强制性国家标准

《汽车密码应用技术要求》

（征求意见稿）

编制说明

2026年7月

目　　次

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）。

该标准归口部门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与产业变革深度演进，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。密码技术作为保障网络与信息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，正是贯彻落实《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，L2 级及以上辅助驾驶功能正加速普及，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。

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。矛盾如下：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、通用要求与安全要求，覆盖汽车整车及零部件产品的设计、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，分析了国内外车企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，通过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，组织主要汽车生产企业、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，标准工作组组织车企、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。

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研软件测评（天津）有限公司的专家分享了企业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。

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，了解了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

实现了安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。

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：本定义的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 车辆采用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。

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。应根据不同密码算法和业务场景，选择适当的参数和选项。

条款5.1.2 车辆采用的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。

注：为保护与云平台通信、远程控制等重要系统关键密钥的安全，一般可采用符合GB/T 37092-2018安全等级第二级（含）以上密码模块，GM/T 0008-2012安全等级第二级（含）以上的安全芯片，符合GB/T 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，不允许使用非标密码模块和安全芯片，针对自动驾驶系统、自动驾驶数据记录系统、汽车事件数据记录系统、基础多车道组合驾驶辅助系统、人工智能模型、车载事故紧急呼叫系统记录数据）、远程控车和车云通信（如TSP平台、OTA平台）场景所使用的密钥，推荐使用符合GB/T 37092安全等级第二级（含）以上的密码模块，符合GM/T 0008安全等级第二级（含）以上的安全芯片，符合GB/T XXXX《汽车芯片信息安全技术规范》安全等级第二级（含）以上的安全芯片中的一种。

条款5.1.3 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。

说明：车辆开展密钥生成、消息签名密钥协商等安全操作时，均依赖高质量随机数作为基础输入；若随机数随机性不足、可预测，会直接导致密钥泄露、签名伪造、身份仿冒等高危攻击。车辆随机数质量需通过GB/T 32915-2026的要求，具体要求可参考本标准试验方法章节6.3.3。

条款5.2.2 涉及远程控制、软件升级、自动驾驶数据记录以及经风险评估识别确需安全启动的应用场景的系统，应具备安全启动机制。安全启动过程中，应对固件、引导程序、操作系统、关键应用软件等启动阶段组件进行逐级安全校验，应采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软件组件真实、完整、可信，防止固件、引导程序、操作系统或关键应用软件被非法篡改、替换或伪造后运行。车辆制造商围绕关键系统建立从底层固件到上层应用的逐级可信启动链，对启动阶段的关键组件进行逐层安全校验，并结合可信根、密钥或证书管理、签名验证、完整性校验等机制保证校验依据本身可信。同时，安全启动机制还应与远程控制、OTA升级、自动驾驶数据记录以及经风险评估识别后确需安全启动保护的关键系统等业务场景相衔接，在校验失败时能够采取阻止加载、进入安全状态、告警、恢复或回退至可信版本等处置措施，避免车辆在不可信软件环境下继续运行。

条款 5.2.3 软件升级密码应用要求如下：

a） 使用车载软件升级系统时，应采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，保障升级包的真实性和完整性；

b） 不使用车载软件升级系统时，各被升级的控制器应在加载升级包前采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与完整性，保护其未被篡改或伪造，在可信环境下执行软件升级的除外；

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等方式。

c） 应采用密码技术保护车辆信任的密钥完整性；

d） 不应以明文方式导出对称密钥、私钥。

说明：在线接收的升级包、依赖车载软件升级系统执行的离线升级包，以及在公开终端下载、无安全通道拷贝等非可信环境下获取的离线升级包均应在执行或加载前采用数字签名、消息鉴别码等密码技术进行真实性和完整性验证，同时通过禁止明文导出等措施防止密钥泄露。

