GM/Y 5011-2024

车联网密码应用标准体系研究

密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2024 年 12 月

摘 要

车联网是一个庞大的物联网应用系统,包含了大量的数据、处理过程和传输节点，必须有一套统一的标准体系来规范其高效运行，从而确保数据的真实性和完整性，完成各项业务的应用。

本研究报告旨在通过分析车联网领域的产品、技术及标准化发展现状，分析车联网中存在的安全威胁及密码应用需求，分析国外和国内的车联网标准现状与发展趋势，进一步分析国内的现有密码应用标准体系对于该技术领域的适应性，并从各层面提出车联网密码应用的标准体系规划与制标建议。

第 1 章给出了车联网的基本概念，分析了典型的安全威胁事件，并提出研究目标。

第 2 章从技术、产业、产品和标准化等方面阐述了车联网的发展现状。

第 3 章给出了车联网的安全层次结构，然后分别从实体网络和交互信息两个角度分析车联网的信息安全风险，进而定义车联网的安全目标。

第 4 章深入研究了车联网的密码应用，首先分析了车联网的密码应用需求及密码应用总体架构，然后从智能网联汽车、安全通信、车联网服务平台等不同层面分析了车联网领域的典型密码应用，对每一个层面分别给出了技术路线、安全框架和密码应用案例。

第 5 章通过调研国际上和国内相关标准化组织的标准活动，分别从智能网联汽车、传输通信网络、车联网服务平台、数据安全及隐私保护等层面对国际标准、国内标准进行了体系化的梳理，并且指出了与密码应用相关性较强的国标、行标。

第 6 章围绕密码行业标准体系的框架，提出了车联网密码应用标准体系，并列出推荐制定标准，还分析了每个推荐标准的必要性及建议标准化的内容。

关键词：车联网、V2X、网联汽车、车联云、Telematics

目 录

缩略语

APDU	应用协议数据单元（Application Protocol Data Unit）
API	应用程序接口（Application Programming Interface
APN	接入点名称（Access Point Name）
APP	应用程序（Application）
APT	高级可持续威胁攻击（Advanced Persistent Threat）
ASIC	专用集成电路（Application Specific Integrated Circuit）
AVN	车载影音导航系统（Audio, Visual and Navigation Unit）
BSM	基本安全消息（Basic Safety Message）
C-V2X	基于蜂窝的车联网（Cellular V2X）
CA	证书认证机构（Certificate Authority）
CAN	控制器局域网络（Controller Area Network）
CMAC	基于分组加密的消息鉴别码（Cipher Block Chaining-Message Authentication Code）
CPU	中央处理单元（Central Processing Unit）
CRL	证书吊销列表（Certificate Revocation List）
CSR	证书签发请求（Certificate Signing Request）
DBA	数据库管理员（Database Administrator）
DCM	车辆搭载的网络通信功能模块（Data Communication Module）
DDN	数字数据网（Digital Data Network）
DoS	拒绝服务（Denial of Service）
DSRC	专用短程通信（Dedicated Short Range Communication）
E2PROM	带电可擦除可编程只读存储器（Electrically Erasable Programmable Read Only Memory）
ECA	注册证书认证机构（Enrollment CA）
ECC	椭圆曲线密码体制（Elliptic Curve Cryptography）
ECDSA	椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm）
ECIES	椭圆曲线集成加密方案（Elliptic Curve Integrated Encryption Scheme）
ECQV	椭圆曲线隐式证书方案（Elliptic Curve Qu-Vanstone）
ECU	电子控制单元（Electronic Control Unit）
EE	终端实体（End Entity）
FLASH	快闪存储器
GBA	通用认证机制（General Bootstrapping Architecture）
GIS	地理信息系统（Geographic Information System）
GPRS	通用分组无线业务（General Packet Radio Service）
GPS	全球定位系统（Global Positioning System）
HMAC	哈希运算消息鉴别码（Hash-based Message Authentication Code）
HSM	硬件安全模块（Hardware Security Module）
HTTPS	超文本传输安全协议（Hyper Text Transfer Protocol over

	Secure Socket Layer）
I2C	集成电路串行通信总线（Inter-Integrated Circuit）
I2V	基础设施到车辆（Infrastructure to Vehicle）
IAM	身份识别与访问管理（Identity and Access Management）
IdP	身份服务提供商（Identity Provider）
IP	网际协议（Internet Protocol）
IPSec	IP 网络安全协议（Security Architecture for the Internet Protocol）
ITS	智能交通系统（Intelligent Transport System）
IVI	车载信息娱乐系统（In-Vehicle Infotainment）
KDF	密钥导出函数（Key Derivation Function）
LA	链接值颁发机构（Linkage Authority）
LTE-V2X	基于 LTE 的车联网（Long Term Evolution V2X）
MA	异常行为管理机构（Misbehavior Authority）
MCU	单片微型计算机（Microcontroller Unit）
MPU	微处理器（Micro Processor Unit）
NFC	近场通信（Near Field Communication）
NGTP	下一代 Telematics 协议（Next Generation Telematics Protocol）
OAuth	开放授权（Open Authorization）
OBD	车载自动诊断系统（On-Board Diagnostics）
OBU	车载单元（On-Board Unit）
OpenID	去中心化身份认证协议开放标准
OTA	空中下载技术（Over-the-Air Technology）
PCA	假名证书认证机构（Pseudonym CA）
PKI	公开密钥基础设施（Public Key Infrastructure）
RA	注册机构（Registration Authority）
ROM	只读存储器（Read Only Memory）
RSA	一种公钥加密算法（Rivest-Shamir-Adleman）
RSU	路侧单元（Roadside Unit）
SAML	安全断言标记语言（Security Assertion Markup Language）
SCMS	安全凭证管理系统（Security Credential Management System）
SDK	软件开发工具包（Software Development Kit）
SE	安全元件（Secure Element）
SHA	安全散列算法（Secure Hash Algorithm）
SIM	用户识别卡（Subscriber Identity Module）
SMS	短消息服务（Short Messaging Service）
SPI	串行外设接口（Serial Peripheral Interface）
SSL	安全套接字协议（Secure Sockets Layer）
TBOX	智能网联汽车的通信网关（Telematics BOX）
TCP	传输控制协议（Transmission Control Protocol）
TCU	远程信息处理控制单元（Telematics Control Unit）
TEE	可信执行环境（Trusted Execution Environment）
TELSA	定时有效流损失容忍认证协议（Timed Efficient Stream Loss-Tolerant Authentication Protocol）

TLCP	传输层密码协议（Transport Layer Cryptography Protocol）
TLS	安全传输层协议（Transport Layer Security）
TOE	评估目标（Target of Evaluation）
TSP	Telematics 服务供应商（Telematics Service Provider）
TU	Telematics 单元（Telematics Unit）
UART	通用异步收发传输器（Universal Asynchronous Receiver/Transmitter）
UDP	用户数据报协议（User Datagram Protocol）
USB	通用串行总线（Universal Serial Bus）
USIM	全球用户识别卡（Universal Subscriber Identity Module）
UTC	国际协调时间（Coordinated Universal Time）
Uu	LTE 空中接口
V2I	车辆到基础设施（Vehicle to Infrastructure）
V2N	车辆到网络（Vehicle to Network）
V2ND	车辆到漫游设备
V2P	车辆到人（Vehicle to Pedestrian）
V2V	车辆到车（Vehicle to Vehicle）
V2X	车联网（Vehicle to Everything）
VANet	车载自组网（Vehicular Ad-hoc Networks）
VCU	整车控制器（Vehicle Control Unit）
VPN	虚拟专用网络（Virtual Private Network）
VSP	车联网服务提供商（V2X Service Provider）
WAVE	汽车环境无线存取（Wireless Access in Vehicular Environments）
Wi-Fi	无线保真（Wireless Fidelity）
WPAN	无线个域网（Wireless Personal-Area Network）
WTLS	无线安全传输层（Wireless Transport Layer Security）

前 言

《车联网密码应用标准体系研究》项目是密码行业标准化技术委员会根据国家密码管理局批准的《2019 年密码行业标准制订计划（商用密码领域）》下达的标准研究任务，项目所属工作组为应用工作组。北京数字认证股份有限公司作为牵头单位，成立相应的编制工作组，组织完成该标准研究报告的编制工作。

车联网作为 5G 和汽车领域最具潜力的应用，已成为我国战略性新兴产业的重要发展方向。车联网面临终端安全、通信安全、接口安全、数据安全、交易安全等各层面的安全威胁，采用公钥基础设施（PKI）来解决 V2X 领域的密钥管理、数据加密、用户隐私保护等问题是当前研究的热点。国内外很多标准组织已经面向车联网系统的不同层面制定了该领域的诸多标准，包括信息安全相关的标准。其中，国家标准、行业标准中还涉及到 PKI 体系相关的内容，但是在密码行业标准中尚未有正式发布的车联网领域的技术标准。在这样的背景下，本研究报告通过深入分析国内外在车联网领域的相关标准，研究车联网领域的安全威胁与密码应用需求，分析密码应用技术架构及具体的密码应用场景，并进一步提出车联网密码技术应用相关的标准化建议。

本研究报告项目承担单位北京数字认证股份有限公司成立编制工作组，参与编制的单位包括北京数字认证股份有限公司、国家智能交通系统工程技术研究中心、中国信息通信研究院、国家密码管理局商用密码检测中心、北京汽车研究总院有限公司、北京信安世纪科技股份有限公司、长春吉大正元信息技术股份有限公司、三未信安科技股份有限公司、飞天诚信科技股份有限公司、上海汽车集团股份有限公司技术中心、格尔软件股份有限公司、深圳奥联信息安全技术有限公司、中国第一汽车股份有限公司、东风汽车有限公司东风日产乘用车公司、重庆长安汽车软件科技有限公司、暨南大学等。

本研究报告得到夏鲁宁和田景成两位专家的指导，主要研究人员有张永强、詹榜华、李向锋、傅大鹏、程朝辉、于润东、李国友、齐志峰、李峰、夏鲁宁、田景成、刘中、王新华、李广超、张庆勇、才君、汪宗斌、高志权、刘会议、谭武征、朱鹏飞、齐晶晶、蔡先勇、董明富、李木犀、彭镇等。

车联网密码应用标准体系研究

1 概述

1.1 政策背景

车联网是信息化与工业化深度融合的重要领域，是 5G 垂直应用落地的重点方向，具有巨大的产业发展潜力、应用市场空间和可观的社会效益，对于带动汽车行业、交通行业和电子信息行业的产业转型升级、系统创新和融合发展具有重要意义。

自 2016 年以来，国务院、国家发改委、工信部、交通运输部等多部门都陆续印发了支持、规范车联网行业的发展政策，内容涉及车联网发展技术路线、车联网先导区建设、车联网与其他领域协同融合等内容。

工业和信息化部在 2018 年印发了《车联网（智能网联汽车）产业发展行动计划》，提出了如下的行动目标：到 2020 年，实现车联网（智能网联汽车）产业跨行业融合取得突破，具备高级别自动驾驶功能的智能网联汽车实现特定场景规模应用，车联网综合应用体系基本构建，用户渗透率大幅提高，智能道路基础设施水平明显提升，适应产业发展的政策法规、标准规范和安全保障体系初步建立，开放融合、创新发展的产业生态基本形成，满足人民群众多样化、个性化、不断升级的消费需求。

2023 年 11 月，工业和信息化部等部委联合发布“关于开展智能网联汽车准入和上路通行试点工作的通知”，对取得准入的智能网联汽车产品，在限定区域内开展上路通行试点。通过开展试点工作，引导智能网联汽车生产企业和使用主体加强能力建设，在保障安全的前提下，促进智能网联汽车产品的功能、性能提升和产业生态的迭代优化，推动智能网联汽车产业高质量发展。

2024 年 1 月，工业和信息化部等部委联合发布“关于开展智能网联汽车‘车路云一体化’应用试点工作的通知”，旨在推动智能化路侧基础设施和云控基础平台建设，提升车载终端装配率，开展智能网联汽车“车路云一体化”系统架构设计和多种场景应用，形成统一的车路协同技术标准与测试评价体系，健全道路交通安全保障能力，促进规模化示范应用和新型商业模式探索，大力推动智能网联汽车产业化发展。

综合来看，车联网行业政策的支持力度较大，结合“十四五”规划对于智慧交通和智慧城市的要求，车联网行业仍处于成长期，需要政策标准进行规范和指导。

1.2 车联网系统

车联网概念引申自物联网(Internet of Things)，根据车联网产业技术创新战略联盟的定义，车联网是以车内网、车际网和车载移动互联网为基础，按照约定的通信协议和数据交互标准，在车与车（V2V）、车与路边设施（V2I）、车与行人（V2P）以及车与网络(V2N)之间进行无线通信和数据交换与共享的网络系统。车联网也常被称为“V2X”网络。

国际上现有的对于车联网的研究大都源自于 Telematics，即应用无线通信技术的车载电脑系统，是基于无线通信、定位导航、网络通信技术和车载电脑的综合产物。目

前比较成熟的Telematics系统有现代汽车的BlueLink,通用汽车的安吉星OnStar,美国的Snap-On等。

车联网是由车辆位置、速度和路线等资讯构成的巨大交互网络，其本质是物联网和互联网的融合。车联网通过人—车—路—网之间的实时感知与协同来实现智能交通管理、智能动态信息服务和智能车辆控制的一体化，向用户提供道路安全、交通效率提升和信息娱乐等各类服务，满足人们交通信息消费的需要。

车联网系统的交互如图 1-1 所示，在典型车联网业务场景下，车联网通信主要涉及智能网联汽车、路侧通信设备、车联网服务平台和终端设备四类实体，这些实体之间通过 Uu 蜂窝网通信接口、PC5 直连通信接口等进行通信。

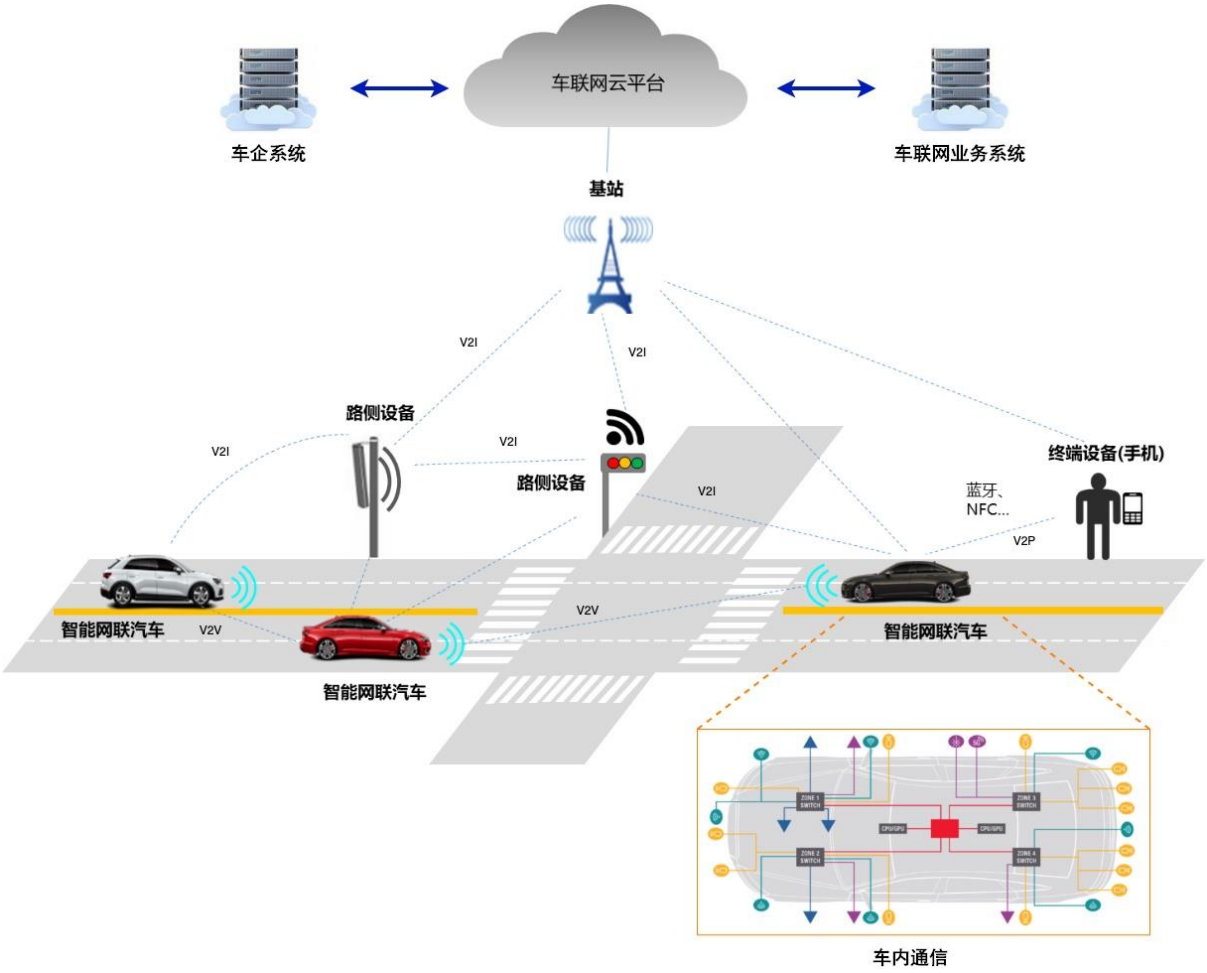

图 1-1 车联网系统交互示意图

下面说明这四类实体在车联网中的作用：

- 智能网联汽车

智能网联汽车是指将车联网与智能车有机联合，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，实现车与人、车、路、后台等智能信息交换共享，实现安全、舒适、节能、高效行驶，并最终可替代人来操作的新一代汽车，是车联网的核心。

借助 V2X 网络，智能网联汽车可实现车与车（V2V）、车与路边设施（V2I）、车与行人（V2P）以及车与网络（V2N）之间进行无线通信。智能网联汽车内部的相关组件（如

ECU 等）通过车内网络实现通信，并且可以通过 TBox 车载设备与车联网云平台进行通信。

- 路侧设备

路侧设备（RSU）通常安装部署于道路路口或路段中心，可与信号灯、雷达、边缘计算服务器等道路交通基础设施连接，其主要作用包括：静态道路交通信息广播，如道路限速信息、红绿灯相位信息等；动态道路交通信息广播，如道路实时交通信息、道路的开放及封闭信息等。路侧设备是车联网服务的重要外部环境。

- 车联网服务平台

车联网服务平台从属性看，包括公共服务平台、行业应用平台、数据平台、业务支撑平台等在云端部署的服务平台。从业务类型看，包括地图服务、位置服务、娱乐服务、远程诊断等业务平台。车联网服务平台是实现车联网服务的业务和数据载体。

- 终端设备

终端设备主要包括充电桩、手机、平板等。其主要支持实现的业务包括充电桩寻找及充电、车况查询、远程控车、自动寻车等。各类终端设备是使用车联网服务的介质载体，也是车联网基础设施的主要构成。

1.3 关联领域及其关系

在车联网的研究中不可避免地会涉及到智能交通、智能网联汽车等技术领域，研究它们之间的关联与差别对于明确技术范畴是非常必要的。图 1-2 表达了车联网与智能交通、智能汽车、智能网联汽车等概念间的相互关系，可见智能汽车隶属于智能交通大系统，而智能网联汽车则属于智能汽车与车联网的交集。

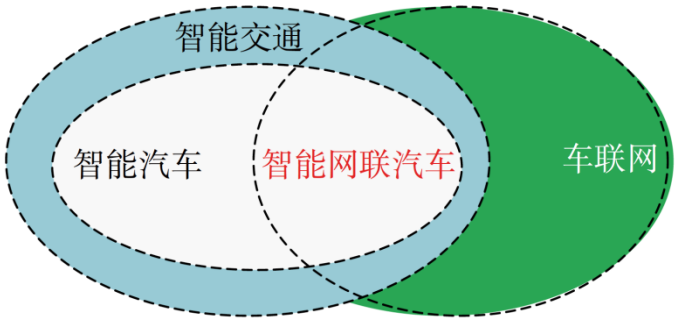

图 1-2　智能交通、车联网与智能网联汽车等的相互关系

1.4 车联网典型应用

车联网有很多的应用场景，其中典型的应用包括：

（1）智能交通系统

车联网从形式上看属于传统物联网技术与智能交通技术相结合的产物,在实施上看就是把各种先进的物联网技术应用于交通管理实践中,达到人、车、道路和环境的有机协调,从而实现车辆定位、监控、导航等各项服务功能。车联网的智能交通系统中有着非常广泛的应用,很大程度上成为了智能交通体系的主要组成部分,具体应用主要有:车辆调度管理、高速公路不停车收费、智能停车场管理、交通违章自动记录等等。

（2）智能车载系统

车联网的各项服务为智能车载系统提供了重要的数据来源,为车内的悠闲娱乐、安全驾驶和舒适环境提供了技术支撑。最典型的智能车载系统主要有导航系统、倒车辅助系统、GPRS 通信系统以及广播音乐系统。这些系统成为了车联网业务的主要使用者,支撑着车联网应用市场的主体。

（3）紧急救援系统

车辆在出行过程中一旦遇到紧急情况,就可以通过紧急救援系统向远程服务中心发出报警信号,服务中心通过卫星定位确定车辆的实时位置,并把信息转发给急救中心、消防队、公安交警等第三方救援机构,为相关人员开展快速的救援行动提供了良好的条件,从而减少人员伤亡和财产的损失。

1.5 车联网的安全威胁事件

随着智能网联汽车和车联网的快速发展,在公开报导中可以看到汽车信息安全攻击事件持续快速增长[1]。

在 2015 年发生了一个里程碑事件,菲亚特克莱斯勒美国公司(FCA)宣布在美召回约 140 万辆车，原因是汽车存在软件漏洞，导致黑客成功攻破了 FCA 旗下的 Jeep 自由光车载系统，并对该车进行了遥控。这是首次发生汽车制造商因黑客风险而召回汽车的事件。

在此之后，不断地有其他汽车厂家的产品遭遇黑客的攻击：

——2019 年 3 月，丰田服务器遭到入侵，导致 310 万个人数据泄露；

——2019 年 4 月,戴姆勒旗下的 Car2Go 手机 APP 被破解,导致 100 余辆汽车被盗；

——2019 年 6 月，德国宝马遭 APT 攻击，攻击者可渗透实现远程监视和控制；

——2017～2021 年，特斯拉多款车型均遭到破解，白帽黑客披露多项漏洞；

——2021 年,黑客成功地为特斯拉汽车开发了一种新的密钥克隆“中继攻击”（Relay Attack），并在特斯拉 Model X 电动汽车上进行了演示；

——2022 年 12 月，现代汽车软件中的一个漏洞允许远程攻击者解锁并启动各种受影响的车型或窃取车主信息；

——2022 年 12 月，黑客窃取了蔚来汽车公司在 2021 年 8 月之前的部分用户基本信息和车辆销售信息,并向蔚来汽车公司以数据泄漏勒索 225 万美元等额比特币；

——2023 年 4 月，现代汽车披露发生数据泄漏事件，意大利和法国车主以及预订试驾数据遭泄露。

根据 Upstream 的数据，2020 年汽车信息安全事件数据增加了一倍。随着汽车网联率的提升，越来越多的联网车辆上路，每起事故的潜在损害呈指数级上升，使得公司和消费者处于危险之中。由此可见，智能网联汽车信息安全问题的形势变得越来越严峻，车联网产业链的参与方不得不正视智能网联汽车和车联网的信息安全问题。

1.6 研究目标

本研究报告通过分析车联网领域的产品、技术及标准化发展现状，分析车联网中安全威胁及密码应用需求，分析国外和国内的 V2X 标准现状与发展趋势，进一步分析国内现有的标准体系对于该技术领域的适应性,并从各层面提出车联网密码应用的标准体系规划与制标建议。

2 发展现状

2.1 车联网的发展阶段

车联网的发展可以分为三个阶段：第一阶段可称为车载信息服务阶段，主要是利用车联网实现简单的定位导航、车载娱乐、信息服务、紧急救援等车云通信功能，仅需要汽车能够和外部信息联通，实现方式为基于传统的蜂窝通信技术（2G/3G/4G）。第二阶段可称为交通智能辅助阶段，在第一阶段的基础上，支持利用车联网提供信息服务、交通效率、安全预警类功能，实现方式为 4G 和 LTE-V2X 技术。第三阶段可称为智慧交通融合阶段，在第二阶段的基础上，支持车联网与自动驾驶和智慧交通的融合发展，主要功能包括远程遥控驾驶、高密度车辆编队行使以及协同变道辅助等，实现方式为 5G+LTE/NR-V2X 技术。

目前中国车联网发展已经从单纯的车载信息服务提升到交通智能辅助阶段，并将迈入智慧交通融合的阶段。在车联网 LTE-V2X 技术和产业方面，已经形成涵盖通信芯片、通信模组、终端设备、整车制造、运营服务、测试认证、高精度定位及地图服务等较为完整的产业链生态。

2.2 技术发展现状

在 V2X 技术选择上，目前主要是 DSRC 与 C-V2X 两大流派[2]。DSRC 是基于 IEEE 802.11p 标准开发的专用短程通信技术，使得汽车间能相互通信，同时实现小范围内车辆和道路的智能连接；C-V2X 是基于 3GPP 蜂窝移动通信演进形成的车用无线通信技术，包含 LTE-V2X、5G-V2X 及后续演进。C-V2X 技术基于蜂窝网络，提供 Uu 接口（蜂窝通信接口）和 PC5 接口（直连通信接口），可复用蜂窝网的基础设施，提供低时延、高可靠、高速率、安全的通信能力，部署成本更低，网络覆盖更广。因此，我国倾向于推广使用 C-V2X 技术。

欧美等国家先后开展了车联网 DSRC 标准的研究制定工作，并且采纳了不同的车联网标准体系。美国的 DSRC 车联网标准制定由 IEEE 和 SAE 共同完成，涉及了对应 MAC 和物理层、网络层和传输层等对应的 IEEE 802.11p、IEEE 1609 和 SAE J2735 等标准体系。DSRC 通信协议参考结构如图 2-1 所示。

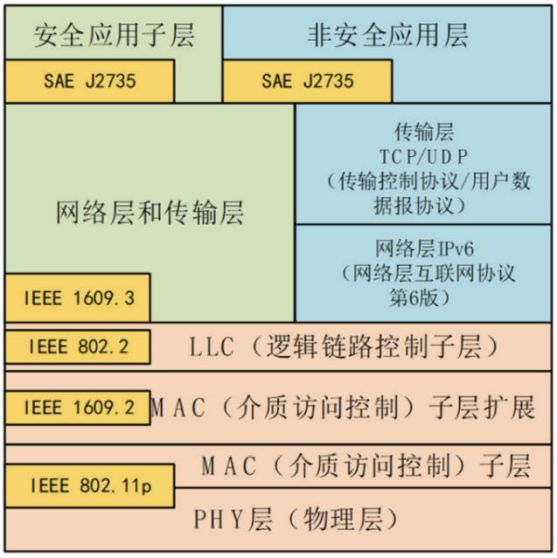

图 2-1　美国 DSRC 通信协议结构图

C-V2X 是由 3GPP 定义的基于蜂窝通信的 V2X 技术，它包含基于 LTE 网络的 LTE-V2X 以及未来 5G 网络的 NR-V2X 系统，是 DSRC 技术的有力补充。通过我国现有部署的 LTE 网络设施，使 V2V、V2N、V2I、V2P 等信息功能的通信得以实现，这项技术能适应于更复杂的安全应用场景，满足现阶段对车联网设备低延迟、高可靠性的要求。LTE-V2X 通信协议参考结构如图 2-2 所示。

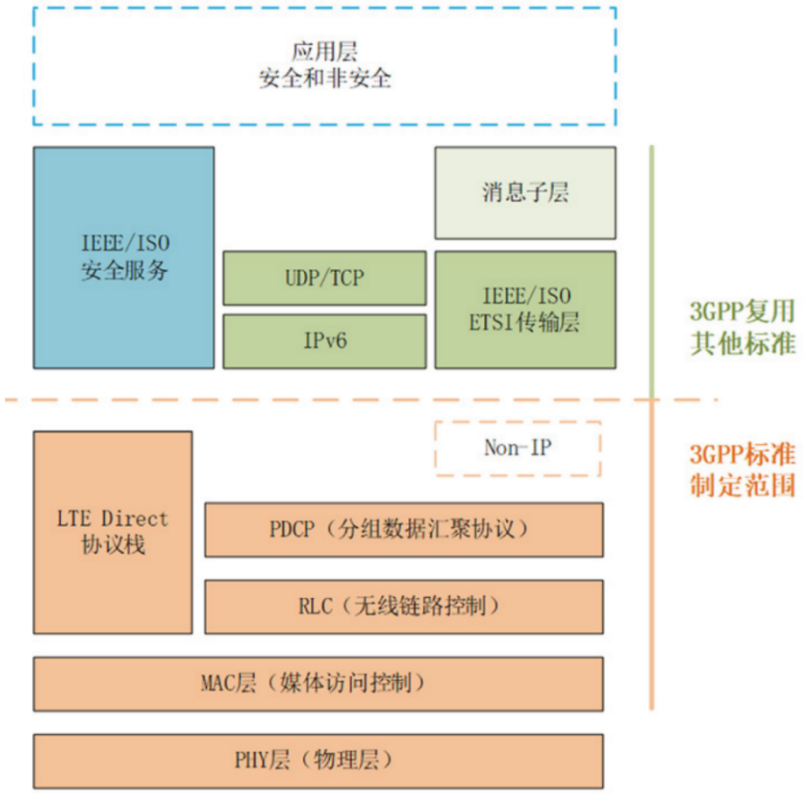

图 2-2　LTE-V2X 通信协议结构图

虽然国内外针对 DSRC 技术的研究起步较早，但是基于 802.11p 标准的 DSRC 技术仍有很多缺陷，如物理层效率低导致性能降低，在通信范围、鲁棒性和可靠性方面，DSRC 标准中没有明确的方法对物理层和 MAC 层进行改进；对比 DSRC，基于 4G 通信的 LTE-V2X 车联网技术在覆盖范围、可靠性、技术演进路线等方面远优于 DSRC 技术。

DSRC 和 LTE-V2X PC5 模式技术对比如表 2-1 所示。

表 2-1 DSRC 和 LTE-V PC5 技术对比

业务类别	DSRC	LTE-V PC5
传输速率	27Mbps	12Mbps
覆盖范围	300-500 米	500-600 米
时延	小于 50ms	小于 50ms
适应车速	200km/h	500km/h
网络部署	需大量部署 RSU	现有蜂窝网基站升级
技术成熟度	相对成熟，已开始商用	技术验证中
标准成熟度	标准已完善	标准制定仍初期阶段
主要支持企业	高通	华为，大唐等
主要应用国家	欧美国家	中国

2.3 产业发展现状

车联网产业生态体系分为“云”、“管”、“端”三大环节，如图 2-3 所示。云端的重点角色有数据和内容提供商、公共与行业服务提供商、通信服务提供商。“管”和“端”的重点角色有整车厂商、系统供应商、关键元器件供应商、软件提供商等。从产业结构看，车联网产业生态体系由芯片、传感器等零部件厂商、终端设备厂商、集成商、平台运营商、数据服务商、业务提供商等环节组成。

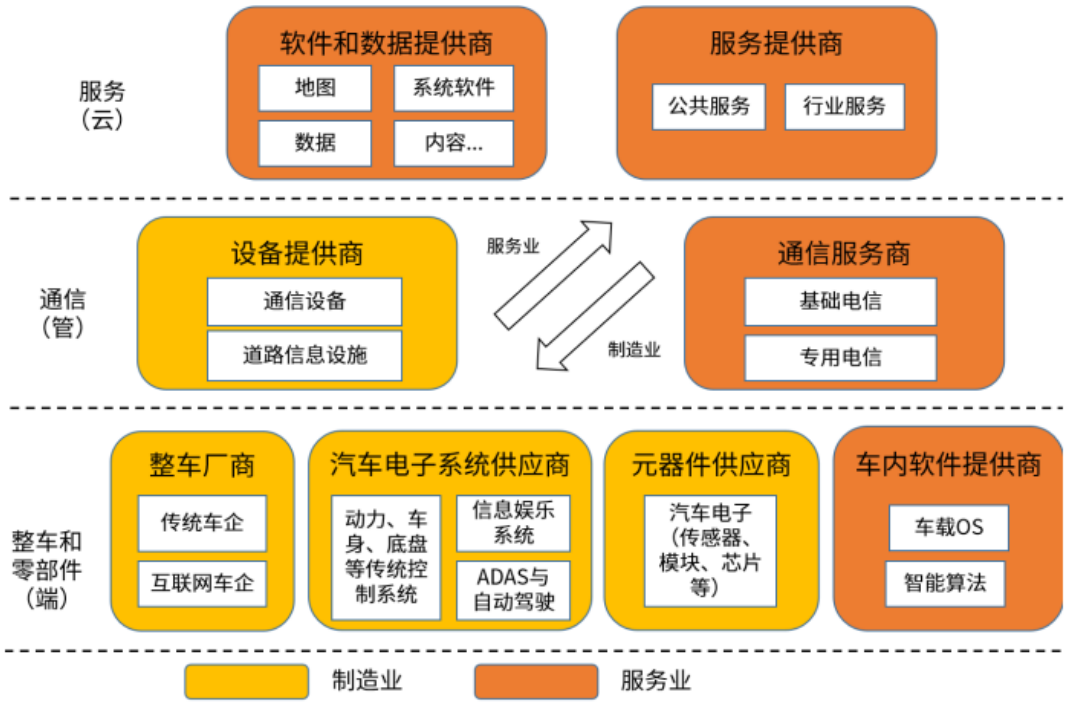

图 2-3　车联网产业结构（来源：中国信息通信研究院）

根据公开的报道，我国在车联网领域的相关产品在 2020 年已覆盖芯片、模组、车载终端、路侧终端、平台、应用等端到端的全产业链产品，支持 LTE-V2X 的通信芯片有 3 家厂商，车规级通信模组有 4 家厂商，C-V2X 车载终端有 10 余家厂商，路侧终端有 8 家厂商。在车联网 V2X 基础数据平台、车企业务平台、示范区测试数据平台、第三方应用平台等均有产品，并在各地车联网示范区开始部署验证。另外，各家车企也针对辅助驾驶业务开发相关应用，并在各地示范区进行联合测试。

测试验证方面，为推进蜂窝车联网（C-V2X）跨行业企业协同研发，解决产业发展过程中遇到的车与车、车与路互联互通的问题，IMT-2020（5G）推进组 C-V2X 工作组、中国智能网联汽车产业创新联盟等行业机构，联合汽车、信息通信、交通运输等跨产业链上下游企业以及各地方建设运营主体，自 2018 年起连续组织开展了车联网 C-V2X“三跨”“四跨”系列先导应用实践活动[3][4]。活动为 C-V2X 产业各环节提供了良好的技术验证和行业交流平台，助力 C-V2X 芯片模组、终端设备、整车应用、安全与云控平台实现跨企业、跨品牌互联互通，推动 C-V2X 产业链发展壮大。

为了推进车联网产业和应用落地，工信部、交通部、公安部设立 30 多个应用示范区，一方面在北京、上海、重庆等地建立了多场景、多环境测试场，验证 C-V2X 端到端的关键技术，推进了车联网产品商用研发进程。另一方面开展车联网业务的规模示范应用，探索车联网可行的商业模式。例如，由中国移动作为牵头单位，在工信部、公安部、江苏省无锡市政府的指导下，联合公安部交通管理科学研究所、无锡交警、信通院等近 30 家单位，在无锡持续开展了 C-V2X 应用示范：2017 年建成了全球首个 LTE-V2X 开放道路示范样板，2018 年打造全球首个 LTE-V2X 城市级规模应用；2019 年获批成为工信部推选的中国首个车联网先导区，后续将进一步推进完成无锡 C-V2X 服务覆盖，实现 V2X 的持续运营。目前，北京、上海、武汉等地也在逐步推进 C-V2X 城市级应用。

2.4 主要产品及供应商

- 底层芯片及模组

V2X 底层芯片及模组的主要厂商包括上海芯钛、苏州国芯、宏思电子、信大捷安等。目前能够支持汽车应用的支持 SM 系列密码算法的安全芯片仍然是目前 C-V2X 应用开发中的一个短板，缺乏车规级安全芯片、HSM 产品等。

- 终端设备

V2X 终端设备包括通信设备、车载终端（如 T-Box、车规级安全网关等）和路侧设备（RSU），主要厂商包括华为、中兴、大唐、东软、千方、星云互联、万集、华砥智行、协进电子等。目前 V2X 终端设备的技术和产品基本成熟，路侧设备部分行业标准在完善中。

- 应用和数据服务平台

应用和数据服务平台主要包括车联云服务和数据服务平台（如 Telematics 系统），主要厂商包括华为、阿里、国汽智联等。

- 安全服务与保障

安全服务厂家主要为汽车提供车内安全解决方案和 PKI 基础设施。其中车内安全的主要厂家包括娜迦、为辰信安等，PKI 基础设施的主要厂商包括吉大正元、格尔软件、北京数字认证、高鸿、国汽智联等。PKI 基础设施的厂家主要为车联网提供电子认证系统及证书运营服务。

2.5 标准化现状

车联网作为一个庞大的物联网应用系统,包含了大量的数据、处理过程和传输节点,其高效运行必须有一套统一的标准体系来规范,从而确保数据的真实性和完整性,完成各项业务的应用。根据车联网发展情况,建立一套高效的标准和安全体系,已成为车联网技术发展的迫切要求。

国际上 ISO、ITU-T、UN/WP29、3GPP、IEEE、SAE 等标准化组织都有涉及车联网不同层面的标准制定工作。这些标准涵盖了生命周期管理、安全威胁、安全目标、安全要求、安全功能组件、信息安全要求、网络通信安全等方面。这些不同的标准组织致力于不同的细分领域的车联网标准制定，其中某些国际标准之间可以很好地协作，基本上形成了比较完善的标准体系，很好地支撑了车联网产业的发展。

