车联网身份认证和安全信任试点
技术指南（1.0）

车联网身份认证和安全信任工作专家委员会

2021 年 9 月

说　明

为贯彻落实《车联网（智能网联汽车）产业发展行动计划》《新能源汽车产业发展规划（2021-2035 年）》《智能汽车创新发展战略》和车联网产业发展专委会第四次全体会议工作任务要求，加快推进车联网网络安全保障能力建设，构建车联网身份认证和安全信任体系，推动商用密码应用，保障蜂窝车联网（Cellular Based V2X，C-V2X）通信安全，工业和信息化部开展了车联网身份认证和安全信任试点工作，包含“车与云安全通信”、“车与车安全通信”、“车与路安全通信”、“车与设备安全通信”四个方向。

本指南给出各试点方向的建设目标、技术要求、通信安全要求、身份认证和安全通信参考方案以及典型应用场景。各试点项目单位可结合申报方向和实际规划，参考指南开展项目实施，建立相关身份认证系统，实现应用场景联动，接入工业和信息化部车联网安全信任根管理平台，协同推动跨车型、跨设施、跨企业互联互认互通，保障车联网安全通信。

目　录

概　述 **1**

1. 车与云安全通信 **3**

1.1. 建设目标 3
1.2. 技术要求 3
1.3. 通信安全要求 3
1.3.1. 数据传输真实性 *3*
1.3.2. 数据传输完整性 *3*
1.3.3. 数据传输机密性 *4*
1.3.4. 抗重放 *4*
1.3.5. 行为抗抵赖 *5*
1.3.6. 隐私保护 *5*
1.4. 身份认证和安全通信 5
1.5. 应用场景 6
1.6. 参考标准 6

2. 车与车安全通信 **8**

2.1. 建设目标 8
2.2. 技术要求 8
2.3. 通信安全要求 8
2.3.1. 数据传输真实性 *8*
2.3.2. 数据传输完整性 *9*
2.3.3. 数据传输机密性 *9*
2.3.4. 抗重放 *10*
2.3.5. 行为抗抵赖 *10*
2.3.6. 隐私保护 *10*
2.4. 身份认证和安全通信 10
2.5. 应用场景 12
2.6. 参考标准 13

3. 车与路安全通信 **14**

3.1. 建设目标 14
3.2. 技术要求 14
3.3. 通信安全要求 14

3.3.1. 数据传输真实性 14
3.3.2. 数据传输完整性 15
3.3.3. 数据传输机密性 15
3.3.4. 抗重放 16
3.3.5. 行为抗抵赖 16
3.3.6. 隐私保护 16
3.4. 身份认证和安全通信 16
3.5. 应用场景 18
3.6. 参考标准 19
4. 车与设备安全通信 20
4.1. 建设目标 20
4.2. 技术要求 20
4.3. 通信安全要求 20
4.3.1. 数据传输真实性 20
4.3.2. 数据传输完整性 21
4.3.3. 数据传输机密性 21
4.3.4. 抗重放 22
4.3.5. 行为抗抵赖 22
4.3.6. 隐私保护 22
4.4. 身份认证和安全通信 22
4.5. 应用场景 23
4.6. 参考标准 23
5. 安全保障 25
5.1. 证书管理系统安全保障 25
5.1.1. 网络安全 25
5.1.2. 密钥安全 25
5.1.3. 管理安全 25
5.1.4. 安全审计 26
5.1.5. 数据备份 26
5.1.6. 可靠性 27
5.1.7. 网络链路冗余 27
5.1.8. 主机及密码设备冗余 27
5.1.9. 存储冗余 27
5.1.10. 电源冗余 27
5.2. 云平台安全保障 27
5.3. 终端安全保障 28

5.4. 参考标准 29
附录 1 X.509 证书管理系统建设参考方案 30
附录 1.1 证书管理系统 30
附录 1.2 密钥管理系统 34
附录 2 C-V2X 安全证书管理系统建设参考方案 36

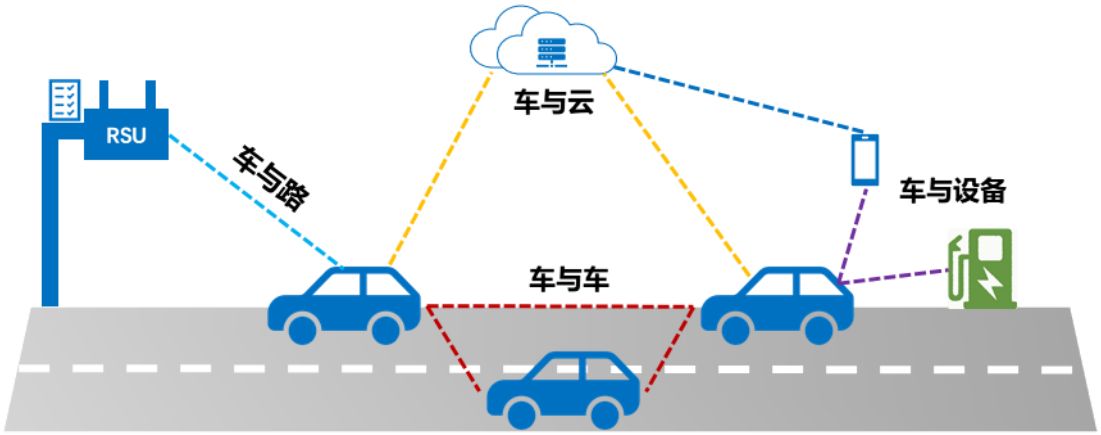
概　述

车联网是通过信息通信技术实现平台、车、路、设备等功能实体之间的数据高效交互和信息敏捷分享，并基于多级多类平台的感知、计算和决策协同，实现车载信息服务、车路协同、自动驾驶、智慧交通等多类应用服务的复杂系统。

安全信任是车联网产业健康发展的前提。在车联网通信过程中，建立车联网通信安全身份认证体系，赋予车辆、路侧设备、信息服务平台等基础设施可信的“数字身份”，抵御信息伪造、篡改等安全攻击，保障车联网系统安全可靠运行。我国车联网产业已经进入规模化部署应用的关键时期，全国多地积极创建国家级车联网先导区，多家整车企业已经发布具备 C-V2X 功能的量产车型。《车联网（智能网联汽车）产业发展行动计划》《新能源汽车产业发展规划（2021-2035）》和国家制造强国建设领导小组车联网产业发展专委会第四次全体会议明确提出“加快建立车联网数字身份认证机制，推进车联网跨行业跨地区互联互通和安全通信”。

推动建立车联网安全信任体系，支持跨企业、跨地区互信互认和互联互通，成为当前车联网产业规模化推广的重要工作任务。车联网身份认证和安全信任试点项目将通过建立相应的证书管理系统，采用数字证书、数字签名、数据加密技术建立车与云、车与车、车与路和车与设备之间的安全信任体系，实现对消息来源的认证，保证消息的合法性；实现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；实现对终端真实身份标识及位置信息的隐藏，防止用户隐私泄露。

本次试点一方面有助于促进车联网产业链上下游以及与相关行业之间的有效融合，对推动跨行业协同创新、促进产学研合作、提升用户规模、发展规模化商用起到积极作用；另一方面有助于构建统一车联网身份认证和安全信任体系，加速车联网网络安全保障能力建设，为车联网安全健康发展奠定基础。



注：虚线标识逻辑连接关系

1. 车与云安全通信

1.1. 建设目标

面向车与云服务平台通信场景，建立车云通信安全信任体系。试点单位研发建立车云通信身份认证、数据加密等技术能力，实现各类车云通信场景下的身份认证、数据机密性和完整性保护，构建车云通信安全保障能力。

1.2. 技术要求

通过基于商用密码的数字证书、数字签名、数据加密等技术，实现车载信息交互系统、汽车网关、C-V2X 车载通信设备等与车联网服务平台间的安全通信。基于安全链路协议，建立车云通信安全隧道，保护车云通信数据真实性、机密性和完整性。基于密码应用中间件，在车端实现消息封装、证书管理，在平台侧实现证书验证、数据解析。车载设备按照有关标准实现与证书管理系统、相关车联网安全信任根的数据交互。

