ICS 43.020
CCS T 40

中华人民共和国国家标准

GB XXXXX—XXXX

汽车密码应用技术要求

Technical requirements for cryptographic application for vehicle

（报批稿）

（本草案完成时间：2026.10.27）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 2
5 密码应用技术要求 2
6 试验方法 7
7 同一型式判定 14
8 标准的实施 15
附录 A（规范性）　确定测试对象的方法 16

前　言

本文件按照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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部、国家密码管理局提出并归口。

汽车密码应用技术要求

1 范围

本文件规定了汽车密码应用技术要求及同一型式判定，描述了相应的试验方法。

本文件适用于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。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 32915—2026 网络安全技术 二元序列随机性检测方法

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB 44495—2024 汽车整车信息安全技术要求

GB 44721—2026 智能网联汽车 自动驾驶系统安全要求

GB 47955—2026 智能网联汽车 组合驾驶辅助系统安全要求

GB/T XXXX—XXXX 汽车芯片信息安全技术规范

GM/T 0008—2012 安全芯片密码检测准则

GM/Z 4001—2013 密码术语

3 术语和定义

GB/T 25069—2022、GB 44495—2024、GB 44721—2026、GB 47955—2026、GM/Z 4001—2013界定的以及下列术语和定义适用于本文件。

3.1

密码 cipher

采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

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，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。

[来源：GB/T 25069—2022，3.379，有修改]

3.3

密钥 key

控制密码变换操作的符号序列。

[来源：GB/T 25069—2022，3.389，有修改]

3.4

安全芯片 security chip

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。

[来源：GM/T 0008—2012，3.1.3]

3.5

一次性编程 one time programming

只能由用户进行一次编程的特性。

[来源：GB/T 22033—2017，2.066]

3.6

根密钥 root key

处于密钥结构中的顶层，用来生成派生密钥的密钥。

[来源：GB/T 25069—2022，3.204，有修改]

4 缩略语

下列缩略语适用于本文件。

OTA：远程在线升级（Over The Air）

TLCP：传输层密码协议（Transport Layer Cryptography Protocol）

TLS：传输层安全协议（Transport Layer Security）

TSP：远程服务提供商（Telematics Service Provider）

VIN：车辆识别代号（Vehicle Identification Number）

V2X：车辆与车外其他设备之间的无线通信（Vehicle to Everything）

5 密码应用技术要求

5.1 密码应用通用技术要求

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。

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。

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。

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。

5.2 系统安全密码应用技术要求

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。

5.2.2 安全启动密码应用要求

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。

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。

5.3 通信安全密码应用技术要求

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，需满足以下要求：

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。

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，需满足以下要求：

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 假名证书需满足以下要求：

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。

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。

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。

5.3.5 授权的第三方应用密码应用要求

5.3.5.1 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，验证授权的第三方应用的真实性。

5.3.5.2 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授权的第三方应用的完整性。

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。

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。

5.4　数据安全密码应用技术要求

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。

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；

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。

5.4.2.2　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。

5.4.3　保护车辆身份识别数据密码应用要求

5.4.3.1　车辆使用密码技术保护存储在车端的VIN等用于车辆身份识别的数据时，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，验证删除和修改存储在车端的VIN等用于车辆身份识别的数据的外部操作实体的真实性。

5.4.3.2　车辆应保护存储在车端的与保护VIN等用于车辆身份识别的数据相关的密钥的安全性。

5.4.3.3　车辆应不支持以明文方式导出存储在车端的与保护VIN等用于车辆身份识别的数据相关的对称密钥、私钥。

5.4.3.4　车辆使用数字证书保护存储在车端的VIN等用于车辆身份识别的数据时，使用的数字证书应满足5.3.1.3的要求。

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。

5.4.5 保护安全日志密码应用要求

5.4.5.1 车辆使用密码技术保护存储在车端的安全日志时，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，验证删除安全日志的外部操作实体的真实性；

b) 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安全日志的完整性。

5.4.5.2 车辆应保护存储在车端的与保护安全日志相关的密钥的安全性。

5.4.5.3 车辆应不支持以明文方式导出存储在车端的与保护安全日志相关的对称密钥、私钥。

5.4.5.4 车辆使用数字证书保护存储在车端的安全日志时，使用的数字证书应满足5.3.1.3的要求。

6 试验方法

6.1 总则

检测人员应依据待测车辆密码应用方案，按照附录A确定测试对象，并从6.3～6.6中选择适用的测试方法开展测试，确认车辆满足第5章技术要求。车辆密码应用方案包括但不限于待测车辆的密码功能及调用接口、选用的密码算法、使用的密钥种类和用途、密钥全生命周期技术设计方案、支持密钥导出的功能、一次性编程技术保护方案、根证书保护机制、选用的密码模块或安全芯片的安全机制说明等。