国内的全国汽车标准化技术委员会（TC114）、中国通信标准化协会（CCSA）、中国智能交通产业联盟（C-ITS）、中国汽车工程学会（C-SAE）等标准组织在近年来也围绕车联网领域开展了很多标准制定活动，推出了汽车电子、通信网络等层面的标准，尤其是 CCSA 制定了《基于 LTE 的车联网无线通信技术 总体技术要求》、《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》等规范，对于推进 LTE-V2X 技术的应用发挥了积极作用。为了推进车联网领域的标准化工作，工业和信息化部与国家标准委还联合发布了《国家车联网产业标准体系建设指南》，该系列指南给出了车联网领域标准体系的顶层设计。从已发布及在研标准的分析来看，目前国内相关组织的标准仅仅覆盖了《国家车联网产业标准体系建设指南》的很小一部分，换言之在车联网领域还存在大量的标准化需求。

本报告的第 5 部分从网联汽车智能终端、车联网通信网络、车联网服务平台等层面详细分析了车联网信息安全相关的国际标准、国内标准。

2.6 发展趋势

网联化与智能化融合成为车联网产业发展的主要趋势。我国《中国制造 2025》发展纲要中提出车联网技术应搭载先进的车载传感器和芯片，融合先进的信息通信技术，要具备复杂环境感知、智能化决策与自动化控制功能，实现交通零伤亡、零拥堵，达到安全、高效、节能的下一代汽车发展要求。

3　车联网的安全风险与安全目标

3.1 安全层次结构

车联网体系架构中的感知层、传送层、应用层等各层面均面临信息安全威胁，因此安全架构也与此相对应。车联网安全层次结构如图 3-1 所示[5]。

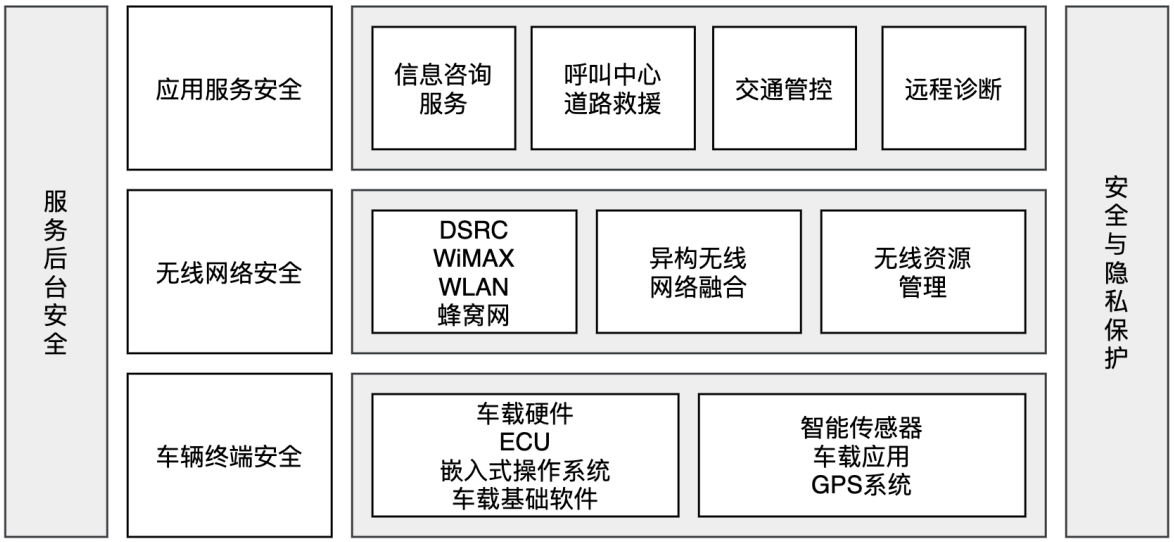

图 3-1　车联网安全层次结构

（1）智能网络汽车终端安全（整车级、关键系统及零部件）

车辆作为车联网终端，主要功能为感知,其内部安装了大量电子控制单元 ECU、智能传感器、执行器等电子系统,使车辆本身成为智能的传感器网络系统。终端安全涉及到硬件安全、嵌入式操作系统等基础软件安全、接口安全等方面。

（2）传输网络安全

车联网的基础网络是互联网和移动互联网、无线网等行业网络,作为承载网的互联网可继续沿用原有的安全策略,而作为接入网的无线网涉及到加密认证、异常流量控制、网络隔离和交换、信令和协议过滤等安全需求。

V2X 通信安全包括汽车之间通信、汽车与交通设施（如路侧单元）、汽车与云服务设施、交通设施与云服务设施等相互通信的安全。由于不同的 V2X 体系采用的通信协议可能不同（如 IEEE 802.11p、LTE 等），需要在通信协议标准中充分考虑安全需求及密码应用需求，并设计安全机制与算法应用。IEEE 1609.2 标准是典型的 V2X 通信安全协议栈。

（3）车联网服务平台安全

车联网应用场景及服务种类广泛,承载这些服务的后台需要利用大数据处理技术、智能计算技术、业务管理控制技术等处理海量信息,从而分发给不同的应用场景。应用服务平台涉及到信息的储存、计算、隐私以及业务控制安全。

（4）数据安全与隐私保护

在车联网体系结构的各个层面都涉及到数据隐私保护,主要存在身份隐私、位置隐私、查询隐私、轨迹隐私威胁。在车联网的服务后台,相关安全技术可继承传统网络与信息安全技术,但可管、可控和可信要求更高。

3.2 安全风险

《车路协同系统的安全研究》对研究车路协同系统安全关键技术开展了研究[6]，提出了车路协同系统（包括车辆与车辆、车辆和交通基础设施之间的通信网络）的应用场景及安全需求分析。

此处从实体网络安全、交互信息安全两个方面对车联网面临的网络安全风险以及密码应用需求进行具体分析。

3.2.1 实体网络安全风险

- 实体身份真实性风险

车联网系统中实体面临身份伪造风险。攻击者可能伪造特权车辆的身份，发送特权指令、控制信号灯等资源或者优先使用道路资源。攻击者可能发送虚假交通信息、伪造交通场景，影响其他车辆的正常判断，导致交通瘫痪或引发交通事故，并逃避责任追查。攻击者也可能伪造车联网服务平台、设备、路侧设施等实体的身份，威胁车联网服务使用者的安全。

- 实体数据完整性风险

车联网系统中的实体面临着数据篡改的风险。车联网实体涉及的数据种类多：智能网联汽车侧，包含行车数据、应用程序数据等；路侧设备侧，包含云端、路侧系统或车辆的数据；云平台侧，包含各类交互平台数据；移动终端测，包含车主信息等数据。攻击者可能会通过篡改破坏这些数据的完整性，达到数据假冒的目的，引发不同程度的事故。

- 实体数据机密性和隐私性风险

车联网系统中的实体面临着数据和隐私泄露的风险。智能网联汽车侧的行车数据、云平台侧和移动终端测的车主信息数据等，涉及车辆状况、行车轨迹、公民个人信息，若被攻击者非法获取，可能导致车主的合法权益受到侵害。特别在云平台端，海量车辆信息和行车信息的汇集使得数据泄露后果更为严重，攻击者通过大数据分析可能会精准定位具体车辆、精准把握地理状况、精准分析特定类型车辆踪迹等，给社会安全乃至国家安全带来潜在损害。

- 实体行为抵赖风险

车联网中的实体面临着抵赖否认风险。车联网实体可能出于自身利益对曾做出的行为进行抵赖否认。例如因车辆信息处理逻辑缺陷发生交通事故后，车联网实体否认曾执行造成事故的操作；又如车联网实体的运行日志是事件回溯分析的关键数据，车联网实体可能抵赖日志记录，归因于系统故障等因素。如果不能有效对抗这种抵赖，会对交通事故或异常的快速正确处理带来很大困难。

3.2.2 交互信息安全风险

- 交互信息真实性风险

攻击者通过伪造车联网实体之间的交互信息，攻击车联网系统。例如攻击者可能假冒特权车辆的身份，发送特权指令、控制信号灯等资源或者优先使用道路资源；也可能通过伪造数据发送虚假交通信息、伪造交通场景，影响其他车辆的正常判断，导致交通瘫痪或引发交通事故，并逃避责任追查。

- 交互信息完整性风险

车联网实体发出的信息在传输或处理过程中被攻击者非法篡改，造成事故风险。例如，车辆的位置信息或者速度信息在传输过程中被非法篡改，其他车辆、路侧设备及应用系统收到该信息后，基于错误的信息进行决策，可能威胁车辆行驶安全。又如，路侧设备在广播气象或者交通指令等信息时，信息被篡改，可能会造成车辆错误决策，导致交通拥堵或者交通事故等。

- 交互信息机密性风险

车联网实体发出的信息在传输过程中，如果缺乏保护，则可能被非授权的第三方获取。如果信息中包含涉及个人隐私、交通安全等的敏感数据，则恶意第三方获取信息后加以分析利用，会对个人、集体、行业甚至国家造成损害。

- 交互行为抵赖风险

当出现重大安全事故时，车联网实体可能会出于利益考虑，对信息发送、接受等行为予以抵赖。例如，因为 A 车辆所发出的消息导致交通事故，在进行事故溯源时，A 车辆否认在特定时间地点在车联网系统中发出了该信息，如果没有有效技术手段对抗这种抵赖，可能会导致事故责任难以认定。

- 重放攻击

车联网实体之间进行身份认证时，可能有攻击者通过截获并重发认证数据，欺骗认证方，达到假冒被认证实体身份的目的。例如，车联云对车辆进行身份认证时，攻击者可能截获合法车辆发送给云的认证信息，并重复发送给云，从而冒充合法车辆的身份欺骗车联云。

3.3 安全目标

为了应对安全威胁，密码技术的应用是必不可少的。尽管安全性不仅仅取决于加密算法，而且还需要包括安全协议和组织措施在内的强大的整体安全设计，但在大多数情况下，加密原语和方案是安全性解决方案的基本组成部分。需要适当组合密码原语和方案才能提供必要的安全服务，实现如下总体安全目标：

- 消息认证和完整性

消息认证和完整性是防止消息篡改和伪造的最重要手段。此外，接收者必须确认发送者的身份。

- 消息不可否认性

不可否认性用于防止实体抵赖发送消息或接收消息。提供不可否认服务的机制之一是使用非对称密钥对车联网系统的通信报文进行签名。因为私钥仅由其所有者控制，在使用私钥对消息签名后，签名者无法抵赖发送消息的行为。

- 隐私性

隐私保护防止在通信过程中从车辆中收集、提取或推断用户的个人信息。在车联网系统的设计之初就应考虑使用隐私增强技术和机制来保护个人隐私。

- 匿名性

车联网系统中匿名性的目标是允许经过身份验证的实体提交交易时无需使用其真实身份进行标识，并且系统应保证实体身份的不可链接性。以匿名性使得进行交易的实体的身份不会完全暴露，而它们的合法性和真实性应得到验证。

- 不可链接性

不可链接性要求攻击者无法在系统中的两个或多个关注项之间建立链接以标识真实身份。在为系统配备了不可链接属性后，用户可以执行不同的交易并使用多种服务而不会被识别。

- 不可观察性

不可观察性要求攻击者无法确定用户正在使用的服务和资源。在为系统配备了不可观察属性后，攻击者通过观察特定实体或媒介以识别其身份，或弄清正在使用的操作、交易或服务，是不可行的。

- 实体认证

实体认证涉及发送方的活动，可以为接收方提供有关发送方行为以及消息的证据。消息认证和完整性可确保已完整接收消息，而实体认证可证明消息是由预期的发送方生成的。

- 消息机密性

消息机密性要求消息内容对未授权实体保密，只有获得了访问密钥权限的授权实体才能解释消息。

- 访问控制

访问控制要求通过策略来确定哪些实体可以使用哪些服务，并且可以指定允许每个节点执行和不允许执行的操作。该服务一般隐含了身份鉴别和授权。

- 可审计性

可审计性要求系统具备由合法机构审核的能力。所有消息和协议的执行都被系统记录，以便在发生故障或非法操作的情况下可以进行调查。

4 车联网密码应用技术研究

4.1 密码应用需求

为了防范车联网面临的安全威胁与网络安全风险，需采用密码技术保障车联网实体、车联网交互信息的真实性、完整性、机密性和抗抵赖性。

对于车联网实体安全，需采用密码技术保障车联网实体身份真实性、数据存储的完整性和机密性、实体隐私性，并满足安全事件回溯所需的可审计性。

车联网实体密码应用需求如表 4-1 所示。

表 4-1 车联网实体密码应用需求

相关实体	密码应用需求				
	实体身份真实性	数据存储完整性	数据存储机密性	隐私保护	安全审计
智能网联汽车	1.车作为实体在进行交通事故溯源时有身份真实性鉴证的需求 2.车与路侧设备交互与控制过程中有身份真实性鉴证的需求 3.车与云端交互过程中有身份真实性鉴证的需求	1.车载终端中所有的应用程序数据有存储完整性保护需求 2.事件数据记录系统中的汽车行驶状态数据有存储完整性保护需求 3.车载终端接收到的来自V2X实体的消息有存储完整性保护需求 4.日志信息有存储完整性保护需求	1.接收到的高精度经纬度坐标位置信息有存储机密性需求 2.存储在车载终端中的敏感信息（如车主的银行卡号、身份信息等）有存储机密性需求 3.用于实体鉴证的数据有存储机密性需求	1.车辆的位置和行驶轨迹有隐私保护需求 2.车辆的身份信息有隐私保护需求	1.对车辆的操作应该有安全审计日志记录 2.对车辆的行驶状态有安全审计日志需求
路侧设备	1.路侧设备与车交互过程中有身份真实性鉴证需求。 2.路侧设备和云端交互过程中有身份真实性需求	1.来自车辆和云端的控制指令消息有存储完整性保护需求 2.系统日志信息有存储完整性保护需求 3.路侧发给车辆的信息（如超速警告等）有存储完整性保护需求	1.用于实体鉴证的密钥数据有存储机密性需求	无	1.对路侧设备有系统安全审计日志需求
云平台	1.云与车、路侧设施、车主交互过程	1.存储在云平台上的数据有完整	1.云平台上的敏感数据（如车辆	无	1.有系统、操作安全

相关实体	密码应用需求				
	实体身份真实性	数据存储完整性	数据存储机密性	隐私保护	安全审计
	中有身份真实性需求	性需求	向平台上传的数据）存储机密性需求		审计需求
终端设备（例如移动智能终端、充电桩等）	1.人对车操作时有身份真实性鉴证需求 2.人对车联云个人空间操作时有身份真实性鉴证需求	1.手持移动智能终端对应用程序数据有存储完整性保护需求 2.接收到的来自云平台的消息有存储完整性保护需求	1.个人敏感信息，如身份证号、银行卡号、位置信息等有存储机密性需求	1.手持移动智能终端内存储的个人敏感信息，（如身份证号、银行卡号、位置信息等）有隐私保护需求	1.手持智能终端APP有安全审计日志需求

对于车联网交互信息，需保障其真实性、完整性、机密性和抗抵赖性，并能够有效防范重放攻击。

车联网信息交互密码应用需求如表 4-2 所示。

表 4-2　车联网信息交互密码应用需求

信息交互	密码应用需求				
	传输数据真实性	传输数据完整性	传输数据机密性	行为抗抵赖	抗重放
车与车	1.车与车之间传输的BSM消息有数据真实性需求	1.车与车之间传输的BSM消息有数据完整性需求	1.BSM消息中的高精度经纬度位置信息有数据机密性需求	1.车与车之间传输的BSM消息有行为抗抵赖需求	车与车之间传输的控制信息有抗重放需求
车与路侧设备	1.车与路侧设备之间传输的控制信息和广播消息有数据真实性需求	1.车与路侧设备之间传输的控制信息和广播消息有数据真实性需求	1.特权车辆，例如警车，在对路侧设备发送控制指令时有数据机密性需求	1.路侧设备所发出的消息有行为抗抵赖需求	车与路侧设备之间传输的控制信息有抗重放需求
车与云平台	1.车与云平台传输的数据有真实性需求	1.车与云平台传输的数据有完整性需求	1.车与云平台传输的数据有机密性需求	1.车与云平台传输的数据有抗抵赖需求	车与路侧设备之间传输的控制信息有抗重放需求
车与手持设备（例如手机）	1.车与手持移动智能终端通过云平台转发的消息有数据真实性需	1.车与手持移动智能终端通过云平台转发的消息有数据	1.手持移动智能终端对车辆发出的控制指令有机密性需求	1.手持移动智能终端对车辆发出的控制指令有	1.手持移动智能终端对车辆发出的控

信息交互	密码应用需求				
	传输数据真实性	传输数据完整性	传输数据机密性	行为抗抵赖	抗重放
	求 2.车与手持移动智能终端通过蓝牙钥匙直接交互有数据真实性需求	真实性需求 2.车与手持移动智能终端通过蓝牙钥匙直接交互有数据真实性需求		行为抗抵赖需求	制指令有抗重放需求
车内网元节点	1.网元节点间传输的数据有数据真实性需求	1.网元节点间传输的数据有数据完整性需求	无	无	1.网元节点间传输的数据有数据抗重放需求
车与充电桩和充电 APP	1、车连接充电桩充电时，充电桩与车之间、充电桩与后端平台之间、充电APP与后端平台间有数据真实性验证需求	1.充电桩中存储的运行数据、用户档案数据、清分结算数据、控制指令、订单数据、支付数据等重要数据，有采用 SM 系列密码算法保证传输完整性需求	1.充电桩中存储的运行数据、用户档案数据、清分结算数据、控制指令、订单数据、支付数据等重要数据，有采用 SM 系列密码算法保证传输机密性需求	1.充电APP中用户敏感信息（如身份证号、手机号、银行卡号、位置信息等）有隐私保护需求	1.充电桩运维操作有安全审计需求

4.2 密码应用的总体思路

4.2.1 密码应用技术架构

密码技术不仅可以实现对信息的加密保护、完整性保护,还可以实现对实体身份和信息来源的安全认证,是保障车联网安全的核心技术和基础支撑。

车联网通信中的密码应用体系涉及云服务平台密码应用、智能网联汽车密码应用、终端设备密码应用、路侧基础设施密码应用和车联网应用系统密码应用，实现各实体之间交互身份认证、数据机密性保护、数据完整性保护、隐私保护等密码应用需求。

车联网密码应用体系的总体架构如图 4-1 所示：

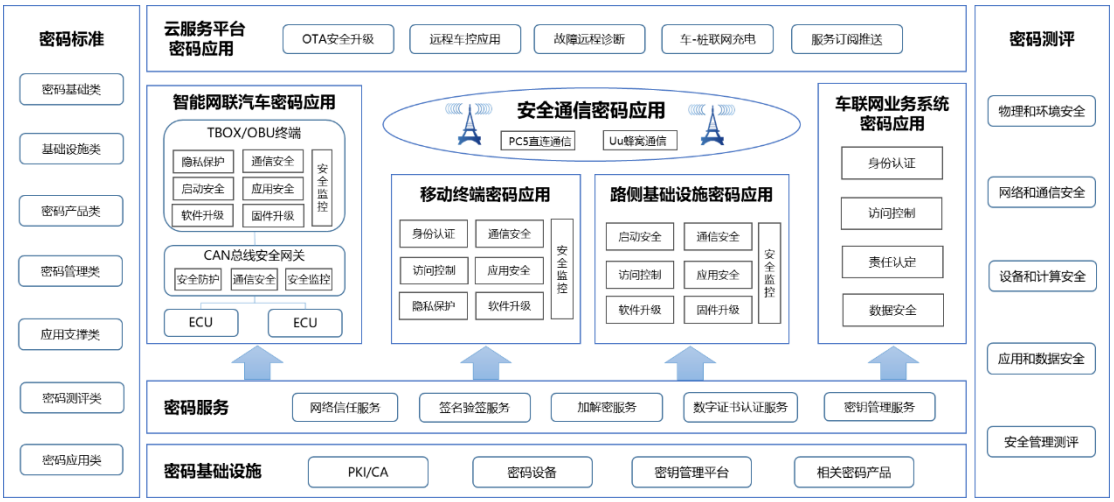

图 4-1　车联网密码应用体系总体架构

下面对总体架构中各层面给出说明：

- 密码基础设施

密钥基础设施包含了数字证书认证系统、密钥管理平台、密码机以及相关的密码产品等。

数字证书认证系统为车联网提供公钥基础设施（PKI）解决方案，实现数字证书全生命周期管理，主要提供终端用户注册、审核，证书签发及发布等基本功能，使智能网联汽车系统各前端车辆、路侧单元、终端设备、云端服务设备能够方便地利用数字证书认证系统实现安全应用，并按需进行加密密钥的产生、分发。

密钥管理平台在终端侧密钥管理功能的协助下，完成对智能网联汽车系统中云服务平台、车载终端、路侧终端和移动终端提供统一的密钥相关服务、权限管理和访问控制等，实现密钥的全生命周期管理，包括密钥的生成、使用、更新、存储、归档、备份、销毁及恢复等环节，保障车联网用户密钥安全。

- 密码测评

密码技术是保障车联网安全的核心技术和基础支撑，密码测评对规范密码应用具有重要意义，能够有效维护车联网网络安全与车联网业务系统安全，增强车联网领域网络与业务系统的安全风险防控能力，充分发挥密码在车联网信息安全方面的重要作用。

- 密码服务

面向云服务平台、车辆端、路侧单元、移动终端及其各网络边界提供统一用户管理、统一身份认证、访问控制、授权管理、安全审计、密钥扩展、签名验签、加解密、密钥全生命周期管理等服务。

- 车联网业务系统密码应用

车联网业务系统指汽车远程服务提供商（TSP，Telematics Service Provider）基于位置服务、GIS 服务和通信服务等现代计算机技术，为车主和个人提供强大的服务，如导航、娱乐、资讯、安防、SNS、远程保养等。车联网业务系统应用对象包括整车制造商、路侧基础设施制造商、移动终端制造商、VSP 服务商等。其相应的车联网业务系统应使用密码技术来提升系统安全防护水平，能够为系统提供身份认证、访问控制、责任认定、数据安全等安全保障服务，实现用户登录系统的身份认证，对核心资源获取的访问控制，对关键业务操作的不可抵赖以及对核心数据、敏感数据的安全保护。车联网业务系统的密码应用需要通过商用密码应用与安全性评估，以确保供应链提供商在密码应用层面的合规性。

- 智能网联汽车密码应用

智能网联汽车 T-Box/OBU 设备应支持数据签名与验签、数据加密与解密、散列与验证等运算服务能力，一是满足智能网联汽车车载终端的数据存储安全要求，二是满足车辆内部通信以及与路侧单元、移动终端和云服务平台之间外部通信数据的加密与解密、数据签名与验签等运算处理需求。

- 路侧基础设施密码应用

路侧设备应支持数据签名与验签、数据加密与解密、散列与验证等运算服务能力，一是满足路侧设备的数据存储安全要求，二是满足路侧设备与智能网联汽车和云服务平台之间外部通信数据的加密与解密、数据签名与验签等运算处理需求。

- 移动终端密码应用

移动终端应支持数据签名与验签、数据加密与解密、散列与验证等运算服务能力，一是满足移动终端的数据存储安全要求，二是满足移动终端与智能网联汽车和云服务平台之间外部通信数据的加密与解密、数据签名与验签等运算处理需求。

- 安全通信密码应用

车联网应用场景下的网络通信分为 Uu 蜂窝通信和 PC5 直连通信。在蜂窝通信过程中,终端与服务网络应对网络通道进行加密,支持完整性以及抗重放保护,对用户数据进行加密保护,确保传输过程中信息不被窃听、伪造、篡改。在直连通信过程中,系统需对消息来源进行认证,保证消息的合法性;支持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；实现对消息的保密性保护,确保消息在传输时不被窃听,防止用户敏感信息泄露。

- 云服务平台密码应用

云服务平台的密码应用需要依赖密码基础设施提供支撑，为车联网智能终端提供密码服务，通过认证服务系统确认用户（车辆、路侧单元、移动终端）身份，来判断该用户是否拥有对某种资源的访问权限及使用权限，防止攻击者通过假冒攻击获取资源的使用权限，以此保护授权用户的合法利益、计算机系统的安全和数据的安全，确保业务接入者及服务者身份的真实性、业务内容访问的合法性，从而使计算机系统或平台的访问策略得到有效和可靠地执行。

云服务平台同时还为车联网智能终端提供 OTA 安全升级服务以及 TSP 车联云服务（导航、娱乐、咨询、远程保养等），在车辆/路侧单位/APP 与云服务平台之间的通信过程中，应基于密码技术保证通信双方的身份真实性以及保证通信数据的安全传输。相关业务场景包括：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。

4.2.2 智能网联汽车密码应用

车载终端设备中密码应用，主要围绕车内网络及关键子系统、零部件的信息资产及其安全防护来设计[7]。ENISA 发布的《Cyber Security and Resilience of Smart Cars》分析了确保智能汽车安全免受网络威胁的良好实践，特别是智能汽车的安全也应保证安全[8]。

智能网联汽车的安全框架如图 4-2 所示。车载系统可以划分为中控系统、网关系统、电控系统等主要子系统。

图 4-2　智能网联汽车安全框架示意图

车载系统涉及大量的嵌入式设备，并且基于以太网、CAN 等总线实现车内网元节点之间的通信。要在车载系统应用密码技术，并不适合在车内集成通用的密码支撑平台或产品，而是需要在这些关键系统、零部件中集成硬件安全模块，或者集成软件密码模块作为密码支撑组件。在集成 HSM 之后，通过应用相关的密码算法、密码协议，来解决前面提出的实体网络安全风险、信息交互安全风险。

汽车网关在车辆网络内提供域隔离。汽车网关是一种路由设备，可以确定哪些消息当前是合法消息，并将通过网关传递到目的地。一旦攻击者获得对不安全网络的访问权限，就可以对目标组件发送消息实施攻击行为。在车内网络可通过各种网络级别的保护措施来保护子域，包括设备认证、消息认证、消息加密、入侵检测、速率限制和流量整形等等。汽车网关的密码应用主要需解决车内总线协议（如 CAN、FlexRay 和 LIN 等）的报文传输的安全性问题，防止攻击者通过控制连接到总线上的 ECU 节点读取和修改报文。应用密码技术可以实现汽车网关与 ECU 的身份认证，并采用数据加密技术来保护传输的报文数据。

T-BOX 可以集成在汽车网关内部，是车内外信息交互的纽带，实现车载设备与车联网服务平台的连接，也是重要的攻击对象。如果攻击者获得了 T-BOX 的访问权限，则可以潜在地发送欺骗性的 CAN 消息并获得对安全性至关重要的组件的控制权。因此，必须通过密码技术来验证交换的消息以保护其真实性和完整性，并保护关键组件免遭未经授权的访问。

智能网联汽车通常包含了超过一百个控制单元（ECU），这些 ECU 共同实现了汽车中的控制功能，其中包括许多高级（自动）驾驶功能。这些 ECU 不断生成、处理、交换和存储大量有价值的（敏感）数据。为了保护这些功能和数据，微控制器需要具有安全启动和实时完整性验证的功能。

此外，密码技术还可以解决车载设备的安全启动和固件完整性验证，以及车载终端的敏感数据的存储加密等安全需求。由于不同类型的车载设备对于密码算法和性能指标的需求有所不同，有必要对车载设备内置的硬件安全模块（HSM）的技术规格进行规范，满足不同应用场合的安全需求。

4.2.3　安全通信密码应用

车联网中的四类实体之间通过 Uu 蜂窝网通信接口、PC5 直连通信接口等进行通信。蜂窝网通信场景下，智能网联汽车、路侧通信设备和终端设备通过 Uu 接口与车联网服务平台或其他终端交互信息，实现长距离和大范围的可靠通信，满足车载导航、车辆监控、紧急救援、信息娱乐等业务需要。直连通信场景下，智能网联汽车和路侧设备通过 PC5 接口进行短距离信息交互，满足交通效率提升、辅助驾驶安全预警、自动驾驶等业务的需要。

车联网应用中在各个层面都应用了通信技术，典型的应用场景包括在车与车（V2V）、车与路边设施（V2I）、车与行人（V2P）以及车与网络（V2N）之间进行无线通信和数据交换，此外在汽车内部的局域网也存在有线通信和数据交换。

车内通信主要用于汽车网关、T-Box 及各类 ECU 之间的数据交换，应用密码技术可以实现对 ECU 的身份验证、消息加密，并借助汽车网关实现对 ECU 之间通信的授权管理。

车载网络和个人智能设备之间的交互主要使用蓝牙技术进行通信，在蓝牙通信中也可以采用密码技术实现数据加密，并对蓝牙链接密钥进行分发管理。

车与车（V2V）、车与路边设施（V2I）之间需要通过蜂窝移动通信网络或 WLAN 网络实现数据交换。不同的应用场景中需要应用不同的通信技术，这些技术体系由 3GPP、ETSI、IEEE 等标准化组织分别提出，并且拥有不同的产业生态。尽管这些技术体系中应用密码技术的技术路线并不一致，主要思路都是在通信协议栈中引入安全服务组件，为上层应用提供通信服务原语，实现端到端的数据加密、数据完整性保护，并提供网元的身份认证服务，因此可以根据车联网的安全威胁和安全需求来梳理安全服务组件及其密码应用需求。

车与云平台、车载设备与车载信息服务系统之间的业务应用需要依赖底层的网络通信连接，并且需要采用适应受限设备和低带宽、高延迟或不可靠的网络通信协议（如 MQTT）。由于应用层面需要传输远程指令等敏感数据，远程通信的安全至关重要，可以采用 MQTT 与 SSL/TLS 协议相互结合的方式来保证传输的机密性、完整性和不可否认性。

此外，由于车联网应用对于个人信息保护提出了强烈的需求，无论是 DSRC 还是 LTE-V2X 技术体系，都引入了 PKI 基础设施，同时创新性地采用了假名证书来解决车联网中的用户隐私保护需求。

4.2.4 车联网服务平台密码应用

车联网服务平台是提供车辆管理与信息内容服务的平台，负责车辆及相关设备信息的汇聚、计算、监控和管理，提供智能交通管控、远程诊断、电子呼叫中心、道路救援等车辆管理服务，以及天气预报、信息资讯等内容服务。

车联网服务平台面临的安全问题主要是系统内产生的数据安全问题，从交互应用场景来看，主要的安全问题分为：采集安全、传输安全、分发安全、云平台及存储安全等。要解决车联网服务平台面临的安全威胁，可以参考 GB/T 39786 标准的安全框架，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等层面分析车联网服务平台面临的安全威胁，采用符合密码规范标准的安全联网终端、密码基础设施、密码应用产品等，同时可以引入适用于云计算环境的先进密码技术（如基于云密码资源池的统一密码服务系统），实现密码合规性与智能网联汽车适应性的统一，保证平台安全、业务安全、数据安全。

车联网服务平台中的车辆智能管理系统为车载终端设备提供远程固件更新（FOTA）的服务。智能终端软件存在潜在的风险和漏洞，必须通过远程升级来进行维护，提高抗风险能力，不然会提高返厂运维成本，特斯拉、Jeep 等车企就此类信息安全问题而不得不召回有关车辆。当终端在进行远程升级时，易发生软件包被劫持等情况，所以必须

确保程序的完整性和准确性，通过加数字签名确定其合法性。在升级过程中，可通过数字签名技术保障云端 OTA 差分升级包下发到车端的真实性、完整性、不可篡改性。

4.2.5 车联网业务系统密码应用

基于车联网可以承载各种类型的业务，如“车-桩”联网充电、车辆保险等等，在开展这些业务的过程中，一般涉及到移动终端和云平台的安全防护，在各类业务系统中应用密码技术可以实现对 APP 的安全分发，可以实现对各类用户角色的安全认证与权限管理，还可以实现对个人隐私信息的保护等等。

4.2.6 车联网数据安全密码应用

联网大数据分析是一个从信息到数据再到信息的过程，包括搜集、分析、传播和利用等环节，其中每一个环节的疏漏都可能造成个人隐私的泄露。应用密码技术可以在数据全生命周期管理的各环节中实现对数据的机密性、完整性、认证性、权限管控和可追溯性。

自动驾驶等业务对高精度地图和导航定位提出了较高的要求，同时也需要应用密码技术来保护车辆的运动轨迹和高精度地图数据。应用密码技术，可以保护客户端和服务端存储的地理信息的机密性，同时还可以实现客户端与服务端的安全通道，保证在传输通道中的地理信息数据的机密性、完整性和认证性。

针对车联网服务平台的用户身份信息、汽车运行状态、用户驾驶习惯、地理位置信息、用户关注内容等敏感信息，可以采用数据库加密、分布式存储加密等技术实现存储数据的加密，并采用密码技术建立完善的权限分级机制，保证数据操作的可追溯性。

密码技术在车联网服务平台的安全审计中可解决审计记录的完整性、不可否认性，还可以用于加密敏感或隐私内容，并建立权限管理机制。

4.3 智能网联汽车密码应用案例分析

4.3.1 车载设备安全应用

4.3.1.1 汽车网关安全

车载安全网络架构使用安全网关和通信总线（例如 CAN，以太网，FlexRay）提供物理隔离和隔离与安全相关的 ECU[10]。

智能网联汽车的车内传感器网络的传感器、控制器、执行器等众多节点根据通信协议,协同工作。但通信过程中可能存在攻击者恶意采集传感器信息,收集行车相关数据,或者根据车内传感器的特点,通过干扰传感器设备的通信,危及行车安全。

当前的车内总线协议，如 CAN、FlexRay 和 LIN 等均采用发送明文报文，除了简单的校验之外，未提供任何加密或是认证等安全机制，使得攻击者可通过控制连接到总线上的 ECU 节点读取和修改报文。

CAN 总线的报文认证机制主要是验证报文的完整性以及数据源认证。报文认证机制可以抵抗攻击者的重放，伪造报文。为实现 CAN 总线认证机制，需考虑两个方面的问题:一是 CAN 总线的数据帧的数据域最多只有 8 字节，难以增加额外的认证数据，且数据帧格式多由厂商确定，若修改数据帧格式，需硬件方面的支持；二是 CAN 总线数据帧不包含发送方和目的方地址，若要实现报文的源认证，需对 ECU 节点进行标识。

基于密码学的方式生成 MAC 认证报文，如在 CAN 总线上传输与该报文相应的等长的认证信息，即需要传输两条报文：原本的报文以及该报文的认证信息。但这种方式需要

两倍的传输成本以及两倍的报文标识符使用空间。再比如将认证信息嵌入其数据域中，即使用数据域的一部分用来表示认证信息。这种方式压缩了数据域所承载的信息容量，但无须额外分配报文标识符。

另一种技术路线是由中央监视节点对网络中的其他节点进行身份验证。一旦发现未授权的报文传输，中央监视节点实时传输更高优先级的错误帧来阻止非法报文的传输。但这种方法需要修改 CAN 控制器。

CAN 报文加密机制是指对 ECU 节点分配密钥，并使用相应的密钥加密报文的数据域。只有拥有密钥的 ECU 节点可以解密报文，以保证报文的机密性。报文加密传输可以在攻击者多重步骤的初期就阻拦该攻击。另一方面，由于车内 ECU 节点的计算存储能力有限，且车内 CAN 总线对实时性的需求高，计算开销大的加密算法并不适用于车内 CAN 总线网络。因此，轻量级的加密算法更受到学术界和工业界的认可。

4.3.1.2 T-BOX 设备安全

T-BOX 是车载智能终端（Telematics BOX）的简称，主要用于车与车联网服务平台之间通信，集成了 OBD、RFID，摄像头，MCU/CPU、FLASH、SENSOR、GPS、3G/4G、WiFi/蓝牙等模块。对内与车载 CAN 总线相连，实现指令和信息的传递；对外通过云平台与手机/PC 端实现互联，把电机数据、电池容量、操作状态等，发送到云平台，也能把云平台的控制指令转发给车辆。

T-BOX 作为系统中网络云端和车辆信息交互节点，既扮演着车载 ECU 的角色，也承担着无线通信模块的的重任，是车内外信息交互的纽带。T-Box 可以通过采集 CAN 总线的数据来分析汽车的行为，而这些数据的加密存储与保护，与 Telematics 汽车信息服务平台之间的数据交换等，都需要应用密码技术来解决。

当用户通过手机端 APP 发送控制命令后，TSP 后台会发出监控请求指令到车载 T-box，车辆在获取到控制命令后，通过 CAN 总线发送控制报文并实现对车辆的控制，最后反馈操作结果到用户的手机 APP 上，仅这个功能可以帮助用户远程启动车辆、打开空调、调整座椅至合适位置等。

车载 T-BOX 也可深度读取汽车 Can 总线数据和私有协议，T-BOX 终端具有双核处理的 OBD 模块，双核处理的 CPU 构架，分别采集汽车总线 Dcan、Kcan、PTcan 相关的总线数据和私有协议反向控制，通过 GPRS 网络将数据传出到云服务器，提供车况报告、行车报告、油耗统计、故障提醒、违章查询、位置轨迹、驾驶行为、安全防盗、预约服务、远程找车、利用手机控制汽车门、窗、灯、锁、喇叭、双闪、反光镜折叠、天窗、监听中控警告和安全气囊状态等。

车载 T-BOX 的信息安全威胁与密码应用主要包括[9]：

（1）数据安全性

TBOX 直接与车上的 CAN 线相连，可以深度读取电机与车身的 CAN 信息，同时也能发送 CAN 信息给 VCU，VCU 再发给相应的 ECU 实现对车辆的操作控制。这其中涉及双向传输过程中数据的安全性，一旦数据被恶意劫持，攻击者篡改甚至伪造指 令信息来通过 TBOX 发送，将会产生不可估量的后果，所以信息安全技术至关重要，必须通过相应的策略来规避风险。

为防止传输过程的风险，必须对终端用户的身份进行认证，可以通过数字签名等方法，认证通过方可进行下一步传输，同时需要对传输的数据进行一定程度的加密，同时采用加密芯片，以确保安全性。

