《智能网联汽车 商用密码应用技术要求》标准化需求研究报告

2021 年 6 月

目录

1 引言

1.1 研究背景

（1）智能化、网联化成为汽车行业发展趋势

据统计，2020 年，我国智能网联汽车（L2 级）销量为 303.2 万辆，同比增长 107%，全年智能网联汽车（L2 级）销量占比达到 15%，在 12 月达到峰值 18%，可以预见，未来智能网联汽车渗透率将持续攀升。在当前汽车销售总量缩水的情况下，智能网联汽车销量逆势大幅上涨，反映了消费者对智能网联汽车产品的接受和认可，汽车的智能化、网联化已毋庸置疑地成为行业发展趋势。

（2）智能网联汽车信息安全问题引起行业高度重视

智能网联汽车产业带来新的经济增长点的同时也带来了新的安全风险，相较于传统网络空间的安全问题，汽车信息安全问题具有攻击面更广、隐蔽性更强、危害性更大等特点，不仅威胁人身财产安全，对社会公共秩序甚至国家安全均造成重大影响，汽车信息安全问题引起行业广泛重视。

2017 年 12 月，国家标准委批准成立全国汽车标准化技术委员会智能网联汽车分委会，下设信息安全工作组，我国汽车信息安全标准化工作开始系统展开，目前全国汽车标准化技术委员会已规划汽车信息安全国家标准 23 项，其中 7 项标准正在制定，4 项标准报批。此外，全国信息安全标准化技术委员会、全国通信标准化技术委员会组织制定的多项汽车信息安全相关标准也已发布。2021 年 1 月，欧盟

WP.29 法规 UN R155 信息安全与信息安全管理体系正式生效，自 2022 年 7 月起，信息安全将成为欧盟车辆准入的最新强检项，所有车辆必须通过信息安全管理体系认证和车辆型式审批。

世界各国纷纷开展汽车信息安全顶层设计，国内外主流汽车企业已充分认识到信息安全的重要性，并开始从汽车的全生命周期开展各项相关工作。

（3）国家鼓励商用密码技术应用，但密码对于汽车信息安全的基础支撑和核心保障作用未充分发挥

国家高度重视密码的安全保障作用，鼓励商用密码技术应用。

2020 年 1 月 1 日，《中华人民共和国密码法》正式实施，规范密码应用和管理，保障网络与信息安全，已上升至立法高度。《密码法》第 21 条和第 25 条，明确提出国家鼓励商用密码技术的研究开发，鼓励从业单位自愿接受商用密码检测认证，提升市场竞争力。

2018 年 7 月，中共中央办公厅、国务院办公厅印发《金融和重要领域密码应用与创新发展工作规划（2018-2022 年）》的通知中提出，要在 30 个重要领域推广密码应用，其中包括基础设施、数字经济、信息惠民等，这些都与智能网联汽车密切相关。

智能网联汽车事关国家安全，需要充分发挥密码在智能网联汽车信息安全中的基础支撑和核心保障作用，维护国家安全、促进经济社会发展、保护人民群众利益，但目前汽车领域商用密码应用顶层设计不完善，汽车制造商往往缺乏密码应用意识，未能掌握密码正确合规应用的方式方法，使得密码的安全保障作用得不到充分发挥。比如前

段时间英国伯明翰大学的一项研究发现，涉及 24 款不同车型的数百万辆汽车的机械钥匙防盗芯片存在安全漏洞。钥匙中的 DST80 芯片原本可以提供最多 80 位的密码长度，而在实际应用中由于方式方法不当，被降级到了 24 位，破解难度大大降低。

由此可见，构建以密码技术为核心的智能网联汽车安全防护体系，大力推动密码科技创新，完善密码标准体系，实现智能网联汽车网络和信息化相关标准与密码国家标准、密码行业标准保持协调统一，对智能网联汽车产业持续健康发展具有重要意义。

1.2 研究内容

当前车联网呈现应用场景多、网络协议多、终端种类多等特点，处理器性能、传输数据包大小、网络带宽以及延迟等各不相同。出于车联网网络安全的考虑，亟需相关国家标准对车用密码安全协议、加密算法、加密强度等进行规范和指导。本报告将对智能网联汽车商用密码应用标准化需求进行分析研究。

本报告将从国内外智能网联汽车商用密码应用相关的法规、标准、场景、产品和检测等方面分析汽车领域商用密码应用现状，总结汽车领域商用密码应用存在的问题；以此为基础，对智能网联汽车商用密码应用标准化需求进行分析，明确拟立项标准的定位、范畴及制定思路；为后续标准研制提出相关建议并制定工作计划。

1.3 研究意义

（1）提供汽车全生命周期网络安全支撑，保障汽车产业持续高质量发展

针对智能网联汽车的功能和应用场景，结合汽车对外远距离通信、近距离通信，以及车内总线通信等通信特点，开展智能网联汽车商用密码应用标准化技术研究，能够在智能网联汽车的研发、生产、运营和维护的全生命周期，给出具体的安全协议、证书格式、算法强度、算法类型等安全策略，和密钥生成、灌装、存储、使用和销毁等管理策略，以及相应的测试验证方法，为汽车全生命周期的网络安全提供坚实保障。

同时，智能网联汽车商用密码应用标准化技术研究，能够促进配套的智能交通领域路侧设备和基础设施的安全通信和防护措施建设，对路侧设备和基础设施的安全通信水平提升、智能网联汽车安全通信闭环形成具有重要意义，有效促进智能网联汽车产业持续健康发展。

（2）把握智能网联汽车发展机遇期，推动汽车商用密码应用核心技术突破

新一轮科技革命的蓬勃发展，也在推动汽车产业加速变革。5G、大数据、人工智能等技术突破推动了汽车诸多技术变革和转型升级发展。以新能源汽车和智能网联汽车为代表的全新产品和技术形态，正在深刻的改变着传统的汽车产业，成为全球汽车产业发展的战略方向。作为汽车与信息技术产业创新融合的代表，智能网联汽车是新一轮科技革命和产业变革背景下出现的新生事物，是车辆、通信、安全等技术交叉互通的新兴产物。汽车的智能化和网联化技术正在引发国际上新一轮的技术竞争。

密码技术作为保障网络安全的核心技术，是网络信任的基石，是

解决智能网联汽车安全问题最有效、最直接、最可靠的手段，发挥着重要而不可替代的作用。利用密码在安全认证、加密保护、信任传递等方面的重要作用，可以有效满足智能网联汽车的安全需求，实现从离散被动防御向整体主动免疫的根本转变。

长期以来，我国商用密码产品一直无法避免被国外高端产品供应商技术垄断的局面。智能网联汽车的出现，将打破传统的产业链、技术链和价值链，对我国商用密码产业自主创新能力和国产化水平提升，实现弯道超车提供重大机遇。因此，必须牢牢把握机会，制定智能网联汽车商用密码应用相关标准，引领国产商用密码产品应用实现突破和更好的发展。

（3）支撑国家相关政策法规制定，提升国家商用密码公共管理水平

通过制定智能网联汽车商用密码应用相关标准，可以准确掌握我国汽车商用密码发展现状、发展重点和存在的短板，科学衡量我国汽车行业商用密码应用综合发展水平，满足中央和地方各级政府宏观管理和科学决策的需求。加强智能网联汽车商用密码应用标准研究，有利于政府部门准确地把握汽车领域商用密码的发展趋势和规律，及时把握影响国家安全的密码运行情况，为制定实施针对性强、可操作性强的产业政策和法规提供参考。

同时，通过智能网联汽车商用密码应用标准化技术研究，明确国家各管理机构的具体职责，建立统一管理，互联互通的高效的顶层规划、实施和监管机制，将切实提升国家对汽车领域商用密码应用的公

共管理水平。

2 智能网联汽车商用密码应用现状

2.1 智能网联汽车商用密码政策法规现状

2.1.1 国际发展现状

2.1.1.1 欧盟

目前欧洲没有专门针对智能网联汽车领域的商用密码应用技术要求的法规。欧盟及个别欧洲国家有关于信息与通信技术应用程序的密码算法相关标准，但没有强制约束力。欧洲的 NIS2.0 指令和德国的 IT-安全法都将重点放在关键基础设施的管理组织上。未来欧洲的网络安全法将定义产品认证方案的框架，届时各领域的密码应用技术要求凸显，也会带来智能网联汽车（Intelligent Connected Vehicle，ICV）领域商用密码技术要求，但目前该法律还在制定中。另外，无线电设备指令可能会迫使 ICT 针对 ICV 商用密码应用技术要求制定欧洲标准，但目前前景仍不明朗。欧盟即将推出的《数字服务法》将更注重在网络互联和多媒体内容，法令中对软件更新提出了全供应链的安全要求，预计也会对 ICV 商用密码应用技术要求产生影响。

2.1.1.2 美国

（1）网络安全法律法规

美国于 1977 年颁布《联邦计算机系统保护法案》；1986 年，颁布首部专门针对网络安全法的《信息自由法》；2001-2022 年，颁布《网

络信息安全研究与发展法》《网络信息安全加强法》《联邦信息安全管理法案》等法案；2015-2016 年，颁布《网络安全法案》（Cybersecurity Act of 2015）、《网络安全国家行动计划》（CNAP）等法案。至此，美国的网络安全法逐渐成型，也逐渐将商用纳入到法律管辖范围。

（2）密码法律法规

美国对密码出口的相关法案：1999 年颁发《国际武器贸易条例》（ITAR）及其配套的“军用物品管控清单”（USML），实施商品管控中对商业密码的出口，旨在防止先进密码技术外流并被第三方使用。随着近十几年的技术、商业的发展，美国开始对密码出口政策进行调整，逐步放宽控制力度，取消了对出口密码产品强度和类别的限制，而改为采用技术审查、许可协议和售后报告等机制对密码出口进行管控。

美国国内对密码的管理：美国政府于 1993 年开始尝试引入密钥托管制度，但受到大部分企业的反对，因而在 1999 年颁布《网络电子安全法》（CESA）中，规定不再强制要求密钥托管制度，而改为建议。

（3）汽车密码法律法规

2015 年，美国国会通过《汽车安全和隐私法案》（Security and Privacy in Your Car Act，简称“SPY Car Act”），公路交通安全管理局 NHTSA 和联邦贸易委员会（FTC）合作建立了联邦标准，从而保护联网汽车的安全。比如要求在美国销售的机动车辆需要防止非授权入侵，以及电子控制及驾驶数据和数据传输安全，其中均涉及到密码技术在联网汽车上的应用。

2017 年 9 月美国交通部发布了《自动驾驶法案》（或《确保车辆演化的未来部署和研究安全法案》）（AV2.0），规定自动驾驶汽车的开发者需制定数据的隐私保护计划，明确提出需要对汽车所有者或使用者的信息进行匿名或加密处理。

2.1.1.3 日本

日本政府高度重视网络安全，新《外汇法》中规定外国资本如想取得日本网络安全企业 1%以上的股份，需事先申报，接受有关方面审查。

针对从事第五代（5G）移动通信系统和无人机等尖端技术开发的企业，将对其是否符合确保网络安全和服务稳定性等重点标准进行认证。

针对汽车自动驾驶中的信息安全，立法方面：

2019 年修订《道路运输车辆法》，明确了对自动驾驶车辆进行信息监管的权利，给予第三方汽车技术综合服务机构监管权力。

配套政策方面：

2013 年 6 月，发布《日本的网络安全策略》，提出构建信息共享平台，对事件的严重性进行分级分类、风险管理、促进安全守则以及增强应急响应能力等要求，并提出发展密码应用技术。

基础研究方面：

2013 年 8 月，日本情报处理推进机构（IPA）发布了《车辆信息安全指南》，提出了汽车信息安全模型“IPA Car”，针对“网联化”车辆信息安全，制定了汽车生命周期各个阶段的安全策略和措施。日本

汽车工业协会（JAMA）还建立了日本汽车信息共享组织J-Auto ISAC。

针对密码应用领域，2001年1月，日本政府制定了《e-Japan战略》，计划5年内把日本建成世界最先进的IT国家，为使国民安全地享受电子政府提供的服务，确保信息安全、可靠，2001年，日本政府专门成立“密码研究与评估委员会”，负责在全社会征集密码技术，并对征集到的密码技术从电子政府可能利用的角度对其安全性及可实现性等方面进行了评估。

2.1.2 国内发展现状

（1）国家密码管理局负责国内商用密码的管理工作

2005年，经中央机构编制委员会批准，国家密码管理委员会办公室正式更名为国家密码管理局。2008年，国务院发布《国务院关于部委管理的国家局设置的通知》（国发[2008]12号），国家密码管理局作为部委管理的国家局正式列入国务院机构序列，主管全国的商用密码管理工作。同时，按照党中央关于加强新形势下密码工作的决定，各级地方政府也都规范了密码管理部门的机构和职责。经过近20年的建设，商用密码管理的政策、法规、标准体系逐步完善。

（2）国家法律层面对密码管理和密码应用的要求

2017年6月1日起施行的《中华人民共和国网络安全法》（简称《网络安全法》），对网络运营者应该履行的安全保护义务做出了明确要求，而维护网络数据完整性、保密性、真实性及不可否认性，都需要发挥密码技术的核心支撑作用。

2019年10月26日，十三届全国人大常委会第十四次会议表决

通过了《中华人民共和国密码法》（简称《密码法》）。这是我国密码领域第一部综合性、基础性法律和上位政策，规定了商用密码的主要管理制度，包括商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度，共计五章四十四条，并已于 2020 年 1 月 1 日起施行。

随着密码法的颁布和实施，我国各部门各行业已正在积极开展业务系统关键信息基础设施认定和检查，推动商用密码应用等工作。在金融领域、政务领域、能源领域等都展开了相关应用示范，但汽车领域相关的商用密码法规应用示范缺失，推进汽车商用密码标准体系的建设显得尤为重要。

（3）国家政策法规层面对密码管理和密码应用的规定

1999 年 10 月，国务院颁布《商用密码管理条例》，明确了商用密码的管理机构、管理体制以及商用密码管理工作的基本原则，对商用密码科研、生产、销售、使用、安全保密等方面的主要制度做出了规定。

2005 年到 2007 年，国家密码管理局相继发布《商用密码产品销售管理规定》、《商用密码产品管理使用管理规定》，规范了商用密码的使用行为。

2007 年 6 月，国家密码管理局颁布《信息安全等级保护商用密码管理办法》，目的是规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信

息化建设。

2009 年 12 月，国家密码管理局印发《信息安全等级保护商用密码管理办法》实施意见，配合《信息安全等级保护商用密码管理办法》实施，规定“第三级及以上信息系统的商用密码应用系统建设方案应当通过密码管理部门组织的评审后方可实施”，“第三级及以上信息系统的商用密码应用系统，应当通过国家密码管理部门指定测评机构的密码测评后方可投入运行。密码测评包括资料审查、系统分析、现场测评、综合评估等”，这些制度均明确了信息安全等级保护第三级及以上信息系统的商用密码应用要求。

2009 年 12 月 1 日起施行的《电子认证服务密码管理办法》，主要规定面向社会公众提供电子认证服务应当使用商用密码，明确申请电子认证服务使用密码许可应当具备的基本条件和程序，对电子认证服务系统的运行和技术改造等作出了规定。同时，要求电子认证服务系统要由具有商用密码产品生产和密码服务能力的单位，按照 GM/T 0034-2014《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》的要求承建，并通过国家密码管理局组织的安全性审查。

2017 年，国家密码管理局修订并发布《商用密码科研管理规定》和《商用密码生产管理规定》。

2017 年 7 月 12 日，国家互联网信息办公室发布了《关键信息基础设施安全保护条例（征求意见稿）》，该部条例属于《网络安全法》的重要配套规定和下位法，规定了重要行业领域的网络安全要求。该条例明确了关键信息基础设施的密码应用要求，压实了网络安全运营

者和主管部门有关密码应用和密码安全的主体责任，为密码管理部门开展网络空间密码保护工作，尤其是网络安全检查和安全审查等工作提供了法律依据，同时也为开展密评工作提供了强有力的支撑。

2018 年 6 月 27 日，《网络安全等级保护条例》向社会公开征求意见，其中设置了密码管理专章，体现了密码管理在网络安全等级保护工作中的重要作用，明确了网络安全等级保护密码管理的主要思路、方式和手段，强调了网络安全等级保护第三级及以上系统使用密码进行保护的义务，突出了商用密码应用安全性评估作为等级保护密码管理主要抓手的地位和作用，强化了密码管理部门在等级保护技术标准制定、监督检查、密码应用安全性评估工作开展等方面的职权，明确规定了“国家密码管理部门负责网络安全等级保护工作中有关密码管理工作的监督管理”，还从网络安全等级保护的事前备案审核、事中应用要求、以及事中事后监管和法律责任各环节对密码管理和应用进行了规定。

2018 年 7 月，中共中央办公厅、国务院办公厅下发《金融和重要领域密码应用与创新发展工作规划》（2018-2022 年），要求大力推动密码科技创新，加强密码基础理论、关键技术和应用研究。

（4）金融及其他重要领域积极部署和稳步推进商用密码应用相关工作

金融行业一直是商用密码应用的积极实践者和先行者。2013 年，央行发布了支持 SM 系列算法的 PBOC 3.0 标准，推动金融领域密码应用。2019 年，央行发布《金融科技发展规划（2019-2021 年）》，制定

