强制性国家标准

《汽车密码应用技术要求》

（报批稿）

编制说明

2026年10月

目　　次

目次 0
一、工作简况 1
二、编制原则、强制性国家标准主要技术要求的依据及理由 4
三、与有关法律、行政法规和其他标准的关系 38
四、与国际标准化组织、其他国家或者地区有关法律法规和标准的比对分析 38
五、重大分歧意见的处理过程、处理意见及其依据 39
六、对强制性国家标准自发布日期至实施日期之间的过渡期的建议及理由 39
七、与实施强制性国家标准有关的政策措施 39
八、是否需要对外通报的建议及理由 40
九、废止现行有关标准的建议 40
十、涉及专利的有关说明 40
十一、强制性国家标准所涉及的产品、过程或者服务目录 40
十二、其他应当予以说明的事项 40

GB 《汽车密码应用技术要求》

编制说明

一、工作简况

1.1. 任务来源

根据国家标准化管理委员会发〔2024〕59 号文《国家标准化管理委员会关于下达〈汽车密码应用技术要求〉等 37 项强制性国家标准制修订计划及相关标准外文版计划的通知》，制定强制性国家标准《汽车密码应用技术要求》（计划号：20243883-Q-339）。

该标准为工业和信息化部与国家密码管理局联合归口，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。主要起草单位由中国汽车技术研究中心有限公司（以下简称“中汽中心”）、商用密码检测认证中心（以下简称“检测中心”）等组成。

1.2. 项目背景

当前，全球新一轮科技革命和产业变革深度演进，智能网联汽车已成为汽车产业转型升级的战略方向，也是大国产业竞争与科技博弈的制高点。随着汽车从传统交通运输工具向移动智能终端、数据交互节点和能源服务单元加速演进，其安全边界已从物理空间向网络空间、从功能安全向信息安全全面延伸。密码技术作为保障信息安全、网络安全以及数据安全的核心技术和基础支撑，是构建汽车产品内生安全防御体系的战略基石。

《中华人民共和国密码法》的颁布实施，确立了密码工作在国家治理体系和治理能力现代化中的重要地位。智能网联汽车作为国家关键信息基础设施的重要关联部分和新型移动网络节点，其密码应用的工程化实现直接关乎国家安全与社会公共利益。工业和信息化部、国家密码管理局联合推进强制性国家标准《汽车密码应用技术要求》制定工作，是贯彻落实《密码法》《网络安全法》《数据安全法》等法律法规的重要举措，是构建国家网络安全等级保护和密码应用安全管理制度闭环的必然要求。

我国已成为全球最大的智能网联汽车市场，2 级及以上驾驶自动化系统正加速普及，L3 级自动驾驶开启商业化试点，单车代码量突破十亿级，车载通信涵盖 V2V、V2I、V2N 等多种复杂场景，数据采集、传输、存储、处理全链路面临前所未有的安全挑战。近年来，针对智能网联汽车的网络攻击事件频发，远程控车、数据窃取、系统篡改等安全风险已从理论验证演进为现实威胁，涉及人身安全、公共安全乃至国家安全的连锁风险不容忽视。

密码技术是实现身份认证、数据加密、完整性保护和抗抵赖性的核心技术手段，能够在整车层面构建起“进不来、拿不走、看不懂、改不了、走不脱”的内生防御体系。然而，当前汽车行业密码应用仍存在顶层设计不足、技术要求分散、实施规范缺失等突出问题。

行业亟需填补汽车密码应用强制性技术标准空白，解决汽车密码应用面临三方面突出矛盾。其中，矛盾包括：一是密码算法与密码模块的选用缺乏统一、强制的技术要求，部分产品使用非标准密码算法或密码模块不合规，存在安全隐患；二是车载密码应用场景覆盖不全，从安全启动到车云通信、远程控制等关键环节，密码技术应用的深度和广度参差不齐，缺乏系统性规范；三是密码管理与密钥全生命周期安全保障能力薄弱，密钥生成、存储、分发、使用、销毁等环节存在安全盲区。

在此背景下，本标准编制旨在明确汽车密码应用的总体框架、通用要求与技术要求，覆盖汽车整车密码应用方案的设计、开发、测试验证全过程，为汽车行业密码合规应用提供权威技术依据，引领汽车密码安全技术规范化、体系化、产业化发展，为我国智能网联汽车产

业安全可控、高质量、可持续发展提供关键标准支撑与技术保障。

1.3. 主要工作过程

自 2021 年 7 月，中汽中心与检测中心在管理部门的指导下，积极开展汽车行业密码应用调研，启动汽车密码相关标准研究工作。经过 3 年的行业深耕与标准研究，标准经更名、合并，于 2024 年 5 月，形成《汽车密码应用技术要求》标准草案及立项建议书。2024 年 6 月—7 月，对国内 39 家相关企业开展调研，掌握了汽车行业密码技术应用的最新情况，分析了国内外车辆制造商在车载系统与核心零部件的密码算法需求强度及应用情况，梳理了汽车密码应用的核心场景及密码技术保护的数据类型，探讨了汽车强标与其他标准协调性以及目前汽车行业存在的困难等问题。2024 年 8 月，该标准通过汽标委立项答辩，2024 年 12 月，下达标准计划号。

2021 年—2024 年期间，主要工作过程如下。

2021 年 7 月启动标准研究与起草工作，组织主要车辆制造商、密码企业、零部件供应商及信息安全企业共同研究编制《汽车数据传输密码应用基本要求》国家标准。工作组通过企业调研、问询讨论等多种形式，广泛组织行业力量共同开展汽车密码应用基本要求标准的研究与编制工作，深入研究汽车行业密码的技术及应用情况，集合行业力量共同修订完成标准草案。

2021 年 9 月，检测中心牵头组织中汽中心等单位专家成立汽车数据安全调研工作组，选取 25 家具有行业代表性的企业，通过问卷调查、电话回访和线上会议调研的方式，开展行业摸底研究工作，深入了解汽车数据安全现状及密码应用情况。工作组通过调研发现目前汽车数据传输安全面临的威胁最为严重，形势也最为急迫。标准工作组确定标准面向对象、适用范围和主要内容，完成《汽车数据传输密码应用基本要求》标准草案并向行业内 11 家企业征集意见。

2024 年 5 月，标准工作组组织车辆制造商、密码行业专家成立汽车数据安全专家组，结合各成员多年技术积累，反复交流，对标准内容形成了一致共识，完成新一版标准草案。

2025 年—2026 年期间，主要工作过程如下。

全国汽车标准化技术委员会智能网联汽车分技术委员会前期依据各单位申请情况组织成立项目组，并在此基础上明确了任务和分工，积极开展标准的研究、调研、起草、研讨等工作。

2025 年 3 月，启动标准项目研讨，确定了标准制定的指导思想和原则。项目组收集、整理、并系统地分析了国内外与汽车密码相关的法规、标准、文献等资料，组织开展相关技术研究工作。

2025 年 4 月—2025 年 5 月，项目组结合我国产业情况和试点经验，系统开展研究和分析，梳理标准框架和内容，形成初版草案。

2025 年 6 月—2025 年 10 月，项目组针对密码算法、密码模块类型、密钥应用需求、差异维度、密钥保护措施等开展第二轮调研，发放调研问卷并实地走访了上汽、理想、芯钛、雅迅四家企业，初步形成了调研报告。

2025 年 10 月—2025 年 12 月，项目组在制定过程中分别多轮征集项目组成员单位意见，并结合专题会议等方式逐步研讨完善标准草案内容。

2026 年 1 月—2026 年 6 月，结合管理需求和行业意见，调整标准结构，完善标准草案，形成公开征求意见稿初稿。

2026 年 7 月，结合行业意见，细化标准条款要求，完善标准草案，形成公开征求意见稿。

2026 年 8—9 月，组织开展强标验证试验围绕密码算法、密码模块与安全芯片、随机数以及系统安全、通信安全、数据安全等典型场景的密码应用要求，对相关技术条款和试验方

法进行测试验证。汇总各机构验证试验开展相关测试中的共性问题，梳理技术条款和试验方法的修改建议，为进一步完善标准内容提供依据。

2026 年 10 月，项目组分阶段、分批次召开公开征求意见处理会和意见协调会，对征集到的意见逐条研究讨论，重点围绕技术要求的适用范围、条款表述及试验方法的可操作性进行分析，明确意见处理结论，并据此修改完善标准文本。

1.3.1. 第1次会议

2025 年 3 月 21 日在北京召开，会议明确了标准编制思路及双归口强标的工作机制。工信部装备工业一司提出要把好强标安全底线，制定能用、好用、易用的强制性国家标准，部署了严控标准周期、严把标准质量、严守工作纪律的“三严”要求，督促秘书处做好组织工作，同起草组专家一起，高效开展标准研制工作。国家密码管理局提出要做好汽车密码应用标准的体系规划，加强对汽车密码应用需求和关键技术研究，促进汽车上的密码合规正确有效应用，引领技术创新和产品提档升级，实现汽车和密码的深度融合创新发展。