（2）固件安全性

作为 T-BOX 的关键组成部分，微处理器和微控制器 MPU、MCU 的之间的通信至关重要，存储在里面的固件程序带来极大便利性的同时，隐患随之而来。如果采用逆向提取反编译技术，改变参数，将会对车辆造成严重影响。所以为了应对这一问题，必须在设计过程中将固件存储在 MCU 或 MPU 的自带存储单元中，避免采用通用指令集，在程序逻辑正常的前提下，设下一些陷阱，提高逆提取反汇编的难度，提高固件安全性。

4.3.1.3 ECU 组件安全

ECU 本质上是单片机,其计算资源和存储能力都较弱，安全性一般较差，攻击者可以通过软件攻击、电子探测攻击、探针技术、远程升级等手段，获取 ECU 的关键信息，甚至破解和控制 ECU。因此 ECU 面临其本身的漏洞安全问题,如固件漏洞、软件漏洞、通信协议漏洞等；同时,ECU 大都支持远程升级和固件重新刷写，以实现功能更新或者漏洞修补，因此，ECU 还面临远程升级带来的安全问题，如升级包篡改。

对于 ECU 固件安全升级，应使用经过汽车生产厂商认证的升级程序，禁止 EC 下载安装第三方固件升级程序。同时 ECU 在固件升级时，要支持固件认证和完整性校验，并且 ECU 要支持回滚机制，确保升级失败后固件仍可回退到之前的版本，确保升级的可靠性。

ECU 部件在通信能力、数据处理能力等方面都受到成本的制约，同时可以使用的存储空间往往较小。考虑到各种设备的功能需求，能耗必须限制在某个范围之内。现有的 SM 系列算法在此类汽车电子产品中应用，并不能获得较好的性价比，甚至无法满足这些产品的安全需求。譬如，SM4 分组加密算法的密钥长度、加密轮数等都并不是针对资源受限的产品而优化,因此在这些场景下应用 SM4 算法,往往无法满足功耗的约束条件，还可能无法满足实时性指标的要求。

4.3.1.4 数字车钥匙安全

移动智能终端设备作为车钥匙的功能是近几年出现的热门技术之一,该功能也叫做数字车钥匙。数字车钥匙是智能网联车的重要革新功能之一，已经有部分车辆制造企业与移动智能终端设备厂商着手开发并提出数字车钥匙解决方案。譬如采用苹果公司的 iOS 设备中安装的 App 来管理密钥，可用于解锁和锁定车辆，启动发动机或将车辆设置为驾驶模式。

与传统车钥匙不同，数字车钥匙无需额外的实体车钥匙，而是将车钥匙功能集成在移动智能终端设备中，基于 SE、TEE 等安全技术，使用 NFC、蓝牙、蜂窝网络、WIFI 等技术实现车辆的开门、启动等功能。除了基于智能设备的汽车钥匙，用户还会使用遥控钥匙（Key fob），这些嵌入式设备采用射频信号或蓝牙协议与汽车进行短距离通信，通过交换 APDU 报文来实现对车门的控制。

文献[12]分析了特斯拉公司的 Model X 车型的一种攻击手段，该文献对被动无钥匙进入和启动系统进行了彻底的安全性分析，该系统依赖于在 Common Criteria 认证的安全元件（SE）中实现的公钥密码（RSA）和对称密码（AES-CTR）原语。文献提供了所有相关组件的详细描述，并证明了这些新一代遥控钥匙增加的复杂性会引入新的攻击向量。通过利用这些攻击向量，文献证明了使用标准的安全元件（SE）不足以获得安全的产品。所演示的攻击主要利用了这些密码产品的使用方式，而不是基于密码算法和产品本身的任何弱点。

数字车钥匙的系统参考架构如图 4-3 所示[13]。移动终端设备作为数字车钥匙是在用户访问车辆时用于身份认证的数字凭证，可实现解锁、上锁车门，启动、关闭发动机引擎等功能。车辆数字车钥匙认证系统中包含了鉴权控制模块，用于识别数字车钥匙身

份的真实性。车辆服务器是由车辆企业管理，用于记录数字车钥匙状态与储存相关隐私信息。安全单元（SE）是位于终端设备中的一种防篡改硬件安全部件，用于保证设备的安全性与机密性，安全单元具有多种形态，包括 eSE、inSE、SIM/UICC、智能卡、智能 microSD 卡等。

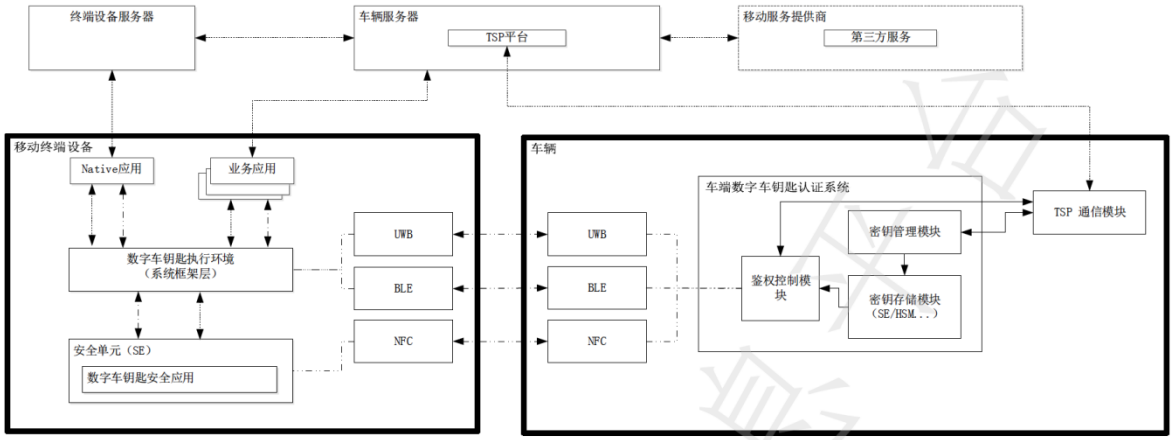

图 4-3　数字车钥匙参考架构

数字车钥匙系统面临的安全威胁主要包括方面：

a)非法用户使用数字车钥匙，导致非法使用车辆。

b)阻碍删除终端设备中数字车钥匙数据的过程，导致非法使用数字车钥匙功能。

c)终端设备中并存多个车辆企业的数字车钥匙时，不安全的隔离机制可能产生安全风险。

为了应对上述安全威胁，可以在数字车钥匙系统中应用密码技术，实现身份鉴别与访问控制等关键功能。数字车钥匙应使用安全公钥密码算法与签名算法，强度不应低于 SM2-256、ECC-256、RSA-2048、ECDSA-256。数字车钥匙应使用安全分组密码算法，强度不应低于 SM4-128、AES-128，加密模式宜采用 GCM、CTR、CBC 模式。数字车钥匙应使用安全哈希函数，强度不应低于 SM3-256、SHA-256。为了实现数字车钥匙与汽车的安全通信，数字车钥匙与车辆建立通信信道时，应使用 TLS 1.2 及以上版本或同等强度 TLS 协议，应具备双向认证机制保证通信双方身份的真实性，并且使用安全密钥协商算法。

除此之外，移动智能终端应具备安全环境以实现安全启动、安全存储、隔离机制等功能。数字车钥匙执行环境安全目标包括保证用户使用钥匙功能时具备用户身份认证机制、已删除钥匙防恢复机制、钥匙迁移时不泄露隐私信息、终端设备中存在多个钥匙数据的安全隔离机制。

文献[11]给出了 iOS 设备用作汽车钥匙的安全指南，其安全策略包括：所有密钥都是在基于椭圆曲线（NIST P-256）的嵌入式安全元件（ECC-OBKG）上创建的，私钥永远不会离开安全元件。设备和车辆之间的通信使用 NFC 标准，iOS 设备通过基于双向认证的 TLS 协议来访问汽车制造商服务器的 API 以完成密钥管理过程。钥匙与 iOS 设备配对后，任何与 iOS 配对的 Apple Watch 都可以收到。在车辆或设备上删除钥匙时，确保密钥无法被恢复。丢失或被盗设备上的密钥可以暂停和恢复，但在新设备上重新设置密钥需要建立新的配对或共享。

数字车钥匙系统可能应用如下相关的密码标准：

- SM2 椭圆曲线公钥密码算法（GM/T 0003）

- SM9 标识密码算法（GM/T 0044）
- SM3 密码杂凑算法（GM/T 0004）
- 密钥管理（GB/T 17901）
- 基于口令的密钥派生规范（GM/T 0091）
- 动态口令密码应用技术规范（GM/T 0021）
- 时间戳接口规范（GM/T 0033）
- 密码模块安全技术要求（GM/T 0028）

4.3.1.5 设备固件安全

安全解决方案应防止恶意软件的安装，并应防止用户分区（例如应用程序单元）中已安装软件的恶意行为。

车辆软件的安全性还依赖于相应车辆组件的初始安装及其正确初始化，不仅限于（临时）停用后、重置后的初始化，还包括车辆处于不受保护的环境中（例如，不在相应产品的生产环境中）之后的初始化。在从不受保护的位置（例如，从外部 ROM 或闪存）初始化（即引导或加载）软件的过程中，至少必须对其完整性进行验证，以使未经授权的（离线）修改不可行或至少可检测到。此外，可选的安全目标可以是真实性、不可抵赖性和新鲜度。但是，任何安全的初始化过程因此都需要验证功能，该功能被认为是合理的防篡改功能，并且始终在每个引导或加载过程中首先执行。

表 4-3 给出了在安全软件初始化中应用的几种密码技术的功能、优点和约束。

表 4-3　设备固件安全的密码应用

	校验码	杂凑函数	MAC	数字签名	物理防护
完整性		√	√	√	√
认证性			√	√	√
不可否认性				√	√
新鲜性					√
优点	简单	简单、快捷	简单、快捷	充分安全	最高安全
限制条件	无安全	保护校验值	共享密钥	效率低、复杂	成本高、不灵活

设备固件安全方面可能应用的密码标准：

- SM2 椭圆曲线公钥密码算法（GM/T 0003）
- SM9 标识密码算法（GM/T 0044）
- SM3 密码杂凑算法（GM/T 0004）

4.3.2 轻量级密码算法应用

随着物联网的发展，RFID、无线传感器的应用越来越广泛，为了保护这类资源受限设备所传输、处理的数据，轻量级密码应运而生，并成为密码学的一个研究热点。轻量级密码的设计目标是在安全、成本和实现效率之间权衡，既要提供足够的安全性，又要在资源受限的设备中具有良好的实现效率。目前，典型的轻量级密码有 DESL、HIGHT、PRESENT 等，ISO 组织还发布了关于轻量级密码的国际标准 ISO/IEC 29192《轻量级密码》。但是在密码行业标准中也尚未有公开发布的轻量级密码算法。

尽管尚未有普适性的轻量级密码算法，但是在国家标准 GB/T 39205-2020《信息安全技术 轻量级鉴别与访问控制机制》中规定了面向身份鉴别领域的轻量级密码应用。GB/T 39205-2020 标准规范了一种基于异或运算的身份鉴别机制，其消息交互过程如图

4-4 所示。基于异或运算的身份鉴别机制要求实体 A 和实体 B 在鉴别之前具备预共享密钥 PSK，通过简单的异或、移位运算来实现实体 A 和实体 B 之间的身份真实性的确认。这种鉴别机制的计算资源占用少，并且交互消息较少，比较适合用于车载设备之间的身份鉴别，譬如 ECU 之间或 ECU 与域控制器之间的身份鉴别。

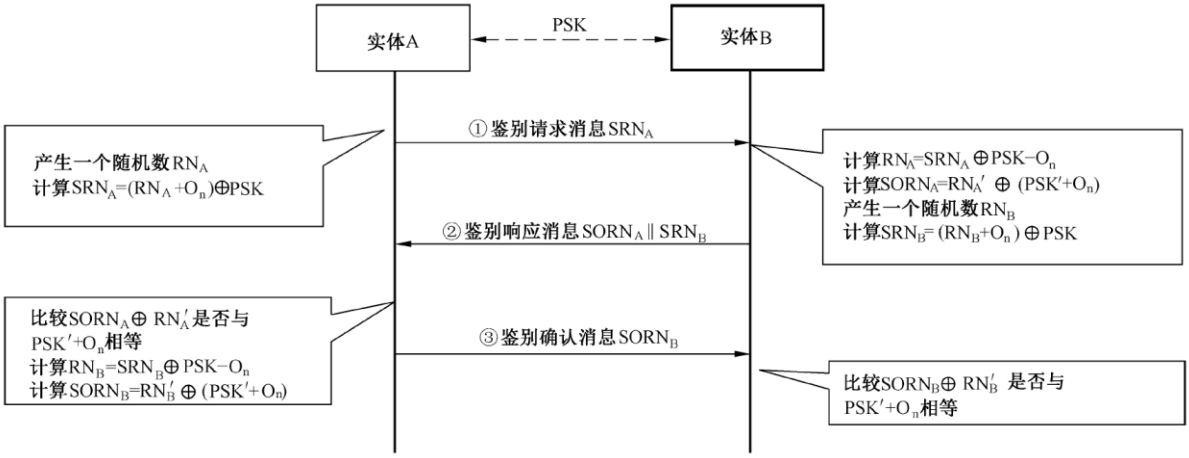

图 4-4　基于异或运算的身份鉴别消息交互示意图

GB/T 39205-2020 标准还规范了一种基于密码杂凑算法的鉴别机制和一种基于分组密码算法的鉴别机制，可以进一步研究这些鉴别机制是否适合于车载网络的应用。

此外，在车载设备之间的数据传输也有机密性需求，对于资源受限的嵌入式设备，SM4 分组加密的运算可能会增加 ECU 组件的负担，需要在标准层面规定新的轻量级密码算法来解决这些这种场景下的新需求。因此，研究面向物联网领域的轻量级密码算法的设计需求，提出安全的轻量级密码算法，同时拓展汽车电子领域的应用是必要的，也有重要的应用价值。

4.3.3　车载设备中的硬件安全模块

智能网联汽车中包含了很多不同类型的车载设别，而设备对于硬件安全模块（HSM）的技术要求存在差异，对 HSM 的能力进行分级有利于效率和成本的权衡。在 OBU、T-Box、中央网关、各域控制器等部件中都可能包含硬件安全模块（HSM），用于保护与安全相关的组件免遭篡改，并保护敏感数据免遭入侵。硬件安全模块（HSM）通过保护微控制器的基本安全功能（例如安全启动、密钥生成、密钥存储、活动内存保护）为软件提供了强大的安全锚点。HSM 用于存储通信实体的密钥，帮助提供硬件安全服务，并为嵌入式 CPU 分担密码运算方面的负载，以提高性能。

4.3.3.1　车载 HSM 的典型形态

在车载设备中包含的 HSM 模块一般可有独立安全芯片和集成式安全模块两种形态。独立安全芯片是指以独立 SoC 芯片的形式存在，典型的形态包括 SE（Secure Element）、TPM、eSIM 和 Secure Flash 等。独立安全芯片是含有密码算法、安全功能，可实现密钥管理机制的集成电路芯片，具备完整的专用密码算法模块、真随机数发生器模块、环境异常检测处理机制、逻辑异常检测处理机制、存储器加密及访问控制机制。独立安全芯片一般都满足一定的 GM/T 0008-2012《安全芯片密码检测准则》定义的安全等级。

集成式安全模块指集成于 MCU、MPU 等处理器单元中的硬件安全组件，包含 HSM、Trust Zone 等形式。这类硬件安全模块以 IP 核的形式集成到 MCU、MPU 中，具备硬件隔离或逻辑隔离边界，对安全敏感数据的处理和其他数据的处理分开，具有一定的安全防护能力，可根据安全需求在安全边界内提供安全功能，而安全边界之外的其他部分通常不具备安全防护能力。

4.3.3.2 EVITA 硬件密码安全模块及其分级模型

对于车载设备中 HSM 的能力分级，目前并没有统一的标准。EVITA 是欧盟资助的项目，旨在为车载网络的体系架构进行设计、验证、形成原型，以防止安全相关的组件被篡改，并保护敏感数据以免受到攻击。

EVITA 提出了面向汽车硬件安全模块的通用结构，如图 4-5 所示。HSM 通过内部通用接口与 ECU 应用核心相连，集成在 SoC 中。应用核心通过接口使用不同的密码算法和密码功能。HSM 负责执行所有密码应用，包括基于对称密钥的加解密、完整性检查、基于非对称密钥的加解密、数字签名的创建与验证，以及用于安全应用的随机数生成功能。

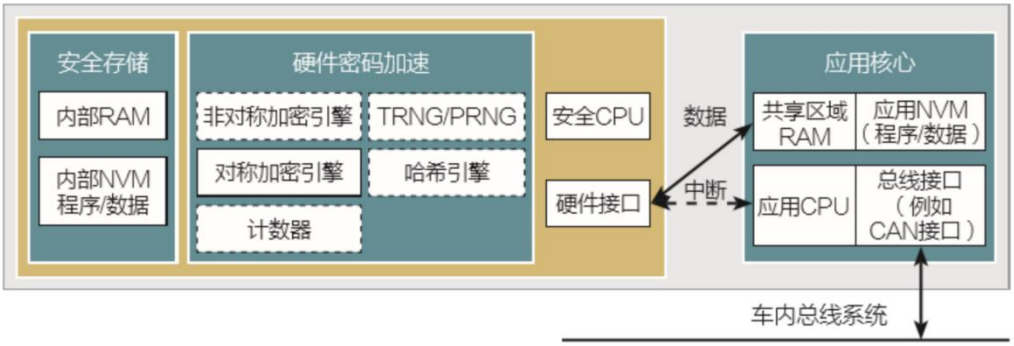

图 4-5　EVITA 关于 HSM 的基本结构

EVITA 项目还对 HSM 能力进行了分级，车内 ECU 可以根据 ECU 负责业务的安全性、重要性来判断所需要的安全级别。EVITA 提出的三个安全级别分别是：

——Full：全功能 HSM 通过提供高性能的对称和非对称加密引擎来实现高效的车载和车联网通信，从而保护高性能 ECU（例如 OBU，中央网关）；

——Medium：中型 HSM 可以保护某些中央多功能 ECU（例如发动机控制，防盗锁），因此与完整的 HSM 相似，但处理性能较差并且没有硬件非对称加密引擎；

——Light：轻型 HSM 通过使用对称加密引擎来确保较小但很重要的 ECU，车辆的传感器和执行器（例如踏板传感器，制动执行器，GPS 或时钟控制器）之间的通信。

4.3.3.3 AUTOSAR 安全硬件扩展（SHE）规范

安全硬件扩展（Secure Hardware Extension，简称 SHE）是由 HIS（由 Audi、BMW、Porsche、Volkswagen 组成）制定的标准，是对微控制器的片上扩展，被应用在车端 ECU 中负责安全存储与安全计算。

SHE 的设计宗旨是将对加密密钥的控制从软件域移到硬件域，从而保护这些密钥免受软件攻击，其主要设计目标包括：

- 保护加密密钥免受软件攻击；
- 提供可认证的可信软件环境；
- 让安全性只依赖于底层算法的强度和密钥的机密性；

- 允许分配密钥所有权；
- 保持高灵活性、低成本。

SHE 可以为 ECU 提供对称加密（AES-128）算法、CMAC 的生成/验证、数据压缩、根密钥安全存储、安全引导加载程序、防止重放攻击等功能，但同时也存在一些局限性，如不支持非对称算法、不支持并发访问等。此外，SHE 规范也不支持商用密码算法（如 SM4 加密算法）。

由此可见，SHE 的设计目标并不是要取代高度安全的解决方案（如 TPM 芯片或智能卡等），而是属于轻型（Light）密码模块。对于电控自动变速器、主动悬架系统等部件，采用带 SHE 的 ECU 完全可以满足安全要求，SHE 规范使得安全性有了硬件级别的保护，同时成本也得到了很好的控制。

SHE 安全模型如图 4-6 所示，在 ECU 内部设计了单独的安全区（Secure Zone），安全区内部是 SHE 模块。SHE 包括控制逻辑（Control Logic）、AES 引擎、内存（Memory），并仅与 CPU 通讯。同时，SHE 必须被实现为微控制器的片上外围设备。除了上图中明确指定的连接之外，SHE 不能有任何其他连接。如果必须包括额外的资源以确保芯片制造过程中的正常功能，则所有端口都要求在物理上停用（如可以通过外部引脚访问）。SHE 可以通过多种方式连接到 CPU，如：通过专用接口或内部外围总线，互连必须以其他外设或外部实体不能修改 CPU 和 SHE 之间传输数据的方式实现。SHE 不需要在特殊工艺中制造以提高安全性，也不需要采取任何措施来增强系统抵御物理攻击，如：蚀刻芯片外壳打开、差分功率分析、错误注入攻击等。

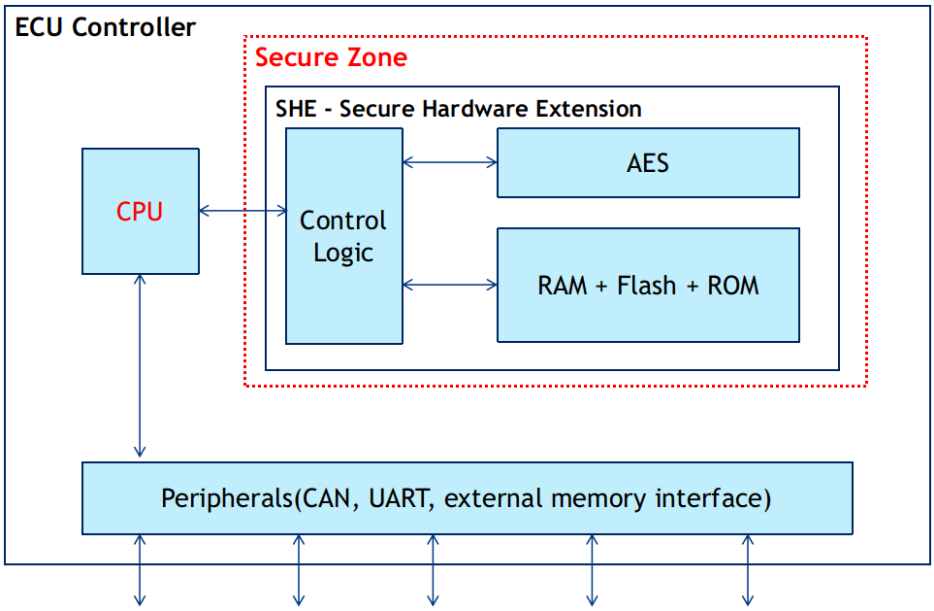

图 4-6　SHE 安全模型

SHE 内部逻辑结构如图 4-7 所示，基本由三个构建块组成：一个存储区用于保存加密密钥和附加相应信息、分组密码（AES）的实现和控制逻辑将这些部件连接到微控制器的 CPU 上，同时 SHE 提供一套指令集，通过这些指令完成相关的操作。譬如，指令 CMD_ENC_CBC 可以完成 AES 对称加密操作。

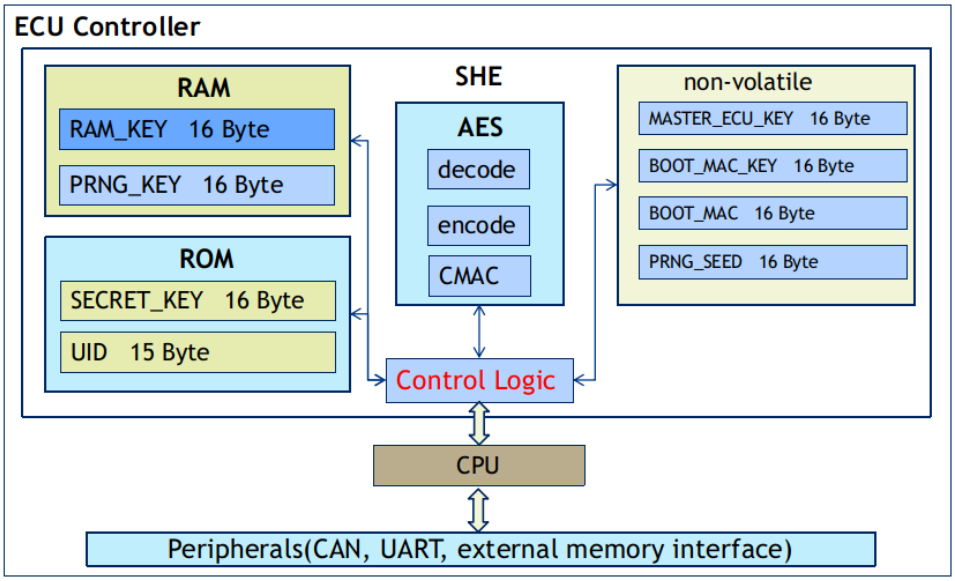

图 4-7　SHE 内部逻辑结构

4.3.3.4　密码行业标准的适用性分析

密码厂家在设计与开发适用于车载设备的 HSM 模块时，可以参考 GM/T 0028-2014《密码模块安全技术要求》和 GM/T 0039-2015《密码模块安全检测要求》等行业标准，然而还应充分考虑车联网 PKI 体系的特殊性，研究适用于车载设备的 HSM 模块的设计方法。EVITA 项目提出的 HSM 能力分级模型与 GM/T 0028 标准对于密码模块的安全分级之间并没有显而易见的对应关系，因此厂家提出了根据 V2X 的业务需求来选择 HSM 的类型，还应从数据安全风险和合规性要求来合理选择 HSM 的安全等级。

在满足 GM/T 0008-2012《安全芯片密码检测准则》相应安全等级的技术要求的基础上，V2X 车载设备一般还需要满足以下列出的典型技术要求：

——证书存储空间需要大于 32K；

——实现安全密钥存储、加解密运算功能；

——验签性能需要满足大于 2000 次/秒，支持数据安全存储，支持访问数据的线路保护、权限设置，对称体系、非对称体系等安全认证；

——芯片应具有独立的存储器保护单元和对外的接口，包括 SPI、UART、ISO7816、I2C 等；

——芯片要支持包括电压、频率检测机制，程序和数据加密存储机制以及代码保护机制等安全机制，以对抗物理攻击、剖片探测等；

——满足低功耗、高性能要求。

目前国内已经有厂家推出了面向 V2X 车载设备的安全芯片，可以支持商用密码算法。但是域控制器、ECU 等设备内置的 MCU 大部分由国外厂家提供，典型的产品是 NXP 公司的 SoC 芯片。对于国内的汽车企业，一定程度上可以促进车企采用支持商用密码算法的硬件芯片或独立安全芯片，但是国外汽车企业在选择汽车底层架构时并不会考虑是否支持商用密码算法，对于此类车载设备进行密码算法的替换将存在较大的困难。尽管可以在后装形态的 OBU 中应用商用密码算法，但是对于 ECU 身份认证、车内局域网通信等场景则无法全面应用商用密码算法。

必须指出，由于 V2X 网络的安全隐私保护的特别需求，车载终端的 HSM 密码模块必须支持密钥衍生机制，支持在不同时刻切换并使用大量的用户私钥。由于 GM/T

0016-2012《智能密码钥匙密码应用接口规范》和 GM/T 0018-2012《密码设备应用接口规范》等标准中并没有充分考虑此类特殊需求，因此不能有效支撑这些密码应用。

4.3.4 车载终端数据安全

安全存储使车辆应用程序可以安全地保存和安全地检索其关键信息，例如个人信息（例如导航路线、通信数据），操作秘密（例如授权、校验和里程）或技术秘密（例如复杂的算法、特殊设置、受保护的专有技术）与持久存储位置之间的通讯。

安全存储基本上可以保护重要的车辆信息免受脱机攻击，如相应的车辆组件被（临时）停用的情形。因此，在相应的车辆部件在不运行时被拆卸，被盗或以其他方式受到破坏的情况下，它可以防止未经授权的访问，未经授权的操纵，未经授权的复制，侵犯隐私或盗窃信息。

安全存储敏感数据，例如私钥是最重要的方面之一，也是实现整体安全系统体系结构必不可少的部分。必须防止攻击者泄露此敏感数据，因为这将使攻击者能够模拟为有效的 V2X 通信伙伴，其消息将被其他通信伙伴信任。因此，不应允许将密钥和其他敏感数据以普通格式存储在普通的非易失性存储器中，例如存储在普通的非易失性存储器中。闪存或 E2PROM。

一种解决方案是使用受篡改保护的存储设备。这些设备具有用于主机 CPU 连接的通用接口，但除了常规存储功能之外，还包括多个传感器，这些传感器监视环境参数（例如电压，温度甚至光线）的变化，以检测可能的硬件攻击。万一检测到异常变化，这些设备便能够立即擦除存储内容或以随机模式覆盖存储内容。这些设备具有非常好的安全性，可以很好地保护敏感数据，但主要缺点是价格昂贵。在任何情况下，不仅设备本身的成本可能很高，而且还需要用于程序代码和数据的通用存储设备。最后，至少必须有两个存储设备，一个用于存储代码和数据，另一个用于存储敏感数据，这些存储设备必须放置在印刷电路板（PCB）上。这可能会增加 PCB 的复杂性和尺寸，从而增加其成本。也可以将可信平台模块（TPM）用于密钥存储，但不幸的是，它具有与防篡改存储设备相同的缺点。

另一个通常便宜得多的解决方案是将敏感数据加密后存储在通用存储设备上。因此，使用不同且唯一的设备密钥来加密密钥对象（机密性）并创建存储的密钥对象的 MAC（真实性）。由于进行了加密，攻击者无法透露密钥，并且由于 MAC 而无法在不通知的情况下修改存储在非易失性存储器中的密钥对象。如果检测到关键对象的修改，则将阻止其将来的使用。

4.4 安全通信密码应用案例分析

4.4.1 智能网联汽车与 TSP 平台的安全通信

汽车远程服务提供商（TSP，Telematics Service Provider）在 Telematics 产业链居于核心地位，上接汽车、车载设备制造商、网络运营商，下接内容提供商。典型的 TSP 平台包括通用安吉星（OnStar）系统、丰田的 G-Book 系统、福特 SYNC 系统和上汽 inkaNet 系统等。

Telematics 服务集合了位置服务、GIS 服务和通信服务等现代计算机技术，为车主和个人提供强大的服务，如导航、娱乐、资讯、安防、SNS、远程保养等。除专门的 TSP 平台服务商外，目前还有许多第三方服务商（如整车厂商、电信运营商、互联网内容服务商等）构建属于自己的 TSP 平台。

车联网 Telematics 系统的应用架构以 NGTP 开放式架构为主流，NGTP 2.0 的系统架构如图 4-8 所示，包含几个主要组成部分：Telematics 单元（TU），Telematics 服务供应商（TSP）和调度器（DSPT），所有这些都是通过标准的接口进行连接。

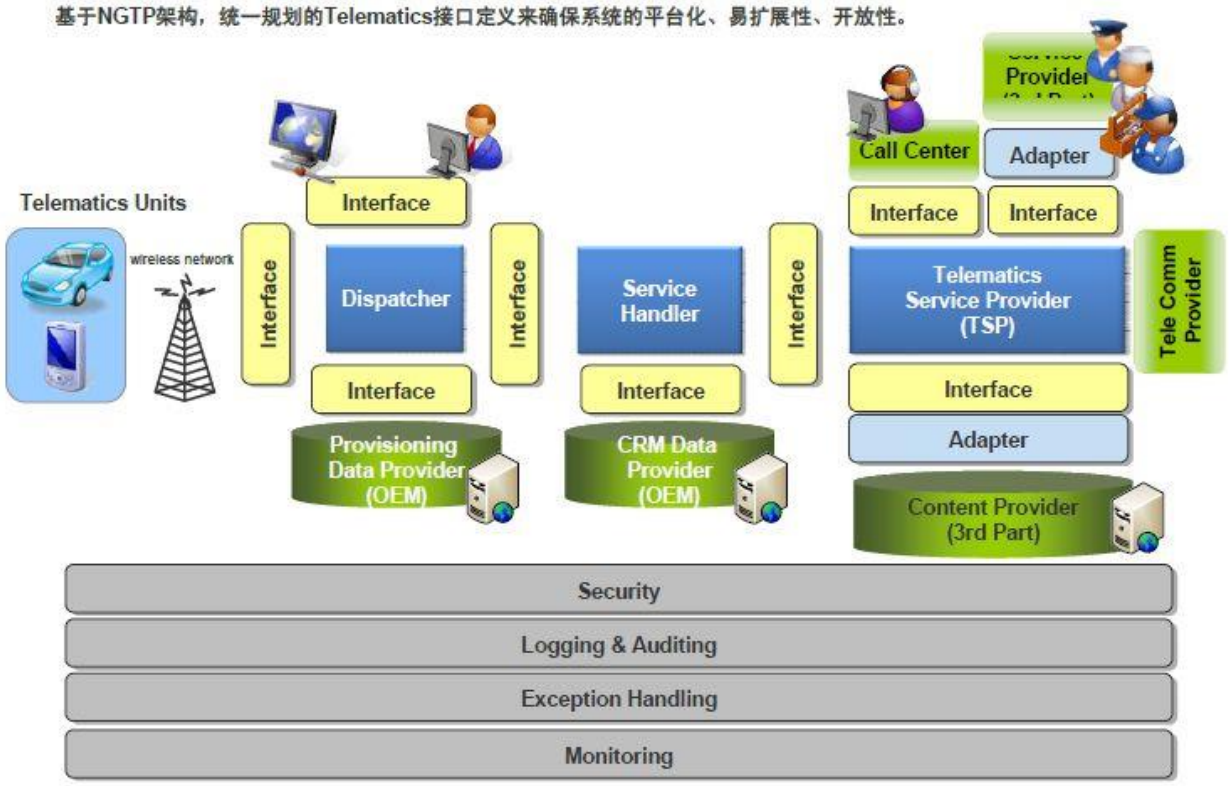

图 4-8　NGTP 架构图

在车云通信可以直接采用支持 TLCP 协议的安全网关实现对车载终端的认证。在建立安全通信通道基础上，云平台中业务系统与车端通信过程中，诸如部分核心的车联网业务系统在数据处理和数据交互时，敏感数据（如远程指令、蓝牙钥匙、远程升级包等）应保障数据传输过程中的机密性。

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信息进行加密，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。

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。

4.4.2　V2X 通信安全服务

通信安全服务是通信系统协议栈中非常重要的组件，一方面用于解决消息窃听，修改和重播的威胁，另一方面要求最大程度地减少未经授权的身份披露。为了达到这些目标，安全通信服务需要定义安全消息的格式和处理，并在协议栈中引入密码算法和技术，使用的数字证书将公钥绑定到由身份信息描述的实体（例如名称和地址）。

欧盟开展的 PRESERVE 研究项目对 V2X 网络安全做了基础研究，同时还研究了网络安全的实现，试验和导入方法。该项目的研究主题包含了消息处理相关的安全软件堆栈、加密加速器、实现安全密钥硬件存储的 ASIC、公钥基础设施相应的安全后端等。

PRESERVE 项目给出了参考性的 V2X 安全通信系统架构，充分考虑了车联网的层次架构和协议栈的关系，如图 4-9 所示。PRESERVE 项目的研究结果也对 IEEE 1609.2 及 ETSI TS 103 097 等国际标准的发展做出了重要贡献。

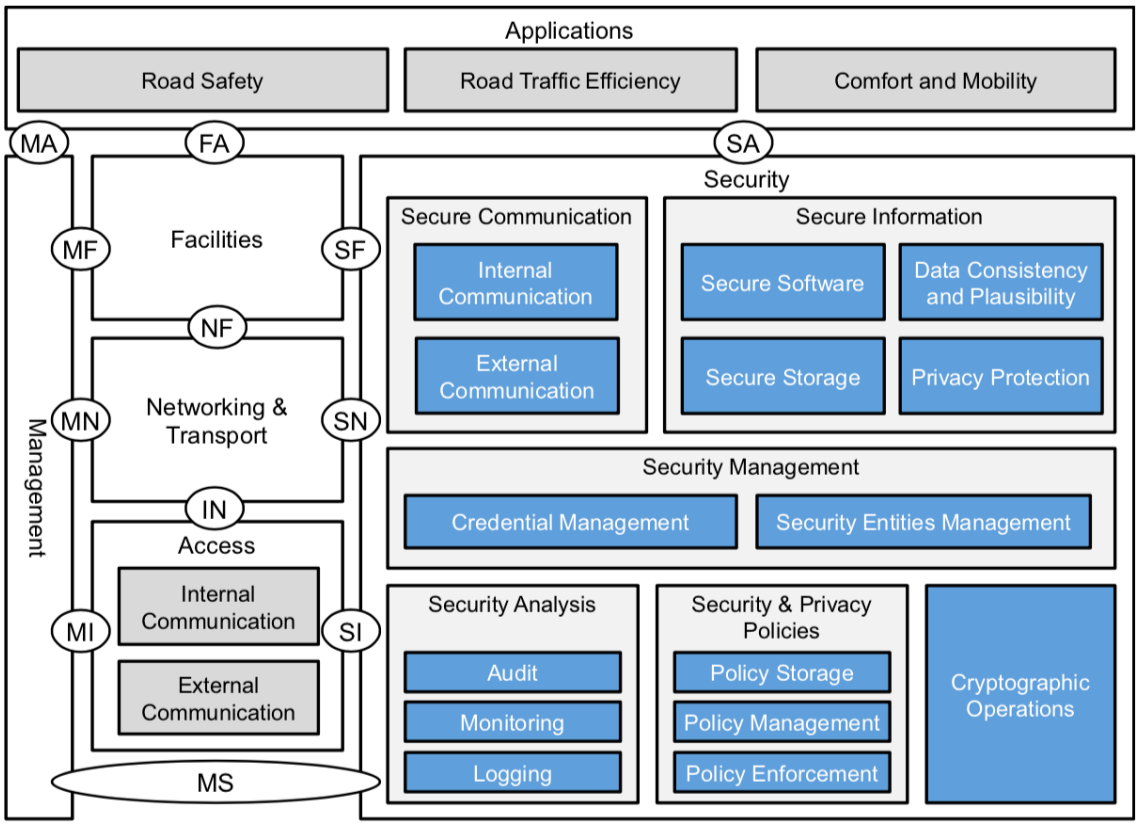

图 4-9　V2X 安全通信系统架构图

4.4.2.1　通信安全服务分组

IEEE 1609.2 该标准为车联网的安全通信指定了 4 种安全和隐私服务，它们是：

——机密性：确保只有接收者才能阅读它；

——真实性：确认消息的来源；

——完整性：确保消息在各方之间传输时没有被更改；

——匿名性：广播的消息不应将信息泄露给标识消息来源的车辆的未授权接收者。

在车联网的通信层需要为发送方、接收方提供注册、授权、安全关联、认证、保密、完整性等安全服务。典型的通信安全服务分组如表 4-4 所示。

表 4-4　通信安全服务分组

安全服务组	发送方安全服务	接收方安全服务
注册	获取注册证书	
		移除注册证书
	更新注册证书	
授权	将授权凭证添加到单个消息	
	获得授权票据	
		验证收到消息的授权凭证