了利用密码等技术健全网络身份认证体系的重点任务。目前，商用密码在金融领域得到了广泛的应用，有力地保障了金融信息安全和金融系统安全运行。

政务外网也一直积极响应国家商用密码的推进计划，在不少方面已经实现了商用密码改造和业务推进。2019 年 12 月 30 日，《国家政务信息化项目建设管理办法》发布，对国家政务信息系统的规划、审批、建设、共享和监管做了规定，其中明确规定了多项密码应用有关要求。政务信息化项目建设单位，应同步规划、同步建设、同步运行密码保障系统并定期运行评估，按要求向发改委备案的备案文件应当包含密码应用方案和密码应用安全性评估报告，项目的密码应用和安全审查情况应当作为项目验收的重要内容之一，密码应用安全性评估报告应当作为提交验收申请的必要材料。

在能源领域，2020 年年初，国家电网有限公司互联网部印发《2020 年信息运行和网络安全重点工作的通知》，要求开展网络安全自主可控装备研发与推广，建设统一密码应用服务体系。2020 年 9 月，中国电科院等单位联合编制了《国家电网公司商用密码应用和服务架构优化方案》和《商用密码试点总结报告》，为统一密码服务平台建设及应用在系统内加快落地提供指导。

其它行业领域：水利部制定了《2020 年水利网信工作要点》，提到“推进商用密码应用，开展水利行业密码应用专题调研、出台推进商用密码应用”等具体措施；教育部办公厅印发《2020 年教育信息化和网络安全工作要点》的通知，明确提出加强教育系统密码应用于管

理，落实《教育行业密码与应用创新发展实施方案》，推进密码基础设施和支撑体系建设，有序推进教育重要业务信息系统开展密码应用性安全评估等；公安部要求，在信息安全等级保护第三级以上的网络信息系统、国家级信息化项目，全国或跨区域地区联网的网络与信息系统、公安信息网基础设施、面向社会服务的政务信息系统中加强密码应用。

2.1.3 国内外发展现状总结

欧盟目前还没有针对 ICV 领域商用密码应用提出明确的技术要求，但相关法案的推出将会促进商用密码相关标准的出台。

美国历来重视网络安全，自 1996 年首部《信息自由法》到《网络安全国家行动计划》，美国网络安全法逐渐成型，但关于密码相关的法律法规多局限于军事领域。在其他领域，密码只是作为防护手段在相关标准规范中有所提及，但值得关注的是，美国在这些规范中提出的很多对密码应用相关的要求，直接影响了国际商用密码使用情况。比如 SAE J3061《信息物理汽车系统网络安全指南》，对密钥明确提出了硬件级加密要求；美国国家标准和技术研究所（NIST） SP800-90A 提出了“使用确定性随机位生成器生成随机数的建议”成为了很多汽车 ECU 内部密码随机数产生的实际标准；SP800-30A 提出了分析组密码操作模式的建议；FIPS 140 按照密码模块的算法以及模块本身的防护程度，定义了四个级别的安全等级。

日本 2001 年专门成立“密码研究与评估委员会”，负责在全社会征集密码技术，并从电子政府可能利用的角度对其安全性进行了评估。

但该委员会更多从传统 IT 角度出发，对于密码技术的重视，也只是在《日本的网络安全策略》中所有体现，并没有提出具体的要求。

所以，从整体上来说，国内商用密码应用的政策法规要求要领先于国际。

国家密码管理局主管全国的商用密码管理工作，经过近 20 年的建设，我国商用密码管理的政策法规体系逐步完善。

法律层面，《网络安全法》《密码法》使得密码管理有法可依。《密码法》作为基础性法律，从立法上提升密码管理和应用的科学化、规范化、法治化。

政策规范层面，我国已颁布很多涉及密码管理和应用的制度和规定：《商用密码管理条例》明确了商用密码管理工作的基本原则，规定了商用密码科研、生产、应用等的主要制度；《商用密码产品销售管理规定》《商用密码产品管理使用管理规定》《商用密码科研管理规定》《商用密码生产管理规定》规范了商用密码的科研、生产和使用等管理要求；《信息安全等级保护商用密码管理办法》《网络安全等级保护条例》明确了网络安全等级保护第三级及以上信息系统的商用密码应用要求；《电子认证服务密码管理办法》提出了电子认证服务使用商用密码的建设、审查具体要求；《关键信息基础设施安全保护条例（征求意见稿）》规定了重要行业领域关键信息基础设施的密码应用要求。

实际应用层面，我国在金融等重要领域已经有多年的密码管理和应用经验，但在汽车领域还缺少商用密码法规、政策和应用示范。随

着汽车信息安全问题的日益凸显，有必要及时开展相关政策规范的制定和研究，为汽车行业的密码管理和应用提供有效的落地指导。

2.2 智能网联汽车商用密码标准现状

2.2.1 国际发展现状

2.2.1.1 欧盟

欧盟网络安全局（ENISA）是致力于实现全欧洲高度共同网络安全的机构。ENISA 在 2014 年推出了《算法，密钥长度和参数报告》，将密码机制分为密码学基础和密码应用，在此基础上扩展了协议部分，比如密钥协议、TLS 和 IPSec 等。在密码学基础部分，对分组密码、哈希功能、流密码和公钥基础从三个角度进行了介绍：过去使用的密码基础，传统算法，以及对未来算法的展望；在密码应用中，首先介绍了分组密码的工作模式，比如 ECB、CBC、OFB 等等，对消息验证码、公钥加密、数字签名等也做了详细的说明和介绍。同年 ENISA 还发布了密钥协议的研究，对常见的密钥协议、标准参考、协议本身的局限以及技术细节进行了详细的介绍。以上 ENISA 提供的两份报告，已经成为了行业重要参考。

此外，德国高级联邦机构联邦信息安全办公室（德语：Bundesamt für Sicherheit in der Informationstechnik，简称 BSI），负责管理德国政府的计算机和通信安全。在 BSI TR-02102 系列技术指南中，BSI 对选定的加密算法进行了安全评估，并对加密协议 TLS（传输层安全）、IPsec（互联网协议安全）、IKE（互联网密钥交换）和 SSH（安全外壳）提出了建议，以便为合适算法的选择提供参考和指导。

在 V2X 车路协同方面，欧洲 ETSI ITS（欧洲电信标准协会 智能交通系统）中的信息安全工作组制定了 ITS 相关的安全性议题，定义了 ITS 相关的无线网络安全通信规范，例如 ETSI TS 103 097 描述了 ITS 系统通信相关的安全标头和证书格式。

在硬件安全方面，2009 年，通过由奥迪、宝马、戴姆勒以及保时捷和大众组成的 HIS（Herstellerinitiative Software）联盟，推出了安全硬件扩展（Security Hardware Extention，SHE）的规范，德国 Escrypt 飞思卡尔等供应商也参与其中。同期，由欧盟资助的 EVITA（E-safety Vehicle Intrusion Protected Applications）项目，也推出了基于硬件安全模块（Hardware Security Module，HSM）规范。针对不同的应用场景，HSM 定义了三个不同配置，轻量型（Light），普通型（Medium）以及完整型（Full）。无论是 SHE 还是 HSM，都从硬件层面支持了一系列的密码应用技术，包括安全存储、安全运行环境，以及特定密码算法的加速等等。基于这两个规范的安全硬件也逐步在汽车行业应用推广。

2.2.1.2 美国

（1）美国 SAE J3061 标准

2016 年，美国 SAE 组织发布了针对车辆整个生命周期网络安全流程的框架指导标准 SAE J3061《信息物理汽车系统网络安全指南》，其中对密钥明确提出了硬件级加密要求，比如直接通过硬件加密模块生成非对称密钥对并进行安全存储等。

（2）美国 NIST SP800 标准

SP800 是美国 NIST（National Institute of Standards and Technology）

发布的一系列关于信息安全的指南（SP 是 Special Publications 的缩写）。NIST SP800 系列标准成为了指导美国信息安全管理建设的主要标准和参考资料。虽然 NIST SP 并不作为正式法定标准，但在实际工作中，已经成为美国和国际安全界广泛认可的事实标准和权威指南。

汽车行业大量引用了该标准里的相关系列。比如 SP800-90A“使用确定性随机位生成器生成随机数的建议”，成为了很多汽车 ECU 内部密码随机数产生的实际标准；SP800-30A“分组密码操作模式的建议”也在汽车内部得到了广泛的应用。

（3）美国 FIPS 标准

FIPS (Federal Information Processing Standards)认证是由 NIST、加拿大通信安全机构（CSE）联合开展的，旨在规范密码模块的设计、实现、使用及销毁过程涉及的技术与流程。

世界上很多国家机构的采购和招标要求中明确提出具有密码模块的产品 FIPS140 的合规要求。因此，美国车企也广泛得以 FIPS140 作为潜在的标准来予以执行或参考。如 FIPS140-2 是硬件、软件和固件解决方案安全标准，在美国政府的采购中，所有使用加密技术的解决方案都必须完成 FIPS 140-2 验证；如 FIPS 140-3 加密模块的安全要求（Security Requirements for Cryptographic Modules）是车联网 ECU 加密要求的实际指南。另外 FIPS 的其它系列，如 FIPS197 AES（Advanced Encryption Standard）已被大部分汽车企业作为对称加密技术标准使用。

FIPS140 定义了四个级别的安全等级，也被汽车行业广泛采用。

Level 1 规定了最低的安全级别，要求密码模块至少使用一种被批准的算法或被批准的网络安全功能。该级别允许加密的软件模块或固件模块能够运行在未经评估的操作系统上。当其它控制如物理安全、网络安全、管理流程不足或缺失时，此类实现可能适用于某些低级别的安全性应用程序；此级别允许使用软件进行加密。

Level 2 在 level 1 的基本要求上，增加了密码模块的物理安全要求，要求对遭受了未授权的物理访问密码模块内明文加密密钥或关键安全参数的证据进行物理层面的明示，如增加防拆卸外壳、封条，或者在门或盖子上增加防撬锁。

Level 3 在 level 2 的基本物理防护上，增加了要求密码模块的更高的物理封装能力，如更加紧固的外壳，以及物理攻击检测、响应电路。当检测到未授权物理访问或攻击时（如门或盖子被强行打开），会擦除内部的关键安全参数等。

Level 4 最高的安全级别，在密码模块周围提供完全的封装，以检测和响应所有的未授权物理访问。当检测到任何方向的渗透破坏后，所有的关键安全参数及密钥文本将被清零。

（4）智能网联汽车相关标准

2016 年，美国国家公路交通安全管理局（NHTSA）发布了《现代汽车网络安全最佳实践》，针对于汽车多个方面提出了网络安全应用建议。2021 年 1 月又发布了新一版最佳实践草案，面向大众征求意见。

在 V2X 车路协同方面，美国采用的 DSRC 技术上层则采用 IEEE

1609 系列标准，IEEE 1609.2 是其中的安全机制标准，定义了车联网中的无线通信方案安全服务，定义了安全信息的格式。

2.2.1.3 日本

2003 年，日本总务省和经济产业省联合公布了 29 种电子政府推荐密码名单，如下表：

密码分类		名称
公开密钥密码	签名	DSA
		ECDSA
		RSASSA-PKCSI-v1_5
		RSA-PSS
	加密	RSA-OAPE
		RSAES-PKCSI-v1_5
	密钥交换	DH
		ECDH
		PSEC-KEM
对称密钥密码	64 比特分组密码	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple-DES
	128 比特分组密码	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	序列密码	MUGI
		MULTI-S01
		128bit RC4
HASH 密码		RIPEMD-160
		SHA-1
		SHA-256
		SHA-384

	SHA-512

同时在标准方面，日本商用密码采用 ISO 18033 系列标准，标准出于数据保密性目的，对分组密码进行了规范，指定了以下算法：

•64 位分组密码：TDEA，MISTY1，CAST-128，HIGH；

•128 位分组密码：AES，Camellia，SEED。

目前日本主要使用标准中 MISTY1、Camellia 两种算法，尚无专门针对智能网联汽车的密码技术要求相关标准。

2.2.2 国内发展现状

（1）商用密码标准领域的整体推进情况

1）密标委成立并纳入国家标准管理体系

2011 年 10 月，经国家标准化管理委员会和国家密码管理局批准，密码行业标准化技术委员会（以下简称“密标委”）正式成立，负责密码技术、产品、系统和管理等方面的标准化工作。密标委的建立标志着商用密码标准化工作正式纳入国家标准管理体系。密标委目前设有总体工作组、基础工作组、应用工作组和测评工作组，分别从密码标准体系规划、通用基础密码标准建立、行业应用密码标准建立，以及产品检测和系统测评标准建立等方面开展工作。

2）密标委发布《密码标准应用指南》，用于指导密码标准体系建设

为指导国内各行业对密码算法、协议及产品等标准的正确使用，密标委编制了 GM/Y 5001《密码标准应用指南》，对已发布的密码行

业标准和国家标准进行分类阐述。行业信息系统用户在信息安全产品研发或信息系统建设中对密码技术应用产生需求时，可根据该指南并结合自身应用特点，查询该领域适用的密码标准，以指导研发和建设工作正确开展。

3）密标委发布的密码行业重要标准

2014 年 2 月，GM/T 0028-2014《密码模块安全技术要求》发布实施，规定了四个递增的、定性的安全等级要求，以满足密码模块在不同应用和工作环境中的要求。后来升级为国标 GB/T 37092-2018《信息安全技术 密码模块安全要求》2018 年发布。

2018 年 2 月，国家密码管理局发布了中华人民共和国密码行业标准 GM/T 0054-2018《信息系统密码应用基本要求》，对信息系统中如何应用密码提出了基本要求。GM/T 0054-2018 是指导、规范和评估信息系统中的商用密码应用的标准依据，该标准提出了总体要求、密码功能要求、密码技术应用要求、密钥管理和安全管理共五个部分的内容。其中，总体要求是所有信息系统都需遵循的基本要求；密码功能要求阐述了密码在信息系统中的作用；密码技术应用要求部分，沿用等级保护 V2.0 标准中的四层结构，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、应用和数据安全共四个层面规范密码技术在信息系统中的应用。

2018 年 2 月，经国密局批准，行标 GM/T 0054-2018《信息系统密码应用基本要求》启动升国标工作。2021 年 3 月，GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》正式发布，该标准针

对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层面提出了第一级到第四级的密码应用技术要求，针对管理制度、人员管理、建设运行和应急处置四个方面提出了相应的密码应用安全管理要求。

到目前为止，我国已发布商用密码相关国家标准 39 项，行业标准 100 余项，范围涵盖密码算法、密码协议、密码产品、密码应用、密码检测等多个方面，标志着我国商用密码标准体系已经基本形成。这些标准能够为我国包括汽车行业在内的各个行业的商用密码应用提供指导，也是未来智能网联汽车商用密码应用标准制定的重要参考。

（2）汽车商用密码标准领域的推进情况

1）汽车信息安全及商用密码应用标准规划

随着智能网联汽车的不断发展，汽车行业信息安全得到行业内外的广泛关注。我国工业和信息化部与国家标准化管理委员会等联合印发了《国家车联网产业标准体系建设指南（总体要求）》、《国家车联网产业标准体系建设指南（智能网联汽车）》、《国家车联网产业标准体系建设指南（信息通信）》、《国家车联网产业标准体系建设指南（电子产品和服务）》、《国家车联网产业标准体系建设指南（车辆智能管理）、《国家车联网产业标准体系建设指南（智能交通相关）》等系列文件，各相关部门加速研制车联网安全标准。总体要求指南明确了车联网产业标准制定的指导思想、基本原则以及建设目标，并给出车联网产业标准体系的参考框架；信息通信指南中计划基于 LTE 的车联网通信技术相关的安全标准，重点针对基于 LTE-V2X、5G-V2X 的车-车、

车-路、车-人等通信过程的安全身份认证开展标准制定；车辆智能管理指南计划制定 17 项身份认证与安全类标准，车联智能管理身份认证主要支撑网联汽车和道路管理系统、设施之间的身份认证，包括智能网联汽车身份与安全、道路交通管理设施身份与安全、身份认证平台及电子证件。

2）已发布或报批的汽车商用密码应用标准

全国汽车标准化技术委员会积极推进汽车领域商用密码应用标准建设，并取得显著成果。目前，汽标委智能网联汽车分标委贯彻落实主管部门规划要求，已开展《智能网联汽车数字证书应用技术要求》《智能网联汽车商用密码应用技术要求》、车用数字钥匙及网联应用场景等多项新标准的立项研究工作，逐步构成适用于汽车行业的商用密码应用标准体系。

即将正式发布的首批汽车信息安全国家标准《电动汽车远程服务与管理系统信息安全技术要求及试验方法》中，规定了车载终端到平台应采用安全通信协议，若使用基于非对称密钥的身份认证机制，宜使用 SM2、RSA（长度不低于 2048 位）或同级别以及更高级的密码算法，应具有对应的证书更新及撤销机制，证书的有效期宜不超过 365 天，证书更新过程应确保密钥安全性；若使用基于对称密钥的身份认证机制，宜使用 SM4、AES（长度不低于 128 位）或同级别以及更高级的密码算法，应具有对应的密钥更新机制，更新过程中应确保密钥安全性。除此之外，在完成报批的其他 3 项汽车信息安全国家标准《汽车信息安全通用技术要求》《车载信息交互系统信息安全技术要

求及试验方法》《汽车网关信息安全技术要求及试验方法》中，也均对汽车领域商用密码应用提出了相关要求。

中国通信标准化协会针对汽车 V2X 产业的信息安全，制定了 YD/T 3594-2019《基于 LTE 的车联网通信安全技术要求》和《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》（报批中），其中《基于 LTE 的车联网通信安全技术要求》中明确了使用商用密码算法 SM2 进行消息报文的签名和验签，《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》中明确了基于 SM2 算法的证书格式及证书管理要求。