会上汽车密码强标联合牵头单位分别介绍了汽车密码强标的制定背景、编制思路、工作计划和工作机制等。与会专家根据企业实践经验，围绕行业反馈的关键问题以及对标准制定的建议等议题展开深入讨论，为汽车密码强标制定贡献了大量的建设性意见。来自东风汽车集团有限公司研发总院、吉利汽车研究院（宁波）有限公司、广州小鹏汽车科技有限公司、郑州信大捷安信息技术股份有限公司、晟安信息技术有限公司和中汽软件测评（天津）有限公司的专家分享了汽车密码应用实践及标准制定建议。

1.3.2. 第2次会议

2025 年 4 月 8 日在合肥召开，会议研讨了标准基础信息、标准框架、项目组工作机制和分工；完成初版草案编写，由起草组成员单位共同完成编写通用要求、密钥管理技术要求与密码应用技术要求。由检测机构共同根据技术要求编写试验方法。

1.3.3. 第3次会议

2025 年 5 月 28 日至 29 日在长沙召开，针对标准草案文本开展起草组内部意见讨论以及处理。本次会议的核心任务是对标准草案文本进行全面、系统的内部意见讨论与处理。参与单位已按照分工完成各自章节的草案起草与组内意见征集，本次会议充分发挥起草组成员的专业优势，逐章逐条审议草案文本，系统收集各方反馈意见，集中讨论分歧较大的争议条款，形成标准草案修改意见的处理方案，确保标准文本的科学性、合理性和可操作性。

1.3.4. 第4次会议

2025 年 10 月 13 日在贵阳召开，会议系统汇报了标准编制进展与行业调研成果，针对密码技术应用现状，涉及应用需求、密码算法、密码模块、密钥管理等多维度研讨；基于不同应用场景，从密钥种类、密钥功能以及密钥的保护等多维度对密钥管理展开探讨。

1.3.5. 第5次会议

2025 年 11 月 11 日在南昌召开，结合行业调研与走访情况，针对汽车密码应用场景、密钥管理等关键问题展开研讨，对汽车密码应用的重点场景进行梳理。此外，针对汽车密码应用是否需要分类分级展开讨论。

1.3.6. 第6次会议

2025 年 12 月 31 日在天津召开，会议研讨草案内容与框架，结合汽车密码应用场景对

标准框架进一步梳理完善。会后基于目前草案内容，请行业针对检测方法的撰写工作提供意见。

1.3.7. 第7次会议

2026 年 7 月 23 日在天津召开，会议围绕密码模块条款开展讨论，重点研讨各方案的技术要求及实施可行性；针对同一型式判定条件、判定范围及标准实施过渡期安排进行交流，并组织测试试验方法分享，讨论相关方法的适用性和可操作性。

1.3.8. 第8次会议

2026 年 9 月 10 日、23 日在天津召开，开展试验方法专项研讨会，讨论验证试验的开展情况及测试结果，重点讨论试验方法适用性、测试条件及实际实施中存在的困难，梳理验证过程中的共性问题，形成相关问题的处理结论及技术条款、试验方法的修改完善建议。

1.3.9. 第9次会议

2026 年在 10 月 9 日、10 月 22 日，以线上和线下相结合的形式分批次召开了标准公开征求意见协调会，组织重点单位针对重点意见处理进行研讨，在 10 月 13 日—15 日，面向 85 家前期反馈意见的单位，组织召开大范围的公开征求意见处理会，会议对公开征求意见期间收到的反馈意见进行逐条研究讨论，重点围绕密码算法、密码模块、随机数、系统安全、通信安全及数据安全场景明确意见采纳情况及处理理由，并结合验证试验结果进一步修改完善标准文本。

二、编制原则、强制性国家标准主要技术要求的依据及理由

2.1. 标准编制原则

本文件编写符合 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。综合标准前期研究成果，根据本标准制定的基本原则，立足于我国汽车产业实际特点及密码技术应用现状，开展本标准的编制。

（1）先进性方面，本标准充分研究了国内外标准法规和企业产品现状，在借鉴国外成熟技术和经验的前提下，结合现阶段我国密码技术的快速发展，提出符合现阶段和未来发展的我国汽车密码应用技术要求。

（2）可行性方面，通过调研整车、零部件、密码模块等领域的代表性企业，了解我国企业在汽车密码应用方面的技术发展水平或技术储备能力，以及密码应用上存在的问题，提出适合且能够引导国内相关行业发展的标准。

（3）协调性方面，汽车密码应用标准的普及在管理和使用上涉及到汽车的各个领域，技术上需要协调整车、零部件、密码模块企业等多方面意见，因此在充分协调各方意见的基础上，研究制定满足我国实际情况的汽车密码应用标准，规范汽车密码应用的设计、开发、测试、实施等工作。

2.2. 主要技术内容

2.2.1. 术语和定义

条款3.2 密码模块 cryptographic module

在密码边界内实现安全功能的硬件、软件、固件或这三者组合。

注：密码模块根据其组成，可分为硬件密码模块、固件密码模块、软件密码模块以及混合密码模块。

说明：密码模块是指实现密码运算、密钥管理等安全功能的硬件、软件、固件或者其组合，用于保护计算节点与信息系统内的敏感信息。

2.2.2. 密码应用技术要求

条款5.1.1 车辆使用的密码算法应符合任一密码国家标准、行业标准或国际标准，并满足国家密码管理要求。在已采用符合上述标准要求的密码算法保护车辆安全的场景下，允许使用其他公开、已发布的、有效的密码算法进行冗余性保护。

说明：车辆制造商不得使用未经标准化验证或未经主管部门认可的自研算法、私有算法，并应根据不同密码算法和业务场景选择适当的参数和选项。其中，国际标准是指国际标准化组织（ISO）、国际电工委员会（IEC）、国际电信联盟（ITU）等国内官方认可的国际标准化组织发布的正式标准，NIST、BSI等国外机构发布的算法清单不属于本条款所指的国际标准。常见的冗余性保护有：

（1）在诊断、车内通信等场景中采用分层校验，且其中一层采用的算法满足本标准要求的；

（2）在软件升级场景中采用分层校验，主节点采用的算法满足本标准要求的；

（3）车辆制造商在采用标准算法的基础上，出于安全、合规考虑，采用尚未标准化的先进算法的（如PQC算法）。

以上特殊场景需结合国家密码管理要求统筹考虑，未来主管部门发布新的密码管理要求后，以最新的管理要求为准，例如发布标准化PQC算法后，企业应采用标准化的PQC算法，不应再使用非标的PQC算法。

条款5.1.2 车辆使用的密码模块和安全芯片应符合任一密码国家标准、行业标准或国际标准要求。对与云平台通信系统、具备远程控制功能的系统所使用的关键密钥的安全保护应使用符合GB/T 37092—2018安全等级第二级（含）以上的密码模块或GM/T 0008—2012安全等级第二级（含）以上的安全芯片或符合GB/T XXXX—XXXX《汽车芯片信息安全技术规范》安全等级第二级（含）以上要求的安全芯片。

注1：关键密钥指与云平台通信系统和具备远程控制功能的系统中，用于保障通信实体真实性、远程控制指令真实性和完整性等核心业务功能网络和数据安全的密钥，由车辆制造商结合车辆功能确认。

注2：具备远程控制功能的系统指部署在车端且具备对远程控制指令进行真实性和完整性校验及分发功能的系统，如远程车载信息交互系统（T-Box）、车载综合信息处理系统（IVI）等。

说明：车辆采用的密码模块和安全芯片必须符合密码国家标准、行业标准或国际标准的要求，不允许使用非标准的密码模块和安全芯片。

条款5.1.3 车辆应存储其使用的各密码模块和安全芯片的型号和软件版本号信息。

说明：车辆应存储各密码模块和安全芯片的型号及软件版本信息，并支持通过企业提供的适当方式进行读取。

条款5.1.4 车辆与云平台通信、V2X直连通信、远程控制通信、通过诊断接口和其他外部无线通信方式与外部实体进行通信时，参与车端密钥生成或运算的随机数质量应符合GB/T 32915—2026的要求，使用可信设备直接访问车内零部件的除外。

注：可信设备指在安全机制下获得授权的设备。

说明：随机数质量要求适用于车辆与外部实体通信时参与车端密钥生成或运算的随机数，场景包括与云平台通信、V2X直连通信、远程控制通信，以及通过诊断接口、其他外部无线通信方式与外部实体进行通信等。例如，车载通信终端与云平台建立安全连接时，参与

车端密钥生成或运算的随机数均应满足本条要求。通过诊断接口和外部实体进行通信的随机数不包括诊断仪与车内ECU直连的场景，也不包括诊断过程中诊断指令在车内通信传递的部分。

条款 5.2.1 重要系统密码应用要求

5.2.1.1 车辆应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术，验证删除车端数据记录系统中记录数据的外部操作实体真实性。

注： 车端数据记录系统指汽车领域其他强制性法规要求装备在车辆上的，具备监测、采集和存储数据功能并支持数据读取的系统，包括自动驾驶数据记录系统、组合驾驶辅助数据记录系统等。