1.3. 通信安全要求

1.3.1. 数据传输真实性

为保证接入车辆的合法性，车端与云平台通信时，可采用基于数字证书的双向认证方式，保证认证的安全强度及身份的合法性。数字证书由云平台证书管理服务签发。在双向身份认证过程中，云平台可采用由云平台建设的密码运算服务提供的高性能密码运算能力完成认证过程中的密码运算。

1.3.2. 数据传输完整性

传输数据的完整性可以通过使用杂凑密码算法（如 SM3）、数字签名算法（如 SM2）来保证。

车辆主动上报场景中，可利用杂凑密码算法计算上报数据的摘要值，再用车辆的签名私钥对摘要值进行签名，然后将上报数据、签名值发送至云平台。云平台系统计算上报数据的摘要值，并使用车辆的签名公钥验证摘要值的签名，保证传输数据的完整性。平台主动下发信息场景中，可通过上述同样方式，保障车云交互过程中重要数据传输的完整性。

1.3.3. 数据传输机密性

传输数据的机密性可以通过对称密码算法（如 SM4）以及数字信封分发对称密钥等方式来保证。

可采用建立车云安全通信链路或采用消息层对称加密方式保障云平台业务系统与车端通信过程中重要数据（如远程指令、蓝牙钥匙、远程升级包等）的传输机密性。

采用对称加密方式时，在平台主动下发数据场景中，平台产生一个对称密钥，使用对称密钥对下发数据进行加密，然后使用车辆的公钥对对称密钥加密，加密的对称密钥和加密后的数据形成一个数字信封，再将数字信封发送给车辆。车辆先用自己的私钥解密对称密钥，然后用对称密钥解密加密数据。车辆主动上报信息场景中，通过上述同样方式，实现基于数字信封的数据传输机密性保护。

1.3.4. 抗重放

在远程通信场景中，车辆与云平台间可以采用时间戳方式抗重放攻击，本环节需要保证通信双方时间同步，且保证来自合法权威的时间源。

1.3.5. 行为抗抵赖

在远程通信数据上报应用场景中，车辆发送方使用自己私钥对上报消息进行数字签名，云平台服务收到发送方的车辆公钥对签名数据验签成功，防止车辆发送方对上报消息的行为进行抵赖。平台主动下发信息时，可采用上述同样方式，防止平台对发送信息的行为进行抵赖。

1.3.6. 隐私保护

在车云通信过程中，应采用技术措施对汽车数据、个人信息、敏感个人信息、重要数据等进行保护，按有关要求进行匿名化、去标识化等处理，保护用户隐私。

1.4. 身份认证和安全通信

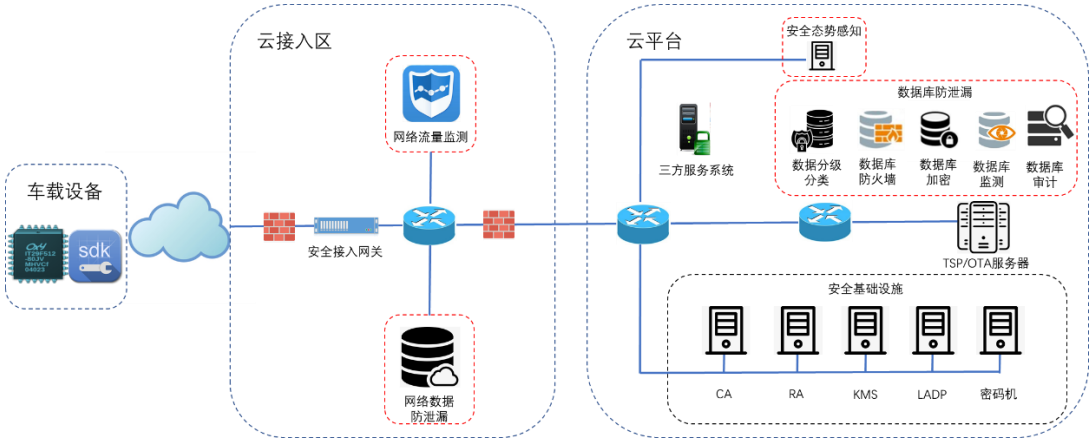


图 1 车云通信身份认证和安全通信架构图

车辆通过安全接入网关接入车联网云平台，可采用基于 X.509 证书实现双向身份认证和数据安全加密功能，使用 TLS（Transport Layer Security）/TLCP（Transport Layer Cryptography Protocol）等安全协议建立安全链路，保证车联网云平台与车辆之间传输信息的安全性和可追溯性，推荐使用 TLS 1.2 及以上版本，鼓励使用国密 SSL（Secure Socket Layer）协议，探索使用 C-V2X

安全证书实现车云身份认证和安全通信。车云通信身份认证和安全通信架构如图 1 所示。

安全接入网关主要负责安全通信链路的建立以及接入设备身份的校验功能。证书管理系统为车载终端、路侧单元、应用服务平台、移动应用程序等签发证书，用于建立安全通信链路，例如车载终端与应用服务平台安全通信、路侧单元向云端回传安全通信等。可参考《信息安全技术 证书认证系统密码及相关安全技术规范》（GB/T 25056-2018）建设 X.509 证书系统，网络部署图可参考附录 1。可参考《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》（YD/T 3957-2021）建设 C-V2X 安全证书管理系统，网络部署图可参考图 8。参考《信息安全技术 证书认证系统密码及其相关安全技术规范》（GB/T 25056-2018）中的安全要求做好安全保障。

1.5. 应用场景

在车端与车企云平台、路侧边缘云平台、智能辅助驾驶服务平台、车载信息服务云平台、高精动态地图服务平台等车联网服务平台的车云通信场景下，实现车辆可信接入、车辆定位及感知数据的可信采集、车辆状态信息的可信上传、汽车远程升级可信验证、基于安全链路的可信车云交互等车云通信应用。

典型应用场景包括车辆导航、车辆远程监控/诊断/接管、紧急救援、信息娱乐服务、空中软件升级（Over The Air，OTA）等。

1.6. 参考标准

[1]. 《信息安全技术 公钥基础设施 数字证书格式》（GB/T 20518-2018）

[2]. 《信息安全技术 证书认证系统密码及其相关安全技术规范》（GB/T 25056-

2018）

[3]. 《信息安全技术 SM3 密码杂凑算法》（GB/T 32905-2016）

[4]. 《信息安全技术 SM4 分组密钥算法》（GB/T 32907-2016）

[5]. 《信息安全技术 SM2 椭圆曲线公钥密码算法》（GB/T 32918-2016）

[6]. 《信息安全技术 SM2 密码算法使用规范》（GB/T 35276-2017）

[7]. 《信息技术 安全技术 可鉴别的加密机制》（GB/T 36624-2018）

[8]. 《信息安全技术 密码模块安全要求》（GB/T 37092-2018）

[9]. 《信息安全技术 密码模块安全检测要求》（GB/T 38625-2020）

[10].《信息安全技术 传输层密码协议（TLCP）》（GB/T 38636-2020）

[11].《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）

2. 车与车安全通信

2.1. 建设目标

面向车与车直连通信场景，建立车车通信安全信任体系。试点单位研发建立车车通信身份认证技术能力，建设 C-V2X 安全证书管理系统，通过接入相关车联网安全信任根和工业和信息化部车联网安全信任根管理平台，在车辆驾驶应用场景中开展跨信任域的身份认证，保障多品牌车辆的安全通信，构建车车通信安全保障能力。

2.2. 技术要求

车端设备通过搭载基于商用密码的安全芯片、软件模块等组件，实现密钥管理、证书管理、安全计算等车端安全凭证管理和数据处理功能。通过车辆生产环节配置、运营商通道配置、服务器令牌授权等方式实现车载设备证书初始化。探索建立车辆全生命周期证书管理方式（如：车辆上牌、车辆年检、交易变更、车辆报废等环节）。建设 C-V2X 安全证书管理系统，为车载设备提供证书发布、更新、撤销等证书管理服务。车载设备按照有关标准实现与证书管理系统、相关车联网安全信任根和工业和信息化部车联网安全信任根管理平台的数据交互。