6.2 测试条件

测试样件包括整车及涉及的零部件，应具备以下开展测试的基本条件：

a) 测试样件可正常运行；

b) 车辆密码应用相关功能处于开启状态；

c) 按照6.1确定的测试对象的密码功能接口可正常调用，且已开放相应调用权限；

d) 按照6.1确定的测试对象的密钥和证书管理接口可正常调用，且已开放相应调用权限；

e) 提供车端密码模块和安全芯片型号及版本信息读取方式。

6.3 通用技术要求测试

6.3.1 密码算法测试

6.3.1.1 对称密码算法测试

测试人员应依据车辆制造商提供的密码算法清单，从中选取3种类型的对称密码算法，并按照以下测试方法开展测试（如密码算法类型不足3种则进行全量测试）：

a) 车辆使用测试用的密钥和给定明文经对称算法加密，测试人员比对结果和给定密文是否完全相同；

b) 车辆使用测试用的密钥和给定密文经对称算法解密，测试人员比对结果和给定明文是否完全相同。

注：若车辆制造商使用密码模块或安全芯片运行被选取的算法，无需重复执行测试。

6.3.1.2 非对称密码算法测试

测试人员应依据车辆制造商提供的密码算法清单，从中选取3种类型的非对称密码算法，并按照以下测试方法开展测试（如密码算法类型不足3种则进行全量测试）：

a) 车辆使用测试用的密钥和公钥密码算法对给定明文加密，测试人员使用对应算法及密钥解密，比对解密结果与给定明文是否完全相同；
b) 车辆使用测试用的密钥和公钥密码算法对给定明文完成“先加密-再解密”全流程操作，测试人员比对解密结果与给定明文是否完全相同；
c) 车辆使用测试用的密钥和公钥密码算法对目标消息签名，测试人员使用对应算法及公钥验签，验签结果是否通过；
d) 车辆使用测试用的密钥和公钥密码算法完成“先签名-后验签”全流程操作，验签结果是否通过。

注：若车辆制造商使用密码模块或安全芯片运行被选取的算法，无需重复执行测试。

6.3.1.3 杂凑密码算法测试

测试人员应依据车辆制造商提供的密码算法清单，从中选取3种类型的杂凑密码算法，并按照以下测试方法开展测试（如密码算法类型不足3种则进行全量测试）：

a) 车辆使用给定消息调用杂凑密码算法计算杂凑值，测试人员比对结果和给定杂凑值是否完全相同；
b) 车辆使用给定消息和参数调用杂凑密码算法计算杂凑值，测试人员比对结果和给定杂凑值是否完全相同。

注：若车辆制造商使用密码模块或安全芯片运行被选取的算法，无需重复执行测试。

6.3.1.4 密码算法脆弱性测试

测试人员应在设定的计算资源条件下，依据车辆制造商提供的密码算法清单，从中选取3种算法，并按照以下测试方法开展测试（如车辆使用的密码算法数量不足3种则进行全量测试）：

a) 测试人员抓取车辆通信报文，提取报文中的密码算法、密码套件、算法参数及工作模式信息，与已知弱密码算法、不安全算法参数及不安全工作模式进行比对，测试是否使用存在安全风险的密码算法或配置；
b) 测试人员触发通信、认证或密钥协商过程 4096 次，采集通信链路中的密钥参数，对采集的数据进行随机性分析，测试密钥相关参数是否存在随机性不足的问题；
c) 测试人员采集车辆通信场景中不少于 1 000 000 比特的密文数据，测试不同通信过程中是否存在密文异常重复，密码算法、密钥、初始化参数或加密实现是否存在异常；
d) 测试人员使用符合要求的随机源生成不少于 10^{15} 比特的测试密钥，尝试对采集的对称密码算法密文解密和密钥碰撞分析，测试是否存在密钥碰撞、密钥分布异常集中等情况，测试实际使用密钥的密钥空间是否存在安全风险。

注：测试人员选取测试算法时无需考虑覆盖所有的算法类型。

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。

6.3.3 随机数测试

测试人员从车辆与云平台通信、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的五类场景中，每类场景各选取一个随机数发生器，采集各随机数发生器产生的20 000比特的随机数，测试是否符合GB/T 32915—2026中附录A.1的随机性测试要求。