全国信息安全标准化技术委员会 2018 年发布《汽车电子网络安全标准化白皮书（2018）》，在汽车电子网络安全标准体系中，专门列出“密码应用（205）”子体系，用于规范当前在汽车电子产品中应用越来越多的密码技术，提供适用于汽车环境的应用指导。

GB/T 38628-2020《信息安全技术 汽车电子系统网络安全指南》中 CAN 总线、车载网关、云服务等关键环节多处提出加密存储、加密通信、加强身份认证和远程访问，以及密钥管理等密码应用相关要求。另外，在研的国家标准《信息安全技术 车载网络设备信息安全技术要求》（征求意见稿）中，专门用一个章节（6.7 密码安全要求）对车载网络设备中的密码应用提出相关要求。

此外，在 GB 17691-2018《重型柴油车污染物排放限值及测量方法（中国第六阶段）》附录 Q 中，明确提出“车载终端存储、传输的数据应是加密的，应采用非对称加密算法，可使用国密 SM2 算法或

者 RSA 算法，并且需要采用硬件方式对私钥进行严格保护 ”。

2.2.3 国内外发展现状总结

目前国际上尚未形成统一的智能网联汽车的商用密码应用技术标准。汽车行业的各大企业，在各自的网络安全实践过程中，正逐步将原有的非汽车行业的密码应用标准，引入到汽车行业中来。

同时，国际上部分行业联盟，也正在制定或已经制定了专门的汽车密码应用标准。随着智能网联汽车信息安全受到越来越广泛的关注，这些联盟标准的影响力也正在逐渐扩大，被越来越多的联盟以外的成员所采纳或引用。

上述的行业联盟标准，主要是以国外的企业或机构为主导。然而，基于国内智能网联汽车的发展现状，以及国内相关法律法规的要求，适应中国智能网联汽车行业发展的密码应用技术标准势在必行。

在密标委发布的《密码标准应用指南》《密码模块安全技术要求》《信息系统密码应用基本要求》等纲领性文件指导下，我国商用密码技术标准体系已经基本形成，但专门针对汽车的商用密码应用标准仍然缺失。为增强汽车行业的商用密码应用领域的风险防控能力，充分发挥密码在维护网络与信息安全方面的重要作用，近几年发布的多项汽车信息安全标准中，都涉及到密码相关安全技术要求，为汽车行业密码技术的应用，提供了标准层面的技术支撑。

密码作为汽车网络安全的核心保障和基础支撑，将在智能网联汽车通信场景中发挥重要作用。所以，开展智能网联汽车领域商用密码标准制定与研究，成为行业发展迫切需求。

2.3 智能网联汽车商用密码典型应用场景分析

商用密码技术在智能网联汽车领域的应用，主要为通信双方的身份鉴别、数据保密、完整性验证等。基于纵深防御的思想，在智能网联汽车的各个系统层级可以对应地部署合适的安全措施。根据车联网及自动驾驶不同的应用场景，采用不同的密码算法组合来实现安全的要求。

2.3.1 车内通信场景

2.3.1.1 总线通信安全应用场景

车内通信主要包括 CAN 总线通信、车载以太网通信等。其中，由于 CAN 总线协议设计简单、没有复杂的分层以及加密扩展协议支持的考虑，易被窃取和伪造。目前主流的技术是采用 AutoSAR 标准组织制定并实现的 SecOC 技术，在发送端和接受端对报文进行验证，以抵御第三方的入侵。基于效率和成本方面的考虑，对于 CAN 网络，可以采用对称加密保护重要报文的机密性，可采用基于对称密钥的消息验证码或基于非对称密码的数字签名技术保护报文的完整性及真实性；对于基于以太网的通信，除了上述用于 CAN 网络通信的密码技术外，也可采用安全强度更高的传输层安全协议以确保通信内容的保密性、真实性和完整性。

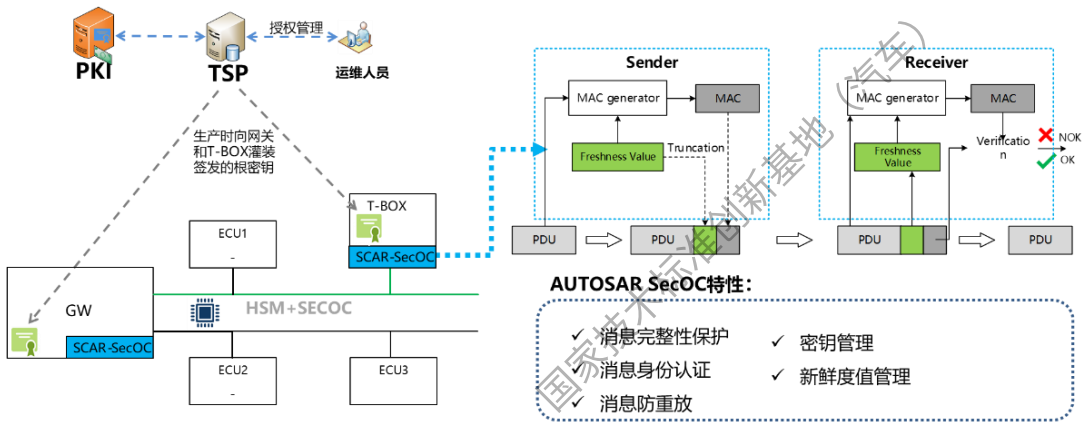

图 1 SecOC 安全架构

2.3.1.2 数据存储安全应用场景

密钥、关键业务信息可通过密码安全芯片实现安全存储，应用 SM2、SM4、SM3 等商用密码算法，或 AES、3DES、RSA、SHA-256 等国际密码算法，实现终端数据的本地加密存储，可以有效提升数据的安全性。

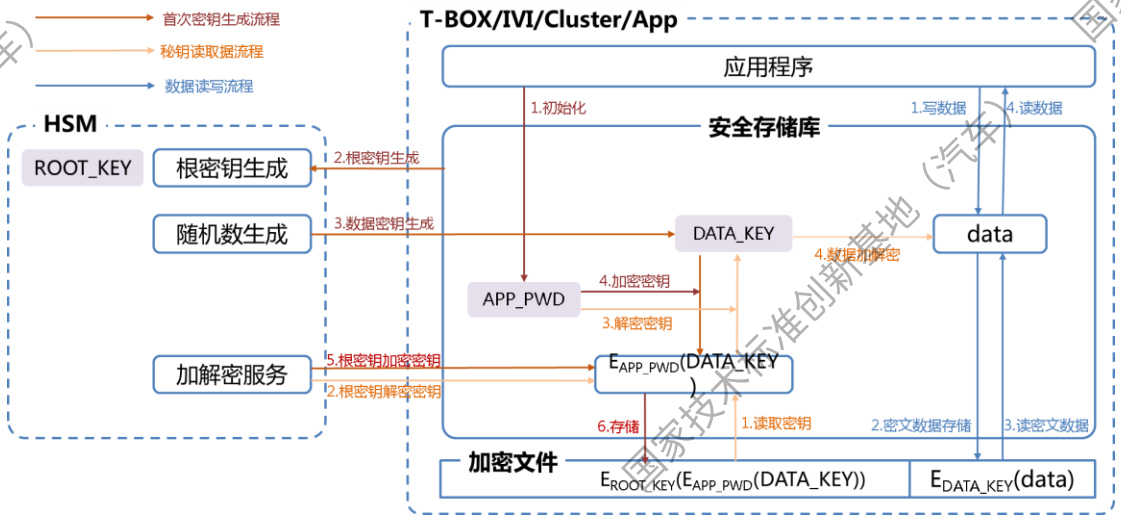

图 2 数据安全存储流程

2.3.2 车辆与外部通信场景

目前车辆常见的对外连接接口为蜂窝网络、蓝牙、无线局域网。在对应的协议栈中，商用密码技术也被广泛应用。例如蓝牙安全配对协议中，无线局域网安全协议 WPA2、WPA3，都使用了对称加密、非

对称加密、杂凑函数、随机数生成等相关的密码技术保护通信的保密性、真实性和完整性。

此外，在智能网联汽车的各类网联服务中，可利用公共密钥体系，对车辆颁发数字证书，用于进行车辆与云端的身份验证，借助传输层安全协议，保证通信内容的保密性、真实性和完整性。

2.3.2.1 车云通信安全应用场景

目前的车云通信主要以传统蜂窝通信为基础，所以仍遗留着蜂窝通信的安全风险，例如：仿冒（用户、服务器）攻击、提权攻击、篡改攻击、信息窃取等。在无认证机制的情况下，攻击者可仿冒正常用户进入服务器，获取服务器内部业务清单，进而获取服务器内部资源信息；或仿冒服务器诱骗用户登录，获取用户信息。

车云通信安全的身份认证机制主要通过基于商用密码的 PKI 技术来实现，通过 PKI 系统来统一表达车辆、设备标识，通过数字签名技术和数字加密技术，保证信息数据在传输过程中的完整性、有效性及行为的不可抵赖性；并通过数字证书提供安全的认证服务，实现对车载终端行为的高强度安全认证，鉴别车辆身份，防止非法连接造成的信息泄露；通过 TLS 链路加密技术，保证信息数据的传输链路的安全，从而为车载终端及智能网联汽车后台服务提供有效的的数据安全防护服务，保证信息数据的安全性，防止信息泄露。

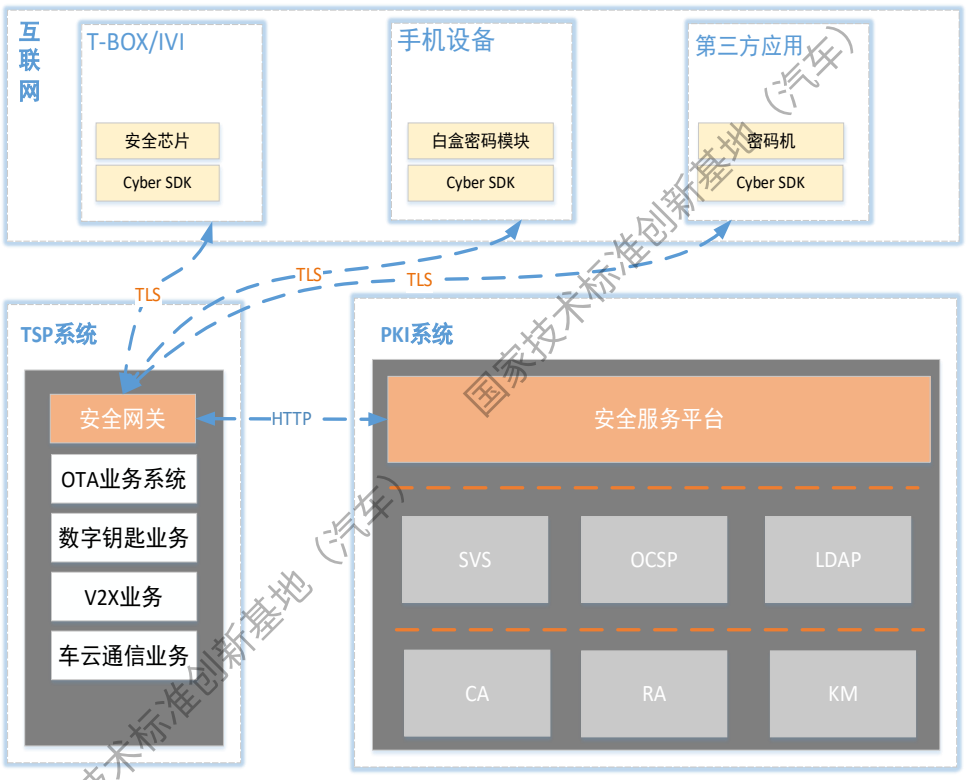

图 3 基于密码技术的车云通信安全架构

2.3.2.2 V2X 通信安全应用场景

车联网（V2X）包含 V2V（车-车）、V2I（车-基础设施）、V2P（车-行人）等应用方式，包含了大量的接入设备、数据、处理过程和传输节点，实现了除了车云交互外，车与外界的快速实时信息交换。如此多样化的交互，也带来大量的信息安全问题，需要建立完整的商用密码应用体系来确保其中错综复杂的身份认证和数据安全。

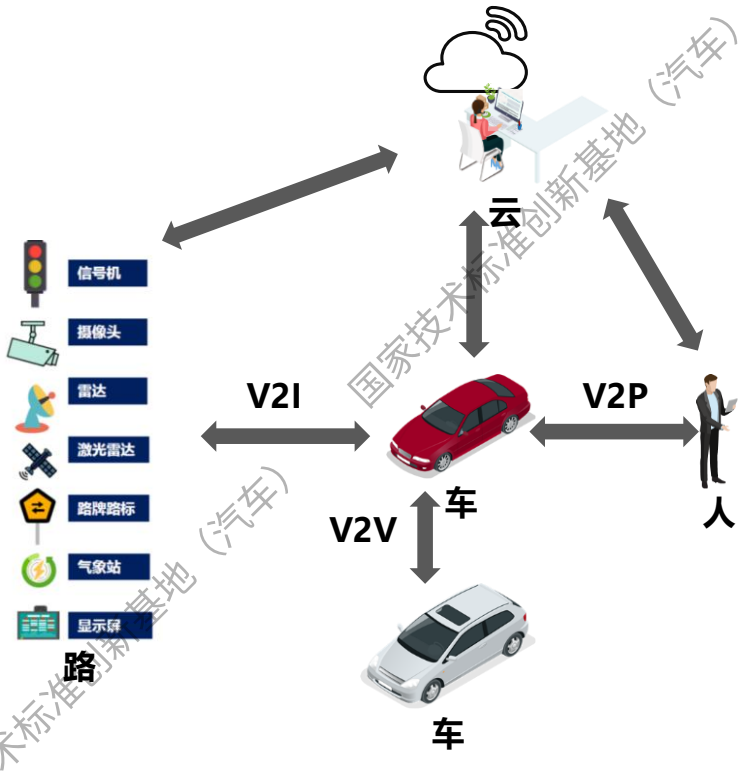

图 4　V2X 通信场景

为保障 V2X 场景下设备间的安全认证和安全通信，基于商用密码算法（如 SM2 算法）的 PKI 机制依然是比较明确的解决思路，同时采用数字签名等技术手段确保 V2V/V2I/V2P 直连通信安全。将数字身份认证技术应用于 V2X 通信中，实现车载设备、路侧设备、应用服务商等各个角色的相互认证，保证通信消息来源的真实性，有效做到防重放、防中间人攻击、防身份假冒等。

2.3.2.3 OTA 升级安全应用场景

整车 OTA 安全解决方案，确保智能网联汽车 OTA 过程中仅执行授权发布的升级指令与升级文件，OTA-Server 对升级包进行加密签名，阻止恶意的或非授权的升级包的被传输或被车端下载，影响升级。车机端在收到升级包后，对升级包进行验签，以确保升级包是经过合法

授权的，且数据在传输和下载程中未被修改，以确保 OTA 升级过程的数据安全。

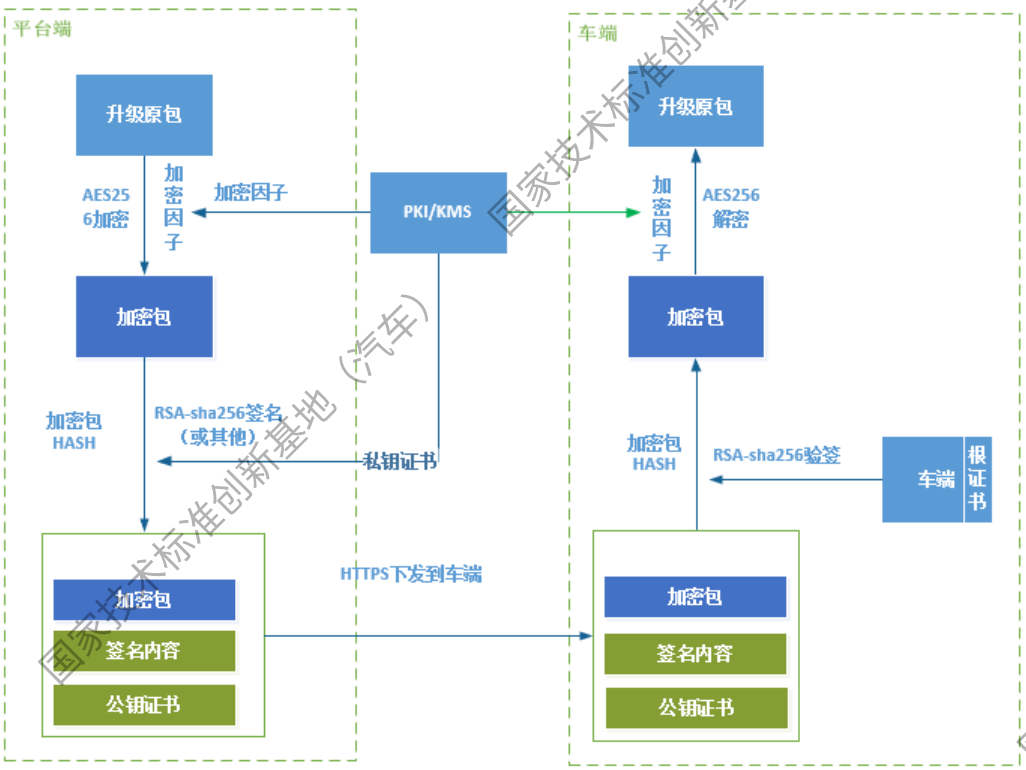

图 5　OTA 升级密码安全方案

2.3.2.4 远程控制/诊断安全应用场景

基于双向身份认证、远程控制指令加密、密钥协商等功能，保障远程控制/远程诊断指令的安全传输，防止车辆被非法控制。

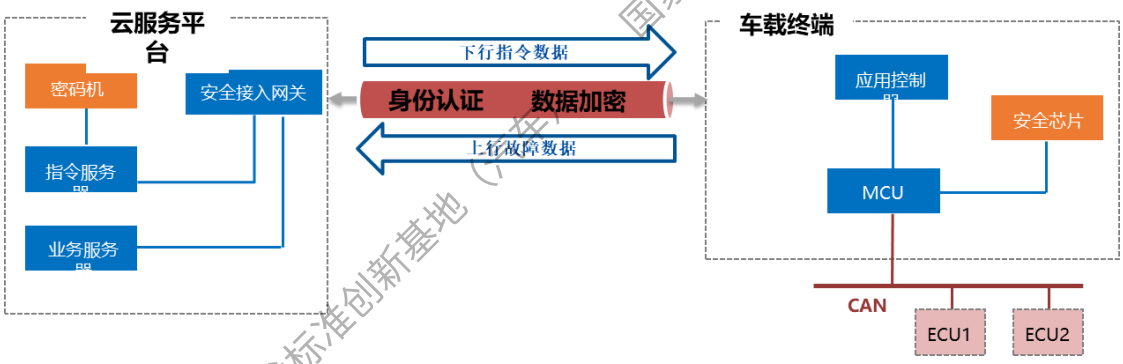

图 6　远程控制/诊断密码安全方案

2.3.2.5 数字钥匙安全应用场景

数字钥匙安全基于数字钥匙密钥管理系统，建立数字钥匙与车载终端的双向身份认证及指令加密机制，数字钥匙密钥管理系统产生的密钥应是动态更新、一次一密，以满足数字钥匙的高安全通信要求。