2.3. 通信安全要求

2.3.1. 数据传输真实性

在车车直连通信中，需要保证传输数据者身份的真实性，防止车辆在传输消息过程中身份被假冒。

车辆首先使用与假名证书对应的私钥对其播发的基本安全消息（Basic Safety Message，BSM）进行数字签名，然后将该签

名消息连同假名证书或假名证书的摘要值一起广播出去。周围接收到该消息的车辆首先利用签发假名证书的证书颁发机构（Certificate Authority，CA）的证书验证消息中的签名证书是否有效，然后利用假名证书中的公钥验证签名消息中的签名是否正确，最后接收车辆利用通过验证的 BSM 消内容确定发送车辆的行驶状态。

2.3.2. 数据传输完整性

在车车直连通信中，需要保证传输数据的完整性，防止消息在传输过程中被篡改。传输数据的完整性可以通过使用杂凑密码算法（如 SM3）、数字签名算法（如 SM2）来保证。

车辆利用杂凑密码算法计算 BSM 消息的摘要值，将该 BSM 消息连同摘要值的签名一起广播出去；周围接收到该 BSM 消息的车辆重新利用杂凑密码算法计算 BSM 消息的摘要值，并使用车辆的签名公钥验证摘要值的签名，保证传输数据的完整性。

2.3.3. 数据传输机密性

在车车直连通信中，需要保证重要数据的机密性，防止消息中的重要数据在传输过程中被泄密。传输数据的机密性可以通过使用对称密码算法（如 SM4）来保证。

车辆通可过密钥分发平台或预置方式获取对称加密密钥，利用对称密钥对 BSM 消息中的重要信息进行加密，然后车辆将该 BSM 消息广播出去，周围接收到该消息的车辆使用对称密钥对 BSM 消息中加密的重要信息进行解密。鼓励探索对称密钥分发机制，保障对称密钥在分发、更新等环节的安全性和有效性。

2.3.4. 抗重放

车辆可以采用时间戳或缓存队列等方式防御抗重放攻击，车辆应判断接收到的消息中的时间戳是否过期。通信双方需要准确的时间同步，且保证来自合法权威的时间源，如：GNSS（Global Navigation Satellite System）时间。

2.3.5. 行为抗抵赖

车辆发送方使用私钥对 BSM 消息进行数字签名，周围接收到该消息的车辆使用发送方的公钥对签名数据验签，防止车辆发送方对其发送 BSM 消息的行为进行抵赖。

2.3.6. 隐私保护

在车车直连通信过程中，应对车辆标识等数据进行匿名化或随机化处理，保护用户隐私。发送 BSM 消息时，应按相关标准规定采用随机切换假名证书、随机变化消息序列号等措施，防止假名证书与车辆形成关联。

2.4. 身份认证和安全通信

按照中国通信标准化协会（China Communications Standards Association，CCSA）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》（YD/T 3957-2021）建设 V2X 安全证书管理系统，包括：中间证书机构（Intermediate CA，ICA）、注册证书机构（Enrolment Certificate Authority，ECA）、假名证书机构（Pseudonym Certificate Authority，PCA）和异常行为管理机构（Misbehavior Authority，MA），如图 2 所示。结合实际配套服务器密码机、签名验签服务器、安全认证网关等密码基础设施。在车辆终端使用安全中间件，为车载设备提供证书申请、下载等

服务。C-V2X 安全证书管理系统网络部署结构可参考附录 2。

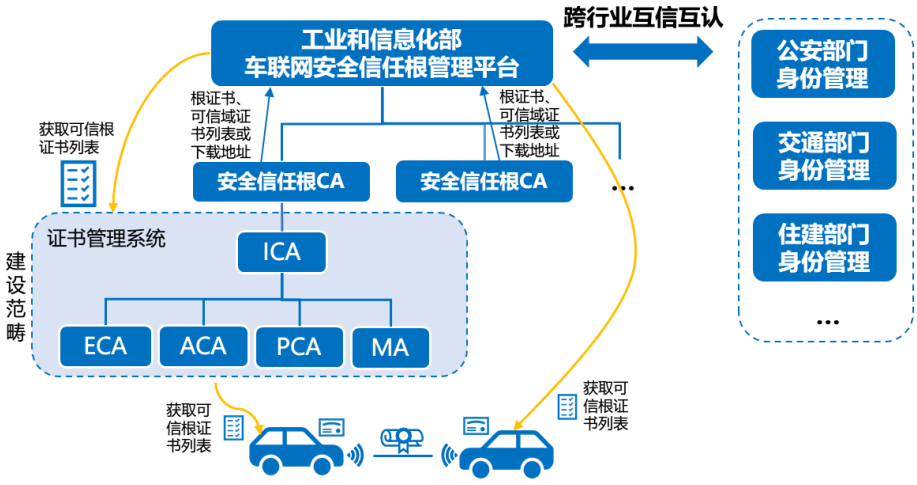


图 2 车辆安全证书管理系统建设范畴和互信方式

各地试点建立的安全证书管理系统作为二级节点接入相关车联网安全信任根 CA。各安全信任根 CA 接入工信部车联网安全信任根管理平台。由工信部车联网安全信任根管理平台生成并发布可信根证书列表（Trusted Root Certificate List，TRCL），如图 2 所示。各安全证书管理系统获取 TRCL 并分发至车辆，或由车辆自行从工信部车联网安全信任根管理平台获取 TRCL，实现车辆之间互认互信互通。

探索建立与其他行业车联网身份管理与认证平台之间实现跨行业互信互认。其他政府行业车联网身份管理及认证平台发送车联网根 CA 证书至工信部车联网安全信任根管理平台，由工信部车联网安全信任根管理平台生成并返回可信根证书列表，再由该行业车联网身份管理及认证平台下发到车辆，实现车辆之间互认互信互通。

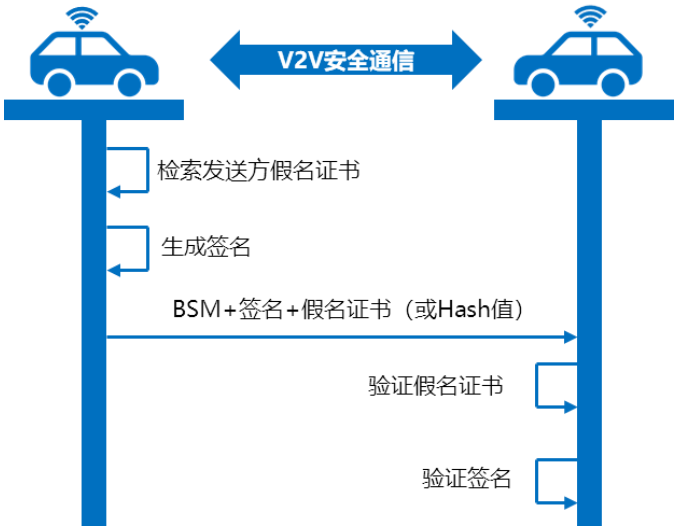


图 3 车与车安全通信流程示意

车与车进行安全通信时，车载设备首先需要获取注册证书和假名证书，使用假名证书对广播的 BSM 消息进行签名，保证消息来源的真实性、机密性、完整性和抗抵赖性，如图 3 所示。

车载终端应符合《基于 LTE 的车联网无线通信技术 网络层技术要求》（YDT 3707-2020）《基于 LTE 的车联网无线通信技术 消息层技术要求》（YDT 3709-2020）《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》（YD/T 3957-2021）等技术要求，做好协议一致性测试，保障不同品牌终端之间互信互认互通。

2.5. 应用场景

在重点城市、高速公路、物流园区、港口、矿山、科技园区等场景下，实现基于安全通信的辅助驾驶和有条件自动驾驶应用。参考《合作式智能运输系统 车用通信系统 应用层及应用数据交互标准（第一阶段）》（CSAE 53-2020）《合作式智能运输系统 车用通信系统应用层及应用数据交互标准（第二阶段）》（CSAE 157-2020）等标准实现前向碰撞预警、交叉路口碰撞预警、左转辅助、