6.4 系统安全密码应用要求测试

6.4.1 重要系统密码应用要求测试

测试人员应按照以下测试方法开展测试，判定车辆是否满足5.2.1的要求：
a) 测试人员尝试以伪造的身份删除车端数据记录系统中记录数据，测试系统是否使用密码技术校验外部操作实体的真实性；
b) 如支持密钥导出功能，测试人员使用车辆制造商提供的方式，尝试导出 2 级及以上驾驶自动化系统的对称密钥、私钥，测试导出的密钥是否为明文；
c) 如支持密钥导出功能，测试人员使用车辆制造商提供的方式，基于人工智能模型实现车身控制的系统的对称密钥、私钥，测试导出的密钥是否为明文。

6.4.2 安全启动密码应用要求测试

测试人员依次尝试替换引导程序、系统固件等启动组件镜像后上电启动，测试系统是否具备安全启动校验流程，能否使用密码技术识别并拦截不真实、被篡改的启动组件，判定是否满足5.2.2的要求。如无法完成替换刷写，检验车辆制造商提供的安全启动机制证明材料。

6.4.3 软件升级密码应用要求测试

6.4.3.1 使用车载软件升级系统密码应用要求测试

测试人员应按照以下测试方法开展测试，判定车辆是否满足5.2.3.1的要求：
a) 测试人员尝试验签、篡改、伪造接收到的升级包，测试车载软件升级系统是否校验升级包的真实性和完整性；
b) 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文；
c) 测试人员按照 6.3.2 的测试方法，测试车辆是否使用密码模块或安全芯片保护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；
d) 如使用密码技术保护车端存储密钥的完整性，测试人员尝试篡改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，尝试调用该密钥，测试车辆是否校验密钥的完整性。

6.4.3.2 不使用车载软件升级系统密码应用要求测试

如未在可信环境下执行软件升级，测试人员应按照以下测试方法开展测试，判定车辆是否满足5.2.3.2的要求：
a) 测试人员尝试验签、篡改、伪造接收到的升级包，测试被升级的控制器是否校验真实性和完整性；
b) 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文；

c） 测试人员按照 6.3.2 的测试方法，测试车辆是否使用密码模块或安全芯片保护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；
d） 如使用密码技术保护车端存储密钥的完整性，测试人员尝试篡改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，尝试调用该密钥，测试车辆是否校验密钥的完整性。

6.5 通信安全密码应用要求测试

6.5.1 与云平台通信密码应用要求测试

6.5.1.1 通信协议密码应用要求测试

测试人员应依据车辆制造商提供的云平台清单，从中选取3个云平台，并按照以下测试方法开展测试（如平台数量不足3个时则进行全量测试），判定车辆是否满足5.3.1.1的要求：

a） 测试人员使用报文捕捉分析工具采集协议交互数据并分析报文格式，测试协议是否实现正确；
b） 测试人员尝试伪造云平台与车辆进行通信，测试车辆是否校验通信实体的真实性；
c） 测试人员应依据车辆制造商提供的车辆通过车云通信向外传输的敏感个人信息和重要数据的功能清单，触发车辆向外传输敏感个人信息和重要数据的功能，获取车辆存储和向外传输的敏感个人信息和重要数据，测试车辆是否对敏感个人信息和重要数据进行机密性保护；
d） 测试人员尝试篡改通信数据，测试车辆是否保护通信数据的完整性。

6.5.1.2 密钥导出测试

如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文。

6.5.1.3 数字证书应用测试

测试人员应依据车辆制造商提供的数字证书场景清单，从中选取3个数字证书使用场景，并按照以下测试方法开展测试（如数字证书使用场景数量不足3个时则进行全量测试），判定车辆使用的数字证书是否满足5.3.1.3的要求：

a） 如未使用硬件保护存储在车端的证书，测试人员尝试修改根证书，判定车辆是否满足 5.3.1.3 a）的要求；如使用硬件保护存储在车端的证书，车辆制造商应声明保护存储在车端的证书所使用的硬件保护机制；
b） 测试人员使用证书分析工具验证车辆生成的证书申请数据，判定车辆使用的数字证书是否满足 5.3.1.3 b）的要求；
c） 测试人员使用工具抓取证书申请数据，判定车辆使用的数字证书是否满足 5.3.1.3 c）的要求；
d） 测试人员尝试下载非车端可信证书信任链签发的数字证书，判定车辆使用的数字证书是否满足 5.3.1.3 d）的要求；
e） 测试人员尝试导入证书中的公钥与车端存储的私钥不匹配的数字证书，判定车辆使用的数字证书是否满足 5.3.1.3 e）的要求；
f） 测试人员使用工具抓取通信过程中的车辆数字证书，并与车辆制造商提供的云平台通信功能对应的车辆证书进行比对，判定车辆使用的数字证书是否满足 5.3.1.3 f）的要求；
g） 测试人员尝试导入数字证书，测试车辆在证书失效后是否继续使用该证书，判定车辆使用的数字证书是否满足 5.3.1.3 g）的要求；
h） 测试人员尝试使用已撤销的数字证书执行业务操作，判定车辆使用的数字证书是否满足 5.3.1.3 h）的要求。