硬件安全模块应至少支持 SM2、SM3、SM4 等国密算法，兼容 RSA2048、ECC256、3DES、AES、ECDSA、SHA256 等国际算法，可提供随机数生成、密钥管理、数据加解密、数字签名、签名验证、密钥协商等多种密码服务。

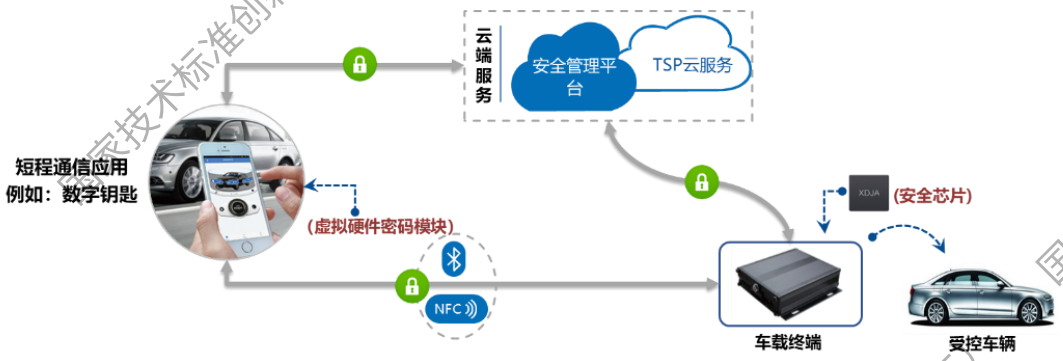

图 7　数字钥匙密码安全方案

2.4 智能网联汽车商用密码产品发展现状

通过 2.3 节中智能网联汽车商用密码应用场景的分析，可以得出，除去云服务平台和路侧设备等配套设施，仅就车端而言，其商用密码产品主要包括密码安全芯片等安全硬件、搭载此类安全硬件或以软件形式实现密码算法功能的车端模块，以及与云端、路侧端、移动端等进行身份识别的身份认证系统。下面分别进行详细介绍。

2.4.1 安全硬件

本报告中的安全硬件指包含密码模块（安全引擎）的芯片，这类

芯片有多种存在形态。以物理存在形态划分，可分为独立安全芯片和集成式安全模块两大类。

独立安全芯片是指以独立 SoC 芯片的形式存在，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 定义的安全等级或 CC EAL 安全等级认证。Secure Element（SE）、TPM、eSIM 和 Secure Flash 都属于独立安全芯片。

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部分，包含 HSM、Trust Zone 等形式。这类硬件安全模块以 IP 的形式集成到了 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。集成 HSM 的 MCU/MPU 一般不具备 CC EAL 安全等级认证。

以下依次展开说明：

2.4.1.1 SE（Secure Element）

SE （Secure Element），即安全单元，也称安全芯片。如下图**错误! 未找到引用源。**所示，SE 是一个独立进行密钥管理、安全计算的可信单元，内部安全存储模块可存储密钥和特征数据。在 SE 的硬件和软件实现上，全面融入多方位的安全防护设计，相关的安全特性涵盖芯

片的防篡改设计、唯一序列号、防 DPA/SPA/DFA/FA/TA 攻击、多种检测传感器、自毁功能、总线加密及屏蔽防护层等。SE 可支持的安全算法包括 NIST 标准算法（RSA/ECC/DES/3DES/AES/SHA-n）和国家商用密码算法（SM2/SM3/SM4/SM9）。

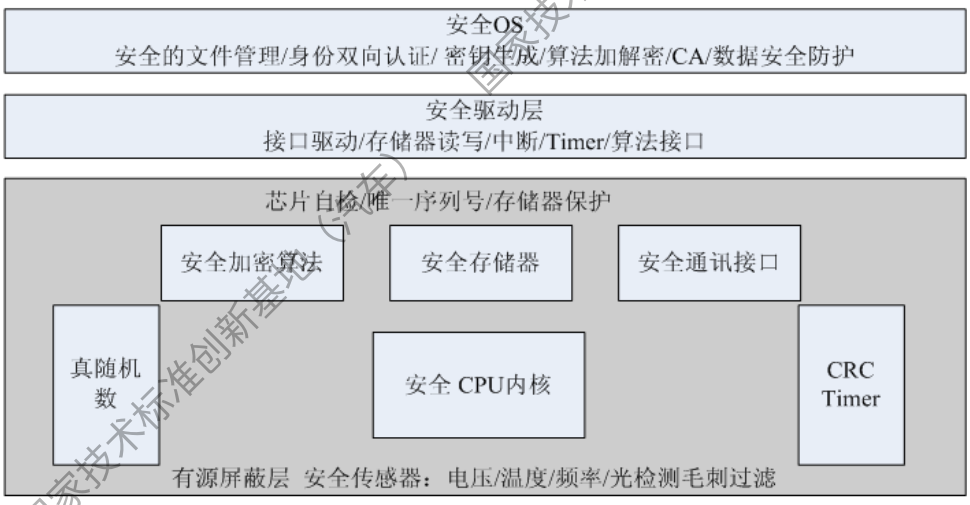

图 8　SE 芯片安全体系

SE 作为独立的安全载体，广泛的应用于联网设备的信息安全防护中，可以满足如下四方面的安全需求：A.设备唯一标识；B.设备端与云端双向身份认证；C.数据加密传输；D.远程 OTA 升级安全。基于 SE 提供的安全存储和安全运算环境，SE 可为物联网设备的运营者提供一个安全的信任根，由联网设备运营者发行 SE 中的设备 ID 号和证书密钥等，再结合安全云，形成一套完整的物联网安全方案，从而实现可信的身份认证、可靠的通讯加密、数据防篡改和防抵赖，为联网设备运营者的业务发展保驾护航。

2.4.1.2 TPM/TCM

TCG 组织（Trusted Computing Group）为计算平台提供了一整套基于 TPM（Trusted Platform Module）及平台中 TBB（平台可信构造块

=TPM+CRTM）的信任建立及可信性证实方法和机制，如图**错误!未找到引用源。**所示。

TPM 是一个拥有受保护的独立执行能力（密码运算部件）和小容量存储能力的硬件芯片，TPM 是可信平台的核心，是实现完整性的度量和报告的基础。TPM 硬件需要具备四个基础能力：A. 对称/非对称加密；B. 安全存储；C. 完整性度量；D. 签名认证。

根据 TCG 发布一系列标准化规范，TPM 需要实现相应的一套软件协议栈，在计算平台中，以可信根（TPM）为起点而建立信任链，在此基础上再将信任关系逐级传递到系统的各个模块，从而建立整个系统的信任关系，形成可信的计算平台。

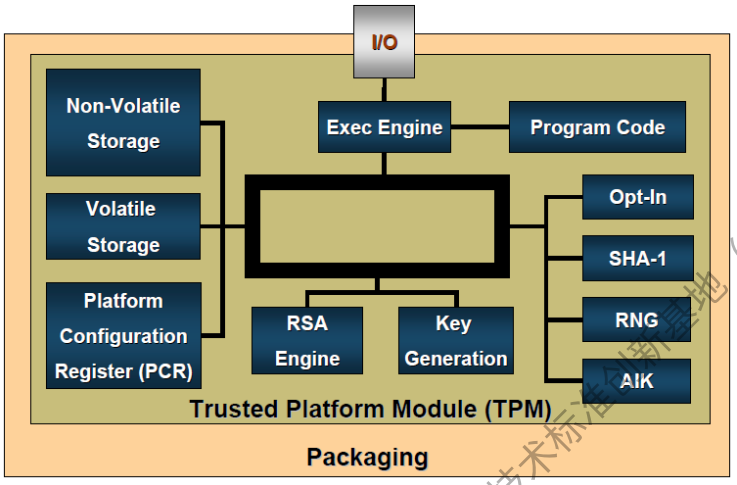

图 9　TPM 技术框架

TCM（Trusted Cryptography Module）是中国可信计算标准，最早由长城、中兴、联想、同方、方正、兆日等十二家厂商联合推出，得到国家密码管理局的大力支持，TCM 安全芯片在系统平台中的作用是为系统平台和软件提供基础的安全服务，建立更为安全可靠的系统平台环境。TCM 与 TPM1.2 有很多的相同点，TCM 借鉴了 TPM1.2 的架

构，是替换其核心算法后的产品。同时 TCM 中也按照我国的相关证书、密码等政策提供了符合我国管理政策的安全接口。

目前国家密码管理局已经对原 TCM 标准（GM/T 0012-2012《可信计算 可信密码模块接口规范》）进行了修订，新发布的标准 GM/T 0012-2020 的部分内容参照了 ISO/IEC 11889:2015 相关章节。GM/T 0012-2020 将于今年 7 月 1 日开始实施，用于代替原来的 GM/T 0012-2012。TCM 相关国家标准（GB/T 29829-2013《信息安全技术 可信计算密码支撑平台功能与接口规范》）目前正在修订中。

2.4.1.3 eSIM

eSIM 是全球移动通信系统协会（简称 GSMA ）推出的全球规范，旨在为任何移动设备提供远程配置。该规范可用于消费电子产品、家庭物联网应用、工业物联网应用如智能计量或物流（资产跟踪）等领域的各种应用。在汽车领域，eSIM 正在改善车内体验和联网服务的安全性。eSIM 是设备中的嵌入式 SIM 芯片，而不是单独的 SIM 卡。

eSIM 的应用可以使得在设计和设备设置过程中将获得以下优势：

- M2M 设备的后期编程
- 无需 SIM 卡即可快捷地设置产品设备
- 每台设备均可实现物联网功能，独立于数据共享的智能手机
- 在产品生命周期内通过远程 SIM 配置技术更改运营商配置文件（安全下载运营商的 SIM 应用程序）

在联网的汽车中，嵌入式 SIM （eSIM） 将汽车环境与电信网络连接起来。在汽车制造商追求最高质量水平的同时，移动网络运营商

（MNOs） 则专注于保护用户的安全凭证不被盗用和复制。

eSIM 也在自动紧急呼叫服务中发挥了重要作用。在发生交通事故时，可自动通知急救服务，从而帮助挽救生命。紧急呼叫服务旨在当司机失去意识或无法拨打电话的情况下，也能呼叫急救服务。

适用于 eSIM 的安全控制器可在车内实现安全可靠的蜂窝网络连接，允许汽车原始设备制造商 （OEM） 和一级供应商远程管理连接，并为终端用户提供和智能手机相似的基于互联网的服务。

2.4.1.4 Secure Flash

汽车 ECU 中使用了大量的 Nor Flash，主要应用包括高级驾驶辅助系统（ADAS）、网关、远程信息处理、仪表盘和发动机/动力总成控制。目前的 QSPI NOR Flash 存在的问题是外部 NOR Flash 不安全，数据可以被随意从 Nor Flash 读出来， 向前迈进的一步是把类似 HSM 的安全引擎集成到 Nor Flash 中。

Secure Flash（安全闪存）一般是指集成安全引擎，嵌入式处理器和 Flash 的芯片。Secure Flash 为安全密钥、证书、应用程序、配置数据、代码版本信息和生物识别传感器数据的安全存储提供了硬件保护。Secure Flash 还支持身份验证，以防止未经授权的访问和其他安全威胁。下图为英飞凌的 Secure Nor Flash 产品，集成了 ARM Cortex M0 处理器，硬件加密引擎和 Nor Flash。

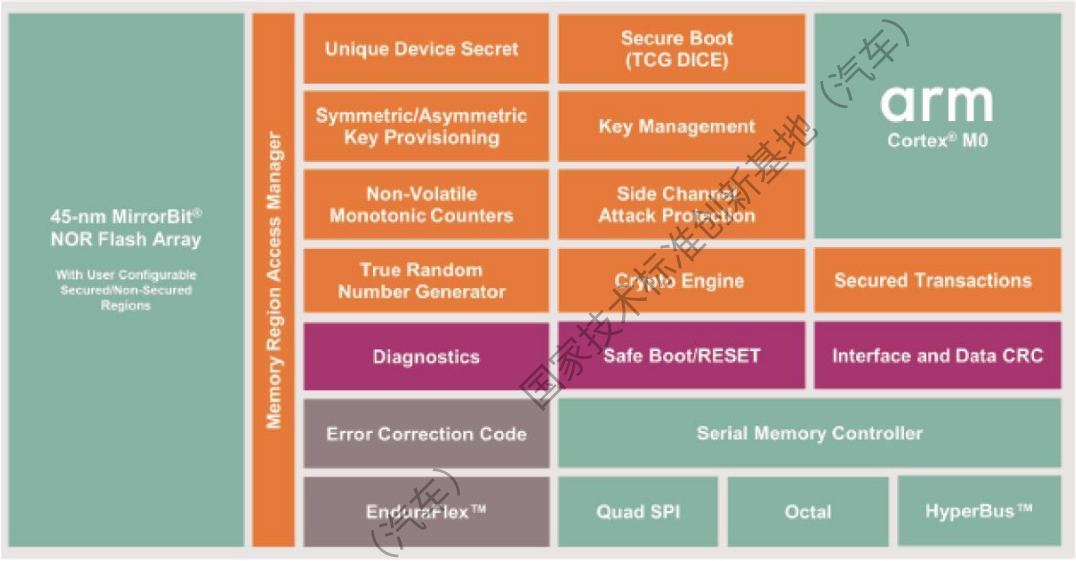

图 10　Secure Flash 框架

在 Flash 中集成嵌入处理器可以有选择地添加特定的功能，减轻系统主 MCU 的工作量。例如，嵌入式处理可以启用创建硬件信任根的功能，以防止对存储的代码和数据进行修改、操纵和其它攻击。嵌入式处理器还可以支持其它与安全性相关的要求，包括 HMAC 密钥生成和存储，以及提供针对固件、启动映像和系统参数的攻击防护。对于用户新系统的认证，可以通过更新嵌入式处理器的程序来满足最新安全法规。

2.4.1.5 SHE（Secure Hardware Extension）

SHE 是 HIS（由 Audi、BMW、Porsche、Volkswagen 形成的组织）制定的标准。如下图所示，其主要内容是通过硬件集成 AES-128 的密码协处理器，来完成加解密、消息认证码、引导加载程序的认证、管理唯一设备 ID 等功能，并规定应用不能直接访问的方式存储密钥。

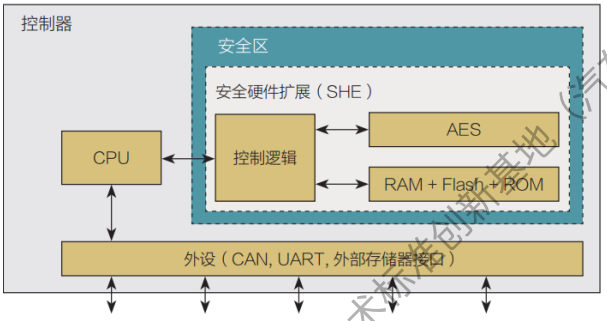

图 11　SHE 标准技术框架

SHE 的提出早于 HSM，是针对硬件的安全规范，主要为了解决密钥存储和密码算法加速提出的，SHE 不仅规定了硬件密码模块的功能，同时规定了硬件和软件的接口，此规范在汽车电子 MCU 中得到了广泛的应用。

2.4.1.6 HSM（Hardware Security Module）

在欧盟 2008-2011 的资助下，EVITA（E-safety vehicle intrusion protected applications）工作组制定了 HSM 的标准，旨在为车载网络的体系架构进行设计、验证、形成原型，以防止信息安全相关的组件被篡改，并保护敏感数据以免受到攻击。

