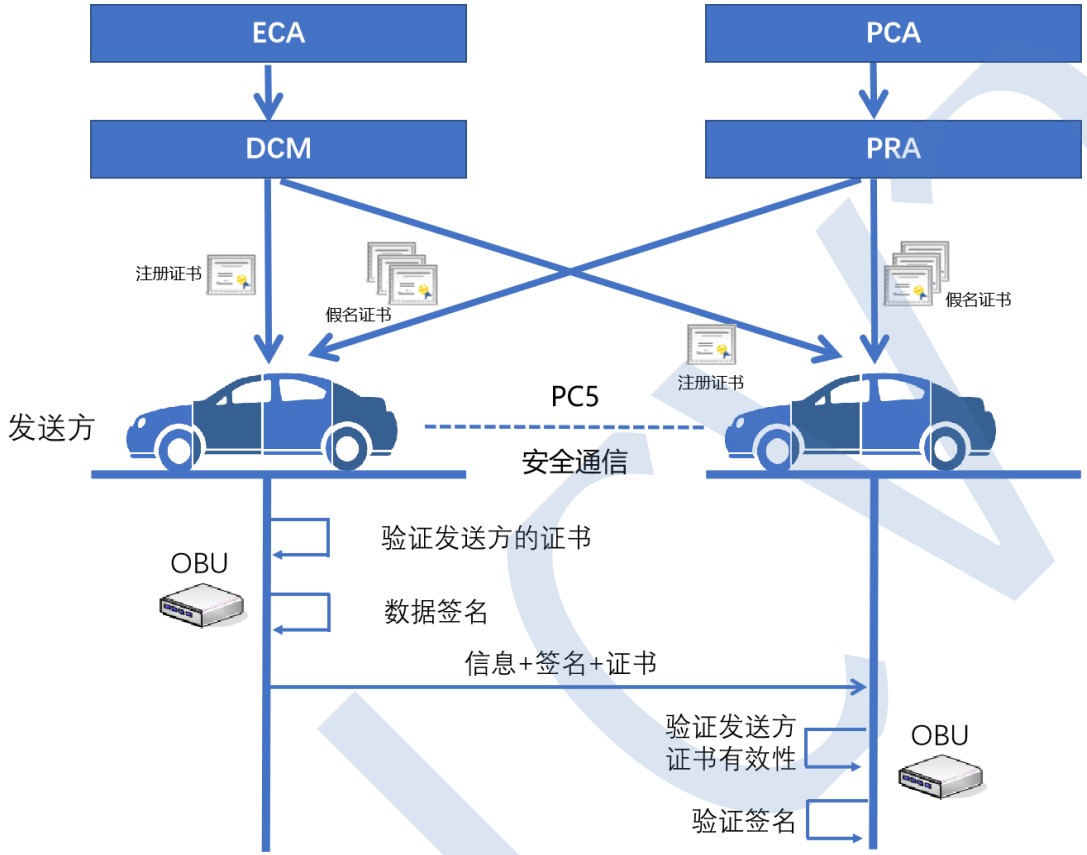
用户移动APP、智能网联汽车服务平台与智能网联汽车均向CA中心申请数字证书，控制指令在由手机端发送至服务平台、车端的过程中均需要利用数字证书进行解密验签，以确保控制指令的可信性。