6.5.2 V2X 直连通信密码应用要求测试

6.5.2.1 通信过程密码应用要求测试

测试人员应按照以下测试方法开展测试，判定车辆是否满足5.3.2.1的要求：

a) 测试人员尝试以伪造的身份发送 V2X 直连通信消息，测试车辆是否校验 V2X 直连通信实体的真实性及发送行为的不可否认性；
b) 测试人员尝试发送篡改的 V2X 直连通信消息，测试车辆是否校验 V2X 直连通信消息的完整性；
c) 测试人员尝试修改、删除存储在车端的密钥，测试车辆是否能保护存储的密钥的安全性。

6.5.2.2 密钥导出测试

如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文。

6.5.2.3 假名证书应用测试

测试人员应按照以下测试方法开展测试，判定车辆使用的假名证书是否满足 5.3.2.3 的要求：

a) 测试人员根据车辆制造商提供或使用工具抓取的 V2X 假名证书申请数据，判定车辆使用的假名证书是否满足 5.3.2.3 a）的要求；
b) 测试人员使用工具抓取证书申请传输报文并尝试篡改报文内容，判定车辆使用的假名证书是否满足 5.3.2.3 b）的要求；
c) 测试人员下载非车端可信证书信任链签发、信任链校验不通过的 V2X 假名证书，执行证书下载流程，判定车辆使用的假名证书是否满足 5.3.2.3 c）的要求；
d) 测试人员导入公钥与私钥不匹配的 V2X 假名证书，执行证书导入流程，判定车辆使用的假名证书是否满足 5.3.2.3 d）的要求；
e) 测试人员使用用途与业务场景不匹配的 V2X 假名证书执行业务操作，判定车辆使用的假名证书是否满足 5.3.2.3 e）的要求；
f) 测试人员待证书临近更新周期时，使用工具抓取车辆广播报文，测试车辆是否自动切换、加载并使用全新的有效假名证书，判定车辆使用的假名证书是否满足 5.3.2.3 f）的要求；
g) 测试人员发起 V2X 假名证书撤销申请，判定车辆使用的假名证书是否满足 5.3.2.3 g）的要求。

6.5.3 远程控制密码应用要求测试

测试人员应按照以下测试方法开展测试，判定车辆是否满足5.3.3的要求：

a) 测试人员尝试以伪造的身份发送远程控制指令信息，测试车辆是否校验远程控制指令信息的真实性；
b) 测试人员尝试篡改远程控制指令信息，测试车辆是否校验远程控制指令信息的完整性；
c) 测试人员尝试重放已成功执行的远程控制指令，测试车辆是否能够识别并拒绝重复指令；
d) 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文。

6.5.4 其他外部无线通信密码应用要求测试

测试人员应按照以下测试方法开展测试，判定车辆是否满足 5.3.4 的要求：

a) 测试人员尝试以伪造的身份与车辆进行其他外部无线通信，测试车辆是否校验其他外部无线通信实体的真实性；
b) 测试人员尝试发送篡改的其他外部无线通信数据，测试车辆是否校验通信数据的完整性；
c) 测试人员尝试使用报文捕捉分析工具抓取通过其他外部无线通信传输的控制指令信息，并重放该指令信息，测试车辆是否执行该指令信息；

d） 测试人员尝试篡改车端存储的与其他外部无线通信相关的密钥，测试车辆是否校验密钥的完整性；
e） 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文。

6.5.5 授权的第三方应用密码应用要求测试

测试人员应依据车辆制造商提供的授权的第三方应用清单，从中选取3个第三方应用，并按照以下测试方法开展测试（如第三方应用数量不足3个时则进行全量测试），判定车辆是否满足5.3.5的要求：
a） 测试人员尝试安装真实性校验值被篡改的第三方应用，测试车辆是否校验第三方应用的真实性；
b） 测试人员尝试安装被篡改的授权第三方应用，测试车辆是否校验第三方应用的完整性。