条款 5.3.1 车辆与 TSP 平台、OTA 平台等云平台通信安全时，应满足如下要求：

a） 应采用 TLS1.2 及以上版本或 TLCP 等安全通信协议建立安全通道；

b） 应采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；

c） 应采用基于对称密码算法等密码技术保障重要数据的机密性；

d） 应采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障通信数据的完整性；

e） 在车端产生的密钥应符合 5.1.3 的要求；

f） 不应以明文方式导出对称密钥、私钥；

g） 使用数字证书时，应满足如下要求：

1）应采用密码技术保护存储在车端的根证书的完整性；

2）证书申请语法应符合国家标准、行业标准或国际标准；

3）应采用密码技术保障证书申请数据在传输过程中的完整性；

4）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禁止导入；

5）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；

6）证书应仅用于证书中指定的功能和用途，应在证书有效期到期前完成证书更新；

7）支持对证书进行撤销申请，撤销后的证书不得继续用于任何业务系统或安全通信，并记录撤销操作日志。

说明：车辆需通过安全通信协议、身份鉴别、数据加密、完整性保护、随机数、密钥管理和证书管理等措施，建立车云之间可信、安全、可持续运行的通信保护机制。车辆制造商需采用1.2及以上版本的TLS或符合GB/T 38636—2020《信息安全技术 传输层密码协议（TLCP）》要求的TLCP安全通信协议建立安全通道，同时通过数字签名、消息鉴别码、对称加密等密码技术保障通信实体真实性、重要数据机密性和通信数据完整性，同时通过使用符合国家标准的随机数、禁止明文导出等措施保护密钥。

条款 5.3.2 远程控制密码应用要求如下：

a） 应采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；

b） 应采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；

c） 在车端产生的密钥应符合 5.1.3 的要求；

d） 不应以明文方式导出对称密钥、私钥。

说明：远程控制涉及车门解锁、空调控制、车辆启动、寻车、充电控制等与车辆状态和用户安全密切相关的功能，在远程控制业务本身需建立可信指令校验机制，确保指令生成、传输、接收、验证和执行全过程可控可信，同时通过禁止明文导出等措施防止密钥泄露。

条款 5.3.3 授权的第三方应用密码应用要求如下：

a） 应采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第三方应用的真实性；

b） 应采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第三方应用的完整性。

说明：车辆制造商在第三方应用授权、接入、调用和数据交互过程中，采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机制，对第三方应用的真实身份及交互数据的完整性进行验证，应覆盖应用接口调用请求、关键业务指令、数据传输内容等关键环节，并与密钥管理、权限控制、访问控制和异常处置等结合，确保只有经过授权且未被篡改的第三方应用才能访问相应车辆资源。

条款 5.3.4 诊断接口密码应用要求如下：

a） 应采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通信实体的真实性；

b） 应采用密码技术保护诊断信任的密钥完整性；

c） 不应以明文方式导出对称密钥、私钥。

说明：保护诊断接口时，应防止未经授权的诊断设备或操作主体通过诊断接口向车辆下发关键配置、标定参数等写操作指令，避免车辆参数被非法修改、功能状态被异常改变或安全边界被绕过。在诊断设备、车辆控制器和关键参数写入流程之间建立可信校验机制，确保写操作指令来源可信、内容未被篡改、密钥未被破坏或泄露，从而保障车辆诊断维护过程的安全性和可控性，同时通过禁止明文导出等措施防止密钥泄露。

条款 5.3.5 使用密码技术保护车辆与车辆、路侧单元、移动终端等进行 V2X 直连通信时，应满足如下要求：

a） 应采用基于公钥密码算法的数字签名等密码技术保障通信实体的真实性、消息发送行为的不可否认性；

b） 应采用基于公钥密码算法的数字签名密码技术保护通信数据的完整性；

c） 在车端产生的密钥应符合 5.1.3 的要求；

d） 如在车端存储密钥，应保障密钥存储的安全性；

e） 不应以明文方式导出对称密钥、私钥；

f） 使用的数字证书应满足 5.3.1 g)的要求。

说明：保护V2X直连通信安全，采用数字签名等密码技术验证通信实体真实性、保护通信数据完整性，并通过证书机制建立车辆与外部通信对象之间的可信关系。安全要求包括：随机数质量、密钥安全存储、禁止对称密钥和私钥明文导出、车辆信任根证书完整性保护、证书申请数据完整性保护、证书导入校验、公私钥匹配校验、证书更新、证书用途和有效性验证、证书撤销及日志记录等全生命周期管理要求。

条款5.4.1 敏感个人信息密码应用要求如下：

a） 使用密码技术保护存储的敏感个人信息时，应保护访问和获取的操作实体身份真实性；

b） 使用密码技术保护存储的敏感个人信息时，应采用对称密码算法或公钥密码算法等密码技术保护其机密性；

c） 向车外传输敏感个人信息时，应采用对称密码算法或公钥密码算法等密码技术保护其机密性；

d） 在车端产生的密钥应符合 5.1.3 的要求；

e） 如在车端存储密钥，应保障密钥存储的安全性；

f） 不应以明文方式导出对称密钥、私钥；

g） 使用数字证书保护敏感个人信息安全时，数字证书应满足 5.3.1 g)的要求。

说明：保护敏感个人信息时，应采用对称密码算法或公钥密码算法等密码技术保护敏感个人信息的机密性，防止存储数据被非法读取。向车外传输的敏感个人信息，还应在传输过程中采取加密保护措施，避免数据在车云通信、第三方服务调用、外部平台交互等过程中被窃听和泄露。密钥应符合随机性要求，并具备密钥存储保护机制。保护证书安全时，应进行车辆信任根证书完整性保护、证书申请数据完整性保护、证书导入校验、公私钥匹配校验、证书更新、证书用途和有效性验证、证书撤销等全生命周期保护。