5.2.1.2 车辆应不支持以明文方式导出存储在车端的与 2 级及以上驾驶自动化系统相关的对称密钥、私钥。

5.2.1.3 车辆应不支持以明文方式导出存储在车端的基于人工智能模型实现车身控制的系统的对称密钥、私钥。

说明：（1）对2级及以上驾驶自动化系统要求的范围不包含摄像头、雷达等传感器；

（2）本条不限定身份真实性验证的具体方案，可采用数字签名、消息鉴别码等密码技术，并可结合挑战应答机制实现。例如，操作实体对随机挑战值生成签名或消息鉴别码，由验证方校验应答以确认其身份；

（3）对称密码技术以共享密钥为基础，双方使用同一密钥完成加解密或消息鉴别码的生成与验证。基于杂凑算法与共享密钥构造的消息鉴别码（如HMAC）同样属于对称密码技术范畴；

（4）重要系统的边界以条款所列功能的系统为准，不因多个系统部署于同一零部件，就将相关密钥保护要求扩展至该零部件上的全部系统；

（5）本标准有关密钥的要求不适用于临时密钥。临时密钥是指为特定会话或单次运算临时生成、仅在相应过程中使用且结束后不再使用的密钥，例如仅用于一次会话的临时会话密钥。

条款 5.2.2 具备远程控制功能的系统、车载软件升级系统、2 级及以上驾驶自动化系统、基于人工智能模型实现车身控制的系统应具备安全启动机制。安全启动过程中，车辆应对涉及的引导加载程序、系统固件等启动阶段组件进行安全校验，应使用密码技术保护其加载前的真实性与完整性。

说明：车辆需通过密码技术确保车辆在上电或重启过程中加载的组件的真实性和完整性，防止引导加载程序、系统固件等启动阶段组件被非法篡改、替换或伪造后运行。该场景仅要求到系统层级，应用层级的校验由企业自行评估实施。

条款 5.2.3 软件升级密码应用要求

5.2.3.1 使用车载软件升级系统密码应用要求

应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术保护接收到的升级包，车载软件升级系统应在加载升级包前，验证升级包的真实性和完整性，且车载软件升级系统所使用的与车载软件升级功能相关的密钥需满足以下要求：

a） 应不支持以明文方式导出存储在车端的对称密钥、私钥；

b） 应使用密码模块或安全芯片保护存储在车端的对称密钥、私钥的机密性；

c） 应使用密码技术或一次性编程技术保护存储在车端的密钥的完整性。

5.2.3.2 不使用车载软件升级系统密码应用要求

如未在可信环境下执行软件升级，车端各被升级的控制器应在加载升级包前，使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术，验证升级包的真实性和完整性，且各被升级的控制器所使用的与车载软件升级功能相关的密钥需满足以下要求：

a） 应不支持以明文方式导出存储在车端的对称密钥、私钥；

b） 应使用密码模块或安全芯片保护存储在车端的对称密钥、私钥的机密性；

c） 应使用密码技术或一次性编程技术保护存储在车端的密钥的完整性。

注： 在可信环境下执行软件升级指通过安全通道拷贝升级包、采取保护措施保证刷写接入端的安全性等。

说明：（1）“车载软件升级系统”指车端负责升级包接收、校验、分发及升级过程管理的软件和硬件系统，行业中通常称为车端OTA Master，可用于在线升级或离线升级；

（2）使用车载软件升级系统时，本条款要求范围为车载软件升级系统及其使用的与车载软件升级功能相关的密钥；未使用车载软件升级系统时，本条款要求范围为车端各被升级控制器及其所使用的与车载软件升级功能相关的密钥；

（3）密钥完整性可通过密码技术或OTP、eFuse等一次性编程技术实现。其中，一次性编程技术通过写入后不可改写等机制，防止密钥被未授权修改；

（4）“不支持明文导出”指针对通过诊断、调试等工具读取并导出明文密钥的操作。车内正常功能交互及必要业务流程中的密钥传递、调用，不属于本条款所指的工具导出范围。

条款 5.3.1 与云平台通信密码应用要求

5.3.1.1 通信协议密码应用要求

车辆与 TSP 平台、OTA 平台等云平台通信时应使用 TLS 1.2 及以上版本或 TLCP 等安全通信协议建立安全通道，且满足以下要求：

a） 应使用基于公钥密码算法的数字签名等密码技术，验证通信实体的真实性；

b） 应使用基于对称密码算法或公钥密码算法的密码技术保护敏感个人信息和重要数据传输的机密性；

c） 应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术保护通信数据的完整性。

5.3.1.2 密钥导出要求

车辆应不支持以明文方式导出存储在车端的与云平台通信相关的对称密钥、私钥。

5.3.1.3 数字证书应用要求

车辆与 TSP 平台、OTA 平台等云平台通信时如使用数字证书，应满足以下要求：

a） 如未使用硬件保护存储在车端的根证书，应使用密码技术保护其完整性；

注： 根证书指自签名的公钥证书，是信任链的起始点。

b） 如车端支持在线申请证书，证书申请语法应符合国家标准、行业标准或国际标准；

c） 如车端支持在线申请证书，应使用密码技术保护证书申请数据在传输过程中的完整性；

d） 如车端支持证书下载功能，证书下载过程中，应对车辆证书及其信任链进行校验，校验失败或与车端预置的可信证书信任链不一致时终止下载；

e） 如车端支持证书导入，应对导入车辆证书的公钥和私钥的匹配性进行校验，校验失败禁止导入；

f） 证书应仅用于证书中指定的用途；

g） 车辆应具备检查证书状态的能力，并在证书失效后停止使用证书；

h） 如支持对证书撤销功能，撤销后的证书不应继续使用。

说明：（1）安全通道可采用TLS 1.2及以上版本，或符合GB/T 38636—2020要求的TLCP协议建立，也允许采用能够满足本条安全要求的其他标准化安全通信协议；

（2）本条款要求的与车辆通信的云平台指所有与车辆直接连接并产生数据交互的平台，包括TSP平台、OTA平台、车载应用（非预装的第三方应用除外）对应的云平台等；

（3）用于密钥生成或运算的随机数应符合国家标准要求。车辆不应支持通过诊断、调试等工具，以明文形式导出与云平台通信相关的对称密钥和私钥；

（4）对于数字证书的要求，分别以车端支持相应证书功能为适用前提，仅对已支持证书功能的安全性提出要求，不要求车辆为满足本条新增上述功能；

（5）卡验证证书（CVC）不属于数字证书。

条款 5.3.2 V2X 直连通信密码应用要求

5.3.2.1 通信过程密码应用要求

车辆与车辆、路侧单元、移动终端等进行 V2X 直连通信时，应满足以下要求：

a） 应使用基于公钥密码算法的数字签名等密码技术，验证通信实体的真实性、消息发送行为的不可否认性；

b） 应使用基于公钥密码算法的数字签名等密码技术保护通信数据的完整性；

c） 如未使用密码模块或安全芯片保护与 V2X 直连通信相关的密钥，应使用密码技术或一次性编程技术保护其完整性。

5.3.2.2 密钥导出要求

车辆应不支持以明文方式导出存储在车端的与 V2X 直连通信相关的对称密钥、私钥。

5.3.2.3 假名证书应用要求

车辆与车辆、路侧单元、移动终端等进行 V2X 直连通信时使用的 V2X 假名证书应满足以下要求：

a） 证书申请语法应符合国家标准、行业标准或国际标准；

b） 应使用密码技术保护证书申请数据在传输过程中的完整性；

c） 证书下载过程中，应对车辆证书及其信任链进行校验，校验失败或与车端预置的可信证书信任链不一致时终止下载；

d） 应对导入车辆证书的密钥的匹配性进行校验，校验失败禁止导入；

e） 证书应仅用于证书中指定的用途；

f） 应具备在证书失效时完成证书更新的能力；

g） 应支持证书撤销功能，且撤销后的证书不应继续使用。

说明：本条适用于车辆与其他车辆、路侧单元、移动终端等进行V2X直连通信的场景。本场景证书应用要求专门针对V2X直连通信使用的假名证书，身份证书等其他证书在5.3.1规定场景中的应用，按相应要求执行，本条不重复要求。

条款 5.3.3 远程控制密码应用要求

5.3.3.1 车辆应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术，验证远程控制指令信息的真实性。

5.3.3.2 车辆应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术保护远程控制指令信息的完整性。

5.3.3.3 车辆应采取有效手段抵御针对远程控制指令的重放攻击。

5.3.3.4 车辆应不支持以明文方式导出存储在车端的与远程控制相关的对称密钥、私钥。

说明：用户通过蜂窝通信传输的控制车辆功能和状态的指令信息，如开启空调、启动车辆、车门解闭锁等，不包含蓝牙等近场控车指令信息。

条款5.3.4 其他外部无线通信密码应用要求

车辆使用除5.3.1～5.3.3以外的无线通信方式与外部实体进行通信时，需满足以下要求：

a) 如未使用标准的安全无线通信协议，应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术，验证通信实体的真实性；