数字证书在智能网联汽车的应用现状-车车、车内通信

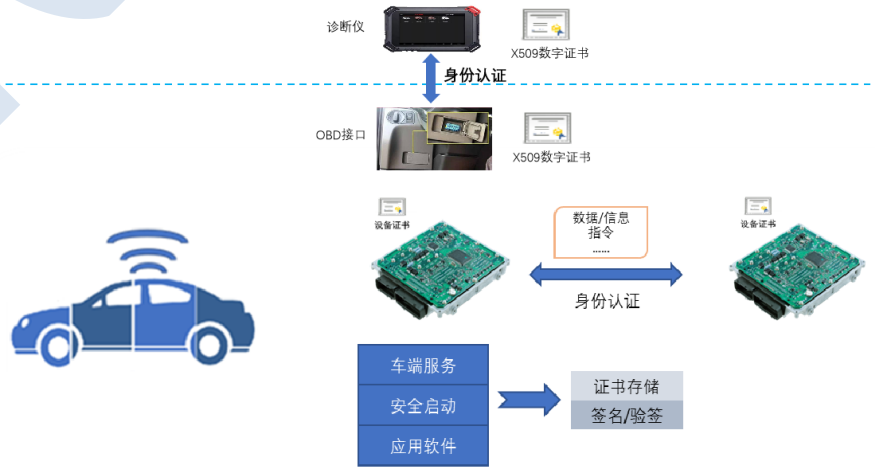
基于V2X数字证书的车车通信

为了满足V2X 通信对低时延、高运算效率的需求，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。



数字证书在车内通信中的应用

1. 利用数字证书可实现车内网络中各关联节点之间在通信过程中的身份认证；
2. 利用数字证书对应的私钥对ECU安全启动的固件、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。