盲区预警、变道辅助、逆向超车预警、紧急制动预警、异常车辆提醒、车辆失控预警、紧急车辆提醒、感知数据共享、协作式变道、协作式车辆编队管理等应用场景。

2.6. 参考标准

[1]. 《信息安全技术 分组密码算法的工作模式》（GB/T 17964-2008）

[2]. 《信息安全技术 SM3 密码杂凑算法》（GB/T 32905-2016）

[3]. 《信息安全技术 SM4 分组密码算法》（GB/T 32907-2016）

[4]. 《信息安全技术 SM2 椭圆曲线公钥密码算法》（GB/T 32918-2016）

[5]. 《信息安全技术 SM2 密码算法使用规范》（GB/T 35276-2017）

[6]. 《信息技术安全技术可鉴别的加密机制》（GB/T 36624-2018）

[7]. 《信息安全技术 传输层密码协议（TLCP）》（GB/T 38636-2020）

[8]. 《基于 LTE 的车联网通信安全技术要求》（YDT 3594-2019）

[9]. 《基于 LTE 的车联网无线通信技术 网络层技术要求》（YDT 3707-2020）

[10]. 《基于 LTE 的车联网无线通信技术 消息层技术要求》（YDT 3709-2020）

[11]. 《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》（YD/T 3957-2021）

[12]. 《合作式智能运输系统 车用通信系统 应用层及应用数据交互标准（第一阶段）》（T/CSAE 53-2020）

[13]. 《合作式智能运输系统 车用通信系统应用层及应用数据交互标准（第二阶段）》（T/CSAE 157-2020）

3. 车与路安全通信

3.1. 建设目标

面向车与路侧设施直连通信场景，建立车路通信安全信任体系。试点单位研发建立车路通信身份认证技术能力，建设 C-V2X 安全证书管理系统，通过接入相关车联网安全信任根和工业和信息化部车联网安全信任根管理平台，开展跨信任域的身份认证，保障本区域多类路侧设备与车辆的车路安全通信，构建车路通信安全保障能力。

3.2. 技术要求

路侧设备通过搭载基于商用密码的安全芯片、软件模块等组件，实现安全凭证管理和数据处理功能。建立 C-V2X 安全证书管理系统，为路侧设备提供证书发布、更新、撤销等证书管理服务。路侧设备按照有关标准实现与车载设备、证书管理系统、相关车联网安全信任根和工业和信息化部车联网安全信任根管理平台的数据交互。

3.3. 通信安全要求

3.3.1. 数据传输真实性

在车路直连通信中，需要保证传输数据者身份的真实性，防止消息在传输过程中被假冒。传输数据的真实性可以通过使用数字签名算法（如 SM2）来保证。

在车路协同过程中，车辆向路侧设备发送控制指令或请求下载交通数据或高精度地图时，需要使用车辆证书的私钥对待发送的数据进行签名，然后将待发送的数据、签名数据以及车辆的证书或证书摘要值一起发送给路侧设备，路侧设备收到消息后，验

证发送的证书有效性和签名正确性，两者通过后即可认定此数据是真实的。

路侧设备向外广播路况消息或者车辆向外广播自身状态信息时，需要使用自己的证书私钥对待发送的数据进行签名，广播接收方对消息进行验签。

3.3.2. 数据传输完整性

在车路直连通信中，需要保证传输数据的完整性，防止消息在传输过程中被篡改。传输数据的完整性可以通过使用杂凑算法（如 SM3）、数字签名算法（如 SM2）来保证。

车路协同过程中，路侧设备向车辆发送高精度地图或者广播交通状况、天气预警等；车辆向路侧设备发送控制指令或者广播自身运行状态时。发送方利用杂凑密码算法计算消息的摘要值，将该消息连同摘要值一起广播出去；接收方重新利用杂凑密码算法计算消息的摘要值，并使用发送方的签名公钥验证摘要值的签名，保证传输数据的完整性。

3.3.3. 数据传输机密性

在车路直连通信中，需要保证重要数据的机密性，防止消息中的重要信息在传输过程中被泄密。数据的机密性可以通过建立安全通信通道或者对称密码算法（如 SM4）及数字信封技术来保证。

部分特种车辆、重点车辆向路侧设备发送控制指令（如控制红绿灯），需要对控制指令进行加密保护。采用数字信封技术时，可以利用路侧设备证书中的加密公钥加密一个随机的会话密钥，然后利用会话密钥对控制指令进行加密，然后将加密的数字信封

发送给路侧设备，路侧设备收到数字信封后，首先使用自己的加密私钥对数字信封解密，获得会话密钥，然后用会话密钥解密获取控制指令明文。其中会话密钥采用即用即销毁策略。也可通过密钥分发平台或预置方式将分发对称加密密钥。鼓励探索对称密钥分发机制，保障对称密钥在分发、更新等环节的安全性和有效性。

3.3.4. 抗重放

车路设备可以采用时间戳与随机数组合、流水号方式防御抗重放攻击，接收方应判断接收到的消息中的时间戳是否过期。通信双方需要准确的时间同步，且保证来自合法权威的时间源。

3.3.5. 行为抗抵赖

车路直连通信中，车辆或路侧设备用自己的私钥对发送的数据进行签名，接收方使用发送方的证书对签名数据验签，防止发送方对其行为进行抵赖。

3.3.6. 隐私保护

在车路直连通信过程中，应对车辆标识等数据进行匿名化或随机化处理，保护用户隐私。发送 BSM 消息时，应按相关标准规定采用随机切换假名证书、随机变化消息序列号等措施，防止假名证书与车辆形成关联。

3.4. 身份认证和安全通信

按照 CCSA 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》（YD/T 3957-2021）建设 V2X 安全证书管理系统，包括：中间证书机构（ICA）、注册证书机构（ECA）、应用证书机构（ACA）、假名证书机构（PCA）（可选）和异常行

为管理机构（MA），如图 4 所示。结合实际建设配套服务器密码机、签名验签服务器、安全认证网关等密码基础设施和终端安全中间件软件，为路侧设备和车辆提供证书申请、下载等服务。V2X 安全证书管理系统网络部署结构可参考附录 2。

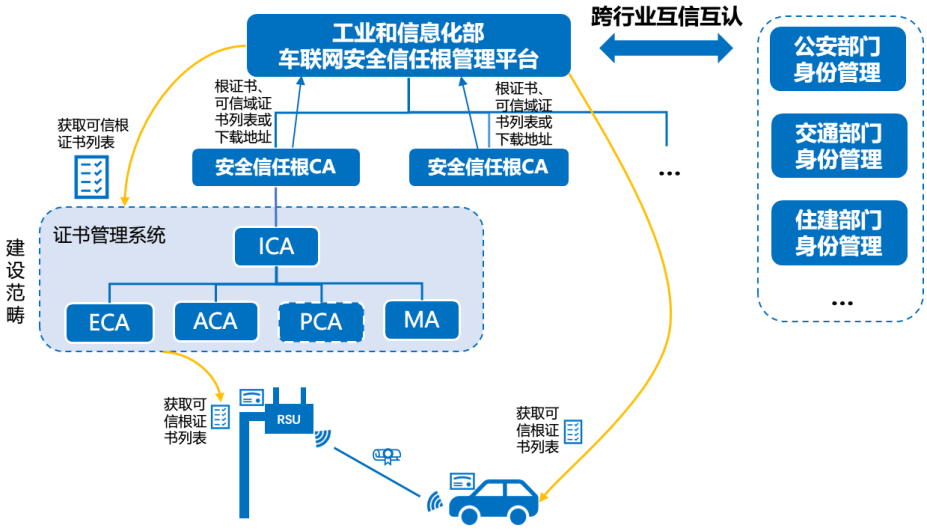


图 4 路侧设施安全证书管理系统建设范畴和互信方式

各地试点建立的安全证书管理系统作为二级节点接入相关车联网安全信任根 CA。各车联网安全信任根 CA 接入工信部车联网安全信任根管理平台。由工信部车联网安全信任根管理平台生成并发布可信根证书列表（TRCL），如图 4 所示。各安全证书管理系统获取 TRCL 并分发至路侧设备或车辆，或由路侧设备或车辆自行从工信部车联网安全信任根管理平台获取 TRCL，实现路侧设施与车辆之间互信互认互通。