注：标准的安全无线通信协议指协议自带安全机制的标准化通信协议，如蓝牙4.2协议、第三代Wi-Fi访问保护协议（WPA3协议）等。

b) 如未使用标准的安全无线通信协议，应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术保护通信数据的完整性；

c) 通过无线通信传输控制指令信息时，应采取有效手段抵御重放攻击；

d) 如未使用密码模块或安全芯片保护与其他外部无线通信相关的密钥，应使用密码技术或一次性编程技术保护其完整性；

e) 车辆应不支持以明文方式导出存储在车端的与其他外部无线通信相关的对称密钥、私钥。

说明：采用蓝牙4.2、WPA3、RFID和NFC通信等自带安全机制的标准化通信协议，并启用相应安全机制时，通信实体真实性和通信数据完整性保护可由协议自身实现。

条款 5.3.6 诊断接口密码应用要求

5.3.6.1 车辆应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术，验证通过诊断接口向车辆发送关键配置及标定参数的写操作指令的通信实体的真实性。

5.3.6.2 车辆应不支持以明文方式导出存储在车端的与诊断接口通信相关的对称密钥、私钥。

5.3.6.3 如未使用密码模块或安全芯片保护存储在车端的与诊断接口通信相关的密钥，应使用密码技术或一次性编程技术保护其完整性。

说明：该场景真实性要求仅适用于诊断接口层级，针对诊断设备与车内网关或其他直接连接的车载零部件之间，发送关键配置及标定参数写操作指令的通信实体开展真实性验证。该要求不扩展至诊断指令在车内转发、处理的整个链路，不要求诊断链路中的各节点逐级验证身份真实性。

条款 5.3.7 车内通信密码应用要求

5.3.7.1 车辆应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术，验证通信过程中发送关键报文的通信实体的真实性，使用标准化的车内诊断通信协议的除外。

注：关键报文指被攻击后将对车辆造成严重损害的报文。

5.3.7.2 车辆应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术保护关键报文的完整性，使用标准化的车内诊断通信协议的除外。

5.3.7.3 车辆应保护存储在车端的与车内通信相关的密钥的安全性。

注：保护存储在车端的密钥的安全性的技术包括安全访问技术、加密技术等，车辆制造商可选择适当的技术保护存储在车端的密钥的安全性。

5.3.7.4 车辆应不支持以明文方式导出存储在车端的与车内通信相关的对称密钥、私钥。

说明：本条仅针对车辆制造商声明的需要保护的关键报文提出要求，关键报文是指被攻击后可能对车辆造成严重损害的报文。对于车内诊断通信场景，采用标准化车内诊断通信协议的报文，可豁免本条规定的通信实体真实性验证和通信数据完整性保护要求。

条款5.4.1 保护敏感个人信息密码应用要求

5.4.1.1 车辆使用密码技术保护存储在车端的敏感个人信息时，应至少满足以下要求中的一项：

a) 使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术，验证访问和获取敏感个人信息的外部操作实体的真实性；

b) 使用基于对称密码算法或公钥密码算法的密码技术保护其机密性。

5.4.1.2 向车外传输敏感个人信息时，车辆应使用基于对称密码算法或公钥密码算法的密码技术保护其机密性。

5.4.1.3 车辆应保护存储在车端的与保护敏感个人信息相关的密钥的安全性。

5.4.1.4 车辆应不支持以明文方式导出存储在车端的与保护敏感个人信息相关的对称密钥、私钥。

5.4.1.5 车辆使用数字证书保护存储在车端的敏感个人信息时，使用的数字证书应满足5.3.1.3 的要求。

说明：（1）使用密码技术保护存储在车端的敏感个人信息时，应使用密码技术验证访问和获取敏感个人信息的外部操作实体的真实性或保护敏感个人信息的机密性；

（2）对于向车外传输的敏感个人信息，应采取基于对称密码算法或公钥密码算法的密码技术保护敏感个人信息的机密性，避免数据在车云通信、平台交互或外部传输过程中泄露。应采用安全技术实现密钥存储保护。

条款5.4.2 保护重要数据密码应用要求

5.4.2.1 车辆使用密码技术保护存储在车端的重要数据时，应至少满足以下要求中的一项：

a) 使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术，验证访问和获取重要数据的外部操作实体的真实性；

a) 使用基于对称密码算法或公钥密码算法的密码技术保护其机密性。

5.4.2.2 向车外传输重要数据时，车辆应使用基于对称密码算法或公钥密码算法的密码技术保护其机密性。

5.4.2.3 车辆应保护存储在车端的与保护重要数据相关的密钥的安全性。

5.4.2.4 车辆应不支持以明文方式导出存储在车端的与保护重要数据相关的对称密钥、私钥。

5.4.2.5 车辆使用数字证书保护存储在车端的重要数据时，使用的数字证书应满足5.3.1.3 的要求。

说明：（1）使用密码技术保护存储在车端的重要数据时，应使用密码技术验证访问和获取重要数据的外部操作实体的真实性或保护重要数据的机密性；

（2）对于向车外传输的重要数据，应采取基于对称密码算法或公钥密码算法的密码技术保护重要数据的机密性，避免数据在车云通信、平台交互或外部传输过程中泄露。应采用安全技术实现密钥存储保护。

条款 5.4.4 保护关键数据密码应用要求

5.4.4.1 车辆使用密码技术保护存储在车内的关键数据时，应使用基于公钥密码算法的数字签名或基于对称密码算法的消息鉴别码等密码技术，验证删除和修改关键数据的外部操作实体的真实性。

注：关键数据包括制动参数、安全气囊展开阈值、动力电池参数等关键配置参数；车辆状态及动态信息、自动驾驶/组合驾驶辅助系统运行信息、行车环境信息、驾驶员操作及状态信息等2级及以上驾驶

自动化系统相关数据；以及其他车辆运行过程中产生的可能影响车辆运行安全的数据。

5.4.4.2 车辆应保护存储在车端的与保护关键数据相关的密钥的安全性。

5.4.4.3 车辆应不支持以明文方式导出保护存储在车端的与保护关键数据相关的对称密钥、私钥。

5.4.4.4 车辆使用数字证书保护存储在车端的关键数据安全时，使用的数字证书应满足5.3.1.3 的要求。

说明：关键数据包括关键配置参数、2级及以上驾驶自动化系统相关数据、以及其他车辆运行过程中产生的可能影响车辆运行安全的数据。其中，2级及以上驾驶自动化系统相关数据可参考GB 44497《智能网联汽车 自动驾驶数据记录系统》、GB 47955《智能网联汽车组合驾驶辅助系统安全要求》等标准。

2.2.3. 试验方法

条款6.3.2 密码模块/安全芯片测试

测试人员应根据车辆制造商提供的密码模块或安全芯片测试报告和接口调用方法，按照以下测试方法中适用的测试方法开展测试，判定车辆是否满足5.1.2和5.1.3的要求：

a) 测试人员使用车辆制造商提供的方式，尝试读取存储在车端的型号和版本信息，测试是否可以读取，并与车辆声明使用的密码模块或安全芯片型号及版本信息清单进行一致性比对，判定是否满足 5.1.3 的要求；

b) 如使用密码模块，测试人员测试密码模块的密钥保护、敏感信息保护、接口安全、软件安全、固件安全、物理安全、自检、抗攻击防护及生命周期管理等，判定是否满足 5.1.2 的要求；

c) 如使用安全芯片，测试人员测试安全芯片的密钥保护、敏感信息保护、接口安全、固件安全、自检、抗攻击防护及生命周期管理等相关机制，判定是否满足 5.1.2 的要求。

说明：汽车制造商应提供车辆使用的密码模块或安全芯片的清单，存储在车内的型号和版本信息读取方式。在密码模块和安全芯片软硬件版本未发生变化的情况下，检验检测机构可在满足主管部门要求的基础上，认可具备资质的第三方检验检测机构出具的密码模块和安全芯片检测报告等证明材料。

2.2.4. 同一型式判定

条款 7.1 直接视同判定条件

7.1.1 直接视同判定基本要求

如符合下述规定，则视为同一型式：

a) 车辆密钥与证书安全机制相同；

注：车辆密钥与证书安全机制相同指车辆密钥安全保护机制、车端生成根密钥的生成主体和车辆信任机制相同，车辆密码应用场景减少导致的方案删减除外。

b) 车辆密码算法类型、算法参数、密钥长度和填充方案相同（车辆功能减少导致的减少除外），且工作模式相同或减少；

c) 密码模块和安全芯片的生产企业、型号和软件版本号相同，且使用场景相同（车辆功能减少导致的减少除外）；

d) 参与车端密钥生成或密码运算的随机数发生器类型、随机数生成机制相同，且使用场景相同（车辆功能减少导致的减少除外）；

e） 车辆 2 级及以上驾驶自动化系统对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；

f） 车辆基于人工智能模型实现车身控制的系统对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；

g） 车载软件升级系统对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；

h） 车辆与云平台直接通信的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；

i） 车辆 V2X 直连通信对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；

j） 车辆具备远程控制功能的系统对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；

k） 车辆其他外部无线通信对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；

l） 车辆数据安全涉及密码应用的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；

m） 与车辆直接连接并产生数据交互的云平台 IP 地址或域名相同或减少；

n） 车辆与云平台通信所使用的安全通信协议类型、协议版本、密码套件参数相同；

o） 车辆存储和使用证书的场景相同或减少。

7.1.2 直接视同判定补充要求

如条款7.1.1中e）～l）涉及的零部件仅发生不涉及密码的硬件型号或软件版本号变化时，车辆制造商应提供涵盖该零部件变化前后的所有密码应用场景的密码功能接口调用说明及对应的代码截图，检验检测机构确认本次变化不涉及密码后，可直接视同。