条款5.4.2 重要数据密码应用要求如下：

a） 使用密码技术保护存储在车内重要数据时，应验证访问和获取的操作实体身份真实性；

b） 使用密码技术保护存储在车内的重要数据时，应采用对称密码算法或公钥密码算法等密码技术保护其机密性；

c） 向车外传输重要数据时，应采用对称密码算法或公钥密码算法等密码技术保护机密性；

d） 在车端产生的密钥应符合 5.1.3 的要求；

e） 如在车端存储密钥，应保障密钥存储的安全性；

f） 不应以明文方式导出对称密钥、私钥；

g） 使用数字证书保护重要数据安全时，数字证书应满足 5.3.1 g)的要求。

说明：保护重要数据时，应验证访问和获取操作实体的身份真实性，确保只有授权主体能够接触相关数据；同时，应采用对称密码算法或公钥密码算法等密码技术保护重要数据的机密性，防止数据在本地存储环节被非法读取。对于向车外传输的重要数据，也应采取相应加密保护措施，避免数据在车云通信、平台交互或外部传输过程中被窃听和泄露。密钥应符合随机性要求，并具备密钥存储保护机制。保护证书安全时，应进行车辆信任根证书完整性保护、证书申请数据完整性保护、证书导入校验、公私钥匹配校验、证书更新、证书用途和有效性验证、证书撤销等全生命周期保护。

2.2.3. 试验方法

条款 6.3.2 测试人员应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 的要求：

a) 测试人员检测车辆使用的密码模块的型号、软硬件版本，并与车辆实际使用的密码模块进行一致性比对；

b) 测试人员检测密码模块所适用的规格、接口、角色/服务和鉴别机制、软件/固件安全保护机制、运行环境保护机制、物理安全保护机制、非侵入式安全保护机制、敏感安全参数管理机制、自测试机制、生命周期保障机制、对其他攻击的缓解机制，判断是否满足 5.1.2 的相关要求；

c) 测试人员检测车辆所使用的安全芯片的型号、软硬件版本，并与车辆实际使用的安全芯片进行一致性比对；

d) 测试人员检测安全芯片所适用的密码算法、安全芯片接口、密钥管理机制、敏感信息保护机制、固件安全保护机制、自检机制、审计机制、攻击的削弱与防护机制、生命周期保证机制，判断是否满足 5.1.2 的相关要求。

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检测记录、检测报告、认证证书等证明文件。若检测对象为密码模块，测试人员应按照密码模块规格、接口、角色/服务和鉴别、软件/固件安全、运行环境、物理安全、非侵入式安全、敏感安全参数管理、自测试、生命周期保障、对其他攻击的缓解等十一个安全域逐项进行独立评级，整体安全等级取各域最低等级，确认密码模块在所有域中均达到声称的安全等级；若检测对象为安全芯片，测试人员应按照密码算法、安全芯片接口、密钥管理、敏感信息保护、固件安全、自检、审计、攻击的削弱与防护、生命周期保证逐项进行独立评级，整体安全等级取各域最低等级，确认安全芯片在所有域中均达到声称的安全等级。

2.2.4. 同一型式判定

条款 7.1 直接视同判定条件

如符合下述规定，则视为同一型式：

——车辆整车电子电气架构相同且密码安全功能实现方式相同；

——车辆密钥安全保护机制相同；

注：保护机制包括密钥来源途径、使用方式和存储介质。

——车辆根密钥生成主体、车端可信根载体和类型相同；

——车辆信任链层级、信任机制相同；

——车辆存储、使用证书的安全性保护机制相同；

——保护与云平台通信、远程控制等重要系统关键密钥的密码模块和安全芯片生产企业和型号相同，且使用场景相同或减少；

——车辆密码算法类型、算法参数、密钥长度和填充方案相同，且工作模式相同或减少；

——车辆用于密码安全的随机数发生器类型、随机数生成机制相同；

——车辆重要系统对应的零部件相同或减少，且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应用的除外）；