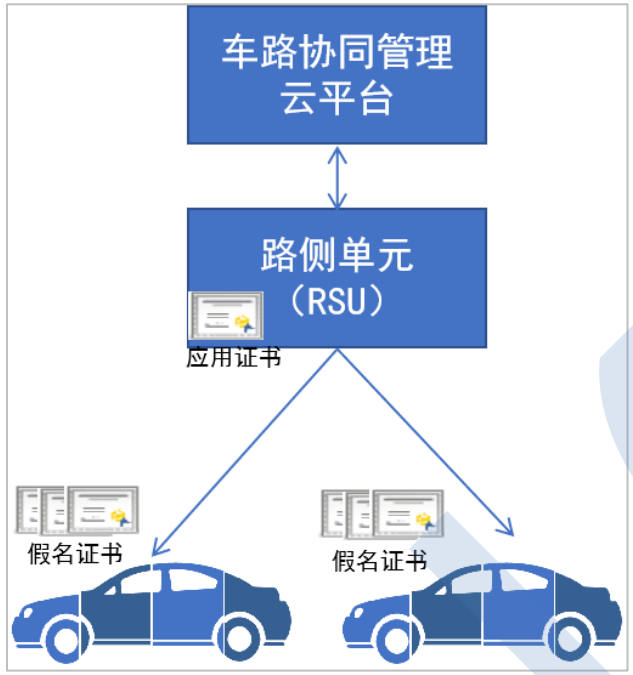


数字证书在智能网联汽车的应用现状-车路通信

■ 数字证书在车路通信中的应用主要用于车辆与路测设施之间的身份认证及通信数据的安全传输。

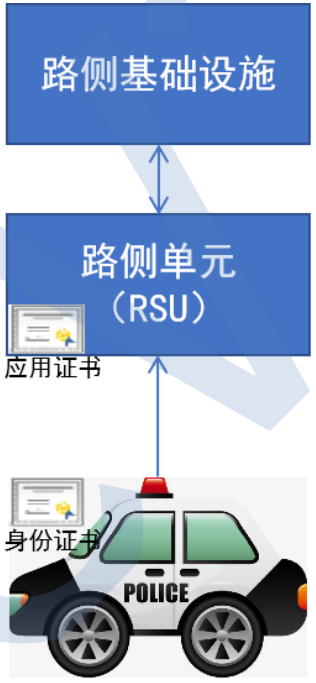
车辆接收路侧设备的广播消息

RSU广播消息包括应用证书及其利用应用证书对应的私钥对广播消息进行的签名，OBU可在验证应用证书及数字签名有效后使用广播消息。



特种车辆配置管理路侧设备

车载OBU利用身份证书对控制指令进行签名、利用RSU公钥对签名进行加密，RSU对消息进行解密、验证身份证书并验签后响应控制指令。



车辆ETC缴费

车载OBU获得RSU的应用证书并使用其身份证书和RSU应用证书生成签名加密消息，RSU解密并验证OBU的签名加密消息，确定OBU的位置。

电动汽车接入充电桩

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，便完成了双向身份认证。

智能网联汽车数字证书应用面临的问题

通用问题

- **对数字证书无分类要求及格式规范：** 应结合证书应用场景、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。
- **数字证书内容仍存在较大差异：** 应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。
- **针对数字证书有效期缺乏统一管理：** 综合考虑证书的可用性、易维护性和安全性等多方面因素，形成有效期设定的统一规范。
- **数字证书存储面临安全问题：** 应形成数字证书安全存储的软硬件规范。
- **根证书、信任链、CRL等初始化环节不规范：** 应明确车端根证书、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。
- **车用数字证书申请流程差异化明显且缺乏安全保障：** 应统一申请流程，建立与认证中心的安全认证机制。
- **数字证书与应用绑定管理要求不明确：** 应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。
- **证书更新管理策略尚不统一：** 应形成统一的证书有效期管理规范。

技术问题

- **针对数字证书应用依赖的安全环境缺少检查机制：** 应明确检查范围及技术要求。
- **数字证书有效性检查不全面：** 应对检查范围、检查内容和相关技术要求进行规范化说明。
- **数字证书应用技术要求不规范：** 应明确数字证书在典型应用场景中的实现流程、注意事项及技术要求，减少数字证书应用过程中的问题。

验证测试问题

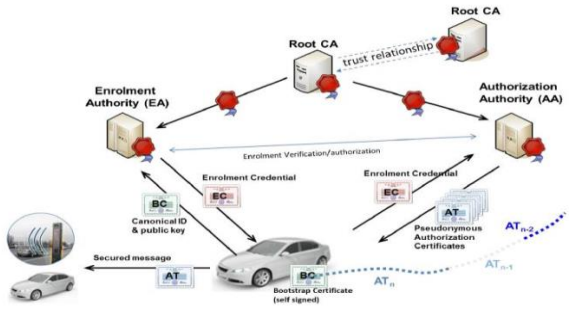
- **无明确的数字证书应用测试规范：** 数字证书应用测试的缺失将导致数字证书应用后的故障频发、追踪困难、增加成本消耗等问题，应明确数字证书应用测试规范，并推动其测试动作的有效执行。

目录

Contents

国外数字证书相关标准分析

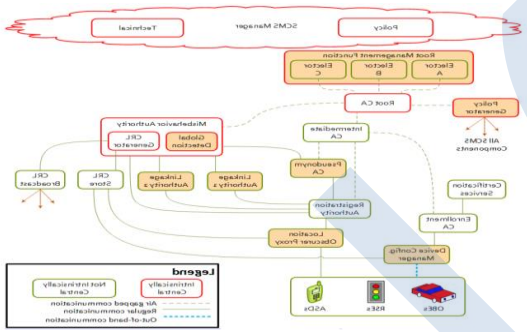
欧盟（ETSI ITS）



欧洲由于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发布了多项规范和标准，对安全体系结构、PKI流程、ITS的安全头和证书格式进行了规范。

- ETSI TS 102 731 ITS; Security; Security Services and Architecture
- ETSI TS 102 940 ITS; Security; ITS communications security architecture and security management
- ETSI TS 102 941 ITS; Security; Trust and Privacy Management
- ETSI TS 102 942 ITS; Security; Access Control
- ETSI TS 102 943 ITS; Security; Confidentiality services
- ETSI TS 103 097 ITS; Security; Security header and certificate formats

电气与电子工程师协会（IEEE）



电气与电子工程师协会制定的IEEE 1609.2为密码安全服务相关的标准，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，解决了不同汽车制造商之间没有同类通信接口的问题。

- IEEE 车载无线通信标准1609.2

国内数字证书相关标准分析

■ **目前国内缺少智能网联汽车行业数字证书应用相关标准，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。**