EVITA 以基于硬件的安全机制为目标，主要对作为信任根的硬件安全模块（Hardware Security Module）进行了研究。研究成果中，ECU 应用 CPU 拥有一个密码协处理器 HSM。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。EVITA 把硬件安全模块划分为三个等级：EVITA Light HSM、EVITA Medium HSM、EVITA Full HSM。

EVITA Light HSM 的架构如下图**错误!未找到引用源。**所示，集成硬

件的 AES128 算法协处理器，用于组件内部数据保护。Light HSM 完全继承了 SHE 的支持，在汽车电子 MCU 中应用较为广泛。

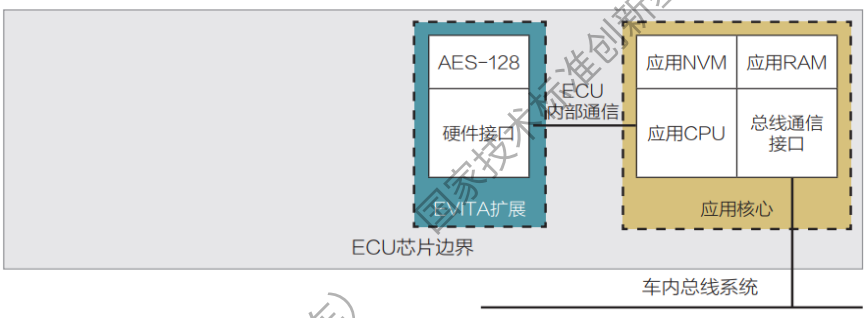

图 12　EVITA Light HSM 技术框架

EVITA Medium HSM 的架构如图**错误!未找到引用源。**所示，集成对称算法的具备独立 CPU 核的安全模块，用于保护组件之间的数据通信。

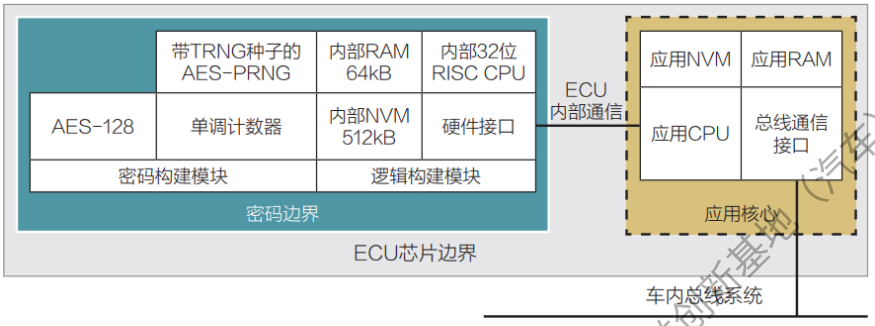

图 13　EVITA Medium HSM 技术框架

EVITA Full HSM 的架构如图**错误!未找到引用源。**所示，集成支持非对称算法的具备独立 CPU 核的安全模块，用于保护组件与网关或其它外部接口设备通信。

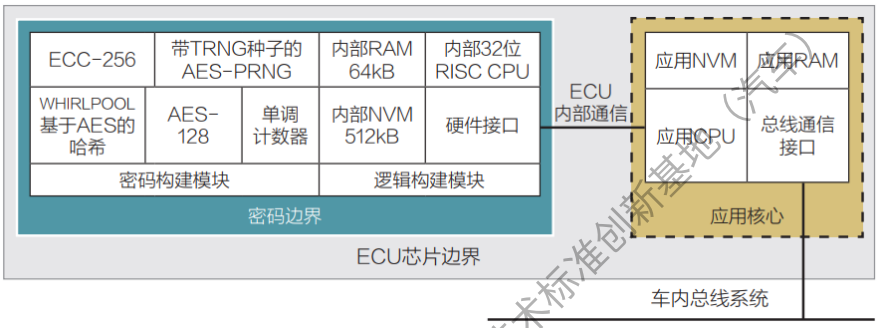

图 14　EVITA Full HSM 技术框架

2014 年开始 Infineon、ST、NXP 的 MCU 产品开始集成 HSM，主要以 Light HSM、Medium HSM 为主。在 2018 年后，这些国际厂商推出的 MCU 产品已经基本支持 Full HSM。

国内芯片厂商也推出了兼具安全性与通用性的安全 MCU 产品，其基于“通用内核+安全硬件加速引擎”的方式进行数据安全保护，芯片内部集成有密码硬件加速引擎，支持国产密码算法和国际密码算法，并且具有唯一硬件 ID、真随机数产生（TRNG）、读写保护（RDP/WRP）、存储加密、分区保护、安全启动等安全芯片的硬件安全特性，同时集成有各种通用的模拟器件与数字通信接口。

2.4.1.7 Trust Zone

Trust Zone 是 ARM CPU 内核支持的安全隔离技术，所有存储器与外设均可分配安全与非安全地址，隔离机制基于硬件实现，如图**错误! 未找到引用源。**所示。当 CPU 访问存储器或外设总线时，存储器检查站与外设检查站会进行地址检查，从而划分安全与非安全世界。即 TEE（Trusted Execution Environment）可信执行环境和 REE（Rich Execution Environment）通用的执行环境。REE 中的应用只能通过全接口访问 TEE，输入输出数据，不能访问 TEE 的存储器和控制外设。

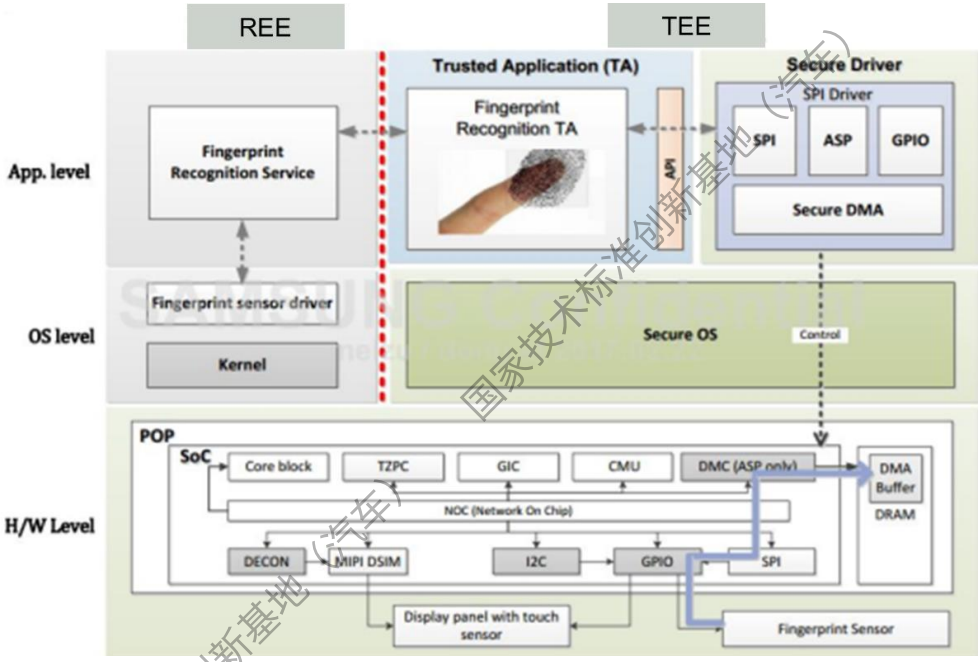

图 15 Trust Zone 技术框架

Trust zone 从内核层面增强了访问权限管理，不仅可以划分存储器的访问权限，亦对外设进行了访问权限管理。Trust zone 可以从硬件上隔离敏感的代码执行环境，从而解决代码运行时安全环境的问题。

2.4.2 车端模块

本报告中的车端模块指智能网联汽车上搭载的以上述安全硬件或者软件形式实现密码算法功能的各类控制器（ECU）。简而言之，即为车载端应用商用密码完成加解密、身份认证等功能的各类 ECU。

2.4.2.1 车端模块信息安全总体需求

针对智能网联汽车面临的信息安全风险，车端模块主要以车载 ECU 作为信息安全防护对象，在《汽车信息安全通用技术要求》中，针对车载 ECU 产品从软件、硬件、数据、车内通信及车外通信等维度

进行了信息安全技术要求。软件安全多指对于软件/固件安全、系统启动安全、软件升级安全等；硬件安全包含 ECU 封装、走线安全及调试接口安全；车内数据安全主要指车内数据的安全存储；车内通信安全主要指车内网络的通信安全；车外通信安全包含车-云安全、车-车/路安全、BLE 等通信安全。

车载 ECU 作为汽车控制单元的统称，涉及的范围广，在功能和应用场景上不尽相同，ECU 的计算能力和系统资源也有很大区别，因此信息安全需求与设计开发也存在很大差异。对于车端关键 ECU 如 CGW、TBOX、IVI 等具有联网功能的控制器，信息安全等级防护等级高；普通 ECU 依据功能定义和风险分析，具有基础安全防护措施或实施最低程度的安全防护措施。

2.4.2.2 软件/固件安全

使用密码技术的零部件主要是车载信息交互系统、T-BOX、网关等，应用密码技术对软件及固件的重要数据资产提供保密性、完整性、真实性等防护能力。

保密性主要通过密码加密技术（对称加密算法 AES 密钥长度：128、192、256 比特；模式：ECB、OFB、CFB、CBC、CTR、GCM）进行实现，保护车端软件及固件的机密信息不被泄露。防护对象包含如下：

1） 内存中的重要数据；

2） Flash 中的重要数据；

3） 软件的身份鉴别信息；

4） 密钥数据；

完整性主要通过数据签名技术（非对称加密算法 RSA 密钥长度：2048、3072、4096；散列函数：SHA256、SHA512 等）实现，保护车端软件及固件免受篡改。通常使用非对称加密算法实现。

真实性主要通过对称加密、动态口令、数据签名、挑战应答等技术（非对称加密算法 RSA 密钥长度：2048、3072、4096；散列函数：SHA256、SHA512 等）实现，保护车端软件及固件免受仿冒。防护对象包含如下：

1） 访问重要区域的应用身份鉴别；

2） 诊断设备接入时的身份鉴别；

3） 采用可信计算技术的平台身份鉴别；

4） 登录车载终端操作系统或超级用户的用户身份鉴别；

现有软件及固件安全使用的主流安全算法，大部分是国际算法。随着国密算法的重要性及自主性的影响，国内车载软件及固件模块的密码技术应用正逐步向自由可控的方向发展。国密算法应用的比例也会逐渐提高。

汽车领域缺少行业商用密码法规及强制性的标准，整车厂在推进商用密码相关合规认证方面，会存在明显的动力不足。软件及固件的商用密码技术的应用方向，更多的是参考国际密码标准进行设计和开发的。

2.4.2.3 系统启动安全

车载信息交互系统、T-BOX、网关等零部件应用可信验证技术对

系统进行安全启动校验，验证系统启动过程中的真实性、完整性（基于非对称加密算法：RSA 密钥长度：2048；散列函数：SHA256 等）（或者使用轻量级 CMAC、HMAC）。安全启动包括可信根、可信链两部分。

可信根使用安全的密钥管理方式来保证其机密性、完整性，硬件要支持 TPM（Trusted Platform Module 可信平台模块）安全芯片或 TCM（Trusted Cryptography Module 可信密码模块），可信根需要使用 OTP（One-Time-Progrm 一次性可编程芯片）方式进行存储，OTP 中通常存储的是公钥 HASH 值，保证可信根不被非法篡改，在硬件初始化开始时保证每个模块代码的载入都是可信的。

可信链是按照链式方式保证每个步骤都是可信的，近而达到系统整体的完整性和安全性。公钥是存在 SBL（Second BootLoader 位于 eMMC 中）镜像中的，PBL（Primary Boot Loader 位于 rom 中）读取 OTP 中的 Hash 来验证公钥的正确性，再用公钥验证 SBL 镜像的签名。

安全启动的防护对象主要是车载终端系统的镜像文件、bootloader、OS Kernel、应用程序等。

国内市场基于安全芯片或 HSM 硬件安全模块开发的安全启动，技术应用过程中无相关的研发门槛，和国外的主流安全产品相比，安全研发能力不会有的较大差距。

安全启动通常是基于硬件可信根来实现，对系统自身的业务流程存在一定的影响，需要进行系统层整体的开发设计，导致安全启动在软件开发生命周期中推进的阻力相对较大。

现有的汽车信息安全标准体系并没有对安全启动作强制性要求，安全启动在整车厂安全配置方面还有很大空间。供应商通常不会主动实施安全启动功能。

2.4.2.4 软件升级安全

1）软件升级包安全

软件升级包为汽车软件升级过程中的重要资产之一，主要面临着被篡改、伪造、泄露以及通过逆向等攻击手段获得软件工作逻辑等信息安全威胁，因此升级包在传输及升级过程中需要进行真实性、完整性、保密性等保护。

本地升级一般通过 OBD 诊断、USB 等设备对 ECU 进行软件升级，这种本地升级包一般由软件开发商进行制作，对升级包进行真实性、完整性、保密性保护。其保密性主要通过密码加密技术（对称加密 AES 密钥长度：128、192、256 比特）进行实现；完整性主要通过数据签名技术（非对称加密算法：RSA 密钥长度：2048、3072、4096；散列函数：SHA256、SHA512 等）或轻量级算法（CMAC\HMAC\CRC 等）进行实现；真实性主要通过数据签名技术（RSA 密钥长度：2048、3072、4096；散列函数：SHA256、SHA512 等）进行实现。当前车端 ECU 的安全分级不明确，本地升级安全防护方案及使用算法不统一，且当前 ECU 国产安全芯片应用率不高，基于 HSM、TEE 等安全升级的 ECU 普遍不支持国密算法。

远程升级通过空中下载技术（OTA），车端升级系统通过无线网络下载远程服务器上的升级包进行软件升级。目前远程升级包一般由车

厂 OTA 服务端统一对本地升级包进行加固，真实性、完整性保护依赖于车厂证书统一进行签名保护，多采用国际非对称算法（RSA 密钥长度：2048；散列函数：SHA256、SHA1 等）；保密性保护，多采用对称算法（AES；密钥长度：256）对升级包进行加密保护。

2）远程升级安全通信协议

升级数据从软件升级服务端到车端的传输过程，常面临着数据嗅探和窃取、数据篡改、数据重放攻击等威胁。因此要确保 OTA 升级过程中通信链路的安全性。

传输过程中的安全保护，需要采用行业内通用的安全通讯协议来实现，车端软件升级系统模块与远程升级服务端一般采用 TLS1.2 及 1.3 安全通信协议。

3）远程服务端身份认证

车载软件升级系统应具备远程升级服务端真实性鉴别能力。车端软件升级系统模块一般基于车厂自建 X509 PKI 系统（RSA）与 OTA 服务端实现双向身份认证。

OTA 软件升级系统一般依赖于车厂自建 PKI 基础密码设施，多为国际算法，且 OTA 软件升级系统供应商为国外厂商，普遍不支持国密算法。

当前联合国 WP29 R156 法规已发布，国内标准《汽车软件升级通用技术要求》预计于 2021 年发布，标准中明确提出了软件升级的安全技术要求，但并未针对使用的密码算法提出相应要求。

2.4.2.5 硬件及接口安全

汽车 ECU 等电子设备中，预留有大量的 JTAG、UART、SPI、USB 等调试接口，这些调试接口在设备量产后，如果硬件没有移除、功能没有禁用或设置安全的访问控制措施，则会为攻击者留下方便之门。一般情况下，由于设备量产后仍需要保留调试接口进行调试和问题修复，因此 ECU 的调试接口有访问可控性的要求。

目前，较为基础的调试接口身份认证措施，是使用口令验证，但口令验证方式存在口令泄露等风险，很多 Tier1 和 OEM 企业会逐步选择使用基于密码学算法的身份认证措施，如使用对称密码算法、非对称密码算法、消息验证码算法等。在此领域，国产商用密码尚未广泛应用，但随着汽车芯片和控制器的国产化率不断提高，在调试接口认证过程中使用国产商用密码算法的比率预计将快速增大。

2.4.2.6 车内数据安全存储

车端 ECU（如 IVI、TBOX、网关、ADAS 等控制器）存在密钥、PIN 码、用户隐私数据、算法模型等敏感数据，数据安全目标是要保证车载端所采集、存储、处理、传输的用户及车辆数据的安全性，确保车辆及用户数据的机密性、完整性和可用性得到有效的防护。基于密码模块，通过实施数据机密性保护措施对相关敏感数据实施安全存储，以防止因敏感数据被非授权访问、窃取给 ECU 系统、应用及用户带来的安全或隐私风险。

安全存储模块可基于纯软件密码模块、HSM、TEE、安全芯片等密码模块实现，需要支持基于 AES 或 SM4 密码算法的安全存储功能。

目前，国产的纯软件密码模块、安全芯片普遍支持 SM2/SM3/SM4 等国密算法，但 HSM 由于主要内置于国外厂商 MPU/MCU 芯片中，普遍不支持国密算法，此外，主流的 TEE 也不支持国密算法。目前车端 ECU 的安全存储模块，主要使用的是 AES 等国际密码算法技术。国产商用密码具备应用的技术条件，但目前仅在部分商用车 TBOX 终端上有安全存储方面的应用，大规模的应用还未形成。

2.4.2.7 车内通信安全

车内通信主要包括CAN总线通信、车载以太网通信等。当前车内通信多采用明文传输方式，一旦攻击者通过网络接口进入车内内部网络，就可以监听报文，甚至可以采用伪造报文、消息重放等方式实现对车辆的远程控制，导致严重的安全威胁。