探索建立与其他行业车联网身份管理及认证平台之间实现跨行业互信互认。其他行业车联网身份管理及认证平台发送其车联网根 CA 证书至工信部车联网安全信任根管理平台，由工信部车联网安全信任根管理平台生成并返回可信根证书列表，再由该行业车联网身份管理及认证平台下发到路侧设施，实现路侧设施

与车辆之间互认互信互通。

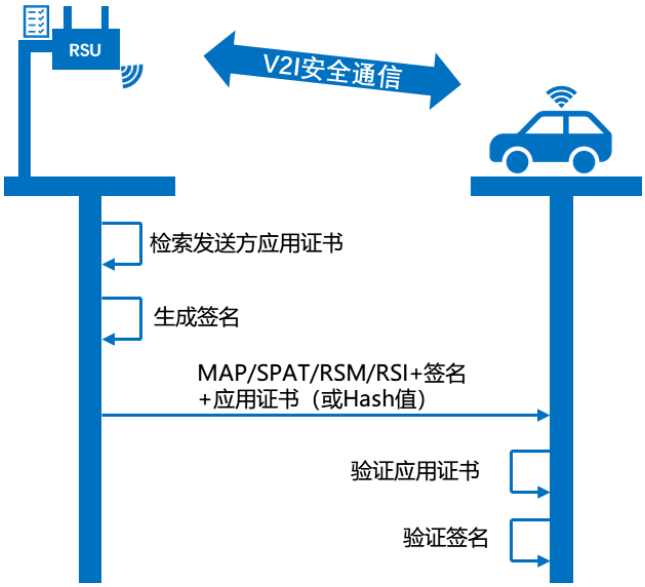


图 5 车与路安全通信流程示意

车辆与路侧设备安全通信时，路侧设备首先需要获取注册证书和应用证书，使用应用证书对广播的 MAP/SPaT（Signal Phase and Timing）/RSM（Road Safety Message）/RSI（Road Side Information）消息进行签名，保证消息来源的真实性、机密性、完整性和抗抵赖性，如图 5 所示。

车载终端和路侧终端应符合《基于 LTE 的车联网无线通信技术 网络层技术要求》（YDT 3707-2020）《基于 LTE 的车联网无线通信技术 消息层技术要求》（YDT 3709-2020）《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》（YD/T 3957-2021）等技术要求，做好协议一致性测试，保障不同品牌终端之间互信互认互通。

3.5. 应用场景

在重点城市、高速公路、封闭测试场、车路协同试点路段等场景下，实现基于安全通信的安全预警、效率提升等车路协同应

用。参考《合作式智能运输系统 车用通信系统 应用层及应用数据交互标准（第一阶段）》（CSAE 53-2020）《合作式智能运输系统 车用通信系统应用层及应用数据交互标准（第二阶段）》（CSAE 157-2020）等标准实现交叉路口碰撞预警、左转辅助、道路危险状况提示、限速预警、闯红灯预警、弱势交通参与者碰撞预警、绿波车速引导、车内标牌、前方拥堵提醒、紧急车辆提醒、感知数据共享、协作式变道、协作式车辆汇入、协作式交叉口通行、差分数据服务、动态车道管理、协作式优先车辆通行、场站路径引导服务、浮动车数据采集、道路收费等应用场景。

3.6. 参考标准

[1]. 《信息安全技术 分组密码算法的工作模式》（GB/T 17964-2008）

[2]. 《信息安全技术 SM3 密码杂凑算法》（GB/T 32905-2016）

[3]. 《信息安全技术 SM4 分组密码算法》（GB/T 32907-2016）

[4]. 《信息安全技术 SM2 椭圆曲线公钥密码算法》（GB/T 32918-2016）

[5]. 《信息安全技术 SM2 密码算法使用规范》（GB/T 35276-2017）

[6]. 《信息技术安全技术可鉴别的加密机制》（GB/T 36624-2018）

[7]. 《基于 LTE 的车联网通信安全技术要求》（YDT 3594-2019）

[8]. 《基于 LTE 的车联网无线通信技术 网络层技术要求》（YDT 3707-2020）

[9]. 《基于 LTE 的车联网无线通信技术 消息层技术要求》（YDT 3709-2020）

[10]. 《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》（YD/T 3957-2021）

[11]. 《合作式智能运输系统 车用通信系统 应用层及应用数据交互标准（第一阶段）》（T/CSAE 53-2020）

[12]. 《合作式智能运输系统 车用通信系统应用层及应用数据交互标准（第二阶段）》（T/CSAE 157-2020）

[13]. 《基于 LTE 的车联网无线通信技术 直连通信系统路侧单元技术要求》（T/CSAE 159-2020）

4. 车与设备安全通信

4.1. 建设目标

面向车与设备通信场景，建立车与设备通信安全信任体系。试点单位研发建立身份认证、安全加固等技术能力，支持各类车与设备通信场景下的身份认证、数据机密性和完整性保护，构建车与设备通信安全保障能力。

4.2. 技术要求

通过基于商用密码的数字证书、数字签名、数据加密等技术，实现车载信息交互系统与手持移动智能终端、新能源汽车与充电桩等车与外部设备交互场景的安全通信。基于商用密码技术，实现车载短距无线通信场景中的密钥可信交换和安全保护，采用安全协议对通信链路进行加密。

4.3. 通信安全要求

4.3.1. 数据传输真实性

在车与设备应用场景中，需要保证传输数据者身份的真实性，防止消息在传输过程中被假冒。传输数据的真实性可以通过使用数字签名算法（如 SM2）来保证。

例如在车与移动终端通信场景中，在近场通信时，车主使用相关的移动终端与车联网云平台建立安全通道，并向车联网云平台发起注册请求，提交移动终端的设备鉴别信息、签名公钥、蓝牙地址信息、认证凭证等信息。车联网云平台对移动终端进行鉴别后，将车辆的签名公钥和蓝牙地址返回至移动终端，再将移动终端的公钥及蓝牙地址信息通过安全通道发送给车辆。在后续开启/关闭车门的过程中，移动终端和车辆使用各自的私钥对传输

数据进行签名，用对方的公钥对消息签名进行验证，保证传输数据的真实性。在远程通信时，车主对移动智能终端进行操作，使用移动终端的私钥对传输数据进行签名，并将数据和签名证书发送至车联网云平台。车联网云平台首先验证签名证书的有效性，再对签名的有效性进行验证，保证传输数据的真实性。车联网云平台采用上述同样的数据签名方式将传输数据转发至车辆，保证数据传输的真实性。车辆的反馈信息采用同样的数据签名方式通过车联网云平台传输到移动终端。

4.3.2. 数据传输完整性

在车与设备应用场景中，需要保证传输数据的完整性，防止消息在传输过程中被篡改。传输数据的完整性可以通过使用杂凑密码算法（如 SM3）来保证。

例如在车与移动终端通信场景中，在近场通信时，移动终端可利用杂凑密码算法计算控制指令的摘要值，再用移动终端的签名私钥对摘要值进行签名，然后将控制指令数据、摘要值发送至车辆。车辆计算接收数据的摘要值，并使用移动终端的签名公钥验证摘要值的签名，保证传输数据的完整性。在远程通信时，可通过上述同样的方式，移动终端将控制指令发送至车联网云平台，再由车联网云平台转发至车辆，保证传输数据的完整性。

4.3.3. 数据传输机密性

在车与设备应用场景中，需要保证重要数据的机密性，防止消息中的重要信息在传输过程中泄露。传输数据的机密性可以通过建立安全通信链路或采用对称密码算法（如 SM4）以及数字信封分发对称密钥的方式来保证。