国内标准

国家标准（GB/T）

《智能交通数字证书应用接口规范》、《交通运输数字证书格式》、《基于LTE-V2X直连通信的车载信息交互系统技术要求》、《数字证书策略分类分级规范》、《车载网络设备信息安全技术要求》等。

行业标准

《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》、《基于LTE的车联网无线通信技术-安全认证测试方法》、《公众IP网络安全要求——基于数字证书的访问控制》、《移动应用身份认证总体技术要求》、《移动互联网应用程序开发者数字证书管理平台技术要求》等。

国密标准

《数字证书认证系统密码协议规范》、《基于SM2密码算法的数字证书格式》、《证书应用综合服务接口规范》、《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》等。

公共安全标准

《公安数字证书硬件介质存储空间划分规则》、《取证与鉴定文书电子签名》等。

国内典型行业标准

金融行业

《用于金融服务的公钥基础设施 实施和策略框架》、《金融业务 证书管理 第1部分：公钥证书》、《银行业务 证书管理 第2部分：证书扩展项》、《金融电子认证规范》、《保险电子签名技术应用规范》、《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》等。

政务行业

《信息安全技术 电子政务移动办公系统安全技术规范》、《政务数字证书规范 第1部分：格式》、《政务数字证书规范 第2部分：应用接口》等。

卫生行业

《健康信息学 公钥基础设施（PKI） 第1部分：数字证书服务综述》、《健康信息学 公钥基础设施（PKI） 第2部分：证书轮廓》、《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》。

目录

Contents

标准定位与撰写思路

■ **通过梳理车用数字证书应用过程中存在的问题及车企对标准编制的诉求和建议，结合工信部发布的网络安全标准体系，明确了标准的定位与撰写思路。**

智能网联汽车网络安全标准体系框架图

撰写思路

- 车云通信
- 车路通信
- 车人通信
- 车车通信
- 车内通信

识别数字证书应用场景

- 数字证书分类及格式要求
- 数字证书基本内容要求
- 数字证书有效期要求
- 数字证书安全存储要求
- 根证书、信任链的初始化要求
- 数字证书申请、灌装要求
- 数字证书关联应用要求
- 数字证书更新要求

梳理车用数字证书基本要求

- 数字证书应用环境初始化技术要求
- 数字证书有效性检查技术要求
- 基于数字证书的身份认证技术要求
- 基于数字证书的消息安全传输技术要求
- 基于数字证书的代码保护技术要求

梳理车用数字证书应用技术要求

- 车用数字证书通用要求符合性验证
- 车用数字证书应用管理要求符合性验证
- 车用数字证书应用技术要求符合性验证

统一车用数字证书应用验证方法

与现有相关标准比对分析

■ **比较了六项强相关的标准，本标准与现行、报批或已立项的标准不存在内容重叠。**

标准名称	标准内容	适用范围	证书应用相关	标准状态
《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。	报批
《基于LTE-V2X直连通信的车载信息交互性系统技术要求》	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”中包含了假名证书改变的要求和时机，未涉及其他类型证书的应用技术要求。	报批

标准名称	标准内容	适用范围	证书应用相关	标准状态
《GBT37374-2019 证书应用接口规范》	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、研发及测试	全文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车的数字证书应用。	现行
《GBT37376-2019 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	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	全文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

标准名称	标准内容	适用范围	证书应用相关	标准状态
《C-V2X车联网系统认证授权系统技术要求》	规范现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	遵循YD/T《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格式	已立项
《C-V2X车辆异常行为管理技术要求》	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YD/T《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格式，进行车辆身份认证	已立项

标准框架

目录

大纲内容说明

第一章	说明本标准的定位和适用范围
第二章	本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了定义说明
第四章	对本标准中使用的缩略语进行定义说明
第五章	描述了本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概述
第七章	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	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	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基本要求和技术要求。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A	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。

中国汽车技术研究中心有限公司

China Automotive Technology and Research Center Co ., Ltd.