安全服务组	发送方安全服务	接收方安全服务
	更新授权票据	
安全关联管理	建立安全关联	建立安全关联
	移除安全关联	移除安全关联
	更新安全关联	更新安全关联
认证服务	认证 ITS 用户	认证 ITS 用户
	认证 ITS 网络	认证 ITS 网络
保密服务	加密单个外发消息	
		解密单个传入消息
	发送安全消息	
		接收安全消息
完整性服务	插入校验值	
		验证校验值
	计算校验值	
重放保护服务	在消息中插入时间戳	
		验证时间戳
	插入序列号	
		验证序列号
	插入挑战码	
		在响应中使用挑战码
	验证挑战码	
审计服务		记录传入消息
	记录外发消息	
合理性验证		验证数据的真实性
		验证动态参数
		验证时间戳
		验证序列号
远程管理	激活 ITS 传输	
	停用 ITS 传输	
报告行为不当的 ITS-S	报告不当行为	报告不当行为

在车联网的通信层提供通信安全服务都是面向 CIA 三种安全目标来定义的，表 4-5 说明了这些安全服务与 CIA 的关联关系。

表 4-5　通信安全服务与 CIA 的映射

通信安全服务	机密性	完整性	可用性
在所有 V2V 消息中包括源地址			X
在其消息被 ITS 系统接受之前，要求 ITS-S 获得 ITS 认证机构授权		X	

通信安全服务	机密性	完整性	可用性
在可能的情况下将消息流量限制为 V2I/I2V			X
对传入信息实施真实性验证		X	X
在发送的每条消息中都包括该消息的非加密校验和		X	
使用广播时间（通用协调时间-UTC-或 GPS）为所有消息加时间戳			X
在每条新消息中都包含一个序列号			X
在每封邮件中包含权威身份并进行身份验证			X
加密个人和私人数据的传输	X		
将审核日志添加到 ITS 站，以存储发送到 ITS-S 和从 ITS-S 发送的每条消息的类型和内容		X	
使用类似 Kerberos / PKI 的令牌对每个消息进行数字签名		X	X
使用不能链接到用户或用户车辆的真实身份的假名	X		
允许远程激活和停用 ITS-S			X

4.4.2.2 密码算法的配用

IEEE 1609.2 标准使用椭圆曲线集成加密方案（ECIES）算法对车辆之间交换的消息进行加密，并使用椭圆曲线数字签名算法（ECDSA）对消息进行签名。11 加密密钥的最小建议大小为 256 位，签名密钥的最小建议大小为 224 位，并且证书颁发机构（CA）密钥的长度为 256 位。

IEEE 1609.2 标准将 AES-CCM 作为批量加密算法，用于验证然后加密它们交换的消息。AES-CCM 是高级加密标准（AES）的一种加密模式，它是 CTR 加密模式和 CMAC 认证算法的混合使用。

该标准建议最大程度地减少唯一标识收件人的数据交换，或者允许未经授权的收件人标识消息的发送方。

在 IEEE 1609.2 标准中规定了 V2X 通信层应用的密码算法，包括随机数生成算法（DRBG）、密码杂凑算法（SHA）、对称加密算法（AES-CCM）、非对称签名算法（ECDSA）、非对称加密算法（ECIES）等，如图 4-10 所示。这里应用的密码算法均为国际标准算法，并不支持 SM 系统算法。

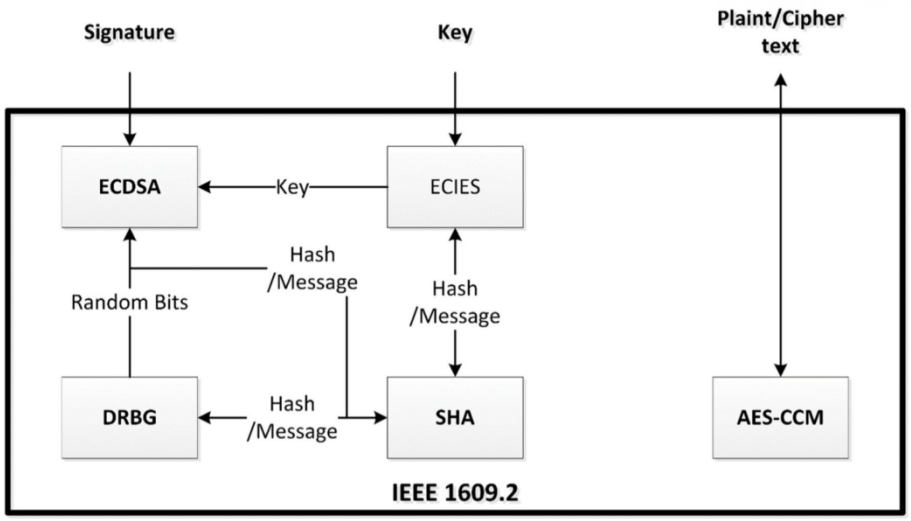

图 4-10　IEEE 1609.2 的密码算法配用

4.4.2.3 不同技术体系的安全特性

由于 IEEE802.11p 和 LTE-V2X 是不同的技术体系，两种标准的安全特性存在很多差别，表 4-6 分别从可用性、完整性、保密性、认证性、不可否认性等角度对这两种技术标准的安全特性做出了比较。

表 4-6　IEEE802.11p 和 LTE-V2X 的安全性比较

安全要求	威胁	IEEE802.11p		LTE-V2X			
		外部	内部	蜂窝通信		直连通信	
				外部	内部	外部	内部
可用性	黑洞/灰眼攻击	✓	✗	✓	✗	✗	✗
	洪水攻击	✓	✗	✓	✗	✗	✗
	干扰攻击	✗	✗	✗	✗	✗	✗
	联合进攻	✓	✗	✓	✗	✓	✗
完整性	篡改报文攻击	✓	✓	✓	✗	✓	✗
	注入虚假消息攻击	✓	✗	✓	✗	✓	✗
	重放攻击	✓	✓	✓	✓	✓	✓
	GPS 欺骗攻击	✗	✗	✗	✗	✗	✗
保密性	窃听攻击	✓	✗	✓	✗	✗	✗
	位置追踪	✗	✗	✗	✗	✗	✗
认证性	证书复制攻击	✓	✓	✓	✓	✗	✗
	女巫攻击	✓	✓	✓	✓	✗	✗
	伪装/假冒攻击	✓	✓	✓	✓	✗	✗
不可否认性	任何	-	✓	-	✓	-	✗

4.4.3　身份认证管理体系

4.4.3.1　PKI 体系框架

为了确保车联网业务中消息来源的真实性、内容的完整性，并防止消息重放，车联网系统采用数字证书通过数字签名/验签等密码技术对 V2X 业务消息进行保护，因此，需要车联网证书管理系统来实现证书颁发与撤销、终端安全信息收集、数据管理、异常分析等一系列功能。

数字身份认证技术应用于车联网通信中，可实现车载设备、路侧设备、应用服务商等各个角色的身份认证，保证通信消息来源的真实性，有效做到防重放、防止中间人攻击、防止身份假冒等，将为依托车联网通信技术实现的安全预警和效率提升等车联网应用提供关键的基础安全保障。

为了保证车联网通信过程的隐私保护需求，LTE-V2X 通信安全过程采取了假名证书更换和去标识化的隐私保护机制。由于车联网中消息发送频率高，对信息交互的实时性具有很高的要求，X.509 证书体系难以满足车联网高频通信的需求。

美国交通部（USDOT）推出的 SCMS 是具有代表性的车联网证书管理系统[15]，体现了该领域的主要技术路线。SCMS 系统是由 Crash Avoidance Metrics Partners LLC（简称 CAMP）根据与 USDOT 的合作协议开发的一套证书管理系统，针对 V2X 应用层安全，设计了证书颁发、证书撤销、终端安全信息收集、数据管理、异常分析等一系列与安全相关的功能，以此确保 V2X 的安全通讯。SCMS 建议采用几种新颖的密码结构，包括：（1）分布式证书配置以保护用户隐私免受内部人员的攻击；（2）Butterfly 密钥扩展，用于通过通信有效地请求任意数量的设备证书；（3）链接值，用于有效撤销一个设备的貌似不相关的假名证书，以及（4）用于管理根证书颁发机构及投票人的选举机制。这些新颖的密码结构，可为用户提供高水平的安全性和隐私性，同时又能保持系统的高效运行。此外，SCMS 设计还提供了用于请求证书和处理吊销的高效方法。

SCMS 系统在两个最重要的方面与传统的 PKI 有所不同，其一是规模（即，它支持的设备数量），其二是在安全性、隐私性和效率之间的平衡。在设备数量的规模方面，其设计目标是在满负荷运行时将每年为 3 亿辆汽车颁发约 3000 亿张证书。在安全和隐私方面，系统的主要目标是保护最终用户的隐私，尤其是使用私家车的人。车联网的证书管理系统将隐私作为最高优先级，其主要设计目标是在合理和最大可能的范围内提供安全性和隐私性，包括针对内部人员和外部人员的隐私泄漏。

基于蜂窝移动通信网络的车联网 LTE-V2X 系统同时可以使用基于公钥证书的 PKI 机制确保设备间的安全认证和安全通信，采用数字签名等技术手段实现 V2V/V2I/V2P 直连通信安全。我国制定的《基于 LTE 的车联网通信技术安全证书管理系统技术要求》标准提出了适用于车联网 LTE-V2X 通信的轻量级数字证书格式，以及包括注册证书机构、假名证书机构、应用证书机构在内的安全证书管理系统参考架构。密码算法均采用发布了行业标准的 SM 系列密码算法，数字证书格式符合国家标准或者行业标准的技术要求。

车联网的证书管理技术架构如图 4-11 所示[17]。车联网 LTE-V2X 证书管理机构 CA 为用户签发证书，负责向车联网设备（OBU/RSU/VSP）颁发通信证书（注册证书、假名证书等）、签发证书撤销列表 CRL 以及更新证书等。

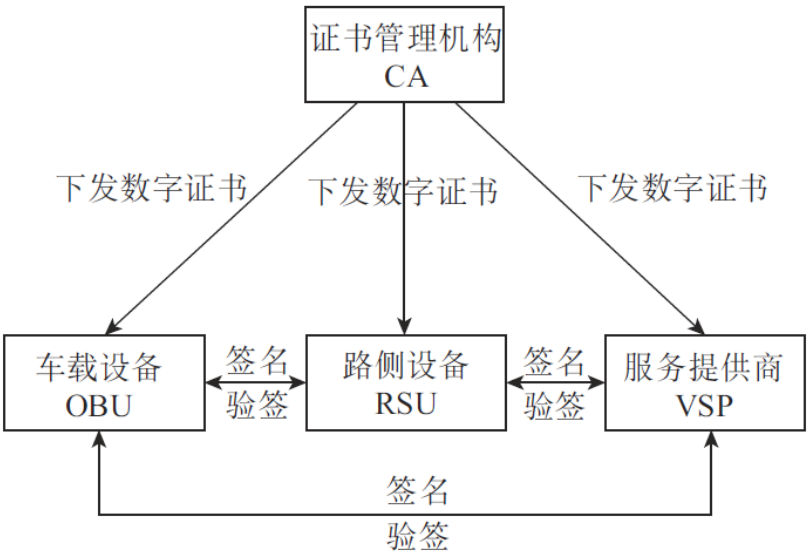

图 4-11　车联网证书管理技术架构

V2X 通信主体（OBU/RSU/VSP）在自己的密码模块中生成各自的签名公私钥对，公钥作为申请材料的一部分向 CA 管理机构申请证书。V2X 通信主体凭借初始信任凭据向注册证书机构(ECA)提交注册申请,注册证书机构向通信主体颁发注册证书(Enrollment Certificate，EC），作为通信主体获取假名证书或应用证书的凭证。

车载设备、路侧设备、服务提供商可向假名证书机构（PCA）或应用证书机构（ACA）申请用于人-车-路-云通信签名的假名证书或应用证书。假名证书或应用证书申请由注册机构（Register Authority，RA）确权，由假名证书机构或应用证书机构进行证书签发。

发送数据时，V2X 通信主体（OBU/RSU/VSP）使用证书管理机构颁发的数字证书（假名证书或应用证书）对其播发的业务消息进行数字签名，之后将业务消息内容、消息签名值以及所使用的数字证书组包后广播；接收数据时，V2X 通信主体（OBU/RSU/VSP）对发送方证书进行验证，验证通过后使用发送方证书中的公钥对消息进行验证，用发送方公钥解密消息签名值，并对业务消息取哈希值验证消息签名，进而完成身份认证并检查消息的完整性。

4.4.3.2 证书类型及其用途

车联网的业务证书可分为注册证书、假名证书、应用证书和身份证书，这些证书分别有不同的用途：

——注册证书与设备唯一对应，由注册 CA 签发给 OBU、RSU 和 VSP。OBU、RSU 或 VSP 被注册机构认证后，注册 CA 会为其签发注册证书。V2X 设备需要使用注册证书从假名 CA 申请假名证书或从各应用授权机构（ACA）申请应用证书和身份证书；

——假名证书由假名 CA 签发给 OBU。OBU 使用假名证书签发其播发的主动安全消息（Basic Safety Message，BSM）。为保护用户隐私，需要使用密码技术对用户的身份信息进行加密；为避免泄露车辆行驶轨迹，OBU 可拥有多个假名证书，用于定期切换使用；

——应用证书由应用 CA 签发给 RSU 和 VSP，用于特定的车联网应用。RSU 和 VSP 使用应用证书签发其播发的某种应用消息，例如交通信号灯状态、交通信息、商业服务消息等；

——身份证书由应用 CA 签发给 OBU，用于特定的车联网应用。OBU 使用身份证书向 RSU 或 VSP 证明其身份，以获得后者提供的某种车联网应用服务，例如警车与红绿灯进行交互，并控制后者的状态。

4.4.3.3 证书格式及隐式证书

车联网的几种业务证书的格式基本类似，最大的特点是并非采用 X.509 标准的数字证书格式。采用自定义数据格式的主要意图是减少 V2X 数字证书的字节大小，一方面节省 V2X 设备存储证书的空间，另一方面减少 V2X 通信的带宽开销。

《基于 LTE 的车联网通信技术安全证书管理系统技术要求》标准定义的假名证书的数据结构如表 4-7 所示[16]，在假名证书中可能包含签发者的签名值（signature）。

表 4-7　假名证书的数据结构

数据域 1	数据域 2	数据域 3	是否必选	说明
版本		version	是	证书结构版本，本标准对应的版本号为 3

数据域 1	数据域 2	数据域 3	是否必选	说明
类型		type	是	证书结构类型： ——显式证书 ——其他结构的证书
签发者		issuer	是	签发此证书的 CA 证书的 HashedId8 值
签名数据	toBeSigned	id	是	证书标识
		cracaId	是	CRL-CA 标识 HashedId3，若不使用设置为全零
		crlSeries	是	CRL 序列号，若不使用设置为全零
		validityPeriod	是	有效期
		region	否	有效地理范围
		assuranceLevel	否	信任级别
		appPermissions	是	应用数据签名权限（例如 OBU/RSU 签名的应用消息类型）
		certIssuePermissions	否	适用于 CA 证书，描述可签发的证书种类和权限范围
		certRequestPermissions	否	适用于注册证书，描述可申请的证书种类、权限范围
		canRequestRollover	否	是否能够用于请求同等权限的证书。
		encryptionKey	否	加密公钥
		verifyKeyIndicator	是	验证公钥
签名值		signature	否	证书结构类型为显式证书时，此字段为必填字段，用于存储证书的签名值。

在 IEEE 1609.2 标准中，引入了一种新型的数字证书格式，称为隐式证书。SCMS 建议强制要求使用隐式证书进行 V2X 通信。与更传统的证书形式相反，隐式证书通过将公钥和签名组合为单个值（称为重建值）来节省空间。

附录 C 阐述了一种典型的隐私证书的密钥生成算法 ECQV，以及签发隐式证书的过程。《基于 LTE 的车联网通信技术安全证书管理系统技术要求》标准并没有具体定义隐式证书相关的密钥生成算法，但是在假名证书的数据结构中已经预留了相关的标识位，因此该标准的后续演进版本有可能会增加对隐式证书算法的定义。

4.4.3.4 密钥衍生机制

由于隐私保护的需求，在 V2X 通信系统中需要使用大量的假名证书，与此同时将需要在设备中生成数千个公钥。设备从 PKI 系统请求证书的典型过程是：设备生成私钥/公钥对，创建包括公钥的证书签发请求（CSR），并通过安全通道将 CSR 提供给 PKI 系统；然后，PKI 系统的 CA 将签署证书并将其提供给申请人。显然，如果使用传统的模式，将会需要传输大量的 CSR 信息，导致系统效率过低。为了克服上述缺点，在 V2X 通信系统中引入了一种新颖的密码结构——Butterfly 密钥衍生机制[15]，它可以通过

允许 OBE 请求任意数量的证书。附录 A 阐述了 SCMS 系统中定义的 Butterfly 密钥衍生的算法和机制。

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》的附录部分给出了密钥衍生流程的一种算法建议，阐述了推荐的对称加密算法和非对称加密算法、密钥衍生函数和密钥衍生流程[16]。

其中，行业标准推荐的密钥衍生函数与 SCMS 的设计基本上是一致的，由于使用分组算法的 Davies-Meyer 结构，本质上是一个带密钥的杂凑函数。与 SCMS 设计的主要区别在于，推荐对称加密算法使用 GB/T 32907-2016《信息安全技术 SM4 分组密码算法》，非对称加密算法使用 GB/T 32918.2-2016《信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法》。

行业标准推荐的密钥衍生流程与 SCMS 设计略有不同。在密钥衍生流程中，PCA 在签发假名证书之后，由 PCA 返回给 PRA 的响应报文中不仅仅包含私钥恢复材料c_t的密文，同时还附加了 PCA 对c_t密文的签名值。这个改进措施有利于防范 PRA 的中间人攻击。典型的攻击场景如下：派生加密公钥J_t是由 PRA 根据密钥衍生算法来产生的，不诚实的 PRA 可以产生一个临时的密钥对，并将其公钥作为J_t发送给 PCA，当 PRA 收到 PCA 返回的密文，使用临时私钥解密来获得 PCA 生成的随机参数c_t，然后再使用真实的派生加密公钥J_t来加密之后发送给 OBE。在这样攻击场景下，OBE 无法甄别收到的密文是由 PCA 加密产生，还是由 PRA 加密产生。行业标准推荐的密钥衍生流程增加了 PCA 的签名值，此时 PRA 将无法在保持签名有效的条件下替换 PCA 返回的响应报文，因此可以避免前面描述的中间人攻击。

4.4.3.5 私钥持有证明

在 SCMS 系统中，由于使用了 Butterfly 密钥扩展机制，证书签发请求（CSR）并不是使用要颁发的证书的密钥签名，而是使用注册证书的密钥签名。换言之，证书请求消息不提供私钥拥有证明（POP）。这种情况下，会引入误绑定攻击（Misbinding Attack）。在这种类型的攻击中，攻击者 Mallory 滥用了目标 Alice 的公钥。Mallory 读取 Alice 的公钥，并向 SCMS 请求该公钥的证书。虽然 Mallory 不知道相应的私钥，但她仍然可以发起攻击，在这种攻击中，她会收到由 Alice 的私钥签名的消息，然后附加她的证书而不是 Alice 的证书。

由于 Butterfly 密钥扩展机制是 SCMS 系统的关键技术，这是无法更改的。为了抵抗误绑定攻击，SCMS 采用的对策是：对消息进行签名时，将对消息本身和证书进行计算，以计算签名的杂凑。将杂凑绑定到证书，并确保与消息一起提供的证书实际上是发件人打算使用的证书。由于此证书误绑定攻击仅在假证书与真实证书不同的情况下才有用，因此这种在杂凑中包含证书的方法可以完全消除这种攻击。

4.4.3.6 设备注册过程

注册过程可以由 OBU 或 RSU 制造商或车辆 OEM 进行。注册可能由 CA 或单独的 RA 处理。然后，CA 生成一个私钥/公钥对，为公钥颁发证书，然后以安全的方式将证书和私钥返回给节点。如果涉及单独的 RA，则 CA 将证书返回给 RA，然后将其转发给节点。如果 CA 不知道节点的 ID 并且 RA 由于从 CA 安全地将证书发送到节点而无法获得证书，则这可能会提高隐私级别。一种更安全的替代方法是让节点生成公用/专用密钥对，并仅将公用密钥提供给 CA 以颁发证书。

在颁发注册证书之前，车联网终端必须完成设备初始化，以安全的方式完成数字证书等敏感参数的初始配置。目前针对该问题，有 2 种解决方案：一种是车企自建证书管理体系，自己维护系统，确保系统的安全可靠；另一种方案则是基于通用认证机制（GBA）的终端认证服务，如图 4-12 所示[18][19]。

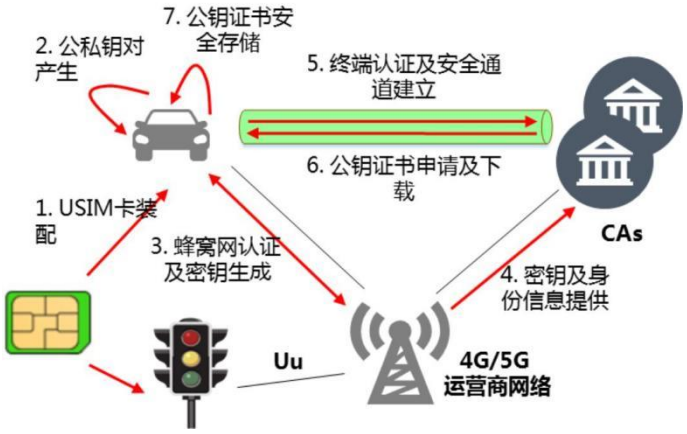

图 4-12　基于 GBA 的车联网证书初始安全配置方案

对于安装 USIM 卡，支持 LTE-Uu 接口通信的 V2X 设备，可基于用户与运营商间的共享密钥 K 和蜂窝网基础认证及密钥协商能力简化设计，实现 CA 管理实体与 V2X 设备间的身份认证，并在两者之间建立初始信任关系，满足 ECA 证书及其他证书初始申请、安全传输的需要。该方案能够使车载单元（OBU）终端仅依靠自身安全硬件和网络 GBA 安全能力即可在线完成初始安全配置，避免了工厂复杂的密钥管理，降低了汽车企业生产线及管理系统安全改造的成本，提高了汽车工业自动化生产水平。未来该技术的演进还可为 5G 车联网的应用提供可靠的安全保障。

4.4.3.7　假名证书的配置过程

在完成设备注册之后，V2X 设备可以向假名证书认证机构（PCA）申请签发假名证书。这里以 SCMS 为例介绍假名证书配置过程的详细步骤，如图 4-13 所示[15]。

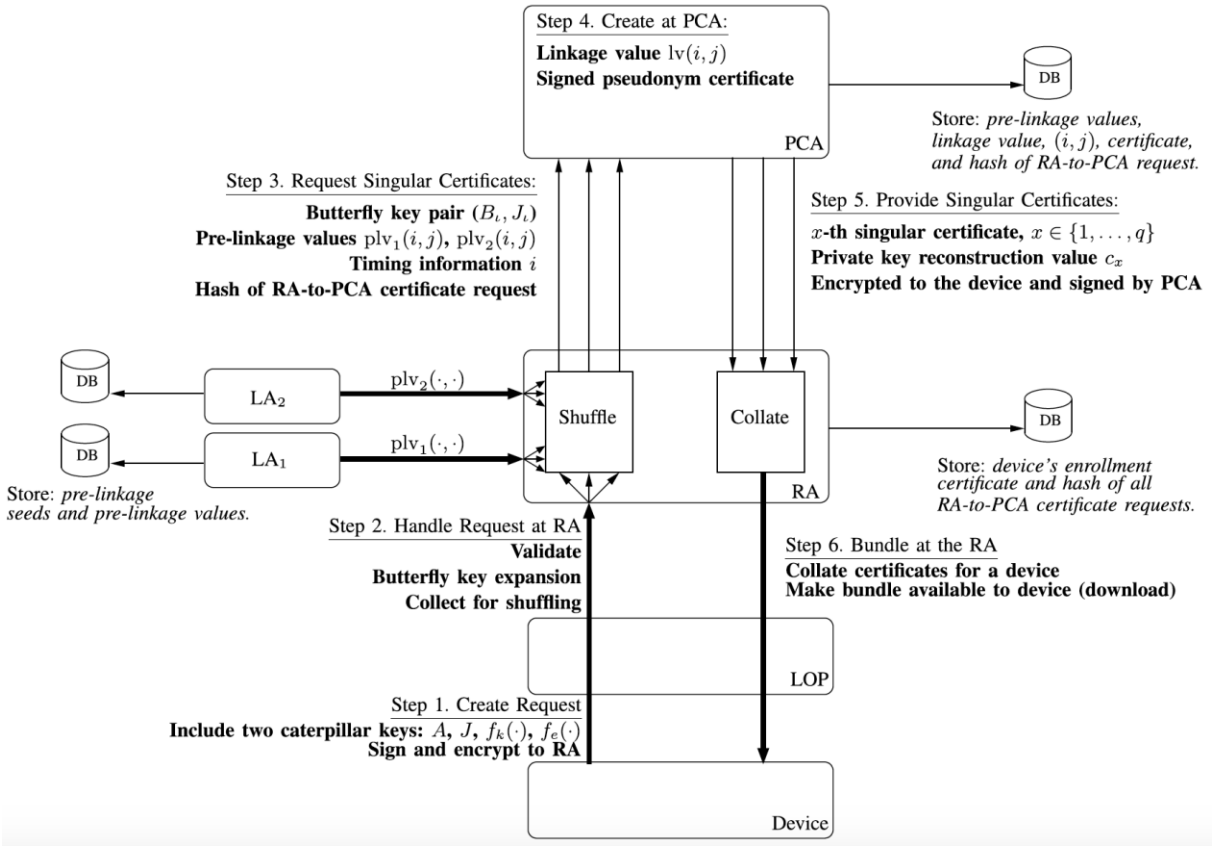

图 4-13　假名证书的配置过程

假名证书的配置过程包含如下 6 个步骤：

步骤 1、V2X 设备通过生成 Butterfly 密钥种子，使用其注册证书对假名证书请求进行签名，附加其注册证书并将证书请求加密后发送到 RA 来提交申请。然后，V2X 设备通过位置代理（LOP）将请求发送到 RA。LOP 的功能与许多 Internet 路由器中实现的伪装功能非常相似，它用自身的标识符替换 V2X 设备的标识符（例如 IP 地址），使 V2X 设备的标识符变得模糊，在 RA 看来证书请求是源自 LOP。

步骤 2、RA 解密证书请求，验证设备的注册证书以对 V2X 设备进行身份鉴别，并验证 V2X 设备未被列入黑名单。如果所有检查均成功，则 RA 将向设备发送确认，并按照第 4.4.3.4 节中的说明执行 Butterfly 密钥扩展；否则，RA 拒绝该请求。RA 收集来自不同 V2X 设备的多个此类请求以及从 LA 接收到的一组预链接值。一旦有足够的此类请求可用，RA 就会随机处理各个扩展的请求。

步骤 3、RA 将对各个假名证书的请求发送到 PCA，每个请求对应一个证书，其中每个请求包括一个待签名证书、一个响应加密公钥、每个 LA 的一个加密的预链接值 $\left(\mathrm{plv}_1(\mathrm{i,j}), \mathrm{plv}_2(\mathrm{i,j})\right)$和 RA 到 PCA 的假名证书请求的杂凑值。

步骤 4、PCA 解密预链接值和计算链接值$\mathrm{lv}(\mathrm{i,j}) = \mathrm{plv}_1(\mathrm{i,j}) \oplus \mathrm{plv}_2(\mathrm{i,j})$。然后，它将链接值添加到要签名的证书，并对其进行隐式签名（implicitly signs）以创建假名证书。然后 PCA 创建一个私钥重构值，并使用响应加密公钥对假名证书和私钥重构值进行加密。

步骤 5、PCA 对步骤 4 中生成的加密数据包进行签名，并将其发送给 RA。对加密的数据包进行签名可为设备提供 PCA 对设备加密的数据包的保证。这可以防止中间人攻击，譬如 RA 的内部人员将有效的响应加密密钥替换为 RA 知道其私钥的另一个密钥，此时 RA 可以看到假名证书的内容，包括链接值。

步骤 6、RA 收集了一个周期（如 7 天）的加密文件包，然后将它们（所谓的批次）捆绑到给定的设备，然后将各批次的文件提供给 V2X 设备以供下载。

在这个案例中，分别设立了一个 RA 机构、一个 PCA 机构和两个链接值颁发机构(LA)，这些角色需要由不同的主体来运营，并保证这些主体的独立性，才能避免来自内部人员的攻击。对于行业标准《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》定义的证书管理系统，仅仅设立了一个 LA 机构，因此建议由同一个实体来同时运营 RA 和 LA。

4.4.3.8 异常行为管理

行为异常或设备故障的 V2V 消息可能包含虚假或误导性信息，良性参与者应忽略来自行为异常的设备的消息。为了识别行为异常的设备，可以在 V2X 设备上运行异常行为检测算法以识别异常节点。异常行为管理的主要目标是以有效的方式消除行为异常的设备。

车联网中可以应用多种手段来实现移除不当行为设备，具体包括：

- 报告不当行为

在本地异常行为检测的基础上，V2X 设备向车联网系统报告可能存在问题的设备。车联网系统将运行不当行为检测算法，然后将证书不再可信的所有情况通知所有参与者。

在不当行为报告过程中，V2X 设备将通过 RA 将不当行为报告发送给 MA。不当行为报告的格式尚未完全定义，但是报告将包括与可疑和告警相关的 BSM、相关的假名证书、不当行为的类型以及报告者的假名证书和自创建报告以来的相应签名。

V2X 设备应以加密形式向 MA 提交报告，并且要求 RA 将来自多个 V2X 设备的报告进行合并和重新排列，以防止 MA 根据报告跟踪 V2X 设备的路径。

- 全局检测不当行为

全局不当行为检测是指 MA 识别系统中潜在不当行为、调查可疑活动，以及如果得到确认则撤销不当行为设备证书的过程。不当行为的一个例子是恶意行为者故意将发送车辆的位置投射到左侧 3 米的位置（对于右侧行驶国家而言，则是右侧）。这些消息将引起对即将到来的交通的警报，即将到来的车辆将检测为潜在的不当行为。

- 调查不当行为

调查不当行为是指 MA 确定可疑活动是否确实是由不当行为引起的过程，并确定不当行为的设备。调查不当行为的过程包含了 MA 接收错误行为的报告和运行全局不当行为检测算法的步骤，要求 MA 在此基础上可以了解是否有多个不当行为报告指向同一设备，还要求 MA 收集在 CRL 中发布的信息以撤消设备的证书。

- 撤销不当行为设备

如果在不当行为调查期间确定 V2X 设备确实存在异常，则 MA 会将 V2X 设备吊销并列入黑名单。此外，MA 需要向 RA 提供执行黑名单所需的信息，这会阻止行为异常的 V2X 设备获得新证书。撤消和列入黑名单的过程，需要 PCA、LA 和 MA 等实体联合执行预先设定的过程来确定链接种子和对应于假名证书的注册证书，这些过程将在第 4.4.3.9 节中具体说明。

4.4.3.9 假名证书的批量撤销

对于 V2V 安全应用程序，每个设备都收到大量证书，这种情况下传统的 CRL 会变得太大而无法使用。为了解决 CRL 文件太大的问题，SCMS 通过使用链接值的新概念来高效地撤销设备以及对应的假名证书。

在链接值的生成过程中需要应用密码杂凑算法。附录 B 中阐述了一种典型的技术方案[15]，包括链接值的生成过程、基于链接值逆向解析注册证书及链接种子的过程、CRL 分发及处理等。

4.4.3.10 多 PKI 系统互认

当车联网安全系统由多个独立 PKI 系统构成时，这些 PKI 系统之间可以根据需要构建可信关系，以便实现证书互认。车联网场景 PKI 互信存在很多场景特殊性，一是跨域验证频繁，相对于电子政务、电子商务，在车联网中，车辆、路侧单元都会更多、更频繁与其它信任域的车辆和路侧单元进行交互通信；二是遭遇性互信验证占绝对多数，实体（例如车辆）在与其它实体通信时，无法预先知悉对端实体是哪个信任域的，且车辆通常在高速行进中也没有足够的时间预先对此进行询问，实体必须支持自动、快速对其它信任域实体通信数据包进行验证签名、验证证书的能力，并在验证其它信任域的证书时，能够自动建立完整的信任链，检查证书是否被吊销；三是带宽受限，实体通信的报文大小是受限的，报文的验证也需要在非常短的时间完成，因此，既不可能在通信中包含完整的证书链、证书吊销信息，时间上难以做到接收到报文时先去下载所需的信息再来验证。

SCMS 中介绍了一种用于车辆对所有车辆（V2X）通信的机制，并提出了基于“投票人”选举的信任根 CA 列表的管理体系，对于大范围的车联网互信、车路互信场景是否可行还有待商榷。在我国车联网产业的 PKI 可信领域，YD/T3957-2021 参考了现有围绕国家根 CA 的 PKI 互信体系，结合车联网信任域的特点，规划了基于证书信任列表的机制 PKI 互信机制[16]。

基于证书信任列表的 PKI 互信机制原理如图 4-14 所示。多个车联网 PKI 系统之间的可信关系是通过一个“可信根证书列表（Trusted Root Certificate List，TRCL）”实现的。该可信列表由可信根证书列表管理机构（Trusted Root Certificate List Authority，TRCLA）签发。

可信根证书列表的存在与否不会影响各个独立 PKI 系统的运行，但会影响不同 PKI 系统证书之间是否能够互认。

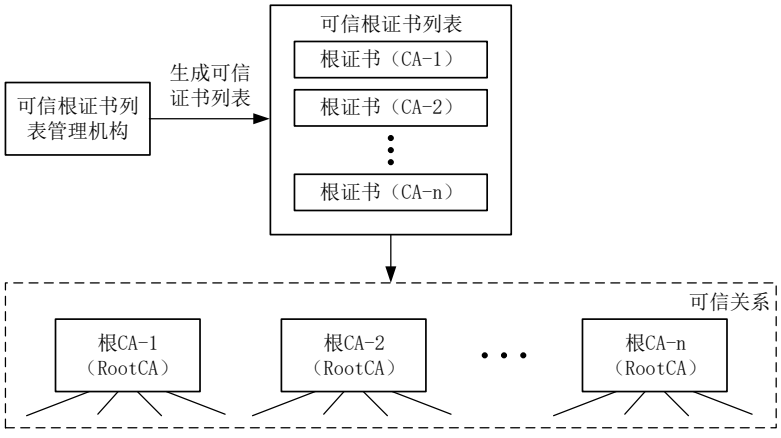

图 4-14　基于可信根列表的 PKI 系统互认

考虑我国现有 PKI 领域的实践，单独的可信根证书列表，在信任域逐渐增多的情况下仍然有可能遇到技术和管理的瓶颈，可采用“严格层次+信任证书列表”的方式，综合两种模式的长处，使车联网信任体系满足统一管理、灵活高效的特点。其思路是首先采用严格层次模型保证所有 PKI 信任域遵从法律法规以及技术和管理的规范，然后采用信任列表模型，将严格层次中部分业务策略和技术能力与车联网业务特殊要求匹配的 CA 纳入车联网的“信任证书列表”体系中。

从信任管理角度，车联网的互信应遵从国家关于网络空间安全治理的总体规划，服从国家对跨行业互信、行业内跨应用互信、应用内跨地域互信的规划，综合考虑车联网信任以及车联网与交通设施、云服务、监管系统等相关系统的跨域互信，建立支持灵活的策略和多种密码技术的信任模型。

除了信任模型的建立之外，PKI 体系的证书生命周期管理依赖于车联网中的异常行为管理机构(MA)来识别存在问题的 V2X 终端，并及时发布黑名单和证书吊销列表(CRL)。在 PKI 互认体系中，跨域的黑名单管理和 CRL 聚合是一个有待研究的关键技术。

4.5 车联网服务平台密码应用案例分析

4.5.1 车联网云平台通用密码应用

车联网服务平台从车载终端、车厂业务平台及运营商平台等获取数据信息，并通过对数据信息的分析和处理，实现车辆故障诊断、服务业务办理以及车辆相关信息管理等应用。实现车厂或经销商用户在车辆售前，售中及售后阶段进行车辆相关的信息管理。目前，许多车企陆续上线车联网“云”服务，包括车载通信、车载娱乐、智能驾驶、人机交互、远程诊断、远程升级、天气预报、信息资讯等。

基于云平台的车联网应用以蜂窝通信为基础，继承了“云-管-端”模式现有的安全风险，包括假冒用户、假冒业务服务器、非授权访问、数据安全风险等。在未经认证的情况下，攻击者可以假冒车联网合法用户身份接入业务服务器，获取业务服务；非法业务提供商可以假冒车联网合法业务提供商身份部署虚假业务服务器，骗取终端用户登录，获得用户信息。在未经访问控制的情况下，非法用户可以随意访问系统业务数据，调用系统业务功能，使系统面临信息泄露及功能滥用的风险，业务数据在传输、存储、处理等过程中面临篡改、泄露等安全风险。