注：测试人员在现场查看代码截图并记录对应截图的哈希值视为车辆制造商提供了对应的代码截图。

说明：同一型式判定分为直接视同和测试验证后视同两类。直接视同主要适用于车辆密码应用基础条件、密码应用机制及各场景密码能力未发生实质变化的情形。密码应用方案相同是指密钥安全保护机制、车端生成根密钥的生成主体及车辆信任机制相同；根密钥是处于密钥结构中的顶层，用来生成派生密钥的密钥，不等同于车辆信任机制中的信任根。密码算法类型应具体到SM2等算法，并结合算法参数、密钥长度、填充方案及工作模式进行判定。7.1.1 a）条款中要求的车辆密钥与安全机制说明填报模板和填写样例见表1和表2，7.1.1 b）中的车辆功能减少的判定，企业和检验检测机构可参考表3进行判定。

表 1. 车辆密钥与证书安全机制说明模板

序号	密码应用场景	是否涉及	密钥安全保护机制	根密钥的生成主体	车辆信任机制
1	对称密码（含杂凑）	□是 □否	保护机制包含密钥存储载体、分层保护方式	根密钥的来源； 车端生成根密钥的生成主体的形式、名称、型号及软件版本号。	密钥生成主体包括但不限于：PKI 系统、密钥管理系统（KMS）、密码机、专用密钥生成设备等具备密钥生成能力的密码组件/系统/实体，由企业据实填报。
2	非对称密码	□是 □否	保护机制包含密钥存储载体、分层保护方式	根密钥的来源； 车端生成根密钥的生成主体的形式、名称、型号及软件版本号。	密钥生成主体包括但不限于：PKI 系统、密钥管理系统（KMS）、密码机、专用密钥生成设备等具备密钥生成能力的密码组件/系统/实体，由企业据实填报。
3	数字证书	□是 □否	保护机制包含密钥存储载体、分层保护方式	根密钥的来源； 车端生成根密钥的生成主体的形式、名称、型号及软件版本号。	说明数字证书信任体系相关信任机制，包含信任模型、信任锚（根证书主体）、证书信任链、证书策略、证书有效性及吊销校验方式、依赖方验证规则等内容，不限于上述示例。
示例 1：密钥安全保护机制：硬件机制/软件机制/一次性编程机制。若使用软件机制，还需提供密钥保护机制说明。 示例 2：根密钥的生成主体：根密钥的来源：车端/车外；车端生成根密钥的生成主体的形式：软件/硬件；名称：产品名称；型号：xxxxx；软件版本号：xxxxx。 示例 3：车辆信任机制：提供所有证书信任链和根证书颁发者主体名称。 注：车辆制造商可自行增补行数。					

表 2 车辆功能清单

序号	车辆功能				涉及的密码算法	是否使用密码模块/安全芯片	涉及的随机数发生器
	一级功能	企业备案	二级功能	企业备案			
1	是否有远程控制系统	□是 □否	安全启动	/	例： 算法 A：算法类型-算法参数-密钥长	例：密码模块 1：（生产企	例：随机数发生器 1：（类型：xxxx：随机数生

序号	车辆功能				涉及的密码算法	是否使用密码模块/安全芯片	涉及的随机数发生器
	一级功能	企业备案	二级功能	企业备案			
					度-填充方案-工作模式，之间用“-”分割。 如： 算法 A：AES-/-128-CBC-PKCS#7； 算法 B：AES-/-256-CBC-PKCS#7	业：xxxx；型号：xxxx；软件版本号：xxxx）	成机制：xxxx）
			是否支持导出密钥、私钥	□是 □否			
2	是否有基于人工智能模型实现车身控制的系统	□是 □否	安全启动	/			
			是否支持导出密钥、私钥	□是 □否			
3	是否有2级及以上驾驶自动化系统	□是 □否	安全启动	/			
4			是否支持导出密钥、私钥	□是 □否			
5	是否有车载软件升级系统	□是 □否	安全启动	/			
6			是否支持导出密钥、私钥	□是 □否			

序号	车辆功能				涉及的密码算法	是否使用密码模块/安全芯片	涉及的随机数发生器
	一级功能	企业备案	二级功能	企业备案			
7	是否具备软件升级功能	□是 □否	升级方式	□使用车载软件升级系统 □不使用车载软件升级系统且使用可信环境 □不使用车载软件升级系统且不使用可信环境			
8			是否支持导出密钥、私钥	□是 □否			
9			密钥、私钥的保护方式	□密码模块 □安全芯片 □密码技术 □一次性编程技术			
10	是否具备与云平台通信功能	□是 □否	平台及安全通信协议清单	例： 平台 1：OTA 平台，TLS1.2； 平台 2：TSP 平台，TLCP。			
11			是否支持导出密钥、私钥	□是 □否			
12			是否使用数字证书	□是 □否			
13	是否具备 V2X 通信功能	□是 □否	通信实体真实性、通信数据完整性	/			

序号	车辆功能				涉及的密码算法	是否使用密码模块/安全芯片	涉及的随机数发生器
	一级功能	企业备案	二级功能	企业备案			
14			是否使用硬件保护在车端存储的密钥	□是 □否			
15			是否支持导出密钥、私钥	□是 □否			
16			假名证书	/			
17	是否具备远程控制功能	□是 □否	远控指令真实性&完整性	/			
18			是否支持导出密钥、私钥	□是 □否			
19	是否具备外部无线通信功能	□WLAN通信	通信实体真实性、通信数据完整性	□一次性编程技术 □安全无线通信协议 □密码技术			
20			密钥、私钥的保护方式	□密码模块 □安全芯片 □密码技术 □一次性编程技术			
21			是否支持导出密钥、私钥	□是 □否			
22		□蓝牙通信	通信实体真实性、通信数据完整性	□安全无线通信协议 □密码技术			
23			密钥、私钥的保护方式	□密码模块 □安全芯片 □密码技术 □一次性编程技术			

序号	车辆功能				涉及的密码算法	是否使用密码模块/安全芯片	涉及的随机数发生器
	一级功能	企业备案	二级功能	企业备案			
24			是否支持导出密钥、私钥	□是 □否			
25		□低功耗蓝牙通信	通信实体真实性、通信数据完整性	□安全无线通信协议 □密码技术			
26			密钥、私钥的保护方式	□密码模块 □安全芯片 □密码技术 □一次性编程技术			
27			是否支持导出密钥、私钥	□是 □否			
28		□NFC通信	通信实体真实性、通信数据完整性	□安全无线通信协议 □密码技术			
29			密钥、私钥的保护方式	□密码模块 □安全芯片 □密码技术 □一次性编程技术			
30			是否支持导出密钥、私钥	□是 □否			
31		□射频（RF）通信	通信实体真实性、通信数据完整性	□安全无线通信协议 □密码技术			

序号	车辆功能				涉及的密码算法	是否使用密码模块/安全芯片	涉及的随机数发生器
	一级功能	企业备案	二级功能	企业备案			
32			密钥、私钥的保护方式	□密码模块 □安全芯片 □密码技术 □一次性编程技术			
33			是否支持导出密钥、私钥	□是 □否			
34		□其他_____	通信实体真实性、通信数据完整性	□安全无线通信协议 □密码技术			
35			密钥、私钥的保护方式	□密码模块 □安全芯片 □密码技术 □一次性编程技术			
36			是否支持导出密钥、私钥	□是 □否			
37	是否有第三方授权应用使用功能	□是 □否					
38	诊断通信		通信实体真实性	/			
39			是否支持导出密钥、私钥	□是 □否			
40			密钥、私钥的保护方式	□密码模块 □安全芯片 □密码技术 □一次性编程技术			

序号	车辆功能				涉及的密码算法	是否使用密码模块/安全芯片	涉及的随机数发生器
	一级功能	企业备案	二级功能	企业备案			
41	车内通信		通信实体真实性、通信数据完整性	/			
42			是否支持导出密钥、私钥	□是 □否			
43			是否在车端存储相关密钥	□是 □否			
44	是否在车端存储敏感个人信息	□是 □否	是否向外传输敏感个人信息	□是 □否			
45			是否向外传输敏感个人信息	□是 □否			
46			是否在车端存储相关密钥	□是 □否			
47			是否支持导出密钥、私钥	□是 □否			
48			是否使用数字证书技术	□是 □否			
49	是否在车端存储重要数据	□是 □否	是否向外传输重要数据	□是 □否			
50			是否向外传输重要数据	□是 □否			
51			是否在车端存储相关密钥	□是 □否			
52			是否支持导出密钥、私钥	□是 □否			