例如在车与移动终端通信场景中，在近场通信时，可采用数字信封方式，由移动终端先产生一个随机对称密钥，使用对称密钥对控制指令进行加密，然后使用车辆的公钥对对称密钥加密，加密的对称密钥和加密后的数据形成一个数字信封，再将数字信封发送给车辆。车辆先用自己的私钥解密对称密钥，然后用对称密钥解密加密数据，保证传输数据的机密性。在远程通信时，通过上述同样的方式保证传输数据的机密性。

4.3.4. 抗重放

车辆和移动终端可以采用时间戳或缓存队列等方式防御抗重放攻击，接收方应判断接收到的消息中的时间戳是否过期。通信双方需要准确的时间同步，且保证来自合法权威的时间源。

4.3.5. 行为抗抵赖

在近场和远程通信应用场景中，发送方用自己的私钥对传输的数据进行签名，接收方使用发送方的公钥对签名数据验签，防止发送方对其行为进行抵赖。

4.3.6. 隐私保护

在车与设备通信过程中，应采用技术措施对汽车数据、个人信息、敏感个人信息、重要数据等进行保护，按有关要求进行匿名化、去标识化等处理，保护用户隐私。

4.4. 身份认证和安全通信

车与设备身份认证和安全通信架构包括：证书管理系统、车端和外部设备的密码应用中间件、车端和外部设备的密码模块、平台侧的安全网关、平台侧的安全服务。整体结构如图 6 所示。

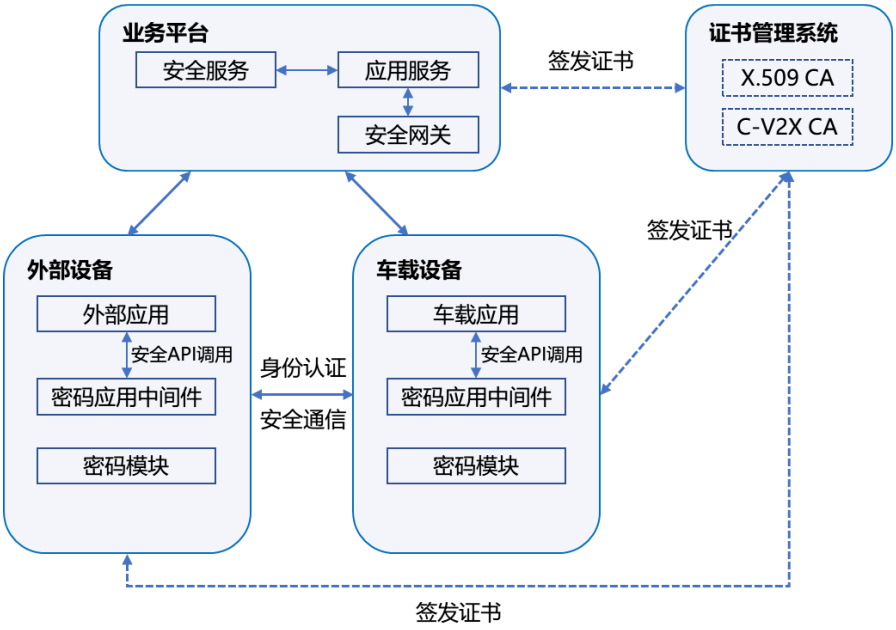


图 6 车与设备通信身份认证系统和安全通信示意

车载设备与外部设备间可使用短距无线通信技术直接通信，也可经云平台中转通信。车载设备与外部设备或云平台之间可采用 TLS/TLCP 等安全协议（推荐 1.2 及以上版本，鼓励使用国密 SSL 协议）建立安全链路，也可基于消息层加密、签名等方式保证数据传输安全。鼓励使用其他安全通信协议，探索使用 C-V2X 安全证书实现车与设备间身份认证和安全通信。

4.5. 应用场景

实现基于身份认证和加密技术的车与设备通信应用，典型应用包括基于移动智能终端的车辆远程控制、车辆信息查询、安全预警等应用，无钥匙进入、车载设备互联等车载短距无线通信应用，以及新能源汽车充电应用等。

4.6. 参考标准

[1]. 《信息安全技术 分组密码算法的工作模式》（GB/T 17964-2008）

[2]. 《信息安全技术 公钥基础设施 数字证书格式规范》（GB/T 20518-2018）

[3]. 《信息安全技术 证书认证系统密码及相关安全技术规范》（GB/T 25056-

2018）

[4]. 《信息安全技术 SM3 密码杂凑算法》（GB/T 32905-2016）

[5]. 《信息安全技术 SM4 分组密码算法》（GB/T 32907-2016）

[6]. 《信息安全技术 SM2 椭圆曲线公钥密码算法》（GB/T 32918-2016）

[7]. 《信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法》（GB/T 34975-2017）

[8]. 《信息安全技术 SM2 密码算法使用规范》（GB/T 35276-2017）

[9]. 《信息技术安全技术可鉴别的加密机制》（GB/T 36624-2018）

[10].《信息安全技术 密码模块安全要求》（GB/T 37092-2018）

[11].《信息安全技术 密码模块安全检测要求》（GB/T 38625-2020）

[12].《信息安全技术 传输层密码协议（TLCP）》（GB/T 38636-2020）

[13].《信息安全技术 车载网络设备信息安全技术要求》（GB/T 征求意见稿-信安标委）

[14].ShangMi（SM）Cipher Suites for TLS 1.3（RFC 8998）

[15].《通用密码服务接口规范》（GM/T 0019-2012）

5. 安全保障

5.1. 证书管理系统安全保障

5.1.1. 网络安全

参考《信息安全技术 证书认证系统密码及其相关安全技术规范》（GB/T 25056-2018）和网络安全等级保护第三级要求，部署安全认证网关、防火墙、入侵防御设备、网络流量检测设备、防病毒网关和软件等设备，做好网络安全防护。

5.1.2. 密钥安全

密钥安全的主要目标是保护证书管理系统中所使用的密钥，在其生成、存储、使用、更新、废除、归档、销毁、备份和恢复整个生命周期中的安全。应采取硬件密码设备、密钥管理安全协议、密钥存取访问控制、密钥管理操作审计等多种安全措施。密钥安全的基本要求是:

a) 密钥的生成和使用应在硬件密码设备中完成;

b) 密钥的生成和使用应有安全可靠的管理机制;

c) 存在于硬件密码设备之外的所有密钥应加密;

d) 密钥应有安全可靠的备份恢复机制;

e) 对密码设备操作应由多个操作员实施。

5.1.3. 管理安全

证书系统管理安全应满足下列要求:

a) 验证证书申请者的身份;

b) 防止非法签发和越权签发证书，通过审批的证书申请应提交至证书管理系统，由证书管理系统签发与申请者身份相符的证书;

c) 保证证书管理的可审计性，对于证书的任何处理都应作日志记录。通过对日志文件的分析，可以对证书事件进行审计和跟踪。

5.1.4. 安全审计

证书管理系统在运行过程中涉及大量功能模块之间的相互调用，以及各种管理员的操作，对这些调用和操作需要以日志的形式进行记载，以便用于系统错误分析、风险分析和安全审计等工作，日志记录里不应出现密码、私钥等数据信息。相关日志留存不少于 6 个月。各模块应该记录如下数据:

a) 调用请求的接收时间;

b) 调用请求的来源网络地址;

c) 调用请求发起者的身份;

d) 调用请求的内容;

e）处理结果等。

5.1.5. 数据备份

数据备份的目的是确保证书管理系统的关键业务数据在发生灾难性破坏时，系统能够及时和尽可能完整地恢复被破坏的数据。应选择适当的存储备份系统对重要数据进行备份，有条件的考虑采用异地备份。不同的应用环境可以有不同的备份方案，但应满足以下基本要求:

a) 备份要在不中断数据库使用的前提下实施;

b) 备份方案应符合国家有关信息数据备份的标准要求;

c) 备份方案应提供人工和自动备份功能;

d) 备份方案应提供实时和定期备份功能;

e) 备份方案应提供增量备份功能;

f) 备份方案应提供日志记录功能;

g) 备份方案应提供数据完整性校验功能;

h) 备份应提供归档检索与恢复功能。

5.1.6. 可靠性

证书管理系统应提供 7×24 小时服务，对影响系统可靠性的主要因素如网络故障、主机故障、密码设备故障、数据库故障和电源故障等，宜采取软硬件冗余配置作为预防措施。

5.1.7. 网络链路冗余

为保证证书管理系统的服务，证书管理系统的网络对外接口应根据具体情况，可有两条物理上独立的链路，同时考虑交换机、路由器、防火墙的冗余配置。

5.1.8. 主机及密码设备冗余

证书管理系统中与关键业务相关的主机、密码设备、在服务网段和核心网段中的服务器应采用双机热备份或双机备份措施。

5.1.9. 存储冗余

证书管理系统应采用磁盘阵列、磁盘镜像等措施存储数据，具备容错和备份能力。

5.1.10. 电源冗余

证书管理系统应采用高可靠的电源解决方案，并应采用 UPS（Uninterruptible Power Supply）为系统提供不间断电源，提供不少于 8 h 供电。