为提高车载网络安全性，汽车开放系统架构AUTOSAR 在发布的新一代汽车软件开发系统架构中定义了车载安全通信模块（secure on-board communication，SecOC）安全验证机制。在SecOC安全验证机制中，使用MAC 机制进行身份认证，使用新鲜度值机制进行重放消息识别，从而保障了CAN 总线通信的安全性。在SecOC 规范中，推荐使用对称加密算法实现MAC 的生成，通过预设的加密密钥作为合法通信ECU 的识别。在SecOC 安全机制中，MAC 生成可以基于对称加密算法，也可以基于非对称加密算法，但是考虑在车载环境下，处理器的计算能力受限，规范推荐使用对称加密算法完成MAC 的生成。

2.4.2.8 车外通信安全

1）车-云安全通信

智能网联汽车与云端存在大量数据交换、信息共享等交互。车云通信数据传输过程中，存在被窃听及信息泄露等安全风险，车云通信的安全建立需要进行高强度身份认证、数据的机密性及完整性保护。

当前车端模块与云端通信一般采用 TLS1.2 双向认证安全协议，确保通信双方的身份认证及通信数据加密保护。一方面车端模块可利用国际开源算法资源，开发难度小、成本低、经验丰富；另一方面 TLS1.2 双向身份认证，依赖于车厂自建 PKI 系统，目前一般为 X509 RSA 证书系统。

目前国家密码管理局发布的《SSL VPN 技术规范》中定义了基于商密算法的安全套阶层协议，但在车联网领域应用范围不广。车-云安全采用国密 SSL VPN 对于车厂已建系统改造难度大、成本高，车-云通信商用密码替换涉及到车端模块、云端安全接入网关、PKI 系统等改造。

2）车-车/路安全通信

随着无线通信技术的发展，配备 V2X 技术的智能网联汽车可以同周围交通环境中的其他交通参与者进行无线通信。V2X 主要包括 V2V 和 V2I。V2V 可以实现车车通信，交换车辆之间的位置、速度等信息。V2I 可以实现车辆和道路设施、甚至是行人、非机动车辆之间的通信。V2X 应用中需要实现高安全的身份认证和数据保密，确保 V2X 通信中信息传递的保密性、完整性、不可否认性，PKI 技术正是解决车与

车、车与路侧单元通信安全问题的有效途径。

当前国内行业及车厂对于 V2X 的安全通信机制处于研究探索、示范应用的阶段，部分车厂已实现 V2X 应用安全的量产车型搭载。国内各车厂的 V2X 安全信任体系建设遵循《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》、GB/T《基于 LTE-V2X 的车载信息交互系统直连通信技术要求》等标准，均采用商密算法。

V2X-PKI 系统，Root CA、ECA、PCA、ACA 等签发证书格式遵循 CCSA/交通部标准，密码算法采用商密算法。

OBU 车端模块支持证书的申请、下载和管理；支持安全消息的签名、验签、加密解密；车规级国产高性能安全芯片使用，满足验签速度及安全要求；密码算法支持 SM2 密钥生成、签名验签、加密解密，SM3 摘要算法，SM4 对称加解密算法；支持基于安全芯片的安全存储等功能。

2.4.3 身份认证系统

2.4.3.1 智能网联汽车对 V2X 身份认证系统的需求

V2X 通信中，直连传输的用户数据在专用频段上通过 PC5 接口以广播方式发送；相应的 V2X 终端可以接收到通信范围内的所有广播消息，无论这些消息来自合法的发送者还是非法的发送者。因此直连通信场景下，V2X 用户面临虚假信息、假冒终端、信息篡改/重放、隐私泄露等安全风险。利用 PC5 无线接口的开放性，攻击者可以通过合法的终端及用户身份接入系统，构造并对外恶意发布虚假信息；也可以利用非法终端发送伪造的业务信息；还可以篡改或者重放合法用户发

送的信息。这些都将影响车联网业务的正常运行，严重的会危害周边车辆及行人的道路交通安全。此外，利用 PC5 无线接口的开放性，攻击者可以监听获取广播发送的用户标识、位置等敏感信息，进而造成用户身份、位置等隐私信息泄露。严重时，用户车辆可能被非法跟踪，直接威胁着用户的人身安全。

根据《LTE-V2X 安全技术白皮书》，V2X 直连通信安全需求包括：系统应支持对消息来源的认证，保证消息的合法性；支持对消息的完整性及抗重放保护，确保消息在传输时不被伪造、篡改、重放；应根据需要支持对消息的机密性保护，确保消息在传输时不被窃听，防止用户敏感信息泄露；系统应支持对真实身份标识及位置信息的隐藏，防止用户隐私泄露。其中，可以使用基于非对称加密体系的数字证书和数字签名技术来对抗针对直连端口传送消息的伪造、篡改和重放等攻击。同样，基于数字证书技术也可以对消息的真实性进行保护。隐私保护在 V2X 通信系统中有着不同于以往的需求——以往通信终端与网络连接，网络运营商会承担保护用户数据个人隐私的义务；但 V2X 车辆与其它车辆进行直连通信时，对方车辆的是否会收集记录发送方信息等具体情况并不了解，需要通过有效的手段加强消息发送者对隐私信息进行自我保护的能力。因此，为了保护驾驶员的隐私，不应将假名证书链接到长期车辆标识符，此隐私保护机制旨在阻止内部和外部攻击者根据记录的通信流量进行长期跟踪。例如，证书提供者不应将车辆的假名证书链接到车辆身份、车牌或车辆识别号（VIN）。同样，检测异常行为和识别攻击者的措施也不得牺牲对驾驶员的隐私

保护。

2.4.3.2 当前市场主流解决方案

CCSA 通信行业标准《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》规定了基于 LTE 的车联网无线通信技术安全证书管理系统技术要求，其中明确了 V2X 安全管理体系架构，如下图所示。该系统架构实现了对 V2X 设备进行数字证书签发的功能，从而该设备能够参与 V2X 安全通信，确保 V2X 通信系统能够持续安全地正常工作。

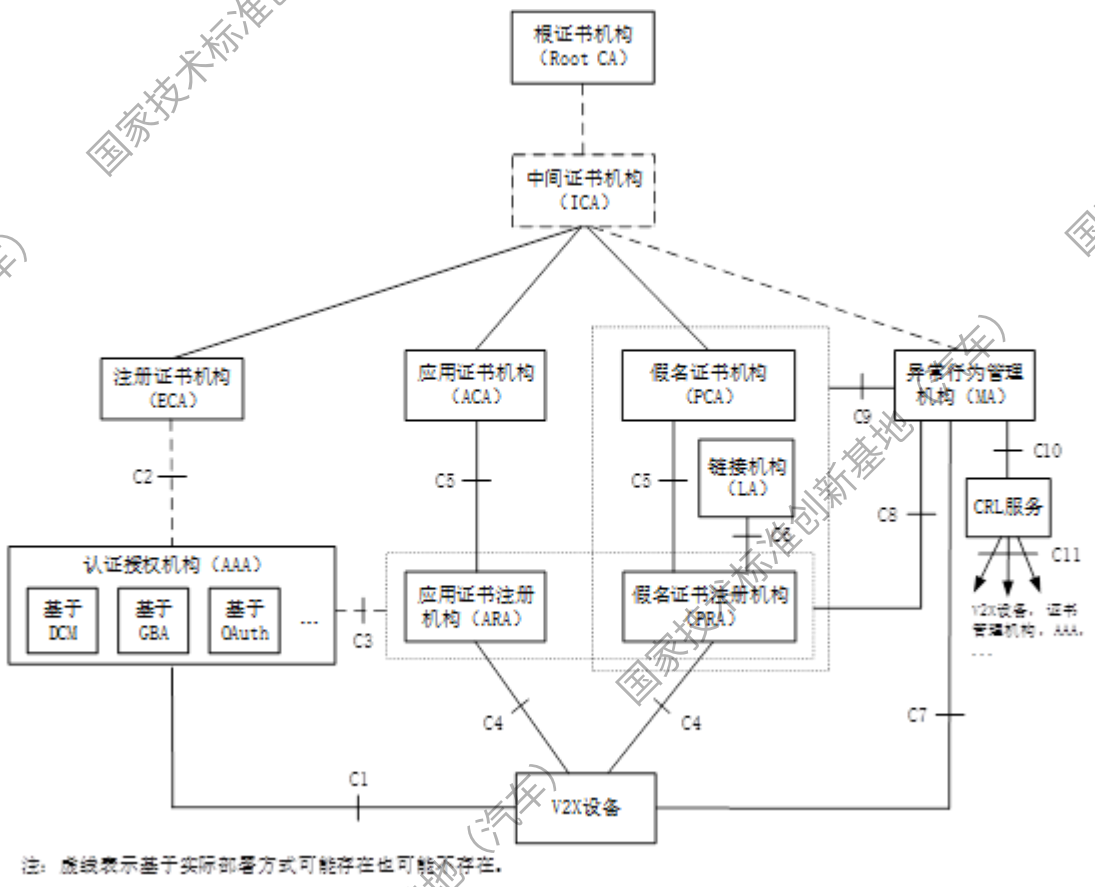

图 16 V2X 证书管理体系架构

V2X 证书管理系统基于公钥基础设施（Public Key Infrastructure，PKI）实现，从层次上看主要包括根证书机构、证书机构、认证授权机

构和证书申请主体四种逻辑实体。

根证书机构（Root CA）： V2X 证书管理系统的信任根，负责系统根证书的管理与维护并对 V2X 证书机构进行注册审批。在确认 V2X 证书机构的合法性之后，根证书机构为其签发管理机构的数字证书，使其成为系统内的有效实体。

中间证书机构（Intermediate CA，ICA）：V2X 证书管理系统可根据 PKI 部署的实际需要，在根证书机构与 V2X 证书机构之间部署中间证书机构，以支持多层级 CA 部署方式 。

认证授权机构（Authentication and Authorization Authority，AAA）：负责证书申请主体的身份认证和授权。在设备初始化阶段，为证书申请主体签发注册数字证书或其他类型的安全凭证，使其能够凭借获得的安全凭证与 V2X 证书机构安全交互并获取相应的证书。认证授权机构还可以对证书申请主体向 V2X 证书机构发起的证书请求进行授权。根据应用场景的不同，认证授权系统可基于设备配置管理（Device Configuration Manager，DCM）服务系统，蜂窝网络通用引导架构（General Bootstrapping Architecture，GBA）认证授权系统或者 OAuth 授权服务系统等多种方式实现。

V2X 证书机构：负责管理 V2X 安全通信应用相关数字证书，负责审核证书申请主体的合法性，签发、撤销证书申请主体的数字证书。V2X 证书机构是证书管理系统中各种证书机构的统称。根据 V2X 安全通信应用的证书类型及用途不同， V2X 证书机构可分为：注册证书机构（Enrolment Certificate Authority，ECA）、假名证书机构（Pseudonym

Certificate Authority，PCA）、应用证书机构（Application Certificate Authority，ACA）。注册、假名和应用证书机构由注册机构（Registration Authority，RA）和证书机构（Certificate Authority，CA）两部分组成。注册机构负责证书申请主体的注册审批管理，证书机构负责数字证书的发行管理。

链接机构（Linkage Authority，LA）：为假名证书生成链接值，以支持假名证书的批量撤销。

异常行为管理机构（Misbehavior Authority，MA）能够接收 V2X 设备对异常行为的上报，分析和识别的异常行为或故障，确定需要撤销的证书，生成证书撤销列表（Certificate Revocation List，CRL）。

V2X 设备（V2X Equipment）：是证书申请主体，向 V2X 证书机构申请获取相关数字证书以参与 V2X 安全通信，包括车载设备（On Board Unit，OBU）、路侧设备（Road Side Unit，RSU）及其他形态的实体。

2020 年 10 月，在 C-V2X“新四跨”暨大规模先导应用示范活动中重点验证了通信行业标准《基于 LTE 的车联网通信技术 安全证书管理系统技术要求》，众多 CA 方案厂商遵循标准搭建了 CA 子系统，分别接入多家根 CA，并与其他根 CA 下的各家 V2X 安全认证系统通过可信证书列表方式打通信任，为新四跨活动中的车辆 OBU 和路侧设备 RSU 提供基于新标准的安全证书，为成功地演示多种 V2V、V2I 应用场景奠定安全基础，如下图所示。

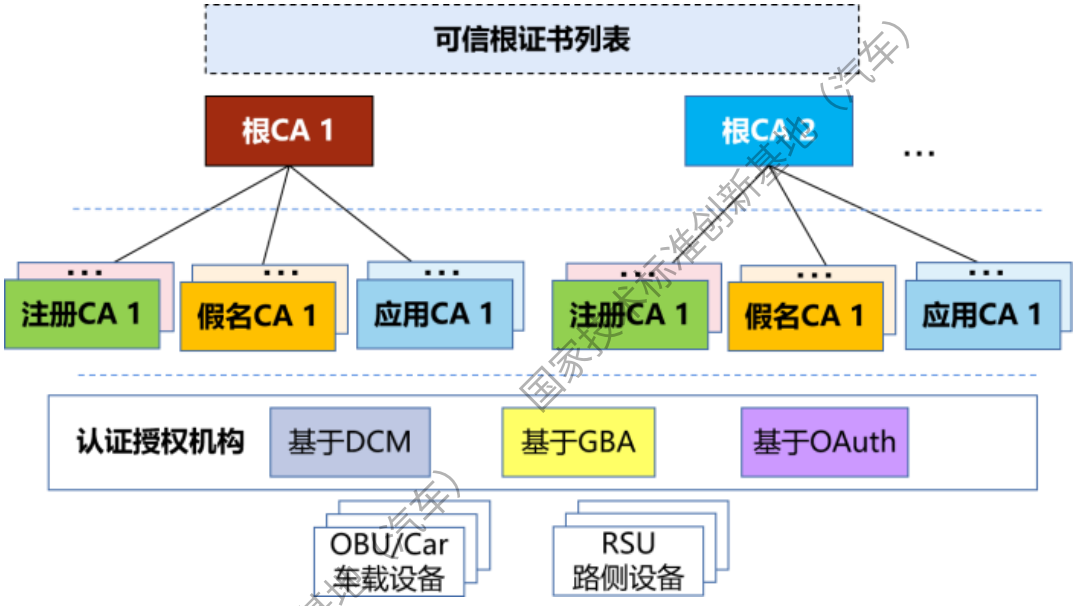

图 17　V2X CA 系统通过可信证书列表实现互信

2.4.3.3 商用密码应用情况分析

当前的 V2X 安全证书管理系统，已经根据 YD/T《基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求》、GB/T《基于 LTE-V2X 直连通信的车载信息交互系统技术要求》等标准要求，使用了 SM2 椭圆曲线公钥密码算法、SM3 密码杂凑算法、SM4 分组密码算法等国产商用密码算法。能够满足现有的 V2X 直连通信对信息安全中消息真实性、完整性，车主隐私防护的需求。

当前国际主流的 V2X 安全证书管理系统相关标准及 POC 系统实现，已经由最初只支持 256 位的椭圆曲线密码算法（Elliptic Curve Cryptography， ECC），更新到支持 384 位的 ECC 算法。相应的密码杂凑算法，也由最初只支持 SHA-256，更新到支持 SHA-384，增加了整体系统的安全性。

2.5 智能网联汽车商用密码应用检测技术现状

2.5.1 政策法规背景

2020 年 1 月 1 日起，《中华人民共和国密码法》正式施行。

《密码法》第二十五条规定，国家推进商用密码检测认证体系建设，制定商用密码检测认证技术规范、规则，鼓励商用密码从业单位自愿接受商用密码检测认证，提升市场竞争力。商用密码检测、认证机构应当依法取得相关资质，并依照法律、行政法规的规定和商用密码检测认证技术规范、规则开展商用密码检测认证。

《密码法》第二十六条规定，涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。

智能网联汽车不仅关系到驾乘人员的人身安全，对社会公共安全以及国家安全也会产生重大影响。按照《密码法》的要求，其相关密码产品可纳入认证目录，由具备资格的机构开展检测工作。

2.5.2 检测认证制度

2020 年 5 月 9 日，国家市场监管总局和国家密码管理局联合发布《商用密码产品认证目录（第一批）》及《商用密码产品认证规则》。

《商用密码产品认证目录（第一批）》规定了 22 类需要经过认证的商用密码产品，并给出相应的检测认证标准，除了每类产品自身需要满足的要求之外，其密码算法还应满足 GM/T 0001《祖冲之序列密码算法》、GM/T 0002《SM4 分组密码算法》、GM/T 0003《SM2 椭圆曲线公钥密码算法》、GM/T 0004《SM3 密码杂凑算法》、GM/T 0009《SM2 密码算法使用规范》、GM/T 0010《SM2 密码算法加密签名消

息语法规范》、GM/T0044《SM9 标识密码算法》等国家密码基本要求；其随机数检测应遵循 GM/T 0005《随机性检测规范》、GM/T 0062《密码产品随机数检测要求》等国家密码基本要求。

《商用密码产品认证规则》要求商用密码产品认证模式为：型式试验+初始工厂检查+获证后监督。其中型式试验要求认证机构应根据认证委托资料制定型式试验方案，并通知认证委托人按型式试验方案提供样品至检测机构。商用密码认证机构应当符合有关行政法规、规章规定的基本条件，具备从事商用密码认证活动的专业能力，并经市场监管总局征求国家密码管理局意见后批准取得资质。商用密码认证机构应当委托依法取得商用密码检测相关资质的检测机构开展与认证相关的检测活动，并明确各自权利义务和法律责任。