序号	车辆功能				涉及的密码算法	是否使用密码模块/安全芯片	涉及的随机数发生器
	一级功能	企业备案	二级功能	企业备案			
53			是否使用数字证书技术	□是 □否			
54	是否在车端存储车辆身份识别数据	□是 □否	是否使用密码技术保护车辆身份识别数据	□是 □否			
55			是否在车端存储相关密钥	□是 □否			
56			是否支持导出密钥、私钥	□是 □否			
57			是否使用数字证书技术	□是 □否			
58	是否在车端存储关键数据	□是 □否	是否使用密码技术保护关键数据	□是 □否			
59			是否在车端存储相关密钥	□是 □否			
60			是否支持导出密钥、私钥	□是 □否			
61			是否使用数字证书技术	□是 □否			
62	是否在车端存储安全日志	□是 □否	是否使用密码技术保护安全日志	□是 □否			
63			是否在车端存储相关密钥	□是 □否			
64			是否支持导出密钥、私钥	□是 □否			

序号	车辆功能				涉及的密码算法	是否使用密码模块/安全芯片	涉及的随机数发生器
	一级功能	企业备案	二级功能	企业备案			
65			是否使用数字证书技术	□是 □否			

条款 7.2 测试验证后视同判定条件

如车型发生涉及7.1的变更，在符合下述规定时，仅需对变更参数相关的技术要求进行补充测试后可获得扩展：

a） 车辆密钥与证书安全机制相同；

b） 车辆密码算法类型相同或减少。

说明：车型在扩展过程中可能发生生产企业、硬件型号、软件版本号等变化，此类变化可能涉及直接视同判定条件中的部分内容。但如车辆密码应用方案相同、车辆密码算法类型相同，未发生影响密码应用安全目标的实质性变化，则原测试结果仍具有一定覆盖基础，可仅针对变更参数相关的技术要求开展补充测试。