5.2. 云平台安全保障

可参考网络安全等级保护第三级要求，在云平台部署安全认

证网关、防火墙、入侵防御设备、网络流量检测设备、防病毒网关和软件等网络安全防护设备做好网络安全防护。依据相关法律法规、标准，做好云平台重要数据和用户个人信息保护。

5.3. 终端安全保障

终端安全保障涉及系统加固防护、固件防护、应用防护、网络安全防护、数据存储安全防护。

——系统加固防护：主要以安全芯片和密钥体系为基础，对终端操作系统各分区进行安全加固。

——固件防护：采用安全存储、安全访问控制、固件校验等技术，防止固件提取、固件逆向、固件篡改等攻击。

——应用防护：检测应用程序和运行环境存在的安全风险，通过加壳混淆、分级文件校验、调试注入防护等技术来提升应用的整体安全防护水平。采用签名和加密存储，保护应用程序的可用性和完整性。

——网络安全防护：采用防火墙、入侵检测与防御等技术，检测并拒绝恶意的网络攻击。

——数据存储安全防护：采用数据加密、签名等方法，保证终端数据的存储安全。建议将重要数据、密钥等存储于硬件安全模块（Hardware Security Module，HSM）。

根据需要使用车规级安全密码芯片，满足车载终端对高并发数字加密、签名的需求，并提供安全的密钥存储、数据存储和密码运算服务。参考《信息安全技术 车载网络设备信息安全技术要求》（GB/T 征求意见稿—信安标委）相关要求做好车载终端安全防护。

5.4. 参考标准

[1]. 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

[2]. 《信息安全技术 证书认证系统密码及其相关安全技术规范》（GB/T 25056-2018）

[3]. 《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）

[4]. 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

[5]. 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

[6]. 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

[7]. 《信息安全技术 个人信息安全规范》（GB/T 35273-2020）

[8]. 《信息安全技术 个人信息去标识化指南》（GB/T 37964-2019）

[9]. 《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）

[10].《信息安全技术 车载网络设备信息安全技术要求》（GB/T 征求意见稿）

[11].《基于 LTE 的车联网通信安全技术要求》（YD/T 3594-2019）

[12].《车联网信息服务 用户个人信息保护要求》（YD/T 3746-2020）

[13].《车联网无线通信安全技术指南》（YD/T 3750-2020）

[14].《车联网信息服务 数据安全技术要求》（YD/T 3751-2020）

[15].《车联网信息服务平台安全防护技术要求》（YD/T 3752-2020）

附录 1 X.509 证书管理系统建设参考方案

附录 1.1 证书管理系统

X.509 证书管理系统为车载终端、路侧设备、应用服务平台签发 X.509 格式证书，用于 TLS/TLCP 等安全通信，例如车载终端与应用服务平台安全通信、路侧单元向云端回传安全通信等。

参考《信息安全技术 证书认证系统密码及相关安全技术规范》（GB/T 25056-2018）建设 X.509 CA 证书系统，参考系统部署拓扑如图 7 所示，包括密钥管理区、核心区、管理区、服务区。

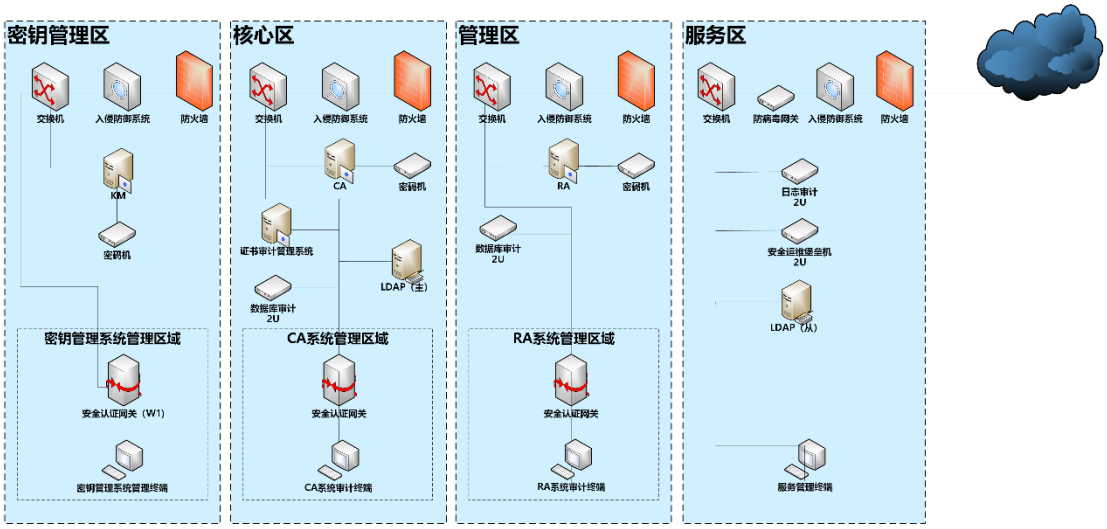


图 7 X.509 CA 证书系统参考部署图

X.509 证书管理系统的网络安全保障包括基于系统安全、通信安全、密钥安全、证书管理安全、安全审计、数字备份和可选性、物理安全等，参考《信息安全技术 证书认证系统密码及相关安全技术规范》（GB/T 25056-2018）中的安全要求建设。

X.509 证书管理系统包含的子系统要求如下：

1. 根证书签发管理系统

负责签发管理二级 CA 系统的数字证书。提供二级 CA 系统数字证书及 CRL 列表查询。

2. 证书签发管理系统

负责颁发 T-BOX（Telematics BOX）、IVI（In-Vehicle Infotainment）、GW（Gateway）、APP（Application）等终端设备和应用程序的 X.509 证书。

1)证书种类

终端设备证书、服务器证书、签名证书、CA/RA（Register Authority）证书、系统管理员证书、个人证书、单位身份证书、机构证书、VPN（Virtual Private Network）证书等，可以根据系统新的需要，增加新的证书类型，满足应用的需求。

2)证书格式

证书管理系统颁发的数字证书和证书撤消列表符合 ITU X.509、GB/T 20518-2006、ITU-T X.509 和 RFC 5280 标准，证书存储格式支持 Base64、DER、PKCS#7 和 PKCS#12 格式，证书和私钥封装符合 PKCS＃12 标准。

3)证书管理

在签发系统中，只有拥有证书管理角色的管理员才能进行证书管理的操作。证书管理主要包括证书的申请、下载、发布、申请并下载、更新、更新并下载、冻结、解冻、撤销、延期、恢复、归档、授权码更新、证书查询、证书实体查询及证书撤销列表的发布等操作。

4)模板管理

为了满足各种业务系统对于数字证书格式的特殊要求，要求在签发管理系统中，提供数字证书模板自定义的功能，实现证书扩展域名称、扩展域值的自定义。

5)权限管理

在签发系统中，要严格按照分权管理的思想，通过以超级管理员管理系统管理员、再由系统管理员向下授权的方式，实现对管理员的控制和管理及事件追踪。

6)审计管理

根据整个系统分权设计管理的思想，只有具有审计管理角色的管理员才能进行审计管理操作，审计管理包括查询业务日志和统计证书。

7)其他要求

根据实际情况选择支持 RSA 或 SM2 非对称双算法，所签发的所有类型证书的密钥长度支持 2048/4096 或 SM2 256 位；对称算法支持 AES128/256、3DES 或 SM4；散列算法支持 SHA256、SHA512 或 SM3。