目前我国形成了以密码芯片、密码板卡、密码整机、密码系统等传统密码产品为主，多种密码产品形态和应用模式的商用密码通用产品共计 2000 余款。国内商用密码产品检测机构共有四家，分别为国家密码管理局商用密码检测中心、鼎铉商用密码测评技术（深圳）有限公司、智巡密码（上海）检测技术有限公司、豪符密码检测技术（成都）有限责任公司。

现阶段我国商用密码产品检测、认证能力供不应求，商用密码产品处于排队等候检测、认证的状态。专门针对智能网联汽车的商用密码产品检测尚处于空白阶段，且缺少经过认证或认定的面向车联网商用密码应用的专业检测机构。

2.5.3 产品检测内容

目前我国密码产品形态和应用模式众多，对于商用密码产品的检测内容简而言之可以分为两部分，一部分是对于密码算法、随机数等共性基础要求的检测，另一部分是针对不同密码模块的特有安全要求的检测。

基础共性检测主要包括如下内容：

（一）密码算法检测

密码学技术为保证信息的安全提供了强而有力的支撑，使用密码学不但能完成数字签名验签、身份验证、加密解密等功能，还能保证信息的完整性和准确性，从而防止信息被泄露、篡改、伪造以及假冒等。现代密码技术中，常见的密码算法包括对称密码算法、非对称密码算法和摘要（杂凑）算法三种。

（二）随机性检测

根据 GM/T 0005《随机性检测规范》、GM/T 0062《密码产品随机数检测要求》，对商用密码产品加密算法随机数生成流程、结果进行验证。

随机数作为密码学的关键元素，应用于明文加密、密钥管理和密码学协议等，保障了信息加密过程中的机密性、完整性和不可抵赖性等性能。中国国家密码管理局于 2012 年公布了我国商用密码领域随机数随机性检测规范，检测步骤为：

1）首先提出待检测的假设，该序列是随机的；

2）同时推算出与原假设相反的假设，即备择假设；

3）在原假设的状态条件下推导结论，如果结论发生的概率大于等于门限值，则认为原假设成立，反之则不成立。

规范中规定了 15 种检测方法，如单比特频数检测、扑克检测、重叠子序列检测等，对随机数的研究和应用起到了引领作用。

针对不同密码产品的特殊安全需求检测主要包括如下内容：

（一）芯片检测

安全芯片是一种重要的基础安全功能单元，在计算机、信息与通信系统中应用非常广泛。特别地，多数安全芯片都具有一种或多种密码功能。

商用密码产品认证标准要求安全芯片产品中的密码算法应为符合 GM/T 0002《SM4 分组密码算法》、GM/T 0003《SM2 椭圆曲线公钥密码算法》、GM/T 0004《SM3 密码杂凑算法》等国家密码管理要求的密码算法。另外，安全芯片产品的随机数检测应遵循 GM/T 0005《随机性检测规范》、GM/T 0062《密码产品随机数检测要求》。

安全芯片在实现的密码算法基础上，根据设计和应用的不同须具有一种或多种安全能力。在 GM/T 0008《安全芯片密码检测准则》中，将安全能力划分为密码算法、安全芯片接口、密钥管理、敏感信息保护、安全芯片固件安全、自检、审计、攻击的削弱与防护和生命周期保证九个部分，对每个部分的安全能力划分为安全性依次递增的三个安全等级，并对每个安全等级提出了安全性要求。安全芯片的安全等级定为该芯片所具有的各部分的安全能力的最低安全等级。

使用安全芯片所具有的密码功能时，安全芯片的安全能力对于保

障整个系统的安全性举足轻重。为提供预期的安全服务，以及满足应用与环境的安全要求，应选择恰当等级的安全芯片，以确保计算机、信息与通信系统的安全使用。

（二）车载模块检测

1. 车载 T-BOX

1.1 重型柴油车车载 T-box

车载 T-box 是车辆与外界通信的关键网络节点。国家标准 GB-17691《重型柴油车污染物排放限值及测量方法（中国第六阶段）》附录 Q 和环保部 HJ 标准《重型柴油车排放远程监控平台技术规范——3 车载终端及测试方法》报批稿附录 C 针对重型柴油车环保监控终端提出了信息安全要求，其中包含了商用密码产品的应用和安全防护要求。

（1）安全策略检测

车载终端应提供技术可行的安全策略，保证产品各种性能和功能处于安全范围内。在《重型柴油车污染物排放限值及测量方法（中国第六阶段）》附录 Q.4 中表明车载终端应提供技术可行的安全策略，保证产品各种性能和功能处于安全范围内。

（2）侧信道分析

侧信道攻击主要包括计时攻击、能量分析攻击和电磁攻击，其攻击本质是利用密码设备在运行过程中产生依赖于密钥的旁路信息来实施密钥恢复，侧信道攻击的防护能力成为衡量设备或芯片安全性的主要指标。

在《重型柴油车排放远程监控平台技术规范——3 车载终端及测试方法》附录 C.5 中规定了密码算法实现安全性测试方法，详细说明了侧信道分析系统的测试设备、测试方法和评价指标。

1.2 电动汽车车载 T-box

由东软集团股份有限公司、中国汽车技术研究中心有限公司牵头起草的国家标准《电动汽车远程服务与管理系统信息安全技术要求及试验方法》针对电动汽车车载 T-box 提出了 10 余项密码应用相关要求，包括车载终端应具备安全启动的功能，可通过可信根实体对安全启动所使用的可信根进行保护；应保证按照 GB/T 32960.3-2016 要求所存储的远程服务与管理数据的保密性和完整性，宜支持 SM2、SM3、SM4、AES、RSA 等算法等。

1.3 普通乘用车车载 T-box

由中国汽车技术研究中心有限公司、北京新能源汽车股份有限公司牵头起草的国家标准《车载信息交互系统信息安全技术要求及试验方法》针对包括 T-box 在内的信息交互系统提出了 10 余项密码应用技术要求，包括车载信息交互系统与平台服务端或外部终端间传输的数据内容应进行加密，宜使用国密算法；车载信息交互系统应实现对平台服务端或外部终端的身份认证等。由中国信息通信研究院、北京豆荚科技有限公司等单位起草的电信终端产业协会标准《车载 TBOX 信息安全技术要求》从硬件、操作系统、数据安全、软件安全、通信安全等方面对密码应用提出技术要求，如设备应具备足够的安全机制保证密钥的产生、分发、存储和销毁过程的安全性；关键加密算法实

现应具备抵抗侧信道分析和故障注入分析等物理攻击的能力，防止根密钥被破解等。

2.车载网关

由广州汽车集团股份有限公司、中国汽车技术研究中心有限公司牵头起草的《汽车网关信息安全技术要求及试验方法》对车载网络提出了 2 项密码应用相关技术要求，包括网关应具备安全启动的功能，网关的可信根、BootLoader 程序、系统固件不应被篡改，或被篡改后网关无法正常启动等。

3.车载 IVI

中国汽车技术研究中心有限公司、北京新能源汽车股份有限公司等牵头起草的国家标准《车载信息交互系统信息安全技术要求及试验方法》对包括车载 IVI 的信息交互系统分别从通信安全、应用软件安全、数据安全等方面提出了 10 余项密码应用相关要求，包括车载信息交互系统与平台服务端或外部终端间传输的数据内容应进行加密，宜使用国密算法；车载信息交互系统应实现对平台服务端或外部终端的身份认证等。

4.数字钥匙

2019 年互联网金融认证联盟（IIFAA）发布了制定了《数字车钥匙系统技术规范》。CCC（全球车联联盟）组织发布了数字车钥匙标准化规范 2.0。拥有数字密钥的消费类设备必须实现保护数字密钥以及防止未经授权使用数字密钥的机制。密钥保护可以防止未经授权而复制，修改和删除现有密钥；未经授权创建和提供新的密钥；拒绝服务。数

字密钥的未经授权的使用包括未经授权的用户的使用或超出使用范围之外的授权用户的使用。与数字钥匙相关的消息是在持有数字钥匙与车辆之间，另一台设备（对等钥匙共享）和远程后端（钥匙配置）之间交换。安全体系结构必须使这些消息的接收者能够验证消息的可信度。与拥有数字钥匙的设备进行的任何消息交换都必须满足以下目标：

（1）可信度：设备应仅接受可信设备的消息，即攻击者不应创建虚假消息

（2）完整性：设备应检测到攻击者已删除了全部或部分消息。

（3）更新：攻击者一定不能重放旧消息。

（4）绑定：数字密钥应与当前用户安全绑定，即攻击者不得伪装成先前的用户。

（5）独立性：消息交换不应泄露有关相同或另一个数字密钥的非必需属性的信息。

5.数字认证

（1）数字证书检测

数字证书是一个经授权证书授权中心签名的包含公开密钥拥有者信息以及公开密钥的文件，对于数字证书的检测应符合：

a.证书必须包含一个有效数字签名确定证书内容没有被修改，一般通过根证书来证明自身身份；

b.起止日期所指定的有效期必须表明证书是可用的；

c.证书没有被作废，可通过 CRL 或 OCSP 进行验证。

（2）密钥检测

非对称密钥的生成一般通常在服务器端通过硬件生成，在非对称密钥加密技术中保障私钥不被窃取是保证数据安全的传送和保管密钥的一个突出问题，所有与密钥生成有关的物品（如加密卡）等都应该有严格的规定。CA 非对称密钥及证书的安全性检测方法应采取分级分类的检测方法，具体检测标准在 GB/T 19714-2005GB/T 19714-2005《信息技术 安全技术 公钥基础设施 证书管理协议 》、GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式》中有详细描述。

（3）数字签名过程检测

签名采用的技术应符合：

a.采用国产 SM3、SM2 算法作为实现签名功能的 Hash 算法和签名算法；

b.为了保证安全通信，采用安全协议如 TLS/TLCP 等解决安全通信问题。

目前针对密码算法、随机数等基础共性要求的国际标准和国家标准趋近完善，但是专门针对汽车商用密码产品的标准缺失。国内外标准化组织纷纷开展汽车信息安全标准制定工作，其中也有密码应用相关的安全要求，但是总体而言，未能形成系统的密码应用要求。

2.5.4 产品检测工具

密码产品测评工具体系主要包括通用测评工具、工具管理平台、专用测评工具等，如下图所示。

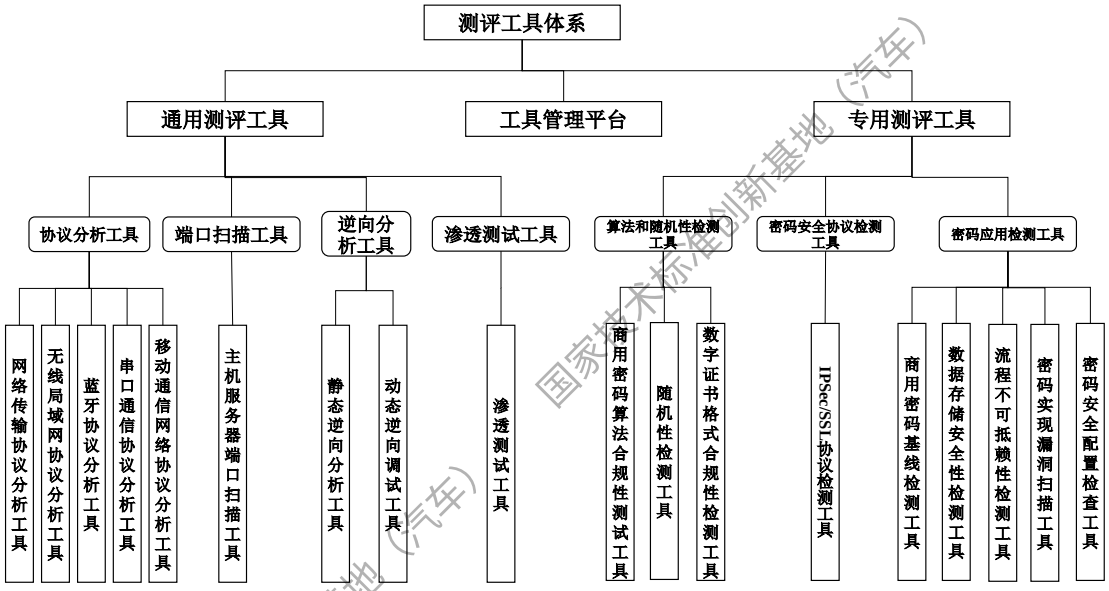

图 18 密码产品测评工具体系

通用测评工具是指在开展商用密码应用系统安全评估过程中，不限定应用于某一特殊领域、行业，具有一定普适性的检测工具。

1）协议分析工具主要用于对常见通信协议进行抓包、解析分析，支持对常见的网络传输协议、串口通信协议、蓝牙协议、移动通信协议（3G、4G、5G）、无线局域网协议等进行协议抓包解析，捕获的解析协议数据进行分析评估通信协议情况。技术指标：能够对常见的网络传输协议、串口通信协议、蓝牙协议、移动通信协议（3G、4G、5G）、无线局域网协议等进行协议抓包解析

2）端口扫描工具主要用于探测和识别被测信息系统的 VPN、服务器密码机、数据库服务器等设备开放的端口服务，以帮助测评人员分析和判断被测信息系统中密码产品和密码应用系统是否正常开启密码服务。技术指标：能够对密码产品、操作系统、web 应用、数据库、网络设备、网络安全设备及应用的端口服务进行自动化探测和识

别。

3）逆向分析工具是指在没有源代码的情况下，通过分析应用程序可执行文件二进制代码，探究应用程序内部组成结构及工作原理的工具，一般可分为静态分析工具和动态分析工具。逆向分析工具主要用于被测系统中重要数据保护强度的深入分析。支持对常见格式文件的静态分析，以及应用程序的动态调试分析。技术指标：能够对常见应用系统下的应用软件进行动态、静态逆向检测分析，可以分析密钥在存储、应用过程中的安全性、脆弱性。

4）渗透测试工具主要用于对被测信息系统可能存在的影响信息系统密码安全的风险进行检测识别，支持对北侧信息系统开展已知漏洞探测、未知漏洞探测和综合测评，并尝试通过多种手段获取系统敏感信息。测评结果能够作为测评人员分析评估被测信息系统密码应用安全的可信依据。技术指标：能够利用漏洞攻击方法及攻击手段，实现对系统、设备、应用漏洞的深度分析和危害验证。

专用测评工具用于检测和分析被测信息系统的密码应用的合规性、正确性和有效性的一部分或全部环节，可以简化测评人员的工作。

由于目前汽车商用密码产品检测标准缺失，无法针对汽车商用密码产品做定制化开发，测试专业化和自动化程度较低，对测试人员技术水平要求较高，测试结果一致性也难以保障。

2.6 问题分析

2.6.1 标准法规层面问题分析

从标准法规层面来说，虽然在智能网联汽车上的很多应用场景都

涉及到密码的使用，但国内外目前并没有专门针对智能网联汽车的商业密码应用的法律法规和标准规范，对汽车产业缺少商用密码应用指导和约束。

1.缺少明确有效的行业指导规范

近几年随着车辆智能化、网联化的快速发展，汽车行业信息安全问题凸显，信息安全保护迫在眉睫。针对密码管理和密码应用，在国家法律层面、政策法规层面，已发布相关的法律和政策文件。金融、政务、能源等行业源于在信息安全保护方面的多年经验，通过颁发相关文件，在各自的领域积极响应国家商用密码的推进计划，积极部署和稳步推进商用密码的应用。但在汽车行业，目前并没有明确的行业应用指导文件。随着信息安全保障工作在汽车行业的稳步发展，应在合适的时机发布商用密码建设实施办法，从而有力推动智能网联汽车商用密码应用。

2.缺少适用于行业应用的技术标准

在标准层面，缺少相关的密码应用技术标准。汽车行业整体的信息安全防护能力薄弱，大量数据没有采用密码技术进行保护。即使采用密码技术措施保护的数据，也存在采用一些被警示有风险的密码算法和密码服务的情况。商用密码技术在保障信息安全中有着核心技术和基础支撑作用。没有统一有效的技术标准作为密码体系建设、密码管理、密码系统运维等执行的参考依据，从而导致密码应用的不规范，这是智能网联汽车信息安全防护的重大隐患。目前正在编制的标准中，有个别标准提到了密码技术的应用，但内容很少，其技术要求并不能

满足行业应用的需要。因此，需要建设适于汽车行业应用的技术标准规范，为汽车行业合规、正确、有效使用商用密码提供依据，促进商用密码在汽车行业应用的大力推进和普及，充分发挥商用密码在保障智能网联汽车信息安全中的核心技术和基础支撑作用。

2.6.2 产品应用层面问题分析

1. 智能网联汽车商用密码算法应用不广泛

对于国内的汽车厂商来说，推广自主可控的密码算法势在必行。针对汽车网络信息安全问题，应在立足国密算法，研发信息安全产品方案。目前很多的汽车厂商并没有使用国密算法。国密算法应用在车联网体系中存在较多困难，由于智能网联汽车对时效性要求高，使得密码算法在保障时效性的情况下，其强度有所下降，这是国密算法应用在工业领域的一个最大的障碍。

2. 智能网联汽车商用密码产品应用经验不足

智能网联汽车包含数量众多的车端模块，复杂性高、安全防护环节众多，且具有强实时、存储空间小等方面的资源约束特性，与传统密码应用场景有显著区别。随着智能网联汽车信息安全行业发展，虽多数车企采取了相应的安全防护措施，但安全防护体系与措施并不完善，且对车端 ECU 的安全等级划分不明确，难以统一密码安全要求。