车联网云服务平台的安全架构如图 4-15 所示。

图 4-15　车联网云服务平台安全架构图

车联网服务平台作为数据中心和服务中心,本身容易遭受传统的网络攻击,导致数据泄露等问题,同时云服务平台本身的安全性也值得关注,传统的操作系统漏洞威胁和虚拟化技术的大量运用导致虚拟机的调度、管理和维护均成为重要的安全挑战。云服务平台可以采用各种措施保护数据安全,如云数据加密技术、数据访问控制技术以及对应的完整性保护、数据存在与可用性证明等。

车联网云服务平台本身的系统安全性也是一个重要问题,如虚拟化的安全技术、虚拟机映像文件安全、以及云资源调度访问安全等。云安全密码应用首先需要密码基础设施的支撑，云服务器密码机等可为用户在云环境下提供密码服务；密钥等重要数据需通过 SSL 协议安全传输，并对关键敏感数据进行数字签名和完整性校验；应用密码技术建立用户资源隔离机制，防止资源非授权访问，确保业务接入者及服务者身份的真实性、业务内容访问的合法性，并做好日志审计，确保可追溯性；同时，建设密钥管理体系，进行密钥产生、分发、运算以及销毁等管理，保障车联网用户密钥安全。

车联网云服务平台可以依据网络安全保护等级,参照 GB/T 39786《信息安全技术 信息系统密码应用基本要求》标准来开展进行密码应用设计和密码应用安全性评估，在 GB/T 39786 规定的各个层面综合应用密码算法、密码技术和密码产品，其中有典型的通用密码应用如表 4-8 所示。

表 4-8　车联网云服务平台的典型密码应用

安全目标	典型密码应用	密码标准
电子门禁身份鉴别	机房应部署符合 GM/T 0036《采用非接触卡的门禁系统密码应用指南》的电子门禁系统，采用身份鉴别的密码技术对进出人员进行身份鉴别，保证重要区域进出人员的身份真实性。	● 采用非接触卡的门禁系统密码应用技术指南（GM/T 0036）
电子门禁	机房部署的电子门禁系统，应使	● SM3 密码杂凑算法（GM/T 0004）

安全目标	典型密码应用	密码标准
记录数据完整性	用密码杂凑算法、消息鉴别码（MAC）、数字签名技术等密码技术对电子门禁系统进出记录数据进行完整性保护，其密码功能应确保正确、有效。	
视频记录数据完整性	机房部署的视频监控系统，应使用密码杂凑算法、消息鉴别码（MAC）、数字签名技术等密码技术对视频监控系统的视频记录等数据进行完整性保护，其密码功能应确保正确、有效。	● SM3 密码杂凑算法（GM/T 0004）
身份鉴别	系统的设备和计算安全层面，对登录设备的系管理人员及用户进行身份鉴别，采用密码技术保证鉴别消息的机密性和完整性，实现防截获、防假冒、防重用。	● 基于数字证书的身份鉴别接口规范（GM/T 0067） ● 动态口令密码应用技术规范（GM/T 0021） ● 开放的第三方资源授权协议框架（GM/T 0068） ● 开放的身份鉴别框架（GM/T 0069）
远程管理设备安全	在远程管理设备时，应采用密码技术建立安全的信息传输通道。	● 传输层密码协议(TLCP)（GB/T 38636）
访问控制信息完整性	应使用密码杂凑算法、消息鉴别码（MAC）、数字签名技术等密码技术对系统设备内系统资源访问控制信息（如访问控制列表）进行完整性保护。	● SM2 椭圆曲线公钥密码算法（GM/T 0003） ● SM3 密码杂凑算法（GM/T 0004）
敏感标记完整性	应使用密码杂凑算法、消息鉴别码（MAC）、数字签名技术等密码技术对系统设备中的重要信息资源安全标记进行完整性保护。	● SM3 密码杂凑算法（GM/T 0004）
日志记录完整性	应使用密码杂凑算法、消息鉴别码（MAC）、数字签名技术等密码技术来保证系统设备日志记录的完整性。	● SM2 椭圆曲线公钥密码算法（GM/T 0003） ● SM3 密码杂凑算法（GM/T 0004）
重要程序完整性	应采用密码杂凑算法、消息鉴别码（MAC）、数字签名技术等密码技术对系统设备或系统中的重要可执行程序进行完整性保护，并对其来源进行真实性验证。	● SM2 椭圆曲线公钥密码算法（GM/T 0003） ● SM3 密码杂凑算法（GM/T 0004）
安全管理与运维	除了在技术上提供安全保障，整个体系也从管理、运维方面提供安全支撑。其中安全管理主要在组织、人员、制度以及应急处理	● 信息安全技术 信息系统密码应用基本要求（GB/T 39786）

安全目标	典型密码应用	密码标准
	等方面从管理角度对整个体系进行安全保障。运维保障从日志的记录、审核、责任的追踪、设备环境的维护、数据的备份恢复等方面进行保障。	
密码资源	为车联网业务系统提供基础的密码资源，实现密码资源池的统一管理。	● 服务器密码机技术规范（GM/T 0030） ● 签名验签服务器技术规范（GM/T 0029） ● 云服务器密码机管理接口规范（GM/T 0088） ● 密码设备应用接口规范（GM/T 0018） ● 对称密钥管理技术规范（GM/T 0051） ● 时间戳接口规范（GM/T 0033）
应用安全	保护业务敏感数据的机密性、完整性、真实性等。	● SM4 分组密码算法（GM/T 0002） ● SM2 椭圆曲线公钥密码算法（GM/T 0003） ● SM9 标识密码算法（GM/T 0044） ● SM3 密码杂凑算法（GM/T 0004） ● 分组密码算法的工作模式（GB/T 17964） ● SM2 密码算法使用规范(GM/T 0009) ● SM2 密码算法加密签名消息语法规范（GM/T 0010） ● SM9 密码算法使用规范(GM/T 0080) ● SM9 密码算法加密签名消息语法规范（GM/T 0081） ● 传输层密码协议(TLCP)（GB/T 38636） ● 安全电子签章密码技术规范（GM/T 0031） ● 基于角色的授权管理与访问控制技术规范（GM/T 0032） ● 开放的第三方资源授权协议框架（GM/T 0068） ● 开放的身份鉴别框架（GM/T 0069）

4.5.2 安防和远程诊断服务

汽车制造商与汽车安全系统研发公司一直都在致力于开发汽车安全系统的研究工作，Telematics 系统可以为客户提供安防和远程诊断相关的服务。譬如，OnStar 系统

通过应用全球卫星定位系统（GPS）和无线通信技术为中国的消费者提供广泛的汽车安全信息服务，包括碰撞自动求助、路边救援协助、全音控免提电话、实时按需检测和全程音控领航（Turn-By-Turn Navigation）的多项服务。

在这些信息安全服务中，尤其需要关注网络安全威胁的服务包括：

——车门远程应急开启及锁闭：在客户的身份被验证后，由客户服务顾问帮助客户进行远程应急开启及锁闭；

——车停位置提示：当客户忘记车辆停放地点，可以发出信号让客户车辆鸣号或启动双闪灯；

——目的地设置协助：车主可在出现前呼叫语音服务人员，提前设置好出行路线，在形成过程中将有语音为车主导航；

——路边救援协助：如果客户遇到爆胎、燃油耗尽、蓄电池没电等苦难，只需按下蓝色按钮寻求帮助，客户服务顾问将获取车辆的准确位置，从而指引道路援助人员及时达到并提供帮助；

——被盗车辆减速：服务顾问发送遥控信号，将减小发动机功率时车速减小到怠速状态；

——车况检测报告：用户每隔 30 天将定期收到相应邮件，以了解汽车关键系统的状态，报告内容涉及：发送机和变速箱、安全气囊系统、防抱死制动系统、OnStar 设备终端、轮胎压力等。

分析这些信息服务可以发现，在提供安防和远程诊断服务等过程中，Telematics 系统需要通过 T-Box 终端从汽车采集相关的状态和工作参数，并且还可以通过网络来远程操控汽车的部件。如果攻击者劫持了 Telematics 系统，则可以通过远程发送操控指令，譬如在高速公里的行驶过程中减少发送机功率使得汽车自动减速，这有可能会威胁用户的生命安全。此外，一个不安全的密码协议涉及还有可能导致攻击者可以通过网络来开启车门，从而达到行窃的目的。

安防和远程诊断服务由 Telematics 系统和 T-Box 终端协同来实现，因此需要在 Telematics 系统中应用各种密码技术来保证安防和远程诊断服务的安全，包括应用身份鉴别技术来识别汽车终端和服务平台的身份合法性，采用 SSL 安全通道来保证采集数据及车控指令的机密性和完整性，采用数据加密技术来保证发送给车主的车况检测报告的机密性等等。

安防和远程诊断服务方面可能应用如下相关的密码标准：

- SM4 分组密码算法（GM/T 0002）
- SM3 密码杂凑算法（GM/T 0004）
- 传输层密码协议(TLCP)（GB/T 38636）
- 密码模块安全技术要求（GM/T 0028）

4.5.3 固件安全更新（OTA）

智能网联汽车的一个趋势是“软件定义”汽车。和硬件相比，软件成了车里迭代最快、最容易个性化的部分。随着汽车电子化程度越来越高，无论是车辆遭遇软件故障还是软件更新，目前的线下店召回模式已经不是满足用户体验的最佳选择了。为了减少成本、提升用户体验，OTA（Over-the-Air Technology)空中下载技术成了智能汽车时代的必备技能。

OTA 分为两类，一种是 FOTA（Firmware-Over-The-Air，固件在线升级），指的是给一个设备、ECU 闪存下载完整的固件镜像，或者修补现有固件、更新闪存。SOTA

（Software-Over-The-Air，软件在线升级）是固件之外的软件更新。应用程序和地图OTA，都属于 SOTA 的范畴。

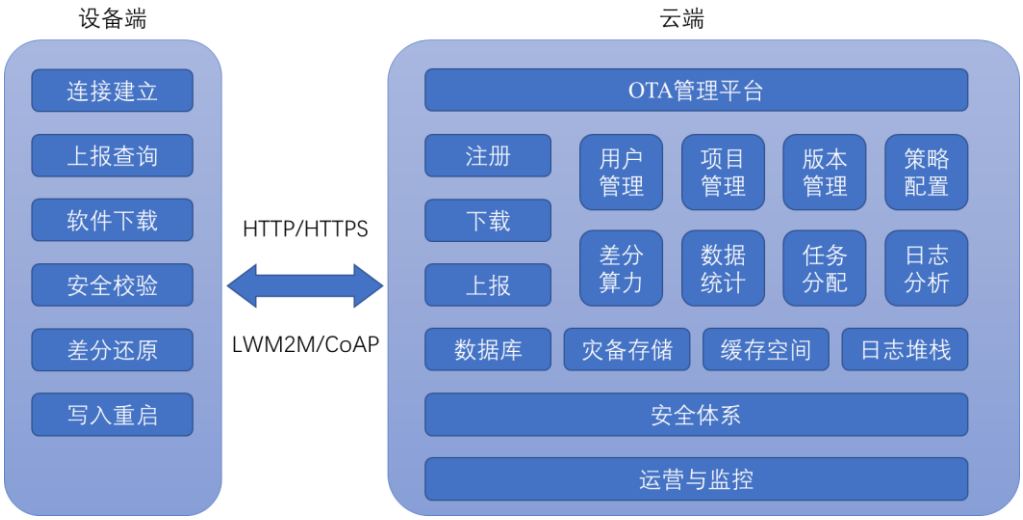

图 4-16　车辆 OTA 升级功能架构

车联网 OTA 升级功能架构如图 4-16 所示。FOTA 和 SOTA 过程可以被分成三个阶段：

第一阶段，云端服务器生成更新包。更新包里不仅仅有要修复的缺陷或者要加入的新功能，分发包的更新顺序、更新前和更新后需要做哪些验证检查等，都会被打包到这个文件里。

第二阶段，传输更新包。更新包生成之后会被发到一个 OTA 云平台。在汽车行业，这个平台一般由 OEM 管理，平台上存放着各种各样、不同版本的更新包。在收到更新请求后，更新包通过网络被下载到合适的车载模块和特定的 ECU。一辆车可能有多个设备需要更新，车端会安装 3G/4G/WIFI 通讯模块，也会由一个网关统一下载接收更新包再做具体分发。车端与 OTA 平台之间会建立安全连接通道（例如：HTTPS），进行双向身份确认，确保更新包安全传输。

第三阶段，安装更新。车端对下载好的更新包进行校验后按照指定顺序安装更新包，整个过程会有更新软件随时监督。

在 OTA 升级的场景下，需要考虑三个方面的安全性：云端的服务器安全、车端安全、车辆和云之间的通讯安全。车载终端、应用程序（APP）与云平台之间需要互相认证对方的身份，当双方身份相互验证合法后，建立通信链路连接（例如：HTTPS，GMSSL）。进行数据传输时，采用加密、认证等安全措施保护关键通信数据的保密性、完整性、可用性和抗重放攻击。云端服务器利用加密机（卡）实现对数据的加密、签名。主要算法为 AES/RSA/SHA、SM2/3/4 等算法。

OTA 固件安全更新方面可能应用如下相关的密码标准：

- SM4 分组密码算法（GM/T 0002）
- SM3 密码杂凑算法（GM/T 0004）
- 时间戳接口规范（GM/T 0033）
- 传输层密码协议(TLCP)（GB/T 38636）
- IPSec VPN 技术规范（GM/T 0022）
- SSL VPN 技术规范（GM/T 0024）
- 密码模块安全技术要求（GM/T 0028）

4.5.4　API 安全防护

现代 Web 编程已经将应用程序的前端（HTML/CSS/JS）从后端（服务器端处理和存储）中分离出来。同样，移动应用程序通常处理应用程序中面向用户的功能，但将数据传递回集中式服务器。这些趋势引发了现在投入生产的 Web API 数量的大幅增加。

应用程序编程接口（API）安全性是使基于 Web 的 API 能够响应请求、安全地处理数据并按预期运行的设计、流程和系统。API 具有独特的威胁模型、安全问题和身份验证模式，这些模型、安全问题和身份验证模式与标准 Web 应用程序不同。API 安全常用的技术手段包括限速、鉴权、审计等。在调用 API 的过程中，应用数据加密、数据签名、添加时间戳等密码技术来保证数据在传输过程中的安全性、判断数据是否到达服务器以及服务器如何识别传到服务器的数据是否正确。

目前尚未发布 API 安全方面的密码行业标准，但是在解决 API 安全防护方面可能应用如下相关的密码标准：

（1）API 鉴权：

- 安全认证网关产品规范（GM/T 0026）
- 动态口令密码应用技术规范（GM/T 0021）
- 基于口令的密钥派生规范（GM/T 0091）
- 基于角色的授权管理与访问控制技术规范（GM/T 0032）
- 开放的第三方资源授权协议框架（GM/T 0068）
- 开放的身份鉴别框架（GM/T 0069）

（2）数据传输加密：

- SM4 分组密码算法（GM/T 0002）
- SM3 密码杂凑算法（GM/T 0004）
- SM2 密码算法加密签名消息语法规范（GM/T 0010）
- 分组密码算法的工作模式（GB/T 17964）
- 密钥管理（GB/T 17901）
- 传输层密码协议(TLCP)（GB/T 38636）
- SSL VPN 技术规范（GM/T 0024）
- 密码模块安全技术要求（GM/T 0028）
- 密码随机数生成模块设计指南（GM/T 0078）
- 对称密钥管理技术规范（GM/T 0051）
- 云服务器密码机管理接口规范（GM/T 0088）

（3）安全审计：

- 时间戳接口规范（GM/T 0033）

4.6 车联网业务系统密码应用案例分析

4.6.1 “车-桩”联网充电

“车-桩”联网服务平台涉及个人移动终端安全，包括个人用户智能手机、平板电脑等移动终端，其上安装充电 APP，存在感染病毒等恶意代码并导致 APP 被篡改、移动终端存储数据泄露等风险。为保证移动终端上安装的应用正常运行，移动应用中应增加关于操作系统版本及应用下载渠道的提示，对发布程序采取文件加密、结构混淆等方法保证 APP 软件的完整性，防止被篡改；对 APP 软件进行加密保护（文件加密、文件保护、内存保护、库文件保护等），防止 APP 被反编译；采用移动安全沙箱技术实现移动终端上的移动应用数据与移动终端其他应用数据之间的可靠隔离。

充电桩采用 APN+VPN 的无线虚拟公网通过信息网络安全接入网关安全接入，配备专用物联 SIM 卡，并安装支持 SM 系列密码算法的专用安全芯片，使用安全接入设备、隔离交换设备等进行安全接入。充电桩接入“车-桩”联网平台的协议采用结构化和标准化，并预留安全芯片接口，实现安全芯片和充电桩的绑定和充电桩的接入认证。

“车-桩”联网平台与充电运营商系统相互通过接口调用进行数据交互，遵循中国电力企业联合会 T/CEC 102.1-2016 标准安全防护措施。

在数据安全方面，“车-桩”联网服务平台涉及充电桩数据、用户档案数据、清分结算数据、充电桩控制指令、订单数据、支付数据等重要采集类、参数设置类、控制类业务数据，建议采用 SM 系列密码算法保证存储安全。另一方面，服务平台中涉及的手机号码、个人身份证号码、银行卡号等为客户敏感信息，为客户端提供数据访问时对敏感字段在服务器端进行脱敏处理。“车-桩”联网服务平台将启动充电、停止充电等控制指令经安全接入区由运营商无线虚拟专网通道下发各充电桩，用户手机通过互联网通道以 HTTPS 加密的方式将充电请求策略发送至于车联网服务平台。“车-桩”联网平台与外部财务管控系统、短信平台、电子发票系统、银行支付平台、第三方支付平台、运营商系统等系统进行业务交互时，根据接口访问策略限制客体的访问权限，接口数据连接建立之前进行认证，认证方式采用共享口令或用户名 / 口令或数字证书等方式。

“车-桩”联网服务平台可能应用如下相关的密码标准：

- SM4 分组密码算法（GM/T 0002）
- SM2 椭圆曲线公钥密码算法（GM/T 0003）
- SM9 标识密码算法（GM/T 0044）
- SM3 密码杂凑算法（GM/T 0004）
- 基于口令的密钥派生规范（GM/T 0091）
- 传输层密码协议(TLCP)（GB/T 38636）
- 安全认证网关产品规范（GM/T 0026）
- 时间戳接口规范（GM/T 0033）

4.6.2 基于区块链的车险应用

由于车辆的增多，发生交通事故的几率将大大提高。车辆维修时会给我们造成诸多不便。车险能够在我们车辆发生交通状况的时候为车子进行核赔，若没有发生交通事故，车险也可以来预防未知的风险。

在传统的车辆保险当中，保险公司运作的挑战在于前面的核保与后面的核赔。由于车辆的状况千差万别，司机的驾驶行为也是参差不齐，要如何精准的确定价格，对于业务的品质有着巨大的影响。一旦发生了交通事故，要用何种方式来确定事故的真实性与合理性，如何进行准确的理赔和规避保险诈骗，都是理赔部门要面临的巨大难题。

区块链技术在车险中也可以起到辅助的作用。由于区块链不可篡改的特性，确保了用户信息的真实性，所以，当中节省了保险公司调查用户信息真实性的工作。依托区块链技术和车联网技术，在车辆上安装相应传感记录设备，保证信息的真实、准确和不可篡改，在出险时，实时或准时地将车辆事故数据提交给应用区块链技术的“事故认证平台”系统，在核验后满足特定条件下会自动触发理赔付款。

区块链的智能合约模块本质上是一套互联网程序，通过计算机代码实现每个区块中智能合约的构建、存储和执行。在智能合约中，只要参与方达成协定，智能合约就会建立起各方的权利和义务，然后通过计算机网络自动实行合约。区块链的智能合约技术在智能车险场景中有着极大的运用空间。无论是现在的传统驾驶的车辆保险，还是车路协同自动驾驶环境下汽车保险的销售、购买和赔付等场景，当车辆发生意外需要进行理赔

时，车险使用越方便、效率越高，就能够促进车主对车辆保险的信任和整个汽车行业运行水准的提升与发展。

此外，通过 OBD 车载智能终端实时监控里程、油耗等车辆数据，结合车主“三急”次数、违章次数等驾驶行为数据，通过大数据技术处理，评估车主驾车行为的风险等级，进而通过风险等级指数为每位车主提供定制化的保单，保费是取决于车主实际行驶里程、驾驶时间、行驶地点、具体驾驶行为等指标的综合考量。

区块链+车险场景下可能应用如下相关的密码标准：

- SM4 分组密码算法（GM/T 0002）
- SM2 椭圆曲线公钥密码算法（GM/T 0003）
- SM9 标识密码算法（GM/T 0044）
- SM3 密码杂凑算法（GM/T 0004）
- 安全电子签章密码技术规范（GM/T 0031）
- 时间戳接口规范（GM/T 0033）

4.6.3 APP 应用的安全分发

车联网中移动终端通过 APP 完成对车辆的控制，如门锁、远程启动车辆等功能。而此类 App 因为广泛应用而且易于获取成为了攻击者的攻击入口，例如攻击者可以通过反编译技术获取通信密钥、分析通信协议等，并结合远程控制系统进一步控制车辆。另一方面，Android 或 IOS 系统 APP 均存在被攻击者植入恶意代码的风险，当移动终端和车辆进行无线通信时，终端 APP 可以作为跳板进一步渗透进入智能汽车内部，从而窃取用户隐私信息或者威胁汽车行驶安全。因此其直接影响到车联网系统的安全。

为防止移动终端软件 APP 代码被恶意篡改，发布应用时考虑使用多重代码签名的机制，包括开发者签名，应用市场签名等。代码签名技术采取商用密码算法，对移动终端代码的指纹数据签名，一旦数据变化，指纹数据签名将验证失败。

应用代码签名技术主要涉及生成代码签名和验证代码签名两个阶段。

生成代码签名阶段指在 APP 发布之前，使用权威数字证书进行签名，并且把签名文件和移动终端软件进行绑定，为以后的验证提供依据。基于商用密码算法，对开发者提供的移动 APP 的 APK 资源、APP 名称、版本号、著作权人以及 APP 首次发布时间等信息进行数字签名，并形成独立的签名文件，与操作系统原有的验证机制无关。代码签名保证软件版本信息的完整性和来源可追溯。生成代码签名的流程如图 4-17 所示:

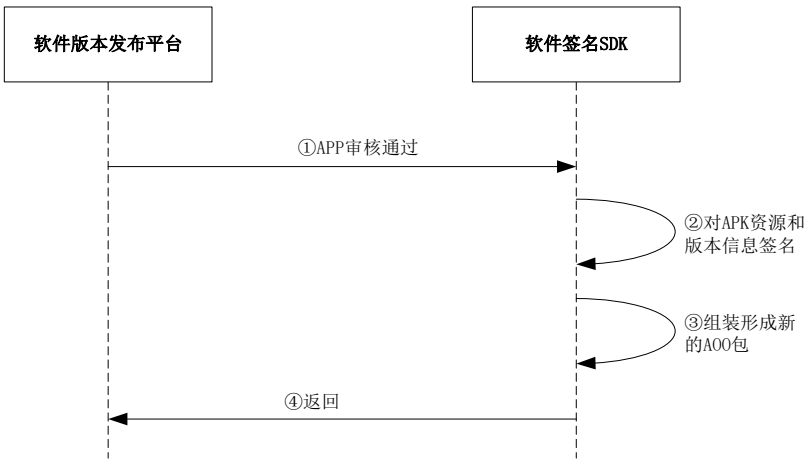

图 4-17　生成代码签名的流程示意图

生成代码签名需要执行如下几个步骤：

a）开发者提交所申请APP的原始资料和带自签名的APK资源到软件版本发布平台，发布平台进行认证和审核后，为APP颁发带版本登记证书；

b）由软件签名SDK对APK资源和版权信息进行数字签名，形成独立的签名文件；

c）签名文件与原APP组装，形成新的APP资源包；

d）保存新的APP资源包，并发布，返回成功信息到申请方。

验证代码签名的阶段主要通过验证电子签名的有效性，进而核实APK来源的真实性和程序数据、版权信息的完整性。验证代码签名的流程如图4-18所示:

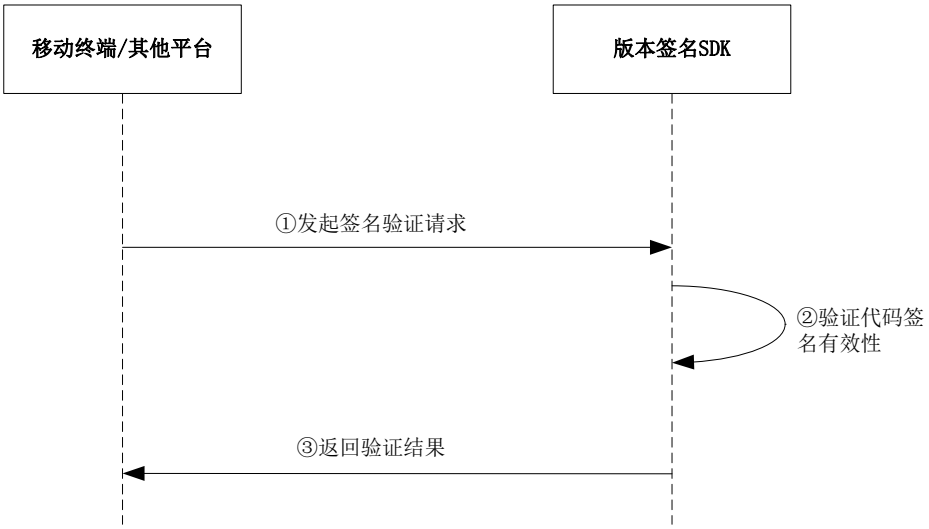

图4-18　验证代码签名的流程示意图

验证代码签名需要执行如下几个步骤：

a）移动终端或其它服务平台发起签名验证请求，调用版本签名SDK的签名验证接口；

b）由版本签名SDK完成签名有效性的验证；

c）将验证结果返回签名验证请求方。

APP安全分发方面可能应用如下相关的密码标准：

- SM2椭圆曲线公钥密码算法（GM/T 0003）
- SM9标识密码算法（GM/T 0044）
- SM3密码杂凑算法（GM/T 0004）
- 时间戳接口规范（GM/T 0033）

4.6.4　用户身份管理

车联网云服务平台承载了车联网相关的业务系统，除了Telematics系统之外，汽车终端还需要从数据和内容提供商、公共与行业服务提供商、通信服务提供商等参与方提供的业务系统获取相关服务。

汽车网关、车载T-Box和车载信息娱乐系统（IVI）在与远程服务平台（Telematics）进行通信时，需要互相认证对方的身份，当双方身份相互验证合法后，建立通信链路连接。进行数据传输时，采用加密、认证等安全措施保护关键通信数据的保密性、完整性、可用性和抗重放攻击。

身份识别与访问管理（IAM）通过为车联网中每个用户赋予一个身份，定义和管理各种用户的角色和访问权限，以及规定用户获得授权（或被拒绝授权）的条件，并确保数字身份在用户的整个“访问生命周期”存续期间都应受到良好的维护、调整与监视。

车联网中引入了证书管理系统（如本报告 4.6 节所述），可以为 V2X 设备颁发注册证书、假名证书、应用证书和身份证书等各种类型的业务证书，这是典型的数字身份。CA 机构也可以为路侧单元（RSU）、Telematics 云服务平台颁发 SSL 服务器证书，用来标识这些角色的可信身份。

除了基于数字证书的数字身份，还会涉及其他的设备身份，如可以通过 SIM 卡来标识用户使用的移动终端的可信身份。

此外，由于不同应用中对于身份信息的信任程度提出了不同的需求，需要用户披露的身份信息也有所不同，因此有必要定义数字身份的分类和分级，并规定不同安全保障级别数字身份的技术标准和管理规程。目前已有标准在研究车联网的数据分类分级，但是还没有车联网领域数字身份的相关研究和标准活动，这是一个值得深入研究的课题。

为用户提供身份识别与访问管理（IAM）服务，需要在车联网云服务平台中引入身份服务提供商（IdP），联合可信身份源（如为自然人、法人单位颁发法定身份的管理部门）、可信第三方（如电信运营商、银行机构等）实现对车主、V2X 设备、服务提供商数字身份的统一管理。

身份服务提供商（IdP）为用户提供数字身份的生命周期管理，提供身份核实、发放身份凭证、身份鉴别等服务。IdP 在这些不同环节中涉及到大量的密码技术和密码产品，譬如为用户提供统一身份认证、单点登录（SSO）等服务，需要采用符合国家标准、行业标准的密码算法和密码协议。

身份服务提供商提供的典型服务包括：

- 统一身份认证

统一身份认证系统提供用户身份认证服务、用户实名验证服务、应用身份认证服务，确保用户访问应用系统时用户身份、应用身份的真实性。统一身份认证系统提供多种身份认证凭证，包括数字证书，生物特征、用户口令、短信等；支持多次认证凭证及认证因子自由组合进行身份认证；支持通过公安、社保、运营商等对用户身份进行实名验证。同时根据用户当前使用的身份凭证划分安全等级，当应用系统需要用户更高等级的身份凭证时，对用户进行二次身份认证。通过统一身份认证系统，建立全网一致的身份认证、实名验证服务，实现“一次认证、全网通行”。

- 单点登录

单点登录服务提供支持 Web 应用、C/S 应用、App 应用等多种应用类型的单点登录服务，使用户只需登录一次就可以访问所有的应用系统。一般应支持 Oauth2.0、OpenID、SAML、Web Service 等多种单点登录协议，建立全网的单点登录服务，实现“一次登录、全网访问”。

- 访问控制

访问控制是安全接入的重要功能之一，是继用户身份认证后，对用户进行控制的另一道屏障，主要确定合法用户有哪些访问权限。访问控制系统基于策略下载权限信息进行访问控制，系统发布鉴权服务为访问控制系统提供在线鉴权鉴别功能，实现“一次认证，按权访问”。

安全接入应支持基于角色的访问控制和权限管理，确保资源受控访问，并提供完善的日志功能，便于事后审计。访问控制策略的完整性应采用消息鉴别码（MAC）、数字签名技术实现。访问控制策略完整性保护应采用 SM3 密码杂凑、SM2 签名算法，重要数据加密应采用 SM4 算法。

车联网业务系统的用户身份管理方面可能应用如下相关的密码标准：

- SM4 分组密码算法（GM/T 0002）
- SM2 椭圆曲线公钥密码算法（GM/T 0003）
- SM9 标识密码算法（GM/T 0044）
- SM3 密码杂凑算法（GM/T 0004）
- 安全认证网关产品规范（GM/T 0026）
- 基于角色的授权管理与访问控制技术规范（GM/T 0032）
- 基于数字证书的身份鉴别接口规范（GM/T 0067）
- 开放的第三方资源授权协议框架（GM/T 0068）
- 开放的身份鉴别框架（GM/T 0069）

4.7 车联网数据安全密码应用案例分析

4.7.1 汽车数据采集与处理安全

车联网中的数据种类包括用户身份信息、汽车运行状态、用户驾驶习惯、地理位置信息、用户关注内容等敏感信息，在车辆保险、用户行为分析等方面具备很大价值，将是未来车联网安全重点。

在汽车数据安全管理领域出台有针对性的规章制度，明确汽车数据处理者的责任和义务，规范汽车数据处理活动，是防范化解汽车数据安全风险、保障汽车数据依法合理有效利用的需要，也是维护国家安全利益、保护个人合法权益的需要。国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部联合发布的《汽车数据安全管理若干规定（试行）》，旨在规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用。《汽车数据安全管理若干规定（试行）》倡导个人信息和重要数据的车载端本地化存储及本地化处理，确有必要向车外提供的，应本着脱敏处理原则，尽可能地进行匿名化和脱敏处理，这对车载芯片计算能力及车辆本地存储能力提出了更高的要求。

车联网大数据分析是一个从信息到数据再到信息的过程，包括搜集、分析、传播和利用等环节，其中每一个环节的疏漏都可能造成个人隐私的泄露。大数据的潜在利益让敏感信息数据安全问题面临着极大的挑战。特别是近年来云服务的出现，大量的个人敏感信息数据都存放于网络空间，增加了敏感信息数据泄露的风险。在将大数据迁移到云环境中时，可能会失去对大数据的安全控制，导致对安全边界之外的数据缺乏必要的控制，这将进一步导致大数据安全防护问题的复杂化。

车联网大数据处理主要面临如下安全风险：1）传输和存储环节存在数据被窃风险；2）数据过度采集和越界使用成为隐私保护主要问题；3）数据跨境流动问题成为威胁国家安全潜在隐患。

在敏感信息中，信息隐私（或隐私信息）是极其敏感的信息，更需要加强保护。个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。《中华人民共和国民法典》和《网络安全法》对隐私和个人信息及其权利保护进行了规定。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。

隐私保护是大数据安全研究中的一个主要问题。当前，信息隐私泄露、个人信息泄露等安全问题使得对大数据隐私保护的研究较多，不少研究关注于数据隐私保护框架和数据匿名处理等方面。隐私保护框架方面，目前涌现了大量的面向静态数据的隐私保护模型、面向动态数据连续发布的隐私保护模型。数据匿名化方法通过删除敏感数据以保护用户隐私，传统的匿名化方法包括 k-Anonymity、t-Closeness 和 l-Diversity 等方法[14]。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。信息处理者不得泄露或者篡改其收集、存储的个人信息。根据 GB/T 35273-2020《信息安全技术 个人信息安全规范》标准的要求，传输个人敏感信息在传输和存储等环节均应采用加密等安全措施。信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失。

数据加密能确保大数据的机密性，但传统的加密算法存在密钥管理复杂、计算开销过大等方面的不足。一些新兴的加密体制能解决大数据面临的安全问题。属性加密体制将用户的属性与数据属性相关联，只有满足解密数据属性的用户才能获得加密的数据，因此它能提供数据的保密性，提升数据的服务效率。代理重加密算法体制能实现数据解密权限的传递，提供消息的保密性和访问控制的灵活性，不会泄露加密数据的内容。全同态加密在不解密数据的前提下，能对加密数据进行检索、比较等操作。可搜索加密技术能实现密文数据的查询和相关排序。但新兴密码体制如何适应车联网大数据应用场景的数据规模和数据增长速度仍需要进一步深入地研究，例如需要解决效率低下的问题。

对于敏感信息而言，数据的彻底删除是实现数据安全的重要保障，如果数据销毁不彻底，极有可能会带来敏感信息泄露的风险。当云端的大数据存储到其他存储空间后，同时确定数据不再使用时，应对数据进行清除。在云环境下，用户失去了对数据的物理存储介质的控制权，无法保证数据存储的副本同时也被删除，导致传统删除方法无法满足大数据安全的要求。因此，如何保证被删除的数据确实被删除，即保证数据可信删除，是一个重要挑战。

在云环境下，大数据中的敏感信息被第三方（云数据存储平台）缓存、复制和存档，而这些数据往往没有真正被用户控制，在网络和云存储系统中，正确删除数据并清除所有痕迹的操作通常是无法预见的，数据可信删除技术在大数据安全保护中是十分关键的，数据的可信删除技术也是未来大数据安全技术的研究要点。

4.7.2 地理信息安全

随着人工智能等技术的广泛应用，车联网领域的自动驾驶等业务对高精度地图和导航定位的需求愈加旺盛。普通地图精度为数米以内，而高精地图则可以精确到厘米级别，基于高精地图的高精定位成为支撑自动驾驶、无人机快递等业务位置与导航服务的关键。高精地图和高精度定位涉及国家安全，目前其数据产品按照涉密测绘成果进行监管，而在实际应用过程中存在着一定的泄露风险。

地理信息保密处理技术是保障涉密地理信息安全应用的关键技术，主要采用特定手段对涉密地理信息的空间位置、精度、属性、相邻关系等进行偏移、变形、伪造、隐藏等处理。脱密后的地理信息数据仍具有一定的敏感属性，还需要在 GIS 系统中采用密码技术来实现数据加密和访问控制。

车联网中应用 GIS 系统，需要加密的数据包括数据库中存储的静态地图数据、通过网络传输的地理信息数据、V2X 设备在移动过程中产生的数据（如运动轨迹）等。在服务端，可以采用密码技术来实现静态数据的安全，如对磁盘数据的加密、采用加密数据库、采用应用内加密等。在客户端采集的地理信息数据也要加密后存储在移动终端。客

户端通过与 GIS 服务器建立 SSL 安全通道，识别 GIS 服务器的身份，同时保证客户端与 GIS 服务器之间传输地理信息数据的机密性、完整性和认证性。

4.7.3 敏感信息存储加密

敏感信息存储的安全在数据生命周期中占有很重要的位置，数据创建以后如果没有进行安全的存储，则极易引发泄露和丢失。敏感数据保存应确保在安全的环境中，在需要的情况下还应该加密存储。

针对 Telematics 信息服务平台的用户身份信息、汽车运行状态、用户驾驶习惯、地理位置信息、用户关注内容等敏感信息，这些敏感信息可能存储在服务的数据库系统中，也可能存储在大数据平台（Hadoop）中分布式地存储。对于这两种情况要采用不同的安全策略和密码技术。

- 数据库加密

采用数据库加密技术可以实现数据库数据的加密存储、访问控制、应用访问安全、权限隔离等功能。数据库数据的加密可采用透明加密技术，即加密不改变应用，业务程序透明访问加密数据。在权限控制方面，应支持实现基于密文、独立于数据库权限体系的独立权限控制，防止 DBA 及高权限用户访问敏感数据。在访问控制机制方面，采用数据库管理员、安全管理员和审计管理员三权分立管理，收回超级管理员等特权用户的权限，防止因权限过大引起安全隐患。