3. 证书注册管理系统

证书注册管理系统提供证书的申请、审核、下载、注销、在线更新等服务。证书注册系统接到证书申请后，对其合法性进行审核，并将请求提交给证书签发系统，具备以下功能:

1) 提供用户管理功能，针对用户信息，提供“增、删、改、查”等相关功能;
2) 提供证书查询、下载和统计功能;
3) 提供日志查询、分析和审计功能;
4) 可定制管理角色，管理权限和业务流程，系统的审计业务和其他业务可实现严格的分权管理，审计业务的管理员和其他业务管理员产生过程相互独立;

5) 面向证书最终用户提供自助服务，可实现用户根证书自助下载、用户信息自助录入、证书自助申请、下载和更新等功能。

4. 目录管理系统

提供二级 CA 系统数字证书及证书吊销列表（Certificate Revocation List，CRL）查询功能。

附录 1.2 密钥管理系统

密钥管理系统（Key Management System，KMS）应使用经国家密码管理局鉴定通过的密码算法和加密设备，遵循国家密码管理局发布的《证书认证系统密码及其相关安全技术规范》（GB/T 25056-2018）的要求，提供对密钥进行全过程管理的功能，包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销、密钥归档、密钥恢复以及安全管理等。

1. 密钥生成：密钥生成根据系统相关参数配置连接服务器密码机，对指定数量或策略指定类型的密钥进行预生成，支持真随机数生成和密钥分散生成方式。如根据车型、设备等情况生成密钥。
2. 密钥分发：密钥以加密形式进行分发，采用传输密钥或非对称密码算法对密钥进行加密保护后分发。
3. 密钥存储：储于硬件密码机内部或加密放于系统数据库内，非相应权限管理员无法查看密钥明文。
4. 密钥注销：提供对指定密钥的注销功能，一般由 CA 发起该请求，填写密钥注销原因，密钥管理系统审核后将密钥移位到历史库。
5. 密钥归档：系统支持对系统内各类密钥进行归档，归档密钥经过加密处理后存储于外部介质。
6. 密钥查询：提供系统内密钥的查询功能，根据输入的查询条件，用户交互界面列举出相应的密钥信息。
7. 密钥恢复：密钥恢复是指为相关机关或者 CA 提供密钥恢复服务。恢复的密钥不以明文的形式出现在载体之外，恢

复的密钥将被存放到相应的密码设备中。

8. 加密、解密功能：系统能够根据密钥索引找到相关密钥，并利用该密钥对输入数据进行加密或解密操作。
9. 算法支持：选择支持 SM2、SM3、SM4、3DES、AES128、AES256 等多种算法。

附录 2 C-V2X 安全证书管理系统建设参考方案

CCSA 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》定义了 C-V2X 安全证书管理系统逻辑架构图，实际部署时可参考图 8 分区部署，包括：服务区、管理区、核心区、根管理区。

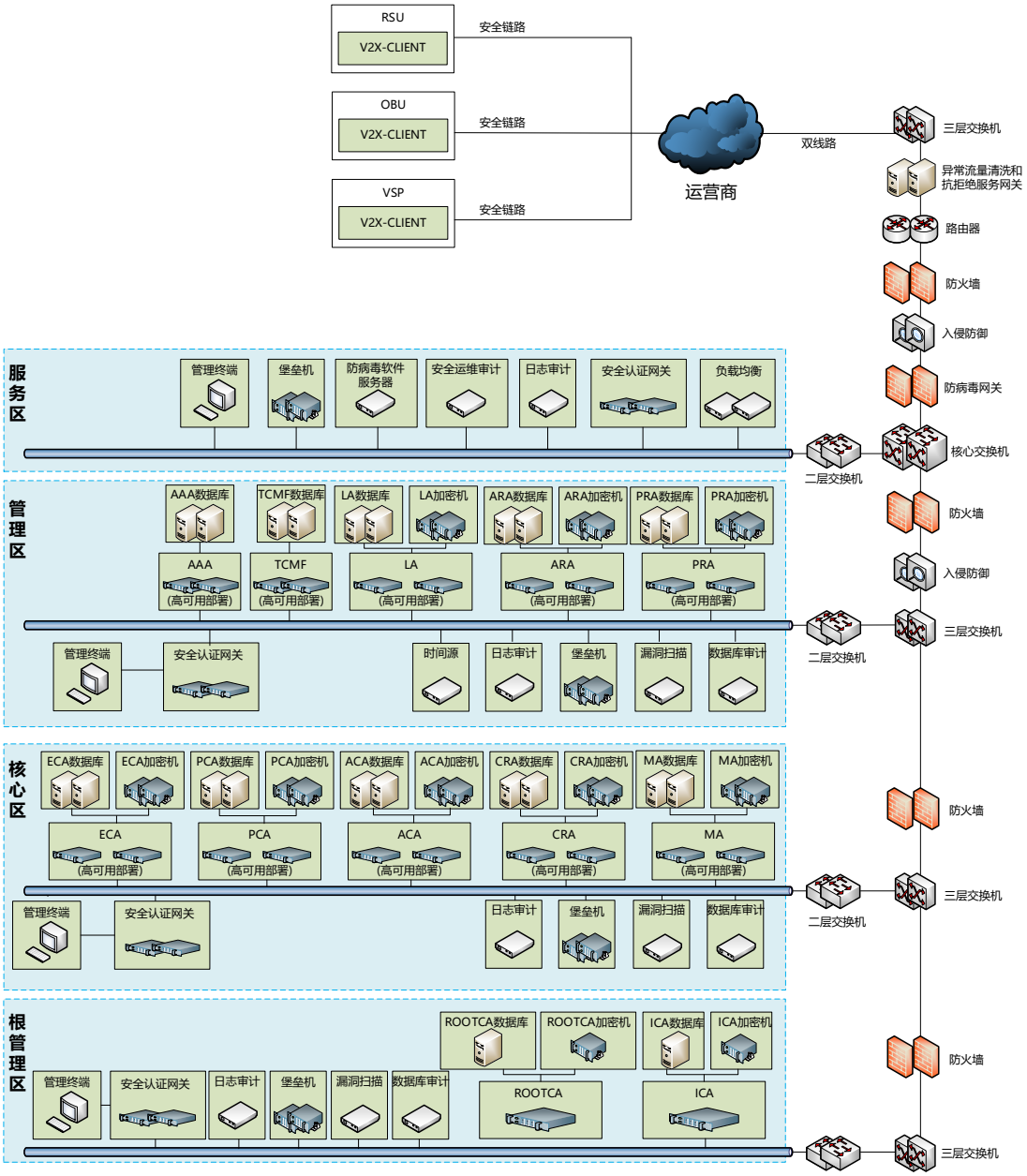


图 8 V2X 安全证书管理系统参考系统部署拓扑图

1. **服务区**：主要由安全认证网关、堡垒机、审计系统等组成，通过互联网线路面向公共互联网提供接入认证和加密通

信服务。

2. **管理区**：主要由注册系统（Registration Authority，RA）、认证授权系统（Authentication and Authorization Authority，AAA）、链接系统（Linkage Authority，LA）以及其他车厂资源组成，通过防火墙及光纤线路与服务区通信。
3. **核心区**：主要由注册 CA 系统、假名 CA 系统、应用 CA 系统、异常行为管理系统组成，通过防火墙及光纤线路与信任层、注册层通信。
4. **根管理区**：主要包含根 CA 系统、中间 CA 系统，通过防火墙及光纤线路与认证层通信。

各试点单位可根据实际情况，综合评估 C-V2X 安全证书管理系统网络安全和数据安全需求，在满足相关安全要求的情况下，选择部署相关网络安全产品，对关键设备采用双机热备、集群等高可用部署方案。