同时智能网联汽车信息安全技术处于发展阶段，密码技术应用不够成熟，如软件安全、安全存储、车内网络安全等部分安全防护手段并未采取完整有效的安全防护措施，存在技术不成熟、实现成本高等诸多问题。

3. 智能网联汽车商用密码应用产业链不健全

从行业资源支撑来看，目前智能网联汽车商用密码应用产业链不健全，密码算法应用以国际算法为主，国密算法的市场主要在国内。从我国汽车 ECU 供应链实际情况来看，主流汽车芯片多来自于国外供应商，受限于主流的汽车芯片大多还无法从硬件上支持国产商密算法，并且开发支持国产商密算法的产品需要较长的认证流程，因此，国际汽车零部件兼容国密算法还有很长的路要走。同时，车载的安全芯片或 HSM 硬件安全模块多以较为独立的产品模块进行销售，基于安全芯片的应用业务开发也要依赖于相应的国外安全芯片供应商。

车端 ECU 密码产品的应用研发及部署需要协同整车厂、零部件商、软件供应商、芯片供应商、检测机构等产业链各方，复杂度高，亟需加强汽车产业与国产商用密码产业的深度合作。

2.6.3 检测认证层面问题分析

智能网联汽车商用密码应用检测认证机制缺失

目前智能网联汽车商用密码应用产业链不健全，尤其是缺乏咨询、测评机构用于指导汽车领域商用密码应用的事前规划、事中检测和事后评价；智能网联汽车商用密码应用标准建设滞后，汽车领域商用密码应用规范类和检测标准缺失，因而导致相应的认证机制缺失，商用密码产品和技术的应用无法作为产品安全质量的要素得以体现；标准政策和认证机制的缺失，也阻碍了专业的汽车商用密码应用测评机构和测试工具的产生和发展。

3 智能网联汽车商用密码应用标准化需求分析

3.1 概述

通过对国内外智能网联汽车商用密码法律法规、标准政策、应用场景、产品技术、检验检测等方面的发展现状和存在问题分析，可以看出，当前汽车商用密码应用标准严重缺失。

因此，定位于智能网联汽车车端商用密码应用技术要求和测试方法的国家标准亟需制定。该标准应不仅仅是汽车密码应用的笼统指南，而是能够切实指导汽车商用密码应用落地和检验检测的参考规范。需要开展的标准化工作包括：汽车商用密码应用的安全分级、不同应用场景中应该满足的密码应用安全等级以及不同的密码应用安全等级中车内系统和车外通信应该满足的具体安全要求。

3.2 商用密码应用安全分级标准化

3.2.1 密码安全分级必要性

理由 1：对汽车密码实行安全分级，针对不同类型的数据使用不同安全级别的密码，有利于提高汽车零部件整体的安全性和可用性。当所有类型数据都使用一种安全性较高的密码时，整体会过度消耗 ECU 零部件系统资源。需要分别将机密性要求低的数据使用安全级别低的密码手段、机密性要求较高的数据使用安全级别高的密码手段加以防护。

理由 2：在 ISO 21434 标准中已经对安全需求提出了信息安全保证等级（CAL）的概念。高等级的 CAL 安全需求对应较高的安全风险，

在软件开发的过程中需要提高安全开发的质量，增加对应的安全开发活动。高等级的 CAL 安全需求可以提高密码安全等级。

理由 3：在《自动驾驶数据安全白皮书 2020》中，对自动驾驶数据安全中的数据涉密性提出了要求，自动驾驶汽车在公开道路驾驶过程中，会采集大量的地理信息数据。根据中国法律法规要求，采集地理信息数据可能涉及涉密测绘成果，因此需要按照《中华人民共和国保守国家秘密法》中的相关规定要求进行分级管理，并且自动驾驶数据具备多样件，根据不同自动驾驶级别，数据产生的来源不同。数据类别不仅包括了汽车基础数据，也包括基础设施、交通数据、地理信息数据，以及车主的大量用户身份类数据、用户状态数据、行为类数据等。这些数据需要针对不同的使用场景，需要设计不同的安全密码级别。

理由 4：GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，通过物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面提出了等级保护不同级别的密码应用的安全性要求。从我国密码应用标准来看，对密码应用实行安全分级是较为科学实用的技术要求和管理方式，等级保护标准也与密码应用的安全等级相关联。

理由 5：欧盟 EVITA 标准中，对硬件安全模块 HSM 提出了三个等级，EVITA Full、EVITA Medium、EVITA Light。Full level：用于 V2X 或者中央网关，采用高速非对称加密；Medium Level：用于 ECU 之间，采用低速非对称加密、高速对称加密，适用于动态通信；Light Level：用

于传感器、执行器采用对称加密，适用于静态通信；EVITA 针对不同的应用场景，使用不同级别的硬件安全模块。硬件间的差异主要体现在支持的安全算法不同。

基于以上分析，在汽车领域实行密码应用的安全分级是可行并且必要的。

3.2.2 密码安全分级方法论

我国已有部分车规级芯片和车载终端产品通过了商用密码检测中心的密码模块安全认证，密码模块的安全分级方法给汽车商用密码的安全分级提供了可行的思路。密码模块是指实现密码运算、密钥管理等功能的硬件、软件、固件或其组合，这与汽车商用密码产品的形态相符合。

GB/T 37092-2018《信息安全技术 密码模块安全技术要求》标准中提出了四个要求递增的安全等级以保护密码模块和密码模块中包含和控制的敏感安全参数。每一级安全等级都包含前一个等级的所有要求。

3.2.2.1 安全一级

安全一级提供了最低等级的安全要求。安全一级阐明了密码模块的基本安全要求。模块应当使用至少一个核准的安全功能或核准的敏感安全参数建立方法。软件或固件模块可以运行在不可修改的、受限的、或可修改的运行环境中。安全一级硬件密码模块除了需要达到产品级部件的基本要求之外，没有其它特殊的物理安全机制要求。

当模块外部的应用系统已经配置了物理安全、网络安全以及管理

过程等控制措施时，安全一级的模块就非常适用。如外部已经提供了全面的安全保护，使用一级模块就非常的经济。这使得密码模块的使用者可以选择多种密码解决方案来满足安全需求。

密码一级模块可以使用软件或硬件进行实现。

安全一级的应用举例：

车载零部件需要使用产品级的密码模块，密码模块自身无安全防护，安全要依赖应用系统的安全防护功能，如防火墙、安全接入、诊断认证等，此类应用的密码模块，可使用安全功能为一级的模块。

3.2.2.2 安全二级

安全二级在安全一级的基础上增加了拆卸证据或基于角色的鉴别功能，以提高物理安全性。拆卸证据机制包括使用拆卸存迹的涂层或封条。拆卸存迹的封条或防物理，以防止非授权的物理访问。当物理访问模块内的安全参数时，模块上拆卸存迹的涂层或封条就必须破碎。

基于角色的鉴别，密码模块需要鉴别并验证操作员的角色，以确定其是否有权执行对应的服务。该环境也可以实现自主访问控制，但是应当至少能够定义新的分组，通过访问控制列表（ACL）分配权限，以及将一个用户分配给多个分组。访问控制措施应防止非授权执行、修改以及读取实现密码功能的软件。

密码二级模块可以使用软件或硬件进行实现。使用软件密码模块能够达到的最大整体安全等级限定为安全二级。

安全二级的应用举例：

在满足物理安全二级的情况下，采用了基于角色的鉴别机制，使用加密或明文的形式调用密码模块接口的输入和输出，这样的密码模块可被定义为安全二级。如安全日志加密、访问策略加密、汽车标定数据加密等处理，建议使用安全二级的密码模块。

3.2.2.3 安全三级

除了安全二级中要求的拆卸存迹物理安全机制外，安全三级还要求更强的物理安全机制，以防止对密码模块内敏感安全参数的非授权访问。这些物理安全机制应该能够以很高的概率对以下行为进行检测及响应。这些行为包括：直接物理访问、密码模块的使用或修改、以及通过通风孔或缝隙对模块的探测。上述物理安全机制可能包括坚固的外壳、拆卸检测装置以及响应电路。当密码模块的封盖/门被打开时，响应电路应当将所有的关键安全参数置零。

安全三级要求基于身份的鉴别机制，以提高安全二级中基于角色的鉴别机制的安全性。密码模块需要鉴别操作员的身份，并验证经鉴别的操作员是否被授权担任特定的角色以及是否能够执行相应的操作。

安全三级要求手动建立的明文关键安全参数是经过加密的，使用可信通道或使用知识拆分来输入或输出。

安全三级的密码模块应有效防止环境因素或电压、温度超出模块正常运行范围对密码模块安全性的破坏。攻击者可以故意让密码模块的环境参数偏离正常运行范围，从而绕过密码模块的防护措施。密码模块应当设计有特殊的环境保护特性，用以检测环境异常并置零关键

安全参数，或者能够通过环境失效测试从而提供一个合理的保障，保障不会因环境异常破坏模块的安全性。

安全三级的密码模块应提供非入侵式攻击缓解技术的有效性证据和测试方法。

安全三级的密码模块增加了生命周期保障的要求，比如自动配置管理、详细设计、底层测试以及基于厂商所提供的鉴别信息的操作员鉴别。

密码三级的模块只能依赖硬件进行实现。

安全三级的应用举例：

车载零部件具备了安全芯片或集成式硬件安全模块， 采用了基于身份的鉴别机制（数字签名）密码模块使用加密方式调用密码模块接口，可提供非入侵式攻击缓解技术的有效性证明，使用物理的方式破坏密码模块外壳，芯片可以将关键安全参数置零，这类的密码模块可定义为密码安全三级，可应用到车载 T-BOX、车载信息交互系统的重要数据处理场景，如数据加解密的使用的密钥存储、安全启动可信根的存储等。

3.2.2.4 安全四级

安全四级是本标准中的最高安全等级。该等级包括较低等级中所有的安全特性，以及一些扩展特性。

安全四级的物理安全机制应当在密码模块周围提供完整的封套保护，其目的是无论外部电源是否供电，当模块包含敏感安全参数时，检测并响应所有非授权的物理访问。从任何方向穿透密码模块的外壳

都会以很高的概率被检测到，并将导致所有未保护的敏感安全参数立刻被置零。

安全四级要求对操作员进行多因素鉴别。最低限度下，要求使用下列因素中的两个：

已知某物，如秘密口令；

拥有某物，如物理钥匙或令牌；

物理属性，如生物特征。

安全四级的密码模块应有效防止环境因素或电压、温度超出模块正常运行范围对密码模块安全性的破坏。密码模块应当设计有特殊的环境保护特性，专门用以检测环境异常并置零关键安全参数，从而提供一个合理的保障，保障不会因环境异常破坏模块的安全性。

安全四级的密码模块应对非入侵式攻击提供缓解能力，包括了能量分析、计时分析、电磁泄露。

针对安全四级的测试指标，测试密码模块中实现的、按照规定的针对非入侵式攻击的缓解方法。

安全四级要求模块的设计应通过一致性验证，即证明前置和后置条件与功能规格之间的一致性。

安全四级的应用举例：

车载零部件具备了安全芯片或集成式硬件安全模块，需要采用基于身份的多因素鉴别机制， 密码模块使用加密方式调用密码模块接口，可提供非入侵式攻击缓解技术的有效性证明，使用物理的方式破坏密码模块外壳，芯片可以将关键安全参数立刻置零，这类的密码模

块可定义为密码安全四级，可应用到安全性要求更高的车载 T-BOX、车载信息交互系统的敏感数据处理场景，如汽车虚拟钥匙数据的处理、车主生物特征的存储等。

3.3 商用密码应用安全要求标准化

3.3.1 车内系统密码应用标准化

车内系统的密码应用标准化需求，包括软件系统、硬件系统、车内数据及通信链路等。

3.3.1.1 软件系统

1）机密性

使用密码加密功能实现加密性，保护对象为：身份鉴别信息；车辆设备软件升级包。

2）完整性

使用消息鉴别码（MAC）或数字签名实现完整性，保护对象为：系统资源访问控制策略、数据库表访问控制信息、重要信息资源敏感标记信息、重要用户信息，包括车载娱乐系统、ADAS 系统、ADS 系统、ECU 系统；重要信息资源敏感标记；系统运行过程中重要程序或文件；日志记录；辆设备软件升级包。

3）真实性

使用对称加密、动态口令、数字签名等实现真实性，应用场景为：用户身份标识和鉴别。

3.3.1.2 电子电器硬件

1）完整性

使用消息鉴别码（MAC）或数字签名实现完整性，保护对象为：视频监控音像记录；电子门禁系统进出记录。

2）真实性

使用对称加密、动态口令、数字签名等实现真实性，应用场景为：进入重要物理区域人员的身份鉴别。

3.3.1.3 车内数据

1）机密性

使用密码加密功能实现加密性，保护对象为：传输的重要数据，包括鉴别数据（PIN 码、用户隐私数据等）、重要数据（V2X 数据、ADS 数据、车端 APP 数据）；存储的重要数据，包括鉴别数据（PIN 码、用户隐私数据等）、重要数据（V2X 数据、ADS 数据、车端 APP 数据）；身份鉴别信息；密钥数据。

2）完整性

使用消息鉴别码（MAC）或数字签名实现完整性，保护对象为：传输的重要数据，包括鉴别数据（PIN 码、用户隐私数据等）、重要数据（V2X 数据、ADS 数据、车端 APP 数据）；存储的重要数据，包括鉴别数据（PIN 码、用户隐私数据等）、重要数据（V2X 数据、ADS 数据、车端 APP 数据）；日志记录。

3）不可否认性

使用数字签名等密码技术实现实体行为的不可否认性，针对所有

需要无法否认的行为，包括数据发送、接收等操作。

3.3.1.4 车内通信

1）机密性

使用密码加密功能实现加密性，保护对象为：传输过程中鉴别信息；通信过程中敏感信息数据（鉴别数据、个人数据）或整个报文。

2）完整性

使用消息鉴别码（MAC）或数字签名实现完整性，保护对象为：网络边界和系统资源访问控制信息；通信过程中数据。

3）真实性

使用对称加密、动态口令、数字签名等实现真实性，应用场景为：网络设备实体身份。

3.3.2 车外通信密码应用标准化

整车与车外终端的通信安全标准化需求，包括车外远距离通信，如蜂窝移动通信、卫星导航等；车外近距离通信，如 OBD、蓝牙、近场无线通信和 Wifi 等。

3.3.2.1 车外远距离通信

1）机密性

使用密码加密功能实现加密性，保护对象为：传输过程中鉴别信息；通信过程中敏感信息数据（鉴别数据、个人数据）或整个报文。

2）完整性

使用消息鉴别码（MAC）或数字签名实现完整性，保护对象为：

网络边界和系统资源访问控制信息；通信过程中数据。

3）真实性

使用对称加密、动态口令、数字签名等实现真实性，应用场景为：网络设备实体身份。

3.3.2.2 车外近距离通信

1）机密性

使用密码加密功能实现加密性，保护对象为：传输过程中鉴别信息；通信过程中敏感信息数据（鉴别数据、个人数据）或整个报文。

2）完整性

使用消息鉴别码（MAC）或数字签名实现完整性，保护对象为：网络边界和系统资源访问控制信息；通信过程中数据。

3）真实性

使用对称加密、动态口令、数字签名等实现真实性，应用场景为：网络设备实体身份。

4 智能网联汽车商用密码应用技术要求标准化研究结论与后续工作建议

4.1 研究结论

（1）智能网联汽车网络安全问题随着产业的发展日益凸显。商用密码技术作为网络安全的核心保障和基础支撑，在车联网的各个应用场景中均可得到广泛应用。但从目前产业安全现状和爆发的安全事

件来看，汽车商用密码应用技术较为落后，没有起到应有的安全保障作用。

（2）智能网联汽车商用密码应用技术落后，主要原因可以归结为汽车领域起引领、指导作用的相关标准政策缺失，这导致汽车产业链普遍缺乏密码应用意识，也缺少正确、规范应用密码的指导和参考；密码供给侧企业发展受限；专业的检测机构和检测工具缺失。

（3）智能网联汽车商用密码应用标准亟待建设，以指导汽车密码规范应用，保障汽车网络安全。标准化的内容应包括密码应用的安全分级、不同应用场景下应满足的安全等级以及不同安全等级中应满足的具体安全要求等。

4.2 标准化建议

（1）《智能网联汽车商用密码技术要求》（以下简称“本标准”）应是聚焦于车端各类控制器、车载通信设备及节点和计算单元等商用密码应用的标准规范。

（2）本标准中，商用密码应用的安全分级应是研究重点，可以参考信安标委、密标委发布的系列商用密码标准以及美国 FIPS 系列标准中的安全分级方法。

（3）本标准中，应根据各类不同的车端控制器或密码应用场景的安全要求，与商用密码应用的安全等级进行对应，以明确指导汽车商用密码应用，对于如何定义或划分控制器及应用场景的安全要求，可以不属于本标准中制定范畴，而是引用其他标准或研究成果，如汽标委标准研究项目《汽车电子控制单元（ECU）信息安全防护技术要

求研究》中的分类分级或 ISO 21434 中 TARA 和攻击树方法论，识别 ECU 相应的风险级别。

（4）本标准起草过程中，应关注《汽车整车信息安全技术要求与测试方法》，可借鉴该标准的制定思路。本标准或将为该标准提供商用密码相关的技术补充。