- 分布式存储加密

数据加密是保障大数据存储安全的主流方法，对大数据进行加密处理后再存储。使用的技术包括基于属性的加密、同态加密等。同态加密技术是云计算安全技术体系的关键技术。同态加密应用在大数据环境中，特别是与安全多方计算相结合，既能满足数据应用的需求，又能保护用户隐私的安全，是一种理想的解决方案，对于大数据环境下的数据机密性保护具有独特的优势。然而对于海量数据来说，加解密操作不可避免会带来无法忽略的额外开销，需要研究解决如何实现高速低时延的密码服务。

对数据存储的访问建立完善的身份鉴别和访问控制机制，通过密码技术保证授权用户身份的真实性及权限访问控制列表的完整性。

安全级别要求较高的重要信息系统，应针对数据建立完善的权限分级机制，建立基于 IP、应用等因素的完善的安全访问控制机制，保证用户仅可访问权限范围内的敏感信息，应采用密码技术保证访问控制列表的完整性。

此外，还应建立完善的数据访问审计规则，通过数字签名技术保证数据操作的可追溯性。

4.7.4 安全审计

安全审计主要是指对车联网信息服务系统中信息安全相关事件进行记录、分析，并针对特定信息安全事件采取相应的动作。信息安全审计的记录用于检查系统上发生了哪些与安全有关的活动，哪个实体对这个活动负责。

安全审计中应记录的安全事件包括：重要区域出入的身份鉴别事件、网络边界/重要网络节点的的身份鉴别事件/访问控制事件、实体的身份鉴别事件/访问控制事件/重要系统资源敏感标记的变更事件等。

安全审计中应可应用如下密码技术：

——使用密码技术对审计记录进行完整性保护，防止篡改；

——使用密码技术对审计记录进行签名，防止抵赖；

——审计信息中的敏感或隐私内容进行加密，防止泄露；

——审计信息的访问应建立完善的权限管理机制，防止非授权访问。

4.8 车联网密码应用中的待研究问题

在上述章节中分别从智能网联汽车、V2X 通信网络、车联网服务平台等层面分析了密码技术在车联网中的典型应用，同时还分析了车联网中 PKI 体系的应用。然而，如何在车联网中规范、有效地应用密码技术尚缺乏技术标准，并且车联网领域还提出了很多不同于其他领域的密码应用需求，还需要通过技术研究和标准制定来克服存在的诸多问题，才能更好地利用密码技术保证车联网的信息安全和数据安全。

4.8.1 V2X 设备的 HSM 技术规格

SCMS 系统假定加密私钥以及其他对安全和隐私敏感的材料在安全硬件中安全存储和使用。

在引入 Butterfly 密钥扩展机制之后，OBU 中的硬件密码模块（HSM）的设计与传统 PKI 体系存在较大差别。对于假名证书的用户私钥，应在 HSM 中安全存储用户私钥的种子，并且须在 HSM 内部执行密钥扩展运算，在 OBU 切换证书时同时切换 HSM 内部派生的用户私钥。在证书签发与激活阶段，HSM 内部还需要利用加密私钥种子及其派生私钥来解密 PCA 返回的响应报文，获得假名证书的明文。尽管密码行业规范中规定了密码模块的技术要求，但是还需深入研究 Butterfly 机制对于密码模块的安全带来哪些新的安全威胁，并研究对于密码模块的技术要求有哪些标准化需求。

4.8.2 轻量级密码算法

在汽车电子产品中，尤其是车内的通信网关及 ECU 等部件，都是嵌入式产品，通常采用单片机作为处理器。这些部件在通信能力、数据处理能力等方面都受到成本的制约，同时可以使用的存储空间往往较小。考虑到各种设备的功能需求，能耗必须限制在某个范围之内。现有的 SM 系列算法在此类汽车电子产品中应用，并不能获得较好的性价比，甚至无法满足这些产品的安全需求。譬如，SM4 分组加密算法的密钥长度、加密轮数等都并不是针对资源受限的产品而优化，因此在这些场景下应用 SM4 算法，往往无法满足功耗的约束条件，还可能无法满足实时性指标的要求。

应用轻量级密码，可以使得 ECU 部件在通信能力、数据处理能力受限的条件下，满足功耗的约束条件，并满足实时性指标。此外，OBU、T-Box、中央网关、各域控制器等部件都需要应用车规级安全芯片，满足 SM 系列算法在汽车电子产品中应用，获得较好的性价比，满足这些产品的安全需求。

4.8.3 提升身份认证管理的效率

在 V2X 通信网络层面，实体通信的报文大小是受限的，报文的验证也需要在非常短的时间完成，因此，既不可能在通信中包含完整的证书链、证书吊销信息，时间上也不允许在接收到报文后再去下载所需的信息，因此，应设计各种协同工作的机制，包括利用边缘计算等方式。

在车联网 PKI 体系建设中，实体（例如车辆）在与其它实体通信时，无法预先知悉对端实体是哪个信任域的，且车辆通常在高速行进中也没有足够的时间预先对此进行询问。因此，实体必须支持自动、高效对其它信任域实体通信数据包进行验证签名、验证证书的能力，并在验证其它信任域的证书时，能够自动建立完整的信任链，检查证书是否被吊销，因此对终端性能提出挑战。

相对于电子政务、电子商务，在车联网中车辆、路侧单元都会更多、更频繁与其它信任域的车辆和路侧单元、交通基础设施、云端平台等进行交互通信，因为，迫切需要建立完善的互信体系，解决车联网中频繁发生的跨域互通互认问题。

在车联网中需要建立异常行为管理机制，规范 V2X 设备提交的不当行为报告的格式，同时还要研究跨域的黑名单管理机制，研究多 PKI 域的 CRL 的聚合技术等等。

4.8.4 隐私保护与数据安全

在数据安全层面，车联网会产生大量的数据，而车辆位置的移动性，很大可能会造成数据存储在各种不同的网络位置，由不同实体掌握。因此，需要设计数据的安全存储、安全传输、安全处理机制，如何支撑车联网数据安全，是一个迫切需要研究的问题。

5 车联网相关标准研究

5.1 国际标准研究

5.1.1 主要标准化组织

国际上各个标准化组织都有涉及车联网不同层面的标准制定工作，其中与信息安全相关的标准活动概括如下：

- ISO

在国际标准化组织（ISO）下，道路车辆技术委员会（ISO/TC 22）、智能运输系统技术委员会（ISO/TC 204）针对智能网联汽车相关技术标准的研究和制定达成共识和协调。ISO/TC 22 侧重基于车辆自身装置而进行信息采集、处理、决策和行为的车辆技术领域；ISO/TC 204 侧重基础道路交通设施的信息传递以及交通管理信息化方面；车辆与道路交通设施的通信及信息共享方面，由 ISO/TC 22 和 ISO/TC 204 两个技术委员会进行沟通与协调。

此外，ISO/IEC JTC1 SC27（信息安全、网络空间安全和隐私保护技术委员会）的 WG3（安全评估、测试和规范工作组）中，《基于 ISO/IEC 15408 的网联汽车信息安全测评准则》标准研究项目，旨在基于 ISO/IEC 15408 标准，分析网联汽车面临的安全威胁和安全目标，提出安全要求和安全功能组件。

- ITU-T

ITU-T 成立了专门的 SG17 来主要负责通信安全研究与标准制定工作。在 ITU-T SG17 工作组已经开展了对智能交通，以及联网汽车安全的研究工作。

- WP.29/GRVA

联合国世界车辆法规协调论坛（UN/WP29）的自动驾驶车辆工作组（GRVA）制定了有关以安全为核心来指导联合国自动驾驶汽车监管工作的框架文件。

- 3GPP

3GPP SA3 在 REL 14 开始进行 LTE-V2X 安全的研究和标准化工作，形成了 3GPP TS 33.185 Security aspect for LTE support of Vehicle-to-Everything (V2X) services 标准规范，规定了 LTE-V2X 的安全架构以及安全机制。目前 3GPP SA3 在 REL 17 开始研究 eV2X 的安全，主要围绕 5G-V2X 的安全需求和安全关键问题进行研究。

- IEEE

IEEE 1609 系列协议是 WAVE 的高层协议，其中 IEEE1609.2 定义了 WAVE 的安全消息格式，规范了 WAVE 安全服务的实体，以及实体之间的通信机制。

- ETSI

2008 年 12 月欧盟发布欧洲实施智能交通系统（Intelligent Transport System，简称 ITS）行动计划，该计划是一个重要的 ITS 发展政策指导性文件。欧盟采用授权法案的形式来推动标准的研究和制订，授权欧洲标准化组织在法案规定的时间内制定一系列标准、技术规范和技术报告，支持将在欧盟广泛实施和部署可互操作的合作 ITS 系统。

ETSI ITS 安全构架包括几个不同的层次，一部分是安全应用层的服务，通过信息签署和认证，结合数据的加解密实现管理，即为安全服务处理，简称 SA。第二部分是安全管理方面，即通过注册和认证建立起 ITS 网络服务，然后实施身份识别管理。第三部分是报告错误行为方面。最后一部分是 HSM 安全要求。

为实施更为安全的保护，ETSI ITS 技术委员会制定了相应的技术规范（简称 TS），该技术规范主要包括安全架构、安全服务、安全管理、隐私保护等方面。主要是 ITS 安全架构与管理以及通讯管理方面，不仅能够实现抽象层面的安全需求，同时可以最大程度上降低安全风险。其中安全服务方面，由系列标准 ETSI TS 102 94x 提供，通过该标准可实现加密认证的跟踪和机密性数据获取，另外还包括消息的内容和签名等。

- 美国汽车工程师协会 SAE

SAE 于 2016 年发布了《信息物理汽车系统网络安全指南(Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)》（SAE J3061），该指南文件定义了完整的生命周期过程框架，将网络安全贯穿了从概念阶段到生产、运营、服务和退役的所有生命周期，为开发具有网络安全要求的汽车电子系统提供了重要的依据。

5.1.2 安全管理标准及通用方法论

5.1.2.1 ISO 标准

- Road vehicles—Cybersecurity Engineering（道路车辆-信息安全）（ISO/SAE AWI 21434）

ISO/SAE AWI 21434 标准，主要从风险评估管理、产品开发、运行/维护、流程审核等四个方面来保障汽车信息安全工程工作的开展。对应分设四个项目组（Project Groups）同步开展工作：威胁分析和风险评估管理（Risk Management）、产品开发（Product Development）、运行/维护（Operation，Maintenance and Other Process）、流程协调（Process Overview and Interdependencies）。目标是通过该标准设计、生产、测试的产品具备一定信息安全防护能力。

- Road vehicles—Functional safety（道路车辆-功能安全）（ISO 26262）

ISO 26262 系列标准是 IEC 61508 对 E/E 系统在道路车辆方面的功能安全要求的具体应用。ISO 26262 标准站在系统和全生命周期的高度，统筹电子电气系统的功能安全，从提出产品概念阶段开始，覆盖系统开发、硬件开发、软件开发、生产运行和售后支持，以系统的方法，指导产品全生命周期的安全事项的实施。该标准适用于所有提供安全相关功能的电力、电子和软件元素等组成的安全相关系统在整个生命周期内的所有活动。

ISO 26262 侧重于功能安全 – 确保汽车零部件能够在正确的时间发挥正确的功能。其专门针对汽车提供方案，用于确定 ASIL 风险等级。ISO 26262 的汽车安全完整性等级 (ASIL)基于三个变量：严重程度、接触概率和驾驶员可控性。ISO 26262 假定车辆有人驾驶，因此不直接涉及完全自动驾驶的车辆。

5.1.2.2 SAE 标准

- 信息物理融合系统网络安全指南（J3061）

《安全指南》旨在通过统一全球标准，来推动汽车电气系统与其他互联系统之间安全流程的建立。《安全指南》详细定义了一个结构化的网络安全流程框架，用于指导建设安全要求极高的计算机系统。

5.1.2.3 UN/WP29 系列标准

联合国世界车辆法规协调论坛（UN/WP29）的自动驾驶车辆工作组（GRVA）制定了有关以安全为核心来指导联合国自动驾驶汽车监管工作的框架文件。

- 《信息安全与信息安全管理系统》

本法规适用于与信息安全相关的 M 类、N 类、至少装有 1 个电控单元的 O 类以及具有 3 级以上自动驾驶功能的车辆。“信息安全”是指道路车辆及其功能受到保护，使其电子电气元件免受网络威胁；“信息安全管理系统（CSMS）”是一种基于风险的系统方法，定义了组织过程，职责和治理，以处理与对车辆的网络威胁相关的风险并保护其免受网络攻击。

法规包括信息安全相关的一般要求、CSMS 合格证书、管理审批等内容，并提出了详细的信息安全威胁、漏洞、攻击方法，以及对应缓解措施，为汽车行业实施必要的流程提供了一个框架：

a) 识别和管理车辆设计过程中的信息安全风险；
b) 验证风险是否得到管理，包括测试；
c) 确保及时进行风险评估；
d) 监控网络攻击并有效应对；
e) 对成功或未遂的攻击进行分析；
f) 根据最新的威胁和漏洞评估安全措施是否仍然有效。

- 《软件升级与软件升级管理系统》

本法规适用于允许软件升级（更新）的 M 类、N 类、O 类、R 类、S 类、T 类车辆。“软件升级”是指用软件包将软件升级或更新到新的版本（包括更改配置参数）；“软件升级管理系统（SUMS）”是一种通过定义组织过程和程序，以符合本法规软件升级要求的系统方法。

法规主要包括有关软件升级过程的车辆类型批准申请、标识、SUMS 合格证书、RX 软件标识号（RXSWIN）、一般要求等内容，为汽车行业实施必要的流程提供了一个框架：

a) 记录与车辆类型有关的硬件和软件版本；
b) 识别与型式批准有关的软件；
c) 验证零部件上的软件；
d) 识别相互依赖性；
e) 确定车辆目标，并验证其更新兼容性；
f) 评估软件更新是否影响型式批准或合法定义的参数；
g) 评估更新是否影响安全或安全驾驶；
h) 向车主通报最新情况；
i) 记录以上所有内容。

5.1.2.4 ITU-T 系列标准

ITU-T 制定了 V2X 安全相关的规范，具体包括：

- Secure software update capability for intelligent transportation system communication devices（X.1373）

该标准通过适当的安全控制措施，未远程更新服务器和车辆之间的提供软件安全的更新方案，包括对安全威胁和风险的分析，对安全防护需求和防护措施的归纳，数据包格式和具体的流程。

- X.itssec-2

该标准为 V2X 通信系统提供安全指导。V2X 是本建议书中 V2V（车辆到车辆），V2I（车辆到基础设施）和 V2ND（车辆到漫游设备）和 V2P（车辆到行人）通信模式的通用术语。

- X.itssec-3

该标准重点从车载诊断 II（OBD-II）端口连接和无线连接的角度确定车辆可访问外部设备的威胁和安全要求。

- X.itssec-4

该标准主要集中在车载网络上的内部通信作为 CAN 通用 IDS 无法支持的部分，以保证利用各种高效光源来检测影响 ECU 通信的威胁重量检测模型，如基于签名的模型，基于熵的模型，基于自相似性的模型，基于危害的模型，本建议书将考虑使用 IDS 来保护连接的车辆。

- X.itssec-5

该标准车辆边缘计算提供安全指导，它涵盖了车辆边缘计算的威胁分析，安全要求和使用案例。

- X.mdcv

该标准是基于大数据分析的联网汽车的安全相关的异常行为检测机制，包括数据获得、数据分析等步骤。

- X.srcd

该标准是 V2X 通讯数据分类的安全要求，它对 V2X 通信数据分为多种类型，定义起安全等级，并在此基础上提出安全要求。

- X.stcv

该标准是联网汽车安全威胁，它首先详述联网汽车模型（汽车生态系统），然后确认对联网汽车（生态系统）高级别的威胁。

5.1.3 网联汽车智能终端相关标准

5.1.3.1 SAE 系列标准

美国汽车工程师协会 SAE 制定了一系列与智能网联汽车相关的技术标准，具体包括：

- Requirements for Hardware-Protected Security for Ground Vehicle Applications（J3101）

该文件为地面车辆的硬件定义一套通用的安全要求，以促进安全性增强的应用程序，提出对实现地面车辆应用硬件保护理想系统所需功能的期望，包括示例，但未明确详细说明实施要求。

- Guidance for Securing the Data Link Connector (DLC)（J3138）

车载诊断（OBD）法规要求轿车以及轻型和中型卡车提供数据链路连接器，以支持将诊断信息传送到车外设备。立法诊断信息也需要及时传达给离线设备。许多汽车制造商还通过该连接器提供增强型诊断信息和车辆系统/子系统。

5.1.3.2 HSM 相关规范

- Protection Profile V2X Hardware Security Module

Car2Car 通讯联盟制定了面向的 V2X 的硬件安全模块（HSM）的保护轮廓规范《Protection Profile V2X Hardware Security Module》，分别定义了用于 V2X HSM 的基础保护轮廓（base PP）和包。

在该规范中，定义了 V2X HSM 的安全问题，包括对 TOE 环境的假设、对 TOE 的威胁、TOE 环境以及为确保 TOE 安全而采用的组织安全策略。规范中还定义了安全功能的意图、安全功能和保证要求、扩展组件等方面的要求，以及一些可选 TOE 细节的包。

《Protection Profile V2X Hardware Security Module》使得阅读者可以充分了解 V2X HSM 的安全目标和功能要求，为 V2X 领域的硬件安全模块（HSM）的设计与开发提供了指引。

5.1.4 传输通信网络相关标准

5.1.4.1 IEEE 1609 系列标准

IEEE 制定的 IEEE 1609 系列协议是 WAVE 的高层协议，构成了专用短程通信（DSRC）的核心。

IEEE 1609 系列标准体系框架如图 5-1 所示。

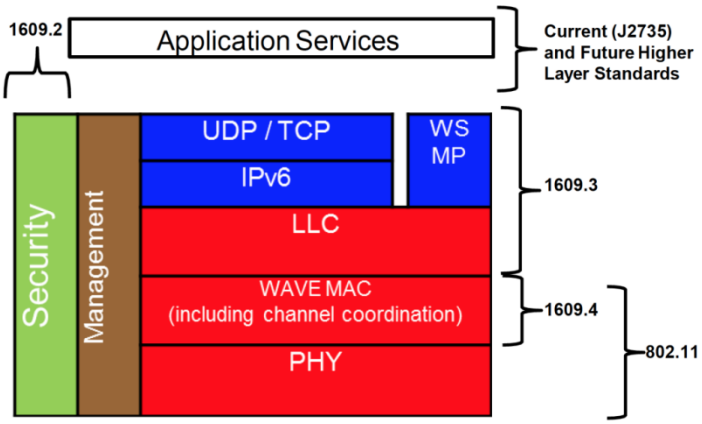

图 5-1 DSRC 标准体系

在 IEEE 1609 标准体系中，主要标准包括：

——汽车环境中无线存取（WAVE）（IEEE 1609.1）标准规定了多个远程应用和资源管理间的控制互换流程。此模块位于应用层，负责信息的交换，定义资源设备与资源管理设备之间通信的格式及方法，以便传送数据、命令和状态信息；

——应用和管理信息的安全服务（IEEE 1609.2）标准规定了 WAVE 信息安全抵制窃听、电子欺诈和其他袭击的方法。此模块定义在 WAVE/DSRC 系统中的安全信息封包格式及处理方式。也定义 WAVE 管理与应用信息的加密方法，车辆引发的安全意外处理方法。此外，IEEE1609.2 标准借鉴了传统 PKI 系统的体系结构，通过证书链实现终端互信；

——网络服务（IEEE 1609.3）标准规定了位于 OSI 的网络模型的网络层与传输层，以便提供 WAVE/DSRC 的网络服务。可以提供两个车辆设备之间的通讯，或者车辆设备与路旁设备（Road device)之间的通讯；

——多渠道运行（IEEE 1609.4）标准规定了通信协议栈媒体接入控制接口和 IEEE802.11p 的多渠道运行对单渠道运行。协调控制频道（CCH）与服务频道(SCH)的多频道运作。它包括优先权(Priority)的使用，频道的切换的机制。

5.1.4.2 3GPP 系列标准

LTE-V2X 是为了支持基本道路安全等车联网业务需求,在蜂窝架构基础上，扩展了终端直连通信特性。3GPP 标准组织在现有 LTE 网络的基础之上引入了 V2X 控制功能网元，对车联网终端及业务进行管控，并对上层业务提供方提供服务支撑，满足业务需要。在此网络架构下，LTE V2X 系统安全分为蜂窝通信场景和直连通信场景的安全[20]。

蜂窝通信场景下的安全架构（如图 5-2 所示）与 LTE 的安全架构类似，包括网络接入安全、网络域安全、认证与密钥管理、车联网接入安全、车联网业务能力开放安全、网络安全能力开放、应用层安全和车内系统及接口安全。其中网络接入安全、网络域安全、认证与密钥管理和网络安全能力开放继承了 LTE 网络现有安全机制。车联业务接入安全是车联网系统新增的安全域，对于 LTE 网络而言属于应用层安全。它在终端与其归属网络的 V2X 控制功能之间提供双向认证，对终端身份提供机密性保护；在终端与 V2X 控制功能之间对配置数据提供传输时的完整性保护、机密性保护和抗重放保护。车联业务能力开放安全也是车联网系统新增的安全域，保证对上层应用提供 LTE V2X 业务能力开放过程中的接入及数据传输安全。它可采取类似于网络域安全的方法来保护，在不同安全域之间采用 IPSec、TLS 等安全机制为业务提供双向认证、加密、完整性保护和抗重放的安全保障。

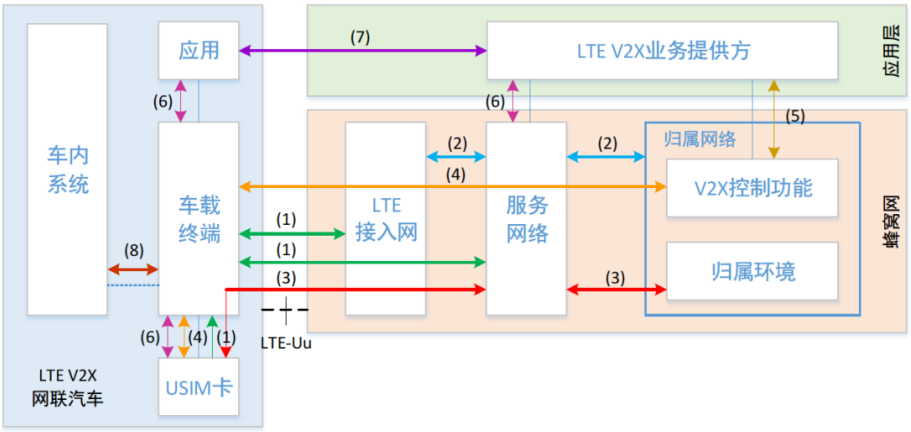

图 5-2　蜂窝移动通信场景下 LTE-V2X 安全架构

直连通信场景下的 LTE-V2X 系统安全架构（如图 5-3 所示）包括网络层安全、安全能力支撑、应用层安全、车内系统及接口安全和外部网络域安全。根据 3GPP 组织的 REL14 的规范，终端在网络层不采取任何机制对 PC5 接口上广播发送的直连通信数据进行安全保护，数据的传输安全完全在应用层 V5 接口保障。网络层仅提供标识更新机制对用户隐私进行保护。终端通过随机动态改变源端用户层二标识和源 IP 地址，防止用户身份标识信息在 PC5 广播通信的过程中遭到泄露、被攻击者跟踪。网络层向应用层提供安全能力支撑，采取用户标识跨层同步机制确保源端用户层二标识、源 IP 地址与应用层标识同步更新，防止由于网络层与应用层用户身份标识更新的不同步，导致用户标识关联信息被攻击者获取，用户隐私信息遭到泄露。

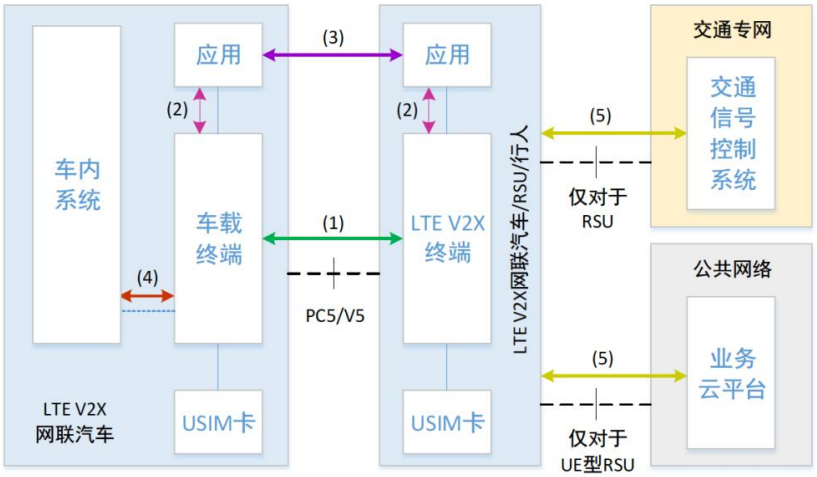

图 5-3　直连通信场景下的 LTE-V2X 安全架构

5.1.4.3　ETSI 系列标准

欧洲电信标准协会（ETSI）为 ITS 安全建立了多个规范[20]。具体而言，TS 102 940 规定了网络模块中安全性的定位；TS 102 941 涵盖节点注册和身份验证过程；TS 102 942 涵盖访问控制；TS 102 943 涵盖机密性服务。

图 5-4 给出了 ETSI 标准的“ITS 通信安全参考模型”，在 TS 102 940–943 系列标准中列出了安全参考模型在 ITS 通信安全中的各自作用，以及与之相关的安全参考模型（如车辆、路侧设备、注册机构、认证机构的参考点）。

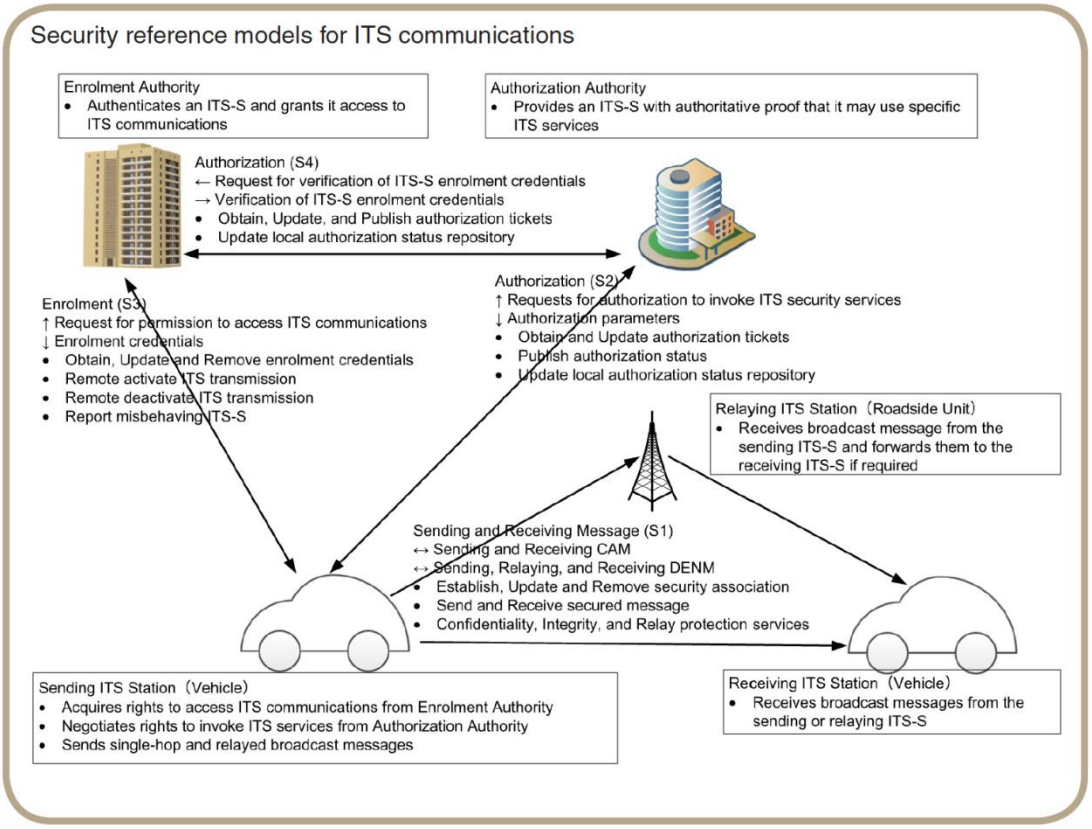

图 5-4　ITS 通信安全参考模型

此外，这些 ETSI 标准还涵盖了以下方面：加密密钥的管理、安全生命周期（在生产过程中、注册期间、身份验证期间以及维护期间）、用于保证安全通信路径的安全关联，以及协议栈中各层的角色。

这些 ETSI 标准的安全机制，利用密码技术建立 ITS Station 之间，以及 ITS Station 与管理方的信任关系。安全信任模型由可信第三方、签发服务、维护服务三部分构成，其中涉及到的机构主要包括注册机构（EA）、授权机构（AA）、证书颁发机构（CA）和 ITS Station 制造商。

5.1.5 智能交通系统相关标准

5.1.5.1 ISO 系列标准

- Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices（智能交通系统—用于可信设备间安全会话建立与认证的 ITS 站点安全服务）（ISO/TS 21177:2019）

ISO/TS 21177 标准规范化了用来确保可信实体时间的消息来源认证以及交互信息完整性的一组 ITS 站点安全服务集合。

5.1.5.2 ETSI 系列标准

CCMS 是欧洲针对合作式智能交通设计的一套证书管理系统，主要结构如图 5-5 所示[20]。CCMS 考虑不同的信任模型，允许一个或多个根 CA 存在，可以实现单根 CA、交叉认证、桥接 CA 和证书信任列表等多种证书管理模式。

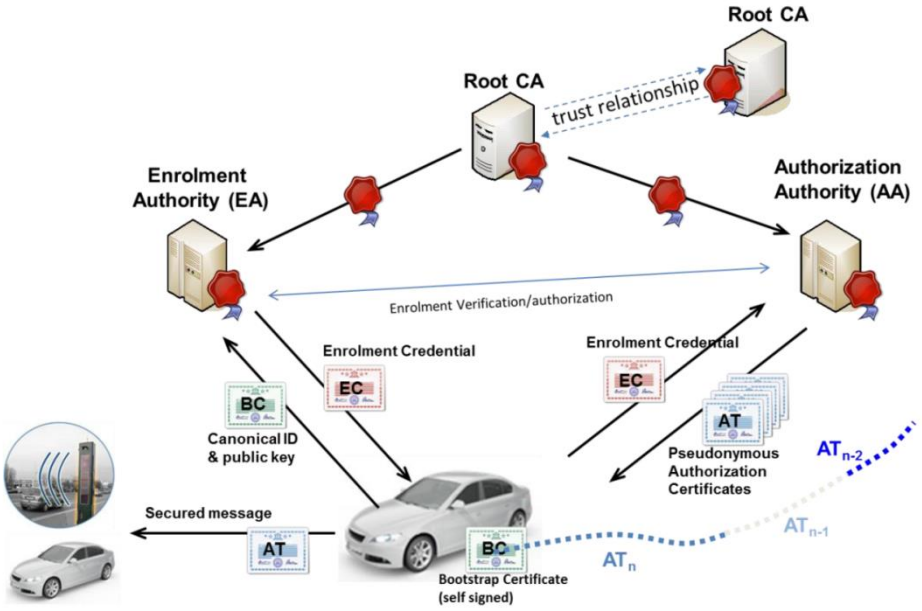

图 5-5 CCMS 安全架构示意图

ETSI 发布的 CCMS 相关的标准包括：

——智能运输系统（ITS）；安全；安全业务和架构（TS 102 731）标准规定了由 ETS 300 387 定义的第 2 阶段的机制，用于 ITS 环境中的安全和隐私保护通信。它描述了凭证和身份管理，隐私和匿名性，完整性保护，身份验证和授权的功能；

——智能运输系统（ITS）；安全；ITS 通信安全体系结构与安全管理（TS 102 940）标准规定了用于智能运输系统（ITS）通信的安全体系结构。基于 ETSI TS 102 731 中定义的安全服务，它标识在 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 参考体系结构的元素之间存在的关系；

——智能运输系统（ITS）；安全；可信与隐私管理（TS 102 941）标准规定了智能传输系统（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，它确定了在 ITS 环境中支持安全性所需的信任建立和隐私管理，以及实体本身与元素之间存在的关系。ETSI EN 302 665 中定义的 ITS 参考体系结构；

——智能运输系统（ITS）；安全；安全头和证书格式（TS 103 097）标准规定了了安全数据结构，包括用于智能传输系统的标头和证书格式。

5.2 国内标准研究

5.2.1 标准体系框架

2022 年 2 月，工业和信息化部印发了《车联网网络安全和数据安全标准体系建设指南》，该《指南》的发布，旨在为加快建立健全车联网网络安全和数据安全保障体系。《指南》提出，到 2023 年底将初步构建起车联网网络安全和数据安全标准体系。期间将重点研究基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等标准，完成 50 项以上急需标准的研制。到 2025 年，完成 100 项以上标准的研制，形成较为完备的车联网网络安全和数据安全标准体系，提升标准对细分领域的覆盖程度，加强标准服务能力，提高标准应用水平，支撑车联网产业安全健康发展。

《指南》中提出了车联网网络安全和数据安全标准体系框架（如图 5-6），标准体系框架包括总体与基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等 6 个部分。

图 5-6　车联网网络安全和数据安全标准体系框架图（摘录自《指南》）

5.2.2　主要标准化组织

在中国，中国通信标准化协会（CCSA）、中国智能交通产业联盟（C-ITS）、中国汽车工程学会（C-SAE）、国际移动通信系统（IMT）-2020 C-V2X 工作组等组织积极推进 LTE-V2X 端到端标准体系的构建。全国智能运输系统标准化技术委员会（SAC/TC268）从事全国性智能运输系统标准化工作的技术组织工作，负责智能运输系统的标准化技术归口工作。此外，全国信息技术标准化技术委员会（SAC/TC28）、全国通信标准化技术委员会（TC485）等也从各自专业的角度制定了部分与智能网联汽车相关的、不同层级的标准。经过调研，本文列举了相关标准化组织截至 2023 年 12 月的在研/已发布标准，并分析相关标准的范围和关键内容，为本文提出标准体系框架提供参考。

目前，已基本建设完成 LTE-V2X 标准体系和核心标准规范制定，包括总体技术、空中接口、安全以及网络层与应用消息层、车载终端和路侧设备等各个部分，初步形成了覆盖 LTE-V2X 标准协议栈各层次、各层面、设备的标准体系。

比较重要的标准化组织的规划介绍如下：

- 全国汽车标准化技术委员会（TC114）

全国汽车标准化技术委员会（TC114）下属的智能网联汽车分技术委员会（SC34）负责归口管理我国智能网联汽车领域的国家标准和行业标准，成立了先进驾驶辅助系统（ADAS）标准工作组、信息安全、自动驾驶等工作组。

TC114/SC34 拟定了汽车信息安全标准的子体系框架（如图 5-7），从评、防、测三个维度和基础、共性、系统部件、功能管理四个层面对汽车信息安全标准制定进行了全面梳理，并通过相关标准部分预留与其他信息安全标准体系的接口。

图 5-7　汽车标委会的信息安全标准体系

- 中国汽车工程学会

中国汽车工程学会成立了智能网联汽车信息安全工作委员会。在智能网联汽车标准体系中，其通用规范（200）中包含了信息安全（204）相关内容。中国汽车工程学会主导成立了中国智能网联汽车产业创新联盟，牵头制定相关团体标准。

5.2.3　通用密码标准

- 《信息安全技术 密码模块安全要求》（GB/T 37092-2018）

全国信息安全标准化技术委员会（SAC/TC260）发布的《信息安全技术 密码模块安全要求》标准针对密码模块规定了安全要求，为密码模块定义了四个安全等级，并分别给出了四个安全等级的对应要求。该标准适用于保护计算机与电信系统内敏感信息的安全系统所使用的密码模块。该标准也为密码模块的设计、开发提供指导，为密码模块安全要求的检测提供参考。

密码厂家在设计与开发用于汽车电子的硬件安全模块(HSM)时可以参照 GB/T 37092 标准的相关要求，但是还需要充分考虑 V2X 领域的特殊应用需求。

- 《信息安全技术 SM2 椭圆曲线公钥密码算法》（GB/T 32918 所有部分）

在相同安全程度要求下,椭圆曲线密码较其他公钥密码所需的密钥规模要小得多。SM2 是国家密码管理局组织制定并提出的椭圆曲线密码算法标准。

全国信息安全标准化技术委员会（SAC/TC260）发布的《信息安全技术 SM2 椭圆曲线公钥密码算法》标准包含了多个部分：

——GB/T 32918.1 规定了 SM2 椭圆曲线公钥密码算法涉及的必要数学基础知识与

相关密码技术,以帮助实现其他各部分所规定的密码机制；

——GB/T 32918.2 规定了 SM2 椭圆曲线公钥密码算法的数字签名算法,包括数字签名生成算法和验证算法,并给出了数字签名与验证示例及其相应的流程；

——GB/T 32918.3 规定了 SM2 椭圆曲线公钥密码算法的密钥交换协议,并给出了密钥交换与验证示例及其相应的流程；

——GB/T 32918.4 规定了 SM2 椭圆曲线公钥密码算法的公钥加密算法,并给出了消息加解密示例和相应的流程；

——GB/T 32918.5 规定了 SM2 椭圆曲线公钥密码算法的曲线参数。

在车联网中，SM2 算法可有各种应用场景，其中最有代表性的应用是为各种实体签发不同类型的数字证书（包括注册证书、假名证书、应用证书等），并在通信协议中用于标识实体的身份，保证传输报文的安全性。

- 《信息安全技术 祖冲之序列密码算法》（GB/T 33133 所有部分）

全国信息安全标准化技术委员会（SAC/TC260）发布的《信息安全技术 祖冲之序列密码算法》是中国自主研制的流密码算法,标准密码算法,该算法包括祖冲之算法、保密性算法和完整性算法三个部分。