表 3 视同基础/扩展判定

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
a)车辆密钥与证书安全机制相同； 注：车辆密钥与证书安全机制相同指车辆密钥安全保护机制、车端生成根密钥的生成主体和车辆信任机制相同，车辆密码应用场景减少导致的方案删减除外。	密钥与证书安全机制	密钥与证书安全机制发生变化	不可视同	不进入补充测试流程，按新型式执行完整测试	无
b)车辆密码算法类型、算法参数、密钥长度和填充方案相同（车辆功能减少导致的减少除外），且工作模式相同或减少；	密码类型清单	算法类型增加	不可视同	不进入补充测试流程，按新型式执行完整测试	无
		因车辆功能减少导致算法类型减少	视同	无	无
	密码算法清单（包括算法类型、算法参数、密钥长度、填充方案、工作模式、	因车辆功能减少导致密码算法类型、算法参数、密钥长度、填充方案发生变化	视同	无	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
	车辆功能）	不因车辆功能减少导致的算法类型、算法参数、密钥长度、填充方案变化	补差测试	6.3.1	应在以下条款中选择涉及的测试项，开展补充测试：6.3.2、6.3.3、6.4.1、6.4.2、6.4.3、6.5.1、6.5.2、6.5.3、6.5.4、6.5.5、6.5.6、6.5.7、6.6.1、6.6.2、6.6.3、6.6.4、6.6.5
		工作模式（如 GCM、CBC、CTR、CCM 等）增加			
c）密码模块和安全芯片生产企业、型号和软件版本号相同，且使用场景相同（车辆功能减少导致的减少除外）	密码模块/安全芯片型号清单（包括密码模块/安全芯片生产企业、密码模块/安全芯片型号、软件版本号、密码模块/安全芯片使用场景）	车辆部署的密码模块或安全芯片的生产企业或型号或软件版本号发生变化	补差测试	6.3.1.4、6.3.2	应在以下条款中选择涉及的测试项，开展补充测试：6.3.3、6.4.1、6.4.2、6.4.3、6.5.1、6.5.2、6.5.3、6.5.4、6.5.5、6.5.6、6.5.7、6.6.1、6.6.2、6.6.3、6.6.4、6.6.5
		密码模块/安全芯片对应的使用场景变化			
		非车辆功能减少导致密码模块/安全芯片对应的使用场景减少			
		因车辆功能减少导致密码模块/安全芯片对应的使用场景减少	视同	无	无
d)参与车端密钥生成或密码运算的随机数发生器类型、随机数生成机制相同，且使用场景相同（车辆功能减少导致的减少除外）；	随机数发生器清单（包括随机数生成器类型、随机数生成机制、随机数发生器的使用场景）	随机数发生器类型发生变化	补差测试	6.3.1.4、6.3.3	应在以下条款中选择涉及的测试项，开展补充测试：6.3.2、6.5.1、6.5.2、6.5.3、6.5.4、6.5.6
		随机数生成机制发生变化			
		随机数发生器的使用场景增加			
		非车辆功能减少导致随机数发生器的使用场景减少			
		因车辆功能减少导致随机数发生器的使用场景减少	视同	无	无
e)车辆 2 级及以上驾驶自动化系统对应的零部件相同或减少，且生产	车辆 2 级及以上驾驶自动化系统对应的零部件	车辆 2 级及以上驾驶自动化系统对应的零部件增加或替换	补差测试	6.3.1、6.4.1、6.4.2、6.6.4	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；		车辆 2 级及以上驾驶自动化系统对应的零部件减少	视同	无	无
	车辆 2 级及以上驾驶自动化系统对应的零部件生产企业	车辆 2 级及以上驾驶自动化系统对应的零部件生产企业发生变化	补差测试	6.3.1、6.4.1、6.4.2、6.6.4	无
	车辆 2 级及以上驾驶自动化系统对应的零部件硬件型号	车辆 2 级及以上驾驶自动化系统对应的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车辆 2 级及以上驾驶自动化系统对应的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.4.1、6.4.2、6.6.4	无
	车辆 2 级及以上驾驶自动化系统对应的零部件软件版本号	车辆 2 级及以上驾驶自动化系统对应的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车辆 2 级及以上驾驶自动化系统对应的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.4.1、6.4.2、6.6.4	无
f)车辆基于人工智能模型实现车身控制的系统对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；	车辆基于人工智能模型实现车身控制的系统对应的零部件	车辆基于人工智能模型实现车身控制的系统对应的零部件增加或替换	补差测试	6.3.1、6.4.1、6.4.2、6.6.4	无
		车辆基于人工智能模型实现车身控制的系统对应的零部件减少	视同	无	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
	车辆基于人工智能模型实现车身控制的系统对应的零部件生产企业	车辆基于人工智能模型实现车身控制的系统对应的零部件生产企业发生变化	补差测试	6.3.1、6.4.1、6.4.2、6.6.4	无
	车辆基于人工智能模型实现车身控制的系统对应的零部件硬件型号	车辆基于人工智能模型实现车身控制的系统对应的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车辆基于人工智能模型实现车身控制的系统对应的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.4.1、6.4.2、6.6.4	无
	车辆基于人工智能模型实现车身控制的系统对应的零部件软件版本号	车辆基于人工智能模型实现车身控制的系统对应的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车辆基于人工智能模型实现车身控制的系统对应的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.4.1、6.4.2、6.6.4	无
g)车载软件升级系统对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的	车载软件升级系统对应的零部件	车载软件升级系统对应的零部件增加或替换	补差测试	6.3.1、6.3.2、6.4.2、6.4.3	无
		车载软件升级系统对应的零部件减少	视同	无	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
除外）；	车载软件升级系统对应的零部件生产企业	车载软件升级系统对应的零部件所在的控制器生产企业发生变化	补差测试	6.3.1、6.3.2、6.4.2、6.4.3	无
	车载软件升级系统对应的零部件硬件型号	车载软件升级系统对应的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车载软件升级系统对应的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.2、6.4.2、6.4.3	无
	车载软件升级系统对应的零部件软件版本号	车载软件升级系统对应的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车载软件升级系统对应的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.2、6.4.2、6.4.3	无
h)车辆与云平台直接通信的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；	车辆与云平台直接通信的零部件	车辆与云平台直接通信的零部件增加或替换	补差测试	6.3.1、6.3.2、6.3.3、6.5.1	无
		车辆与云平台直接通信的零部件减少	视同	无	无
	车辆与云平台直接通信的零部件生产企业	车辆与云平台直接通信的零部件生产企业发生变化	补差测试	6.3.1、6.3.2、6.3.3、6.5.1	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
	车辆与云平台直接通信的零部件硬件型号	车辆与云平台直接通信的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车辆与云平台直接通信的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.2、6.3.3、6.5.1	无
	车辆与云平台直接通信的零部件软件版本号	车辆与云平台直接通信的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车辆与云平台直接通信的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.2、6.3.3、6.5.1	无
i)车辆 V2X 直连通信对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；	车辆 V2X 直连通信对应的零部件	车辆 V2X 直连通信对应的零部件增加或替换	补差测试	6.3.1、6.3.3、6.5.2	无
		车辆 V2X 直连通信对应的零部件减少	视同	无	无
	车辆 V2X 直连通信对应的零部件生产企业	车辆 V2X 直连通信对应的零部件生产企业发生变化	补差测试	6.3.1、6.3.3、6.5.2	无
	车辆 V2X 直连通信对应的零部件硬件型号	车辆 V2X 直连通信对应的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
		车辆 V2X 直连通信对应的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.3、6.5.2	无
	车辆 V2X 直连通信对应的零部件软件版本号	车辆 V2X 直连通信对应的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车辆 V2X 直连通信对应的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.3、6.5.2	无
j)车辆具备远程控制功能的系统对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；	车辆具备远程控制功能的系统对应的零部件	车辆具备远程控制功能的系统对应的零部件增加或替换	补差测试	6.3.1、6.3.2、6.3.3、6.4.2、6.5.3	无
		车辆具备远程控制功能的系统对应的零部件减少	视同	无	无
	车辆具备远程控制功能的系统对应的零部件生产企业	车辆具备远程控制功能的系统对应的零部件生产企业发生变化	补差测试	6.3.1、6.3.2、6.3.3、6.4.2、6.5.3	无
	车辆具备远程控制功能的系统对应的零部件硬件型号	车辆具备远程控制功能的系统对应的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车辆具备远程控制功能的系统对应的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.2、6.3.3、6.4.2、6.5.3	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
	车辆具备远程控制功能的系统对应的零部件软件版本号	车辆具备远程控制功能的系统对应的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车辆具备远程控制功能的系统对应的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.2、6.3.3、6.4.2、6.5.3	无
k)车辆外部无线通信对应的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；	车辆外部无线通信对应的零部件	车辆外部无线通信对应的零部件增加或替换	补差测试	6.3.1、6.3.3、6.5.4	应在以下条款中选择涉及的测试项，开展补充测试：6.3.2
		车辆外部无线通信对应的零部件减少	视同	无	无
	车辆外部无线通信对应的零部件生产企业	车辆外部无线通信对应的零部件生产企业发生变化	补差测试	6.3.1、6.3.3、6.5.4	应在以下条款中选择涉及的测试项，开展补充测试：6.3.2
	车辆外部无线通信对应的零部件硬件型号	车辆外部无线通信对应的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车辆外部无线通信对应的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.3、6.5.4	应在以下条款中选择涉及的测试项，开展补充测试：6.3.2
	车辆外部无线通信对应的零部件软件版本号	车辆外部无线通信对应的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
		车辆外部无线通信对应的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.3.3、6.5.4	应在以下条款中选择涉及的测试项，开展补充测试：6.3.2
l)车辆数据安全涉及密码应用的零部件相同或减少，且生产企业、硬件型号和软件版本号相同（硬件型号和软件版本号变化不涉及密码的除外）；	车辆保护敏感个人信息涉及密码应用的零部件、生产企业、硬件型号和软件版本号	车辆保护敏感个人信息涉及密码应用的零部件增加或替换	补差测试	6.3.1、6.6.1	无
		车辆保护敏感个人信息涉及密码应用的零部件减少	视同	无	无
		车辆保护敏感个人信息涉及密码应用的零部件生产企业发生变化	补差测试	6.3.1、6.6.1	无
		车辆保护敏感个人信息涉及密码应用的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车辆保护敏感个人信息涉及密码应用的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.1	无
		车辆保护敏感个人信息涉及密码应用的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车辆保护敏感个人信息涉及密码应用的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.1	无
	车辆保护重要数据密码涉及密码应用的零部件、生	车辆保护重要数据密码涉及密码应用的零部件增加或替换	补差测试	6.3.1、6.6.2	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
	产企业、硬件型号和软件版本号	车辆保护重要数据密码涉及密码应用的零部件减少	视同	无	无
		车辆保护重要数据密码涉及密码应用的零部件生产企业发生变化	补差测试	6.3.1、6.6.2	无
		车辆保护重要数据密码涉及密码应用的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车辆保护重要数据密码涉及密码应用的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.2	无
		车辆保护重要数据密码涉及密码应用的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车辆保护重要数据密码涉及密码应用的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.2	无
	车辆保护车辆身份识别数据涉及密码应用的零部件、生产企业、硬件型号和软件版本号	车辆保护车辆身份识别数据涉及密码应用的零部件增加或替换	补差测试	6.3.1、6.6.3	无
		车辆保护车辆身份识别数据涉及密码应用的零部件增加或替换	视同	无	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
		车辆保护车辆身份识别数据涉及密码应用的零部件生产企业发生变化	补差测试	6.3.1、6.6.3	无
		车辆保护车辆身份识别数据涉及密码应用的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车辆保护车辆身份识别数据涉及密码应用的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.3	无
		车辆保护车辆身份识别数据涉及密码应用的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车辆保护车辆身份识别数据涉及密码应用的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.3	无
	车辆保护关键数据涉及密码应用的零部件、生产企业、硬件型号和软件版本号	车辆保护关键数据涉及密码应用的零部件增加或替换	补差测试	6.3.1、6.6.4	无
		车辆保护关键数据涉及密码应用的零部件减少	视同	无	无
		车辆保护关键数据涉及密码应用的零部件生产企业发生变化	补差测试	6.3.1、6.6.4	无
		车辆保护关键数据涉及密码应用的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
		车辆保护关键数据涉及密码应用的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.4	无
		车辆保护关键数据涉及密码应用的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无
		车辆保护关键数据涉及密码应用的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.4	无
	车辆保护安全日志涉及密码应用的零部件、生产企业、硬件型号和软件版本号	车辆保护安全日志涉及密码应用的零部件增加或替换	补差测试	6.3.1、6.6.5	无
		车辆保护安全日志涉及密码应用的零部件减少	视同	无	无
		车辆保护安全日志涉及密码应用的零部件生产企业发生变化	补差测试	6.3.1、6.6.5	无
		车辆保护安全日志涉及密码应用的零部件硬件型号发生变化（变化不涉及密码）	视同	无	无
		车辆保护安全日志涉及密码应用的零部件硬件型号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.5	无
		车辆保护安全日志涉及密码应用的零部件软件版本号发生变化（变化不涉及密码）	视同	无	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
		车辆保护安全日志涉及密码应用的零部件软件版本号发生变化（变化涉及密码）	补差测试	6.3.1、6.6.5	无
m)与车辆直接连接并产生数据交互的云平台 IP 地址或域名相同或减少；	与车辆直接连接并产生数据交互的云平台 IP 地址或域名	与车辆直接连接并产生数据交互云平台的 IP 地址或域名增加或替换	补差测试	6.3.1.4、6.5.1	应在以下条款中选择涉及的测试项，开展补充测试：6.3.1.1、6.3.1.2、6.3.1.3、6.5.3
		与车辆直接连接并产生数据交互云平台的 IP 地址或域名减少	视同	无	无
n)车辆与云平台通信所使用的安全通信协议类型、协议版本、密码套件参数相同；	车辆与云平台通信所使用的安全协议类型	安全协议（如 TLS1.2 及以上、TLCP 或其他安全协议）类型变化	补差测试	6.3.1.4、6.5.1	应在以下条款中选择涉及的测试项，开展补充测试：6.3.1.1、6.3.1.2、6.3.1.3、6.5.3
	车辆与云平台通信所使用的安全协议版本	协议版本变化			
	车辆与云平台通信所使用的安全协议密码套件	密码套件参数发生变化			
o)车辆存储和使用证书的场景相同或减少。	与云平台通信使用证书的场景	车辆存储和使用证书的场景增加	补差测试	6.5.1	应在以下条款中选择涉及的测试项，开展补充测试：6.5.3
		车辆存储和使用证书的场景减少	视同	无	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
	车辆 V2X 直连通信使用证书的场景	车辆存储和使用证书的场景增加	补差测试	6.5.2	无
		车辆存储和使用证书的场景减少	视同	无	无
	使用证书保护敏感个人信息的场景	车辆存储和使用证书的场景增加	补差测试	6.6.1	无
		车辆存储和使用证书的场景减少	视同	无	无
	使用证书保护重要数据的场景	车辆存储和使用证书的场景增加	补差测试	6.6.2	无
		车辆存储和使用证书的场景减少	视同	无	无
	使用证书保护车辆身份识别数据的场景	车辆存储和使用证书的场景增加	补差测试	6.6.3	无
		车辆存储和使用证书的场景减少	视同	无	无
	使用证书保护关键数据的场景	车辆存储和使用证书的场景增加	补差测试	6.6.4	无
		车辆存储和使用证书的场景减少	视同	无	无
	使用证书保护安全日志的场景	车辆存储和使用证书的场景增加	补差测试	6.6.5	无

标准要求	参数	判定方法	判定结果	测试内容	
				必测项	条件测试项
		车辆存储和使用证书的场景减少	视同	无	无
注：如某个零部件对应多个功能，应依次识别需要开展的补差测试项，并执行所有补差测试。					

2.3. 主要试验（或验证情况）分析

为支撑标准编制工作，2026 年 1 月—6 月，由国家商用密码产品检测认证中心和中国汽车技术研究中心有限公司两家牵头单位联合，在车载终端、密码模块、安全芯片上针对本文件核心技术条款开展试验验证。在前期验证基础上，汽标委于 2026 年 7 月 23 日启动更大范围的标准验证试验活动，进一步验证技术要求与试验方法的适用性和可操作性。