——车辆涉及安全启动的零部件相同或减少，且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应用的除外）；

——车辆软件升级系统对应的零部件相同或减少，且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应用的除外）；

——车辆与云平台通信的零部件相同或减少，且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应用的除外）；

——车辆远程控制系统对应的零部件相同或减少，且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应用的除外）；

——车辆V2X直连通信对应的零部件相同或减少，且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应用的除外）；

——车辆外部无线通信对应的零部件相同或减少，且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应用的除外）；

——车辆数据安全涉及密码应用的零部件相同或减少，且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应用的除外）；

——车辆通信所使用的安全协议类型、协议版本、密码套件参数相同；

——与车辆直接连接并产生数据交互的车辆生产企业云平台IP地址或域名相同或减少。

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、关键密码应用机制及相关密码能力未发生实质变化的情形。车辆密码应用涉及系统安全、通信安全和数据安全等多个应用场景，其安全能力通常由整车电子电气架构、密码安全功能实现方式、密码保护机制、可信根及信任关系、密码模块和安全芯片、密码算法、随机数生成机制、密码应用相关零部件以及通信安全配置等共同支撑。当上述内容未发生影响密码应用安全目标的变化时，原车型测试结果能够覆盖扩展车型，因此可直接视同。

其中，整车电子电气架构指车辆电子控制单元、传感器、执行器、通信网络、安全域及其连接关系；密码保护机制包括密钥来源、使用方式和存储介质等；可信根及信任关系包括根密钥生成主体、车端可信根载体、信任链层级、信任建立机制以及证书安全保护机制；密码模块和安全芯片主要用于保护重要系统、与云平台通信、远程控制等场景的关键密钥；密码应用相关零部件包括涉及密码运算、密钥存储、随机数生成、可信根建立、证书存储与使用等功能的零部件；通信安全配置包括通信协议类型、协议版本、密码套件参数以及云平台通信配置等。

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，经审批许可后获得扩展：

——车辆整车电子电气架构相同且密码安全功能实现方式相同；

——车辆根密钥生成主体、车端可信根载体和类型相同；

——车辆信任链层级、信任机制相同；

——车辆密码算法类型、算法参数、密钥长度、填充方案、工作模式相同或减少。

说明：车型在扩展过程中可能发生局部配置、软件版本、接口配置等变化，此类变化可能涉及直接视同判定条件中的部分内容。但如车辆整车电子电气架构、密码安全功能实现方式、根密钥生成主体、车端可信根载体、信任链层级、信任机制等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。

其中，要求整车电子电气架构和密码安全功能实现方式保持一致，是为了确保车辆密码功能部署位置、保护对象、保护路径及安全边界未发生实质变化；要求根密钥生成主体、车端可信根载体、信任链层级和信任机制保持一致，是为了确保车辆身份真实性验证、安全启动、软件升级、安全通信等密码应用所依赖的信任基础未发生变化；要求密码算法及随机数生成机制等保持一致，是为了确保车辆密码运算能力、密钥保护能力和密码应用能力未发生降低。因此，对于满足上述条件的车型，可通过补充测试验证变更部分是否仍符合相关密码应用技术要求，无需重新开展全部测试。

2.3. 主要试验（或验证情况）分析

为支撑标准验证工作，2026年1月—6月间，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了试验验证。小规模验证结束后，于2026年7月，向工作组开展了更大范围的标准验证征集活动。

后续验证工作按三阶段推进，期间每周三召开线上周会同步试验进展：第一阶段为2026年7月15日—2026年7月31日，主要完成试验验证活动参与单位最终确认及验证方案编制；第二阶段为2026年8月1日—8月20日，全面开展整车级的标准验证活动；第三阶段为2026年8月21日—8月28日，开展试验总结工作，并计划于8月28日召开总结会，针对验证试验情况进行说明并针对标准内容提出修改意见并纳入标准处理流程。

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，车端实现密码功能的相关零部件可参照实施。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

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。

美国：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；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，对以 CPU 为主的车载密码模块包括 CGW、TBOX、IVI 等网络关键设备提出了安全要求。2017 年 9 月美国交通部发布的《自动驾驶法案》规定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。

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工业和信息化部、国家市场监督管理总局、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

本标准主要涉及汽车密码应用的相关产品，包括但不限于密码算法、密码模块、安全芯片及相关车载零部件等。

十二、公平竞争审查情况及结论说明

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》，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，对本标准正在开展公平竞争审查工作。

十三、其他应当予以说明的事项

无。