祖冲之序列密码算法已经被运用于下一代移动通信 4G 网络中的国际标准，在车联网中采用 LTE 等通信制式来传输报文时将会应用该密码算法。

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

全国信息安全标准化技术委员会（SAC/TC260）发布的《信息安全技术 SM3 密码杂凑算法》标准规定了 SM3 密码杂凑算法的计算方法和计算步骤,并给出了运算示例。该标准适用于商用密码应用中的数字签名和验证、消息认证码的生成与验证以及随机数的生成,可满足多种密码应用的安全需求。

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

全国信息安全标准化技术委员会（SAC/TC260）发布的《信息安全技术 SM4 分组密码算法》标准规定了 SM4 分组密码算法的算法结构和算法描述,并给出了运算示例。该标准适用于商用密码产品中分组密码算法的实现、检测和应用。

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

全国信息安全标准化技术委员会（SAC/TC260）发布的《信息安全技术 传输层密码协议（TLCP）》标准规定了传输层密码协议，包括记录层协议、握手协议族和密钥计算。该标准适用于传输层密码协议相关产品（如 SSL VPN 网关、浏览器等）的研制，也可用于指导传输层密码协议相关产品的检测、管理和使用。

在车联网中，汽车网关、车载 T-Box 和车载信息娱乐系统（IVI）在与远程服务平台（Telematics）进行通信时，需要互相认证对方的身份，当双方身份相互验证合法后，建立通信链路连接。采用 TLCP 传输层密码协议，可以实现在进行数据传输时采用加密、认证等安全措施保护关键通信数据的保密性、完整性、可用性和抗重放攻击。

- 《基于 SM2 算法的无证书及隐式证书公钥机制》

《基于 SM2 算法的无证书及隐式证书公钥机制》是密标委基础组的在研项目。该标准旨在规定基于 SM2 算法的无证书签名机制、加密机制及密钥生成机制。目前车联网安全使用的是显式证书，安全开销比较大，未来可能会使用隐式证书等新机制来减少空口开销及算力消耗。该标准规定的公钥密码机制可应用于需要隐式证书公钥机制的系统中，以节约传输、存储以及计算等开销。

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

全国信息安全标准化技术委员会（SAC/TC260）发布的《信息安全技术 公钥基础设施 数字证书格式》标准规定了数字证书和证书撤销列表的基本结构、各数据项内容。该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。

《信息安全技术 公钥基础设施 数字证书格式》规定的数字证书格式基于 X.509 规范，尽管《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/T3957-2021）标准规定了在 V2X 网络中的注册证书、假名证书、应用证书等采用完全不同的数字证书格式，但是在车联网的业务层面也同样需要应用基于 X.509 规范的数字证书格式，譬如用于 SSL 传输的服务器证书、用于识别移动终端身份的客户端证书等等。

- 《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）

全国信息安全标准化技术委员会（SAC/TC260）发布的本标准规定了数字证书认证系统的密码及其相关安全技术要求，包括：证书认证系统，密钥管理系统，密码算法、密码设备及接口，证书认证中心，密钥管理中心，证书认证中心运行管理要求，密钥管理中心运行管理要求，证书操作流程等。该标准适用于指导第三方认证机构的数字证书认证系统的建设和检测评估，规范数字证书认证系统中密码及相关安全技术的应用。

根据第 4.6 节的分析，车联网中引入了假名证书的机制，这对于数字证书认证系统带来了很多新的挑战和密码应用需求，包括：

——支持全新的数字证书格式；

——支持对用户公钥的衍生算法；

——支持假名证书的批量撤销机制；

——支持全新的 CRL 数据格式。

对第三方认证机构而言，在数字证书认证系统的建设和检测评估过程中，需要同时满足《信息安全技术 证书认证系统密码及其相关安全技术规范》和车联网相关证书认证系统标准的要求。目前，尚未形成车联网电子认证系统的相关证书策略和电子认证业务规则，同时也缺乏车联网电子认证系统的运营管理规范。

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

全国信息安全标准化技术委员会（SAC/TC260）发布的《信息安全技术 信息系统密码应用基本要求》标准规定了信息系统从第一级到第四级的密码应用的基本要求，从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个技术层面提出从第一级到第四级的密码应用技术要求，并从管理制度、人员管理、建设运行和应急处置四个方面提出从第一级到第四级的密码应用管理要求。该标准适用于指导、规范信息系统密码应用的规划、建设、运行及测评。

由于车联网信息服务平台（Telematics）系统是一个通用的信息系统，因此也要依据网络安全保护等级，参照《信息安全技术 信息系统密码应用基本要求》标准来开展进行密码应用设计和密码应用安全性评估。

5.2.4 安全管理标准及通用方法论

- 《信息安全技术 汽车电子系统网络安全指南》

全国信息安全标准化技术委员会（SAC/TC260）发布的《汽车电子系统网络安全指南》的研究目标是提供一个网络安全过程框架及指南，以帮助组织识别和评估网络安全威胁，并将网络安全的设计融入到汽车电子系统的整个生命周期（从概念阶段到开发、生产、运行、服务和退役等阶段）的过程中，将网络安全控制性要素嵌入到每一个环节，

并能够应对不断发展的汽车网络安全的威胁；指导组织从管理及流程的层面，消除/缓解汽车电子系统网络安全威胁，提升网络安全防御水平。

- 《C-V2X 车联网证书策略与认证业务声明框架》

密标委应用组的在研标准《C-V2X 车联网证书策略与认证业务声明框架》，旨在规范定义 C-V2X 车联网电子认证服务应提供的服务内容要求、服务质量保障、具体的服务操作规范及相关法律责任等；用于指导电子认证服务机构开展 C-V2X 车联网电子认证服务体系建设以及相关服务的开展和实施，也用于为国家密码管理局组织开展 C-V2X 车联网电子认证服务能力评估提供依据。

5.2.5 车载智能设备相关标准

- 《汽车信息安全通用技术要求》

全国汽车标准化技术委员会（SAC/TC 114）正在制订的《汽车信息安全通用技术要求》标准规定了汽车信息安全的保护对象和技术要求。

- 《汽车整车信息安全技术要求》

在研的国家标准计划《汽车整车信息安全技术要求》由工业和信息化部组织起草，委托 TC114SC34（全国汽车标准化技术委员会智能网联汽车分会）执行。该标准是强制性国家标准。

《汽车整车信息安全技术要求》规定了汽车信息安全管理体系要求、车辆信息安全一般要求、车辆信息安全技术要求、审核评估及测试验证方法。该标准适用于 M 类、N 类及至少装有 1 个电子控制单元的 O 类车辆，其他类型车辆可参考执行。

- 《汽车网关信息安全技术要求》

全国汽车标准化技术委员会（SAC/TC 114）正在制订的《汽车网关信息安全技术要求》标准规定了汽车网关产品硬件、通信、软件、数据的信息安全技术要求与测试方法。

- 《车载信息交互系统信息安全技术要求》

全国汽车标准化技术委员会（SAC/TC 114）正在制订的《车载信息交互系统信息安全技术要求》标准规定了车载信息交互系统硬件、通信协议与接口、操作系统、应用软件、数据的信息安全技术要求与试验方法。

- 《信息安全技术 车载网络设备信息安全技术要求》

全国信息技术安全标准化技术委员会（TC260）正在制订的《信息安全技术 车载网络设备信息安全技术要求》规定了车载网络设备的信息安全技术要求，适用于指导和规范整车制造商、设备供应商进行车载网络设备信息安全功能的设计、研发、生产、实施以及测试评估，也可作为职能部门进行监督、检查和指导的依据。

- 《智能网联汽车车载端信息安全技术要求》（T/CSAE 101-2018）

中国汽车工程学会发布的《智能网联汽车车载端信息安全技术要求》提出了智能网联汽车车载端的安全架构，把车载端信息安全架构分为车载端自身的硬件、操作系统、应用三个层面的安全、对外通信和对内通信的安全，以及数据安全共六个部分。规范从这六个方面提出了信息安全技术的分级要求，具体包括：

（1）硬件安全主要是对车载端设备硬件设计生产过程中的安全技术要求，能够防范物理层面对车载设备的多种信息安全攻击；

（2）操作系统安全技术要求主要集中在漏洞管理、身份认证、文件完整性保护以及资源管理等措施，强调访问控制策略的落实；

（3）应用安全措施主要考虑对抗逆向分析、反编译、篡改、非授权访问等各种针对应用的安全威胁，保证应用为用户提供服务时，以及应用在启动、升级、登录、退出等各模式下的安全性；
（4）对外通信安全通过隔离、加密、认证、完整性保护等多种手段，对抗外部对车载端甚至车辆的攻击行为；
（5）对内通信安全的重点是车载端应力争不破坏车辆内部的重要子系统信息安全可用性和完整性；
（6）数据安全是保护车载端参与操作的用户数据在其生命周期各环节的安全性。

- 《电子收费 单片式车载单元（OBU）技术要求》

交通运输部发布的《电子收费 单片式车载单元（OBU）技术要求》规定了电子不停车收费（ETC）系统中单片式车载单元（OBU）设备要求、OBE-SAM、典型交易流程、测试方法等方面的内容。其中包含了密钥存储、密钥维护、鉴别码计算等与密码应用有关的技术要求。

- 《LTE-V2X 车载单元（OBU）设备的安全模块研究》

中国通信标准化协会（CCSA）正在开展的标准研究项目《LTE-V2X 车载单元（OBU）设备的安全模块研究》主要针对 LTE-V2X 通信场景的特点，对 OBU 安全模块的架构、功能要求、性能指标等方面进行研究，分析并提出区别于通用安全模块的特色方面和标准工作建议，为产业提供指导建议。

- 《汽车记录仪数据安全芯片技术要求》

中国道路交通安全协会制定并发布的团体标准《汽车记录仪数据安全芯片技术要求》规定了适用汽车记录仪的数据安全芯片的一般要求、功能要求、性能要求、试验方法和包装，适用于安装在车辆上的各类汽车记录仪的数据安全芯片的设计、制造和使用。

该标准中明确要求采用 SM 系列密码算法来实现汽车记录仪数据安全芯片的安全功能，同时兼容国际通用的安全算法。

- 《汽车智能处理器硬件可信根和安全启动密码应用技术研究》

《汽车智能处理器硬件可信根和安全启动密码应用技术研究》是密标委应用组的在研项目。智能处理器在汽车上的不断应用，使得其面临多种威胁，可能遭受物理破坏、硬件替换、固件非授权操作、网络暴力破解等攻击。安全启动赋予汽车启动状态的正常稳定，是汽车安全驾驶的基础。

该项目通过研究汽车智能处理器的硬件可信根，提供一种智能驾驶领域处理器的信任机制，解决从上电启动到进入系统期间各个环节设备硬件、固件的可信，称为硬件可信安全启动，确保可防止非授权的硬件、固件侵入。在此基础上制定相关联的行业标准，以商用密码为基础，规范汽车智能处理器的硬件可信根的定义、实现要求和使用指导，用于指导智能驾驶厂商构建更安全可信的硬件平台和产品，可供汽车智能驾驶硬件的安全性评估和认证标准参考。

5.2.6 智能终端相关标准

- 《移动智能终端数字车钥匙信息安全技术要求》（T/TAF 074-2020）

电信终端产业协会制定的《移动智能终端数字车钥匙信息安全技术要求》标准规定了基于移动互联网的数字车钥匙信息安全的技术要求，包括数字车钥匙执行环境、应用软件、通信模块和用户隐私等[13]。

《移动智能终端数字车钥匙信息安全技术要求》标准根据数字车钥匙的不同实现方案，提出了不同的信息安全技术要求。《移动智能终端数字车钥匙信息安全技术要求》

还依据移动智能终端数字车钥匙的实现方式与安全功能要求的差异，将安全能力级别划分为三级，其中一级、二级与三级安全能力依次递增，最高安全级别为三级。

5.2.7 传输通信网络相关标准

- 《基于 LTE 的车联网无线通信技术 总体技术要求》（YD/T 3400-2018）

中国通信标准化协会（CCSA）发布的《基于 LTE 的车联网无线通信技术 总体技术要求》标准规定了基于 LTE 的车联网无线通信技术的总体业务要求、系统架构和基本功能要求。

- 《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）

中国通信标准化协会（CCSA）发布了《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》标准[16]，并且该标准已列入国家标准计划。

《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》标准提出适用于 LTE-V2X 的车联网通信安全认证技术要求。

具体内容包括：

——LTE-V2X 通信安全认证需求，包括法律法规要求的隐私保护、安全保障等要求；

——LTE-V2X 通信安全认证机制总体技术要求，包括安全证书、认证机构等在内的总体技术要求；

——LTE-V2X 通信安全认证交互流程及接口技术要求，主要规定包括触发条件、认证交互流程、数据接口格式等在内的流程和技术要求。

《安全证书管理系统技术要求》标准中规定使用的密码算法基本上与 IEEE 1609.2 类同，包括随机数生成算法、密码杂凑算法、对称加密算法、非对称签名算法、非对称加密算法等。同时，该标准充分考虑了中国的国情，增加了国标 SM 系列算法的支持，并且约定 SM 系列算法为默认支持算法。

- 《C-V2X 车联网系统 认证授权系统技术要求》

为了实现 C-V2X 设备间的安全认证和安全通信，C-V2X 使用基于公钥证书的 PKI 机制,采用数字签名等技术手段实现 V2V/V2I/V2P 直连通信安全。中国通信标准化协会（CCSA）制定的《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》标准中提出了认证授权机构，支持 DCM、GBA 和 OAuth 方式进行证书申请和颁发，是车联网安全中一个重要的组成部分。

中国通信标准化协会（CCSA）的在研标准《C-V2X 车联网系统 认证授权系统技术要求》主要规定 C-V2X 车联网认证授权系统架构、V2X 设备认证与授权系统安全需求、V2X 设备标识、V2X 设备认证和 V2X 设备授权过程。

5.2.8 车联网服务平台相关标准

- 《车联网信息服务平台安全防护技术要求》（YD/T 3752-2020）

中国通信标准化协会（CCSA）发布的《车联网信息服务平台安全防护技术要求》标准针对车联网信息服务平台对于安全防护方面的需求，规定了车联网信息服务平台的安全防护的总体技术要求，主要包括基础设施安全、平台安全和应用服务安全等。

- 《电动汽车远程服务与管理系统信息安全技术要求》

全国汽车标准化技术委员会（SAC/TC 114）正在制订的《电动汽车远程服务与管理系统信息安全技术要求》标准规定了电动汽车远程服务与管理系统的信息安全要求。

- 《电动汽车充电系统信息安全技术要求》

全国汽车标准化技术委员会（SAC/TC 114）正在制订的《电动汽车充电系统信息安全技术要求》标准规定了电动汽车车内充电系统信息安全技术要求与试验方法。

- 《车联网安全管理平台通用技术要求》

中国通信标准化协会（CCSA）在研的《车联网安全管理平台通用技术要求》标准规定了车联网安全管理平台通用技术要求，包括通用要求、功能要求、技术要求、安全要求。该标准适用于车联网企业，覆盖智能网联汽车与车联网服务平台，实现统一的网络安全和数据安全管理。

- 《车联网应用软件通用安全技术规范》

中国通信标准化协会（CCSA）在研的《车联网应用软件通用安全技术规范》标准规定了车联网应用软件的通用安全技术规范，包含安全技术要求与测试评价方法两部分。该标准适用于指导整车厂商、软件供应商、车联网服务提供商、汽车零部件供应商等企业开展车联网应用软件的开发测试、运行维护等生存周期过程的安全防护与测试评估工作。

- 《车联网网络安全异常行为检测机制》

中国通信标准化协会（CCSA）归口的在研国家标准《车联网网络安全异常行为检测机制》提供了一种针对车联网网络安全异常行为的检测机制，适用于车联网，目的是方便设计人员和安全解决方案提供方检测网络安全异常行为。

该标准提出了数据采集要求和异常行为检测机制，其中数据采集指定可用于网络安全异常行为检测的、从不同来源获取的数据和信息类型，检测机制可分析采集的数据以检测网络安全异常行为。

- 《车辆 C-V2X 异常行为管理技术要求》

中国通信标准化协会（CCSA）制定的行业标准《车辆 C-V2X 异常行为管理技术要求》规定了车辆 C-V2X 功能异常行为的管理技术要求，包括异常行为的定义、分类、异常行为检测、异常行为报告数据结构、异常行为处置以及异常行为管理系统与安全证书管理系统之间的接口协议、交互流程等内容。

在标准中有明确要求异常行为消息可以通过安全签名验证和协议一致性检查。车辆在使用 C-V2X 消息时，需要判断消息来源的真实性，并验证 C-V2X 消息中字段值的合理性。该标准在数字证书、签名算法、哈希算法等方面的技术要求均引用了 YD/T 3957-2021 标准。

5.2.9 智能运输系统相关标准

- 《交通运输 数字证书格式》（GB/T 37376-2019）

全国智能运输系统标准化技术委员会(SAC/TC 268)发布的《交通运输 数字证书格式》标准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。

该标准首次发布实施以来，对保障智能交通运输系统的应用安全起到了积极作用。随着业务场景的丰富和车辆数量的增加，当前证书格式在证书类型、批量吊销、权限等相关字段上的缺失，使得智能交通运输系统安全管理效率、可商用性、可扩展性上大大降低，甚至会影响到某些安全场景的开展，例如对于前向碰撞预警、紧急制动预警等对时延要求尤其严格的应用场景而言，要求查询 CRL 的时间开销尽可能小，而当前的 CRL 格式缺失 series 字段，无法满足上述要求。2021 年，全国智能运输系统标准化技术委员会提出修订该标准，相关修订工作正在开展中。

- 《智能交通 数字证书应用接口规范》（GB/T 37374-2019）

全国智能运输系统标准化技术委员会(SAC/TC 268)发布的《智能交通 数字证书应用接口规范》标准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。

- 《车路协同路侧设施证书认证技术规范》

全国智能运输系统标准化技术委员会（SAC/TC268）提出的在研标准《车路协同路侧设施证书认证技术规范》规定了车路协同环境下路侧设施各实体之间实现信息交互安全的证书认证体系，以及支持与车载设备信息交互安全的证书认证体系。标准适用于车路协同环境下路侧设施的证书认证系统的规划、设计、建设。

- 《交通运输 信息安全规范》（GB/T 37378-2019）

全国智能运输系统标准化技术委员会(SAC/TC 268)发布的《交通运输 信息安全规范》规定了交通运输信息安全技术体系架构和信息安全总体技术要求，包括构成交通运输信息系统的用户终端、载运装备单元、基础设施单元、计算中心、网络和通信各基本组成部分的信息安全通用和专项技术要求。

- 《合作式智能运输系统 信息安全总体技术要求》（T/ITS 0035-2015）

中关村中交国通智能交通产业联盟发布的《合作式智能运输系统 信息安全总体技术要求》主要针对合作式智能运输系统的信息安全进行研究，提出了合作式智能运输系统信息安全总体技术要求，针对合作式智能运输系统中的车载设备、路侧设备、出行者设备、中心设备、通信服务和应用服务提出了相应的安全技术要求。

- 《公路工程适应自动驾驶附属设施总体技术规范》

交通运输部公路科学研究院牵头制订的《公路工程适应自动驾驶附属设施总体技术规范》规定了公路工程适应自动驾驶附属设施的总体技术要求，包括：总则、术语与缩略语、总体架构、高精度地图、定位设施、通信设施、交通标志标线、交通控制与诱导设施、交通感知设施、路侧计算设施、供能与照明设施、自动驾驶监测与服务中心、网络安全。

- 《车联网网络安全异常行为检测机制》

全国通信标准化技术委员会（TC485）在研的《车联网网络安全异常行为检测机制》标准等同采用 ITU 国际标准 ITU-T X.1376，该标准提供了一种针对车联网网络安全异常行为的检测机制。该标准适用于车联网，目的是方便设计人员和安全解决方案提供方检测网络安全异常行为。

- 《车辆 C-V2X 异常行为管理技术要求》

中国通信标准化协会（CCSA）在研的《车辆 C-V2X 异常行为管理技术要求》标准规定了车辆 C-V2X 功能异常行为的管理技术要求，包括异常行为的定义、分类、异常行为检测、异常行为报告数据结构、异常行为处置以及异常行为管理系统与安全证书管理系统之间的接口协议、交互流程等内容。该标准适用于车辆 C-V2X 功能异常行为管理。

5.2.10 数据安全及隐私保护相关标准

- 《智能交通 数据安全服务》（GB/T 37373-2019）

全国智能运输系统标准化技术委员会(SAC/TC 268)发布的《智能交通 数据安全服务》规定了基于智能运输系统安全体系架构的安全支撑平台基本功能和系统构成，及安全支撑平台所提供的数据安全服务内容（包括身份鉴别、授权管理、安全传输、数据保护、责任认定、安全管理等）。

- 《信息安全技术 个人信息安全规范》（GB/T 35273-2020）

全国信息技术安全标准化技术委员会（SAC/TC260）发布的《个人信息安全规范》标准针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》等相关法律，严格规范个人信息在收集、存储、使用、共享、转让与公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄露等乱象，最大程度的保护个人的合法权益和社会公众利益。

- 《信息安全技术 网联汽车 采集数据的安全要求》

全国信息技术安全标准化技术委员会（SAC/TC260）正在制定的《信息安全技术 网联汽车 采集数据的安全要求》标准规定了网联汽车采集的数据在传输、存储和跨境等环节的安全要求。

《信息安全技术 网联汽车 采集数据的安全要求》标准主要提出了以下要求：不得基于网联汽车所采集数据及经其处理得到的数据开展与车辆管理、行驶安全无关的数据处理活动；网联汽车采集的车辆位置、轨迹相关数据在车内存储设备、远程信息服务平台（TSP）中保存时间均不得超过 7 天；网联汽车行驶状态参数、异常告警信息等数据如需出境，应当符合国家关于数据出境的相关规定。

- 《数据出境安全评估指南》

在研的国家标准《数据出境安全评估指南》旨在积极研究借鉴国内外数据出境领域相关管理实践，紧密结合《网络安全法》和《办法》等上位法律法规的要求，搭建了一套科学、合理的个人信息出境安全评估的方法体系，可以为企业数据出境安全评估提供有效的规范指引。

国外的汽车企业在为中国地区的用户提供车联网云服务平台业务的过程中，需要采集用户的个人信息，并且有可能将数据传输到中国地区之外进行存储、分析，因此此标准对于规范汽车企业对用户数据的隐私保护与安全管理具有重要的指导意义。

- 《车联网信息服务 数据安全技术要求》（YD/T 3751-2020）

《车联网信息服务 数据安全技术要求》标准规定了车联网服务过程中数据生命周期内保护的总体要求，主要包括数据采集、传输、存储、使用、迁移、销毁、备份恢复等方面的安全保护要求。

《车联网信息服务 数据安全技术要求》标准规定的数据，涵盖车联网信息服务过程中的除了用户个人信息以外的所有数据，包括但不仅限于来自车辆、移动智能终端、路边设施和车联网服务平台等载体相关的数据。

- 《合作式智能运输系统 车用通信系统 应用层及应用层数据交互标准》（T/CSAE 53-2017）

中国汽车工程学会制定的《应用层及应用层数据交互标准》标准包含了三部分主体内容：17 个一期典型应用场景，支撑这些场景的应用层交互数据集，以及 API、SPI 接口。

《应用层及应用层数据交互标准》标准提出了一个“应用数据交换服务（ADS）层”的概念，负责应用数据的编解码以及交互控制，实现了具体应用场景与底层交互技术之间的隔离。ADS 层的核心是应用层交互数据集，即 V2X 技术的“语言和文字”。标准定义了 5 种基本的 V2X 消息，以及构成这些消息的数据帧与数据元素。在 ADS 层的下层定义了一套 SPI 规范，能够适应 LTE-V2X/DSRC 甚至未来 5G 等多种技术。在 ADS 层的上层则定义了一套参考性的 API 规范，以此向用户提供网联数据和操作接口，为用户封装繁琐的交互控制与数据编解码操作。

- 《车联网数据采集要求》（T/CSAE 100-2018）

中国汽车工程学会制定的《车联网数据采集要求》标准主要包含应用领域、数据采集周期、数据包结构和定义、数据流编码规则、数据采集项等几部分。

根据数据采集周期综合数据应用场景、现有技术实现能力及流量费用限制，可以将数据采集分为周期性数据采集和触发性数据采集两类。

数据包的结构和定义给出了数据封装和解读的整体规则。一个完整的数据包应由起始符、命令单元、识别码、数据加密方式、数据单元长度、数据单元和校验码组成，该标准给出了具体的定义。

数据流编码规则实现了数据流的统一管理，确保各方对数据流的定义保持一致，本标准对车联网数据流按周期性数据和事件触发性数据两类进行了规定。

- 《智能网联汽车数据共享安全要求》（T/CSAE 211-2021）

中国汽车工程学会（CSAE）联合中国智能网联汽车产业创新联盟（CAICV）制定了《智能网联汽车数据共享安全要求》规定了车联网服务过程中数据生命周期内保护的总体要求，主要包括数据采集、传输、存储、使用、迁移、销毁、备份恢复等方面的安全保护要求。

《智能网联汽车数据共享安全要求》标准规定的数据，涵盖车联网信息服务过程中除了用户个人信息以外的所有数据，包括但不限于来自车辆、移动智能终端、路边设施和车联网服务平台等载体相关的数据。

为提升数据的流通效率，使数据便于共享使用，《智能网联汽车数据共享安全要求》提出了智能网联汽车数据分级分类共享模型，建立科学、统一、通用的数据分类方式，规范智能网联汽车的内置属性数据和行驶数据。

《智能网联汽车数据共享安全要求》依据数据来源对数据做出初步划分，总体上分为车厂数据和第三方数据。根据数据的作用场景、影响范围、关联性等因素将数据分为不同的包（域）。每个包（域）由多个实体组成，实体中包含具体的属性字段。

为保证数据在存储与使用过程中的隐私安全，《安全要求》参考相关项目建立数据分级准则，保护隐私敏感数据。《智能网联汽车数据共享安全要求》根据不同类别数据遭到篡改、破坏、泄露或非法利用后，可能对个人、车厂、行业、社会秩序造成的潜在影响对数据进行分级，并结合智能网联汽车数据场景，提出数据安全等级五级分类方法。

5.2.11 信息安全和密码检测相关标准

- 《智能网联汽车证书认证系统密码应用检测规范》

密码行业标准化委员会在研的《智能网联汽车证书认证系统密码应用检测规范》标准规定了智能网联汽车证书认证系统的检测内容与检测方法，适用于对智能联网汽车证书认证系统产品检测，规范智能网联汽车证书认证系统中密码及相关安全技术的应用，也可为该类系统的研制提供参考。

- 《车载领域 SoC 密码安全子系统的保护轮廓和测评要求研究》

密标委在研项目《车载领域 SoC 密码安全子系统的保护轮廓和测评要求研究》聚焦对车载领域 SoC 芯片的密码安全子系统开展研究，涉及密码安全子系统的定义，边界和功能，以及密码安全子系统的相关测评要求和测评实施指导和建议。

该标准项目研究车载领域 SoC 密码安全子系统的密码技术现状、密码安全子系统的标准现状、密码安全子系统的边界定义和密码需求、密码安全子系统的测评要求、密码安全子系统如何适配当前国内测评体系等内容。并进一步探究该如何去测评车载领域 SoC 密码安全子系统，保证密码安全子系统的安全性，为后续此类密码安全子系统提供设计指南和测评指导。

- 《车载信息交互系统密码应用检测规范》

车载信息交互系统通常为远程车载信息交互系统（T-box）、车载综合信息处理系统（IVI）以及其混合体。密标委在研标准《车载信息交互系统密码应用检测规范》旨在制定适用于车载信息交互系统密码应用的检测内容与检测方法。该标准的草案从通用要求、硬件安全、软件/固件安全、通信安全、密钥安全、证书安全、数据安全等方面提出了车载信息交互系统密码应用的检测内容与检测方法。

5.3 密码应用相关标准研究

综合上述分析，车联网领域的信息安全问题已经获得了广泛的关注，在车联网领域存在很多密码应用的需求，并且 IEEE 1609.2 等标准均规定了密码技术的应用。在国际标准和国内标准都有较完整的标准体系规划，并且在方法论、安全管理、终端安全、通信安全、基础设施安全等各个层面形成了完整的体系，制定的安全标准也已经在车联网中获得了工程应用。

《车联网网络安全和数据安全标准体系建设指南》除了提出重点领域及方向，还给出了相关标准的明细表，主要从业务领域角度来梳理，涵盖了车联网应用的基础设施、网联通信和数据安全各个层面。在《指南》列出的建议标准中，除了“103 密码应用”之外，在“身份认证”、“平台安全”、“数据安全”等方向也涉及了密码应用相关的标准（参见表 5-1）。《指南》中规划的与密码相关的标准，其中部分为已经发布，也有部分是在研标准，但还有很多标准尚处于空白状态。

表 5-1　车联网网络安全和数据安全标准体系中密码相关标准

领域/方向	标准名称	标准号/计划号	状态
103 密码应用	车联网密码应用通用要求		待制定
	智能网联汽车商用密码应用技术要求		待制定
	车联网通信设备密码应用技术要求		待制定
	车云通信密码应用基本要求		待制定
302 身份认证	交通运输数字证书格式	GB/T 37376-2019	已发布
	基于 LTE 的车联网无线通信技术安全认证技术要求	2019-0021T-YD	制定中
	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	制定中
	基于 LTE 的车联网无线通信技术安全认证测试方法	2019-0022T-YD	制定中
	汽车数字证书应用规范		待制定
	车联网服务 V2X 安全证书应用接口规范		待制定
	车联网 V2X 密钥管理系统技术规范		待制定
	电子驾驶证安全技术要求		待制定
	车联网数字证书应用接口规范		待制定
	基于 PKI 的车联网应用服务安全认证体系框架		待制定
	车联网关键部件轻量级安全认证通用技术要求		待制定
401 通用要求	智能网联汽车数据保护密码应用技术		待制定

领域/方向	标准名称	标准号/计划号	状态
	要求		
405 应用数据安全	车联网应用服务数据脱敏实施方法		待制定
501 平台安全	车联网服务平台密码应用基本要求		待制定
	车联网在线升级（OTA）平台安全技术要求及检测方法		待制定
502 应用程序安全	车联网 APP 安全技术及测试要求		待制定
601 风险评估	车联网密码应用安全评估要求		待制定
602 安全监测与应急管理	车联网密码应用安全监测平台通用技术要求		待制定

密码行业标委会目前已经发布 132 余项行业标准，在《密码标准应用指南》（GM/Y 5001-2023）标准中从技术维度将这些标准分为密码基础类、基础设施类、密码产品类、应用支撑类、密码应用类、密码测评类、密码管理类等七大类别。已发布的密码相关的国标/行标既有基础性的算法标准，也有与业务场景紧密结合的应用类标准。有些标准可能与车联网应用完全无关，但是有很多标准都可能在车联网的系统和设备开发中相互结合，提升车联网系统的安全防护能力。

表 5-2 具体分析了相关的密码标准与车联网应用相互结合的潜在应用前景，从表格中可见在车联网产业链中的各类角色（设备部件厂家、车企、移动通信运营商、平台运营商、业务系统开发商等）均不可避免地需要应用密码相关的标准，以达到保障用户数据安全的目标，同时满足合规性要求。

表 5-2　密码相关标准在车联网的潜在应用分析

类别	标准号	标准名称	车联网潜在应用			
			智能网联汽车	安全通信	业务系统	云服务平台
密码标识	GM/T 0006	密码应用标识规范		协议互操作	协议互操作	协议互操作
密码算法	GM/T 0001	祖冲之序列密码算法		移动通信数据加密		
	GM/T 0002	SM4 分组密码算法			业务数据加密	数据库透明加密
	GM/T 0003	SM2 椭圆曲线公钥密码算法		BSM 消息签名	业务数据签名、加密	
	GM/T 0044	SM9 标识密码算法				
	GM/T 0004	SM3 密码杂凑算法		消息 HMAC	业务数据完整性	日志完整性
算法使用	GB/T 17964	分组密码算法的工作模式			数据加密模式	数据加密模式
	GB/T 31503	电子文档加密与签名消息语			文档数据安全	

类别	标准号	标准名称	车联网潜在应用			
			智能网联汽车	安全通信	业务系统	云服务平台
		法				
	GM/T 0009	SM2 密码算法使用规范		BSM 消息签名	业务数据签名、加密	
	GM/T 0010	SM2 密码算法加密签名消息语法规范		BSM 消息签名	业务数据签名、加密	
	GM/T 0080	SM9 密码算法使用规范				
	GM/T 0081	SM9 密码算法加密签名消息语法规范				
密钥管理	GB/T 17901	密钥管理			密钥分发	
	GM/T 0091	基于口令的密钥派生规范			用户身份鉴别	
密码协议	GB/T 38636	传输层密码协议(TLCP)			安全通道建立	安全通道建立
基础设施	GM/T 0014	数字证书认证系统密码协议规范		信任体系构建	信任体系构建	信任体系构建
	GM/T 0034	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		信任体系构建	信任体系构建	信任体系构建
	GM/T 0015	基于 SM2 密码算法的数字证书格式规范		（身份）数字证书格式	数字证书格式	数字证书格式
	GM/T 0089	简单证书注册协议规范				设备证书配置
	GM/T 0092	基于 SM2 算法的证书申请语法规范			证书在线申请	证书在线申请
	GM/T 0093	证书与密钥交换格式规范			私钥转移	私钥转移
	GM/T 0094	公钥密码应用技术体系框架规范		信任体系构建	信任体系构建	信任体系构建
密码产品	GM/T 0028	密码模块安全技术要求	OBU 密码模块规格		密码设备规则	密码设备规则
	GM/T 0078	密码随机数生		随机数安	随机数安	随机数安

类别	标准号	标准名称	车联网潜在应用			
			智能网联汽车	安全通信	业务系统	云服务平台
		成模块设计指南		全	全	全
	GM/T 0082	可信密码模块保护轮廓	OBU 密码模块规格		密码设备规则	密码设备规则
	GB/T 29829	可信计算密码支撑平台功能与接口规范	OBU 处理器安全			平台安全防护
	GM/T 0016	智能密码钥匙密码应用接口规范			UKey 互操作	UKey 互操作
	GM/T 0018	密码设备应用接口规范			密码设备互操作	密码设备互操作
	GM/T 0087	浏览器密码应用接口规范			终端互操作	
	GM/T 0051	对称密钥管理技术规范			密钥安全管理	密钥安全管理
	GM/T 0088	云服务器密码机管理接口规范				密码资源池管理
	GM/T 0021	动态口令密码应用技术规范			用户身份鉴别	
	GM/T 0022	IPSec VPN 技术规范			安全通道建立	安全通道建立
	GM/T 0024	SSL VPN 技术规范			安全通道建立	安全通道建立
	GM/T 0030	服务器密码机技术规范			密码设备规格	密码设备规格
	GM/T 0029	签名验签服务器技术规范			密码设备规格	密码设备规格
	GM/T 0031	安全电子签章密码技术规范			业务审批安全	业务审批安全
	GM/T 0026	安全认证网关产品规范			统一身份管理	统一身份管理
应用支撑	GM/T 0032	基于角色的授权管理与访问控制技术规范			统一身份管理	统一身份管理
	GM/T 0067	基于数字证书的身份鉴别接口规范			统一身份管理	统一身份管理
	GM/T 0033	时间戳接口规范			数据防篡改	数据防篡改

类别	标准号	标准名称	车联网潜在应用			
			智能网联汽车	安全通信	业务系统	云服务平台
	GM/T 0068	开放的第三方资源授权协议框架		注册证书申请身份识别	统一身份管理	统一身份管理
	GM/T 0069	开放的身份鉴别框架		注册证书申请身份识别	统一身份管理	统一身份管理
密码应用	GM/T 0035	射频识别系统密码应用技术要求	电子车钥匙			
	GB/T 39786	信息安全技术信息系统密码应用基本要求			业务系统建设合规性	平台建设合规性
	GM/T 0098	基于 IP 网络的加密语音通信密码技术规范		IP 电话安全		
	GM/T 0099	开放式版式文档密码应用技术规范			业务单证安全	
	GM/T 0036	采用非接触卡的门禁系统密码应用技术指南				机房门禁安全
检测认证	GM/T 0005	随机性检测规范	OBU 密码模块认证			
	GM/T 0039	密码模块安全检测要求	OBU 密码模块认证			

尽管相关密码标准在车联网及智能网连汽车中有很多潜在的应用场景，但是目前已发布密码行业标准在很多层面还不足以完全支撑车联网领域的业务需求。为了满足车联网的快速发展迫切，一方面需要密码从业单位在密码技术、密码产品和标准化等方面开展自主创新，深入研究密码技术与车联网的深度融合，推出适用市场需求的新产品与新服务模式；另一方面也需要通过标准引领作用来促进密码技术/产品/标准与车联网领域的深度融合，既要根据应用需求优化和完善已有标准，制定迫切需要的新标准，同时也要促进密码标准与相关标准化组织的交叉融合，最大化释放密码技术与产品在车联网领域的产能。

在分析发展现状和密码应用需求的基础上，本文作者建议相关标准化组织重点考虑考虑表 5-3 列出的若干标准化方向，并优先开展通用性、基础性的标准，同时优先考虑产业亟需解决的数据规范、服务规范、互联互通规范等难点。