本次验证试验公开征集了 12 家整车及系统零部件企业参与，共计 13 个样车，由全国 6 家检测机构同步开展测试验证及能力比对。验证范围涵盖通用技术要求、系统安全密码应用要求、通信安全密码应用要求和数据安全密码应用要求四个部分，共 18 个测试场景，涉及密码算法、密码模块及安全芯片、随机数、安全启动、软件升级、云平台通信、远程控制、诊断接口、V2X 直连通信及数据安全等内容，因验证时间受限，且受车辆状态和功能配置等条件限制，未能在每款车型上单独完成全场景试验。参与主体广泛，验证范围覆盖标准主要技术内容。



图1. 验证试验环境

验证工作于 2026 年 7 月—8 月集中开展，其中，7 月 15 日—7 月 26 日征集参与单位，7 月 27 日—8 月 20 日组织企业与检测机构确认被测对象状态、对接试验计划并开展验证试验，8 月 21 日—8 月 28 日整理试验结果。各场景验证情况如下：

（1）密码算法。2 个样车开展验证。送检整车未开放算法调用接口，主要依托零部件样品完成算法正确性测试方法验证。

（2）密码模块和安全芯片。需进一步明确技术要求后开展一致性测试。

（3）随机数。部分无线通信场景可通过空口抓包获取随机数；其他涉及随机数的场景普遍无法提供相应数据包，取样条件成为主要实施难点。

（4）重要系统。7 个样车开展随机数以外条款的验证。

（5）安全启动。4 个样车开展验证，相关试验需在零部件上执行。

（6）软件升级。5 个样车开展密钥导出以外条款的验证。整车不支持相关密钥导出。

（7）与云平台通信。9 个样车开展证书以外条款的验证，整车大部分无证书无导入接口。

（8）远程控制。4 个样车开展密钥导出以外条款的验证，密钥导出相关测试受限。

（9）授权第三方应用。3 个样车开展 APP 相关验证。

（10）诊断接口。6 个样车开展密钥导出以外条款的验证；整车不支持密钥导出。

（11）V2X 直连通信。1 个样车开展验证，验证在 V2X 零部件层面完成。送检整车均未搭载 V2X 功能，未开展整车层面的该场景测试。

（12）外部无线通信。6 个样车开展密钥导出以外条款的验证。通过无线通信抓包可完成部分随机数测试，密钥导出测试仍受接口条件限制。

（13）车内通信。6 个样车开展密钥导出和随机数以外条款的验证。

（14）数据安全方面，本轮试验围绕敏感个人信息、重要数据、车辆身份识别数据、关键数据和安全日志五类场景，共对6个样件开展综合验证，覆盖标准规定的主要数据安全应用场景。除密钥导出、随机数及证书相关条款外，其余相关条款均已开展验证。

本轮验证试验反映出的共性问题主要集中在测试接口、数据获取及样件条件等方面。除部分外部无线通信场景可通过空口抓包获取数据外，针对随机数发生器的测试，难以调用底层接口，数据获取较为困难；量产整车普遍不具备证书在线申请、下载及导入等功能；由于车辆除正常业务，无额外导出车端密钥需求，送检整车均不具备密钥导出功能。上述情况表明，验证条件需进一步明确。

综合本轮验证情况，主要技术要求已具备相应的验证基础，部分试验方法的可操作性仍需完善。应明确整车、台架和零部件验证的适用条件，调整依赖导出实际业务密钥的技术要求或测试方法，细化随机数的适用范围和数据采集要求，完善证书测试的前置条件及判定依据，同时明确未配置相关功能时的适用性判定。

三、与有关法律、行政法规和其他标准的关系

本标准由以下部分组成：范围、规范性引用文件、术语和定义、缩略语、密码应用技术要求、试验方法、同一型式判定、标准的实施。适用于M类、N类车辆，不适用于基于已获得型式批准的二类底盘或整车改装的专用汽车。与我国现行的法律法规无冲突，与现行国家标准相互协调、相互补充。本标准与GB 44495—2024《汽车整车信息安全技术要求》为协同关系。GB 44495—2024从整车信息安全层面规定了信息安全管理体系要求以及外部连接安全、通信安全、软件升级安全、数据安全等方面的总体技术要求，属于整车信息安全的基础要求；本标准在GB 44495—2024所确立的整车信息安全基础上，聚焦车端密码应用，对车端实现密码功能所涉及的密码算法、密码模块和安全芯片提出的技术要求，两者相互衔接、互为补充。数据安全要求层面，本标准界定的敏感个人信息、重要数据范围与GB/T 44464保持一致。GB/T 44464的豁免规则，本标准同步对应适用，法律、行政法规、部门规章及强制性国家标准等另有规定的，从其规定。

本文件所述的密码算法应符合密码国家标准、行业标准或国际标准，并满足国家密码管理要求；密码模块和安全芯片应符合密码国家标准、行业标准或国际标准要求。

四、与国际标准化组织、其他国家或者地区有关法律法规和标准的比对分析

国际标准：ISO/SAE 21434《道路车辆 网络安全工程》针对道路车辆电子电气系统及其零部件和接口，规定了概念、开发、生产、运行、维护及报废等全生命周期的网络安全风险管理要求，强调通过风险分析确定安全目标并落实相应保护措施，未统一限定具体密码算法或技术实现方案。ISO/IEC 19790《信息安全、网络安全和隐私保护-密码模块的安全要求》规定了用于保护敏感信息的密码模块应满足的安全要求，针对不同的数据敏感程度和应用环境设置四个安全等级，为密码模块的安全设计和评价提供通用依据。本标准面向汽车密码应用场景，对车辆采用的密码算法、密码模块、安全芯片及随机数等提出具体要求，并明确系统安全、通信安全和数据安全等场景的密码保护要求，与上述国际标准在车辆密码应用等层面形成衔接。

欧盟：目前欧洲没有专门针对汽车领域的密码应用技术要求的法规。欧盟《网络韧性法案》（Cyber Resilience Act，CRA）已对具有数字元素的产品提出横向网络安全要求，强调

产品在设计、开发、上市和全生命周期维护过程中应具备安全默认配置、漏洞管理、安全更新、数据保护和持续防护能力。汽车领域密码技术要求还在制定中，CRA 法案的推出将会促进密码相关标准的出台。

日本：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。密码技术方面，2013 年 6 月发布的《日本的网络安全策略》提出发展密码应用技术，但没有提出具体的要求。

五、重大分歧意见的处理过程、处理意见及其依据

无。

六、对强制性国家标准自发布日期至实施日期之间的过渡期的建议及理由

由于该标准涉及密码模块合规改造、车辆密码应用架构调整、车辆密码功能开发、检测机构试验准备等问题，建议预留一段时间的过渡期，为各相关方预留充分准备时间。

本标准建议实施日期：2029-01-01

实施过渡期：

（1）对于新申请车辆型式批准的车型，自本文件实施之日起开始执行；

（2）对于已获得车辆型式批准的车型，自本文件实施之日起第 25 个月开始执行。

七、与实施强制性国家标准有关的政策措施

本标准的实施监督管理部门是中华人民共和国工业和信息化部、国家市场监督管理总局和国家密码管理局。对于违反强制性国家标准的行为，应按照下列法律、行政法规、部门规章相关规定进行处理：

（一）《中华人民共和国产品质量法（2018年修订）》

第十三条　可能危及人体健康和人身、财产安全的工业产品，必须符合保障人体健康和人身、财产安全的国家标准、行业标准；未制定国家标准、行业标准的，必须符合保障人体健康和人身、财产安全的要求。

禁止生产、销售不符合保障人体健康和人身、财产安全的标准和要求的工业产品。具体管理办法由国务院规定。

（二）《中华人民共和国密码法（2019年公布）》

第二十六条　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。商用密码产品检测认证适用《中华人民共和国网络安全法》的有关规定，避免重复检测认证。

商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。

（三）工业和信息化部《车辆生产企业及产品生产一致性监督管理办法》（工产业〔2010〕第109号）

第十条　对于不能保证产品生产一致性的车辆生产企业，工业和信息化部将视情节轻重，依法分别采取通报、限期整改、暂停或撤销“免予安全技术检验”备案、暂停或撤销其相关产品《公告》等措施。

八、是否需要对外通报的建议及理由

本标准为强制性国家标准，涉及进出口贸易，为促进国际贸易便利性，作为 WTO 成员国，有义务向 WTO 各成员通报即将实施的重要标准情况，因此，依据 WTO 有关规定，进行 WTO/TBT 通报。

九、废止现行有关标准的建议

无。

十、涉及专利的有关说明

本标准不涉及专利问题。

十一、强制性国家标准所涉及的产品、过程或者服务目录

本标准涉及产品包括 M 类和 N 类车辆，不包括基于已获得型式批准的二类底盘或整车改装的专用汽车。

十二、其他应当予以说明的事项

根据《国家标准化管理委员会关于国家标准起草中开展公平竞争审查的通知》，本标准已通过由全国汽车标准化技术委员会智能网联汽车分技术委员会联合标准起草单位开展的公平竞争审查，不对公平竞争造成影响。