表 5-3　密码相关的标准化方向

序号	建议的标准化方向	必要性或意义
1	轻量级密码算法	轻量级密码可实现在安全、成本和实现效率之间权衡，对于车载设备中资源受限的 ECU 等部件有较好的应用潜力，在提高安全性的同时可以降低相关设备的制造成本。
2	车联网 HSM 设计指南	密码厂家在设计与开发适用于 OBU 设备的 HSM 模块时，可以参考 GM/T 0028-2014《密码模块安全技术要求》和 GM/T 0039-2015《密码模块安全检测要求》等行业标准，然而还应充分考虑车联网 PKI 体系的特殊性，研究适用于 OBU 设备的 HSM 模块的设计方法。
3	车联网 HSM 接口规范	车载终端的 HSM 密码模块必须支持密钥衍生机制，支持在不同时刻切换并使用大量的用户私钥。由于 GM/T 0016-2012《智能密码钥匙密码应用接口规范》和 GM/T 0018-2012《密码设备应用接口规范》等标准中并没有充分考虑此类特殊需求，因此不能有效支撑这些密码应用。
4	汽车网关密码应用技术研究	CAN 总线和以太网总线及其对应的网关设备的安全设计，对于车内通信安全有至关重要的作用，在《汽车网关信息安全技术要求》的基础上，还有待进一步深入研究在汽车网关的产品设计中如何应用密码技术来应对和解决各种安全威胁，实现通信安全、权限控制、固件安全防护、日志的完整性保护等安全目标。
5	数字车钥匙密码应用指南	通过分析基于移动智能终端的数字车钥匙的信息安全威胁，研究数字车钥匙系统中应用密码技术的技术架构和关键技术点，可以为移动智能终端设备商、移动智能终端应用商、智能网联车解决方案供应商与车辆制造企业等开展数字车钥匙系统的设计提供参考性指导。
6	车联网服务 V2X 安全证书应用接口规范	基于车联网领域数字证书的特殊应用需求，尤其是隐式证书的应用，制定新的规范或修订已有的相关规范。
7	车联网 V2X 密钥管理系统技术规范	V2X 设备的密钥类型与传统产品有较大的差异，除了密钥衍生机制之外，AUTOSAR 提出的 SHE 规范也提出了全新的管理模式，因此有必要研究 V2X 密钥管理系统的密钥管理层次，提出密钥管理系统的技术架构，规定密钥生命周期各环节的流程与接口要求，并且对密钥管理的关键元数据进行定义，为车联网中密钥管理体 8 系的设计与产品实现提供指导。
8	车联网关键部件轻量级安全认证密码应用指南	分析汽车网关和 ECU 等车载设备对于轻量级密码算法的需求，并指明如何将轻量级密码算法用于实体身份认证与数据加密等安全目标。

序号	建议的标准化方向	必要性或意义
9	车联网 PKI 跨域互认互通机制研究	根据实际应用需要，研究适用于车联网领域的跨域互认策略，提出更多的跨域互认互通模型。同时还可考虑异常行为管理机构（MA）对于跨域互认互通的影响，研究跨域的黑名单管理和 CRL 聚合等关键技术，研究信任列表及黑名单/CRL 的大规模快速分发的相关技术，为跨域互认互通的高可用提供切实可行的技术路线。
10	LTE V2X 证书认证系统密码及其相关安全技术规范	基于 GM/T 0034 提出适用于车联网领域的证书认证系统的技术要求，针对注册证书、假名证书、身份证书、应用证书和机构证书的全生命周期管理提出相关功能要求，规范化 RA 与 CA 的信息交互格式，并规范化设备注册、设备身份认证、证书签发、证书撤销列表生成与签发、证书/链接值/证书撤销列表存储以及安全管理等过程。在此基础上还可以考虑制定关联的检测规范。
11	车联网服务平台安全接入技术指南	分析车联网服务平台的安全接入风险，研究车联网服务平台的安全接入框架，对接入的车辆、人员、第三方企业及机构进行细粒度的授权及动态访问控制，降低安全风险。
12	车联网在线升级（OTA）平台安全技术要求及检测方法	研究并提出车联网在线升级（OTA）平台的总体技术架构，定义标准的 OTA 更新流程，规定在 OTA 更新过程中如何应用代码签名技术来保护分发的更新固件的完整性和认证性。
13	智能网联汽车数据保护密码应用指南	通过研究并提出在车联网中的汽车数据的分类与分级，并针对各类汽车数据的防护提出密码技术方案，可以指导智能网联汽车在设计、生产、销售、使用、运维等过程中数据处理活动的密码应用。
14	车联网电子认证服务运营管理规范	在 GB/T 28447 的基础上，充分考虑 PKI 体系架构与传统 PKI 的差别（如包括 PRA/PCA/LA/MA 等不同的运营实体），充分考虑个人隐私保护的安全需求，为建设和运营面向车联网的电子认证服务提供指引。

6 总结

本研究报告深入分析了车联网领域的技术及标准发展现状，通过分析车联网的信息安全风险和安全目标，挖掘车联网的密码应用需求，从智能网联汽车、安全通信、车联网服务平台、证书管理等层面分析密码应用的技术路线、安全框架，并给出典型密码应用案例。在此基础上，分析了国外、国内有关车联网的信息安全标准、密码应用标准，最后分析了密码相关标准在车联网的应用前景，并提出了建议的标准化方向。

本报告有助于读者全面了解车联网中密码应用的需求与潜力，同时也为车联网产业链的厂家制定标准提供了有益的思路和方向。

附录 A　Butterfly 密钥衍生机制

由于隐私保护的需求，在 V2X 通信系统中需要使用大量的假名证书，与此同时将需要在设备中生成数千个公钥。设备从 PKI 系统请求证书的典型过程是：设备生成私钥/公钥对，创建包括公钥的证书签发请求（CSR），并通过安全通道将 CSR 提供给 PKI 系统；然后，PKI 系统的 CA 将签署证书并将其提供给申请人。如果使用传统的模式，将会需要传输大量的 CSR 数据，导致系统效率过低。为了克服上述缺点，在 V2X 通信系统中引入了一种新颖的密码结构——Butterfly 密钥衍生机制，这种机制使得设备可以同时申请任意数量的 V2X 证书。

下面介绍 SCMS 体系中建议的 Butterfly 密钥衍生机制[15]。图 A-1 概述了用于签名密钥的 Butterfly 密钥扩展的原理。

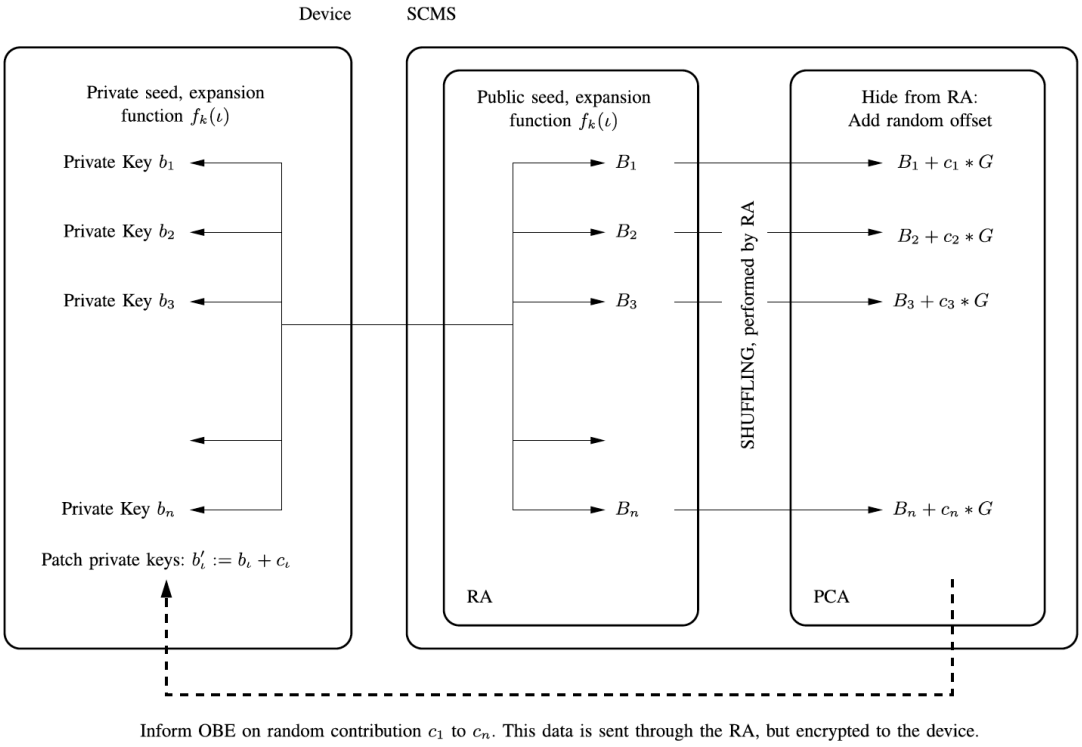

图 A-1　Butterfly 密钥扩展原理

PCA 为设备签发的每个 V2X 证书具有不同的签名密钥，并且每个 V2X 证书均具有不同的加密密钥。如果没有 Butterfly 密钥扩展，设备必须为每个 V2X 证书发送唯一的签名密钥和唯一的加密密钥。Butterfly 密钥扩展的提出使得设备仅需要提交一个请求即可获得大量 V2X 证书，并且提交的请求中仅需包含一个签名公钥种子、一个加密公钥种子和两个扩展函数。Butterfly 密钥扩展缩减了上传信息的大小，允许设备网络连接不佳的情况下发出证书申请，并且还减少了设备计算密钥的工作量。此外，由 PCA 发送到设备的证书将被加密，使得 RA 无法将 V2X 证书与某个设备关联。

典型的 Butterfly 密钥扩展基于 ECC 密码体制，但是可以很容易将其推广到其他的密码体制。加密密钥的 Butterfly 扩展与签名密钥类似，只是在使用对称加密算法进行派生时，输入内容上有一个细微差别。

在下文中，用小写字母表示整数，用大写字母表示椭圆曲线点。假定 ECC 的基点为G，其阶为l。种子密钥对（caterpillar keypair）是整数a和曲线点$\mathrm{A}=[\mathrm{a}]\mathrm{G}$。设备向 RA 提供公钥$\mathrm{A}$和签名密钥扩展函数$\mathrm{f}_{\mathrm{k}}(\iota)$，典型的签名密钥扩展函数$\mathrm{f}_{\mathrm{k}}(\iota)$定义为

$$f_k(\iota)=f_k^{int}(\iota)\ mod\ l$$

其中，

- $f_k^{int}(\iota)$是如下计算结果的大端整数表示：$DM_k(x+1)|\left|DM_k(x+2)\right||DM_k(x+3)$；
- $DM_k(m)$是在 Davies-Meyer 模式下使用密钥k对m进行对称加密的结果，其中对称加密的输出与输入进行异或运算以生成最终输出，即：$DM_k(m)=AES_k(m)\oplus m$；
- 每次简单地将x加 1 即可获得$x+1$，$x+2$和$x+3$；
- 从时间段$\iota=(i,j)$根据运算$x=\left(0^{32}||i||j||0^{32}\right)$来得出对称加密的 128 位输入$x$。

加密密钥的密钥扩展函数也如上定义，但是导出x的方式调整为$x=\left(1^{32}||i||j||0^{32}\right)$。$i$是全局值（例如代表一个星期）；$j$是$i$周期内的计数器，并且对应于每个$i$的证书数量（例如每周 20 个证书）。

请注意此处对称加密使用 Davies-Meyer 模式，因为f_k并不需要可逆运算。此外，执行对称加密 3 次以确保f_k的输出均匀分布，并且可以忽略产生的误差。

RA 在获得了种子公钥 A 之后，可以基于公钥 A 来按规则生成2^{128}个派生公钥（cocoon public keys），每一个派生公钥的形式如$B_\iota=A+[f_k(\iota)]G$，其对应的私钥是$b_\iota=a+f_k(\iota)$。RA 在生成派生公钥之后，将向 PCA 发送证书请求，并在证书请求中包含这些派生公钥。请注意此处 RA 仅获知了签名公钥，而只有设备才能获得对应的签名私钥。

如果 PCA 在收到这些扩展的签名公钥之后，直接用于签发 V2X 证书，则 RA 可以根据 V2X 证书中的公钥来跟踪设备。为了避免这种情况，PCA 将为每一个派生公钥B_ι均产生一个随机数c_ι，并且计算曲线点$C_\iota=\left[c_\iota\right]G$，并且计算$B_\iota+C_\iota$作为 V2X 证书的公钥。PCA 将 V2X 证书和私钥重构参数c_ι一并返回给 RA，并由 RA 下发给设备。PCA 会对证书和私钥重构参数进行加密，然后以密文形式发到 RA，从而防止 RA 根据证书内容来跟踪设备。

PCA 必须使用不同的密钥来对每个证书进行加密，而每个证书的加密密钥也通过 Butterfly 密钥扩展方法生成。在提交证书申请时，设备还提供了一个种子加密公钥$H=[h]G$，RA 将其扩展为派生加密公钥$J_\iota=H+\left[f_e(\iota)\right]G$，而 PCA 使用这些密钥来加密返回的数据。设备在获得 PCA 返回的数据之后，必须重建派生加密公钥J_ι对应的加密私钥，然后利用加密私钥来解密 PCA 返回的数据，从而获得私钥重构参数c_ι，现在设备可以计算出与 V2X 证书对应的私钥$b_\iota^{'}=b_\iota+c_\iota$。

上述介绍的 Butterfly 密钥衍生机制，使得 RA 联合 PCA 可以为设备同时签发大批量的 V2X 证书。并且通过合理设计的流程，使得 RA 和 PCA 均无法利用传递的数据追踪设备与 V2X 证书的对应关系。

附录 B　假名证书的批量撤销机制

对于 V2V 安全应用程序，每个设备都收到大量证书，这种情况下传统的 CRL 会变得太大而无法使用。为了解决 CRL 文件太大的问题，SCMS 通过使用链接值的新概念来高效地撤销设备以及对应的假名证书[15]。在链接值的生成过程中则需要应用密码杂凑算法。

B.1 链接值的生成

SCMS 会在提供给设备的某一组假名证书中插入链接值，并可以基于这些链接值来撤消所有等于或晚于某个时间i（例如当前星期）的 V2X 证书。

SCMS 设置了 LA 角色来负责预先生成预链接值（pre-linkage），然后由 PCA 将来自两个 LA 实体（如LA_1和LA_2）生成的预链接值执行异或运算，并将计算结果作为 V2X 证书中的链接值。

图 B-1 概述了链接值的生成过程。

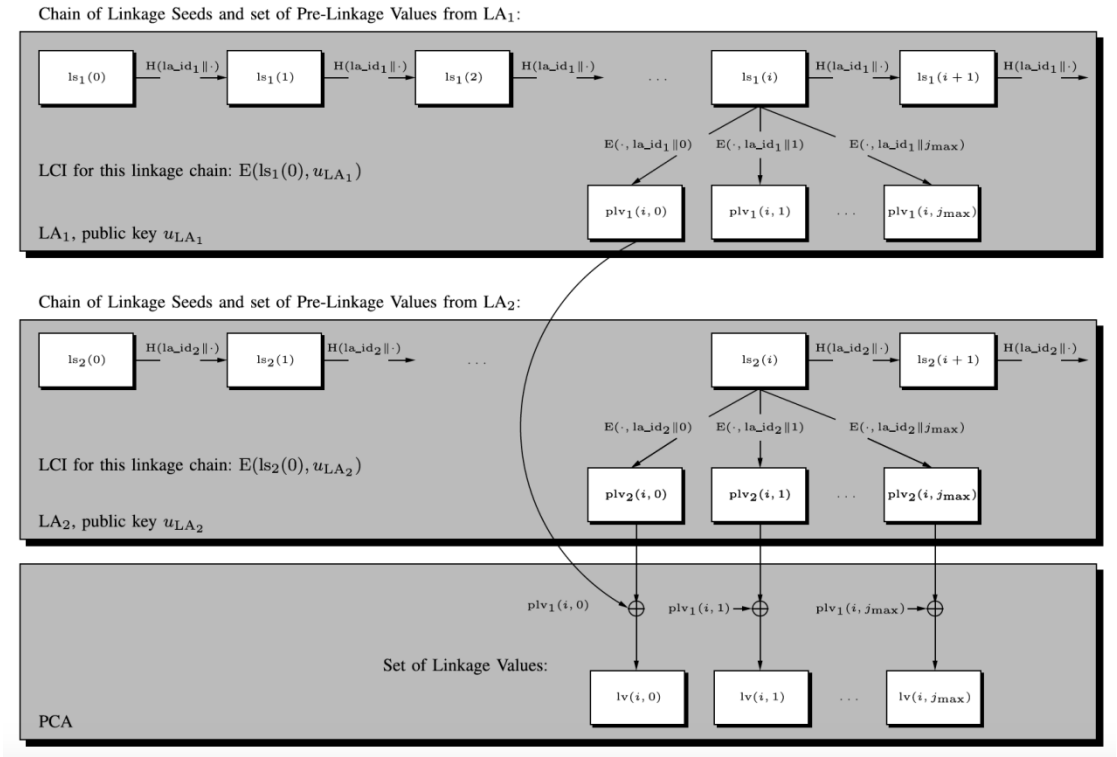

图 B-1　链接值的生成

其中，la_id_1，la_id_2分别为与LA_1，LA_2关联的 32 位标识字符串。对于一组 V2X 证书，首先LA_1（或者LA_2）选择一个随机的 128 位字符串，称为初始链接种子$ls_1(0)$（或者$ls_2(0)$），然后每一个周期（例如一周）$i > 0$计算链接种子$ls_1(i) \leftarrow H_u\left(la_id_1 || ls_1(i-1)\right)$（或者$ls_2(i) \leftarrow H_u\left(la_id_2 || ls_2(i-1)\right)$）。其中，$H_u(m)$表示采用密码杂凑算法在$m$上

输出的u个最高有效字节，而$a||b$表示位串a和b的串接。SCMS 建议使用$u=16$。请注意，由 LA 创建的链接种子（即杂凑链）具有易于前向计算的属性（即从$ls(i-1)$计算$ls(i)$），但是后向计算是在计算上不可行的（即从$ls(i)$计算$ls(i-1)$）。可以采用伪随机函数来计算预链接值，SCMS 选择了应用 Davies-Meyer 模式的对称加密算法来实现此功能。每个 LA 将链接种子加密为$plv_x(i,j) \leftarrow \left[E\left(ls_x(i),\left(la_id_x||j\right)\right)\oplus\left(la_id_x||j\right)\right]_v$，$x\in\{1,2\}$，其中$E(k,m)$是用密钥$k$对$m$执行对称加密，a$\oplus b$是位串$a$，$b$的异或，$[a]_v$表示位串$a$的$v$个有效字节。SCMS 建议灵活地使用$v$来说明已部署设备的数量以及潜在的基于密码的原始密码学弱点的抗碰撞性。目前，$v=9$似乎足够。i表示时间段（例如一星期），j表示时间段内的证书（例如每周 20 个证书）。每个 LA 都以相同的方式计算预链接值，但是每个设备都有随机选择的初始种子。将结果值表示为plv_1和plv_2。为了从 LA 中选择特定的链接链，使用链接链标识符（LCI）。LCI 是LA_1和LA_2的初始链接种子$ls_1(0)$或$ls_2(0)$分别是对自身进行加密的结果。例如，$E\left(pk_1,ls_1(0)\right)$，其中$pk_1$是$LA_1$的公钥。

LA 分别为 PCA 加密单个预链接值，但将其发送给 RA 用于关联证书请求。PCA 通过将预链接值执行异或来获得链接值$lv=plv_1\oplus plv_2$。

B.2 基于链接值逆向解析注册证书及链接种子

如果在不当行为调查期间确定设备确实存在异常，则 MA 会将设备吊销并列入黑名单。为了实现证书吊销和将设备列入黑名单，MA 需要联合 PCA、RA 和 LA 执行图 B-2 所示的假名证书吊销过程，确定链接种子和对应于假名证书的注册证书。

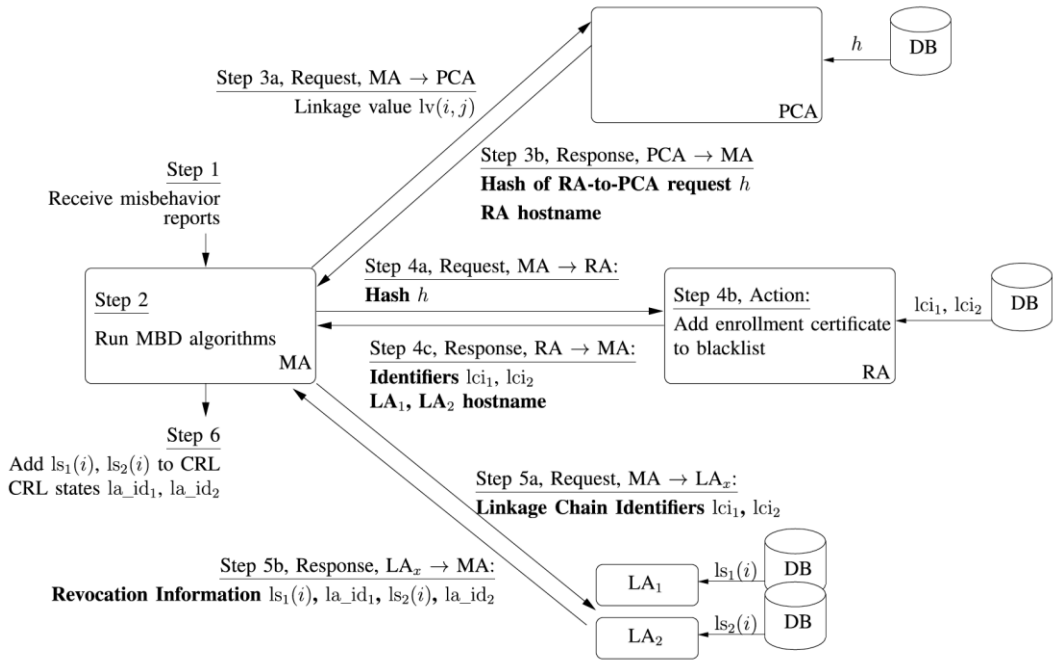

图 B-2　假名证书吊销

步骤 1、步骤 2 描述了不当行为调查的过程。

步骤 3. MA 请求 PCA 将所标识的假名证书的链接值lv映射到 RA 到 PCA 的假名证书请求的对应杂凑值。PCA 将该杂凑值和相应 RA 的主机名返回给 MA。

步骤 4. MA 将 RA 到 PCA 的假名证书请求的杂凑值发送到 RA。RA 可以将杂凑值映射到相应的注册证书，并将其添加到其黑名单中。RA 不会向 MA 透露注册证书。MA 从 RA 接收以下信息，然后将其用于收集撤销所必需的信息：

- 创建假名证书链接值所涉及的 LA 的主机名；
- 每个 LA 的 LCI 数组。LA 可以使用 LCI 查找链接链和底层链接种子。作为一种例外情况，仅当设备拥有来自多个独立链接链的证书时，RA 才会返回多个链接链标识符。

步骤 5. MA 请求LA_1（或相应的LA_2）将lci_1（或lci_2）映射到链接种子$ls_1(i)$（或$ls_2(i)$），其中i是当前有效时间段。两个 LA 都将其链接种子返回给 MA。此外，每个 LA 向 MA 提供其链接授权机构标识符（la_id_i）。注意，给定一个链接种子$ls_1(i)$和相应的la_id_i，仅可以计算前向链接种子（即$j \geq i$时的$ls_1(j)$），因此可以保持已撤销设备的后向隐私。

步骤 6. MA 将链接种子$ls_1(i)$和$ls_2(i)$以及对应的一对链接授权机构标识符la_id_1，la_id_2添加到 CRL。CRL 中全局标识当前时间段i。出于效率原因，CRL 可以将具有相同链接授权机构标识符对的条目分组在一起，以节省空中接口的字节。然后，MA 的 CRLG 签署 CRL 并将其发布。

B.3 CRL 分发及处理

当前用于 CRL 分发的基准方法是通过多个通道（例如 RSU、蜂窝、卫星通信或客户 WiFi）分发到每个设备。一种可能的创新方法是使用分布式协作分发模型。在协作分发中，某些设备提供最初的 CRL 种子（通过 RSU、蜂窝数据或其他某种方式），然后在正常事件过程中将 CRL 分发给驶过它们的对等设备。收到 CRL 的设备将依次成为分发者，从而可以使用少量的初始播种者来有效覆盖整个系统。

如图 B-3 所示，为了从某个时间段i以后撤消给定设备的所有假名证书，种子$ls_1(i)$和$ls_2(i)$，LA 标识符la_id_1，la_id_2以及时序信息i和j_{max}都发布在 CRL 并分发。接收到 CRL 的设备会分别对两个种子值独立地执行杂凑处理，计算当前时间段的预链接值，然后对这些预链接值进行异或运算以获得当前链接值。图 B-3 显示了在时刻i撤销给定设备所需发布的信息，以及查找该设备和$i' > i$的所有可能链接值的过程。注意，此机制可保护后向隐私，因为在发布链接种子之前无法在一段时间内确定已撤销设备的证书。

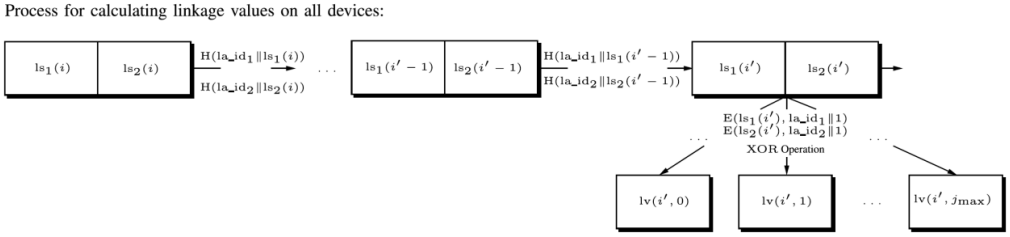

图 B-3　链接值撤销

附录 C　隐式证书简介

SCMS 建议强制要求使用隐式证书进行 V2X 通信。与更传统的证书形式有所不同，隐式证书通过将公钥和签名组合为单个值（称为重建值）来节省空间。为了验证此证书的所有者签名的消息，接收者首先必须通过组合 CA 的公共密钥和重建值来重建关联的公钥。

C.1 ECQV 隐式证书

一种类型是椭圆曲线 Qu-Vanstone（ECQV）隐式证书[22]。ECQV 证书没有显式说明标识符，公钥和签名，而是具有公钥的大小，并且需要从隐式证书中重建信息。对于公共密钥和 CA 签名，隐式证书仅需要 33 个字节，而不是 97 个字节。

图 C-1 描述了 Bob 向 Alice 颁发 ECQV 隐式证书的过程，其中 u;U 是颁发者密钥对，V 是公钥重构值，s 是私钥重构值，H 是防冲突哈希函数，并且 meta 对应于与证书关联的某些元数据，例如有效期或某些标识有关主题或发行者的信息。

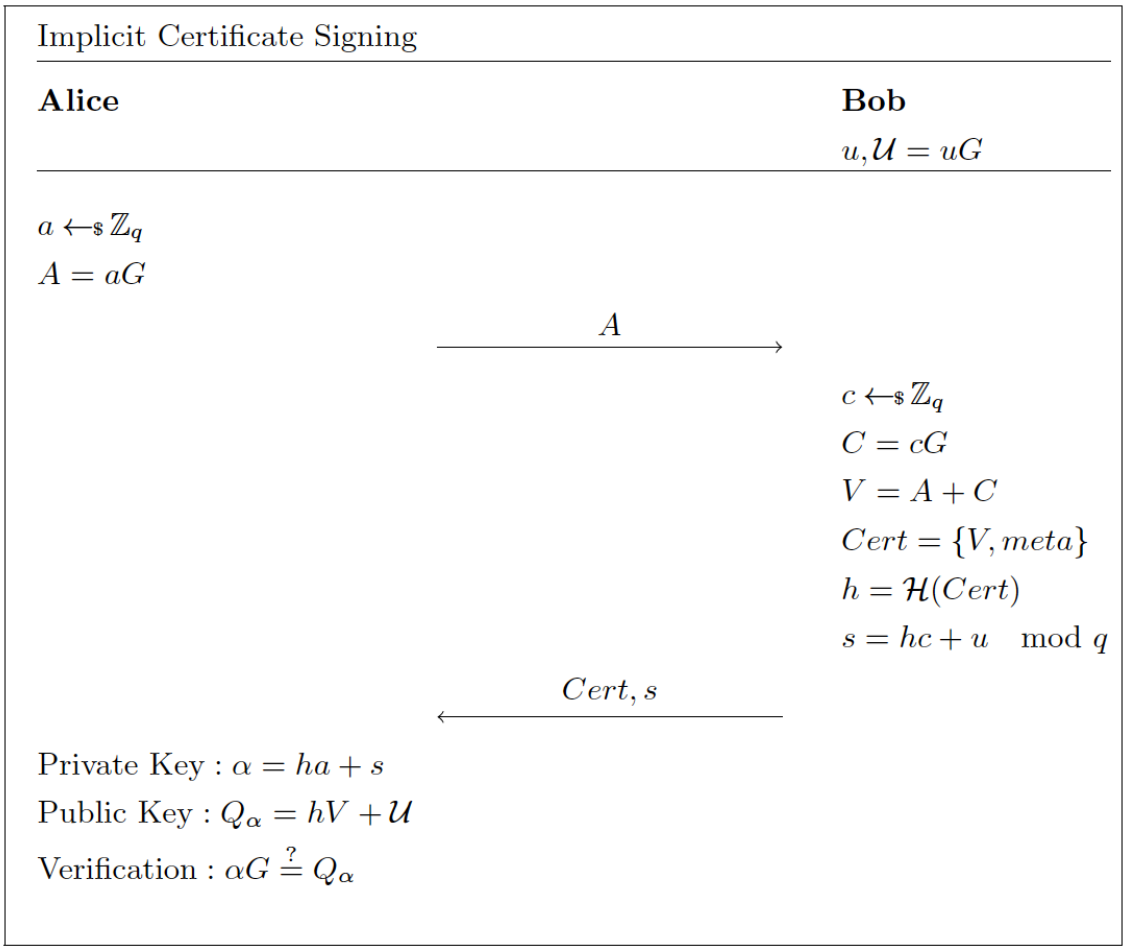

图 C-1　ECQV 隐式证书的颁发过程

图 C-2 描述了 SCMS 中提出的隐式证书设置过程，其中隐式证书是 ECQV 证书，如中所定义。请注意，我们有时也将这些隐式证书称为化名证书，因为这是它们在 SCMS 中给出的名称。

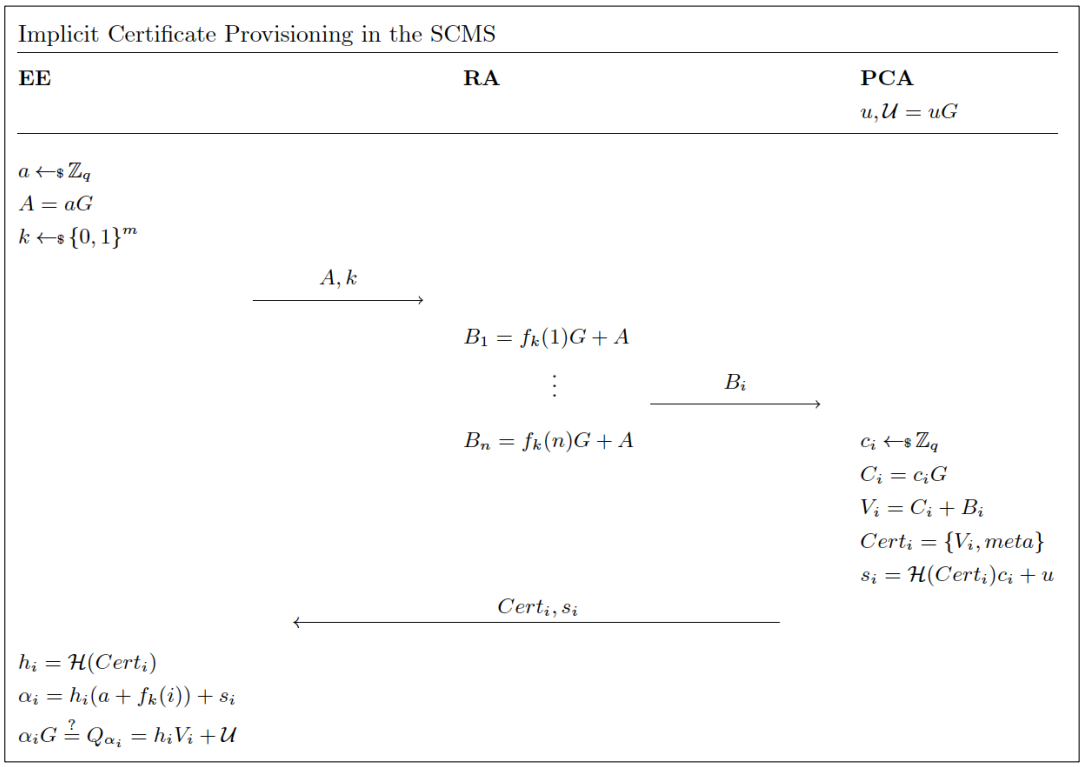

图 C-2　ECQV 隐式证书设置过程

验证隐式证书的本质上有两个目的：首先，它确保 EE 确实是颁发证书的 PCA；其次，它确保认证的值是提交的证书：因此，确保了公众的利益。重建密钥对应于私有重建密钥，因此其他参与者将能够验证消息上的签名。

支持批量验证的另一个更务实的观点是，一个无效的认证证书的存在可能意味着 RA 或更糟的 PCA 受到损害这一事实。在这种情况下，准确了解哪个证书可能是次要问题，因此应丢弃整批作为预防措施。

C.2 SM2 隐式证书

密码行业标准化技术委员会已发布的《基于 SM2 算法的无证书及隐式证书公钥机制》（GM/T 0130-2023）标准描述了基于 SM2 算法构造的无证书公钥机制和隐式证书公钥机制，包括密钥生成与校验机制、数字签名机制、公钥加密机制。

在标准的第 6 章给出了一种由 KGC 与用户协同生成密钥对的流程，如图 C-3 所示。采用标准给出的密钥生成机制，可将 KGC 产生的 W_A 参数作为隐式证书的公钥还原参数。

用户A和KGC一起协同生成用户的密钥对:用户私钥d_A和声明公钥W_A。两者应实现以下运算步骤:

A_1：用户A用随机数发生器产生随机数$d_A' \in [1, n-1]$；

A_2：用户A计算$U_A=[d_A']G$，并将标识ID_A和U_A提交KGC；

KGC_1：KGC计算$H_A=H_{256}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_{Pub} \| y_{Pub})$；

KGC_2：KGC用随机数发生器产生随机数$w \in [1, n-1]$；

KGC_3：KGC计算$W_A=[w]G+U_A$；

KGC_4：KGC按GB/T 32918.1-2016中4.2.6和4.2.5给出的方法将W_A的坐标x_{WA}、y_{WA}的数据类型转换为比特串，计算$\lambda=H_{256}(x_{WA} \| y_{WA} \| H_A) \bmod n$，按 GB/T 32918.1-2016中4.2.4和4.2.3给出的方法将λ的数据类型转换为整数；

KGC_5：KGC计算$t_A=(w+\lambda * ms) \bmod n$，并将$t_A$和$W_A$安全地返回给用户A；

A_3：用户A计算$d_A=(t_A+d_A') \bmod n$；

A_4：如果$0<d_A<n-1$，则输出(d_A, W_A)；否则返回A1。

生成加密密钥对时，KGC可使用确定性方法生成t_A和W_A。生成方法见附录D。

KGC将t_A返回用户A时可使用U_A作为公钥使用加密方法ENC加密包括t_A的数据后将密文传递到用户A。用户A使用d_A'解密密文后还原包括t_A的数据。

注：在隐式证书系统中，步骤KGC_3生成的W_A为隐式证书中的公钥还原数据，步骤A_3生成用户私钥。

图 C-3　SM2 隐式证书的用户密钥对生成过程

在标准的附录 B 中还给出了使用密钥机制生成密钥对和隐式证书以及使用数字签名机制保护消息的一个示例，具体的隐式证书格式和签名应用可参见标准文本。

参考文献

[1] 杨南，康荣保，车联网安全威胁分析及防护思路，通信技术 2015,48(12),1421-1426
[2] 郭蓬等，LTE-V2X 标准分析及发展现状的研究，中国汽车 China Auto，2019
[3] 中国智能网联汽车产业创新联盟，V2X“三跨”互联互通应用示范专报，2019 年第 01 期（总 004 期）
[4] IMT-2020(5G)推进组 C-V2X 工作组，车联网 C-V2X“四跨”先导应用实践活动总结报告（2022）
[5] 刘宴兵，王宇航，常光辉，车联网安全模型及关键技术，西华师范大学学报（自然科学版），2016,37(01)
[6] 中国通信标准化协会（CCSA），车路协同系统的安全研究
[7] AUTOSAR, Requirements on V2X communication
[8] ENISA, Cyber Security and Resilience of Smart Cars
[9] 刘彤彤，车联网终端 T-Box 技术及信息安全分析
[10] 冯志杰，何明，李彬，邓明，汽车信息安全攻防关键技术研究进展，信息安全学报， 2017,2(02),1-14
[11] Apple Inc., Apple Platform Security, May 2021
[12] Lennert Wouters; Benedikt Gierlichs; Bart Preneel; My other car is your car: Compromising the Tesla Model X keyless entry system, CHES 2021
[13] T/TAF 074-2020 移动智能终端数字车钥匙 信息安全技术要求
[14] 李露，车联网环境下基于假名的隐私保护研究，重庆邮电大学，2017 年
[15] B Brecht , etc., A Security Credential Management System for V2X Communications, IEEE Transactions on Intelligent Transportation Systems, 2018
[16] YD/T 3957-2021《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
[17] 徐秀等，车联网密码应用体系研究，信息通信技术与政策，2020 年第 8 期
[18] 陈维，李源，刘玮，车联网产业进展及关键技术分析，中兴通讯技术，2020 年 2 月
[19] 中国移动，车联网通信安全与基于 GBA 的证书配置白皮书（2019 年）
[20] 中国通信学会，车联网安全技术与标准发展态势前沿报告，2019 年
[21] 汽标委智能网联汽车分标委，智能网联汽车数字证书应用技术要求研究报告，2021 年
[22] The Standards for Efficient Cryptography Group (SECG), SEC4：Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), Version 1.0, 2013