6.5.6 诊断接口密码应用要求测试

测试人员应按照以下测试方法开展测试，判定车辆是否满足5.3.6的要求：
a） 测试人员尝试通过诊断接口向车辆发送 3 个关键配置及标定参数的写操作指令（若关键配置及标定参数的写操作指令数量不足 3 个时，进行全量测试），测试车辆是否校验通信实体的真实性；
b） 测试人员尝试篡改与诊断接口通信相关的密钥，测试车辆是否校验密钥的完整性；
c） 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文。

6.5.7 车内通信密码应用要求测试

测试人员应选取3个关键报文按照以下测试方法开展测试（如关键报文不足3个时则进行全量测试），判定车辆是否满足5.3.7的要求：
a） 测试人员尝试以伪造的身份发送车内关键报文通信数据，测试车辆是否校验车内通信实体的真实性；
b） 测试人员使用车载总线报文捕捉分析工具、车载以太网协议分析仪，解析车内设备间通信交互关键报文数据，测试是否具备完整性功能，然后测试人员尝试发送篡改的车内关键报文通信数据，测试车辆是否校验车内通信数据的完整性；
c） 测试人员尝试修改、删除存储在车端的与车内通信相关的密钥，测试车辆是否能保护其安全性；
d） 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文。

6.6 数据安全密码应用要求测试

6.6.1 保护敏感个人信息密码应用要求测试

6.6.1.1 车辆使用密码技术保护存储在车端的敏感个人信息时，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，判定是否满足 5.4.1.1 的要求：
a） 测试人员尝试以伪造身份访问敏感个人信息，测试车辆是否校验真实性；
b） 测试人员获取车辆存储的敏感个人信息，测试车辆是否对存储的敏感个人信息进行机密性保护。

6.6.1.2 测试人员应依据车辆制造商提供的车辆向外传输的敏感个人信息的功能清单，触发车辆向外传输敏感个人信息的功能，获取车辆向外传输的敏感个人信息，测试车辆是否对向外传输的敏感个人信息进行机密性保护，判定车辆是否满足 5.4.1.2 的要求。

6.6.1.3 测试人员尝试修改、删除存储在车端的与保护敏感个人信息相关的密钥，测试车辆是否能保护其安全性，判定车辆是否满足 5.4.1.3 的要求。

6.6.1.4 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文，判定车辆是否满足 5.4.1.4 的要求。

6.6.1.5 使用数字证书时，测试人员按照 6.5.1.3 的测试方法，判定车辆是否满足 5.4.1.5 的要求。

6.6.2 保护重要数据密码应用要求测试

6.6.2.1 车辆使用密码技术保护存储在车端的重要数据时，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，判定是否满足 5.4.2.1 的要求：

a) 测试人员尝试以伪造身份访问重要数据，测试车辆是否校验真实性；
b) 测试人员获取车辆存储的重要数据，测试车辆是否对存储的重要数据进行机密性保护。

6.6.2.2 测试人员应依据车辆制造商提供的车辆向外传输的重要数据的功能清单，触发车辆向外传输重要数据的功能，获取车辆向外传输的重要数据，测试车辆是否对向外传输的重要数据进行机密性保护，判定是否满足 5.4.2.2 的要求。

6.6.2.3 测试人员尝试修改、删除存储在车端的与保护重要数据相关的密钥，测试车辆是否能保护其安全性，判定是否满足 5.4.2.3 的要求。

6.6.2.4 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文，判定是否满足 5.4.2.4 的要求。

6.6.2.5 使用数字证书时，测试人员按照 6.5.1.3 的测试方法，判定车辆是否满足 5.4.2.5 的要求。

6.6.3 保护车辆身份识别数据密码应用要求测试

测试人员应按照以下测试方法开展测试，判定是否满足5.4.3的要求：

a) 尝试以伪造身份删除和修改存储在车端的与保护 VIN 等用于车辆身份识别的数据，测试车辆是否校验真实性；
b) 测试人员尝试修改、删除存储在车端的与保护 VIN 等用于车辆身份识别的数据相关的密钥，测试车辆是否能保护其安全性；
c) 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文；
d) 使用数字证书时，测试人员依次按照 6.5.1.3 的测试方法，判定车辆是否满足 5.4.3.4 的要求。

6.6.4 保护关键数据密码应用要求测试

测试人员应按照以下测试方法开展测试，判定是否满足 5.4.4 的要求：

a) 尝试以伪造身份删除和修改存储在车端的关键数据，测试车辆是否校验真实性；
b) 测试人员尝试修改、删除存储在车端的与保护关键数据相关的密钥，测试车辆是否能保护其安全性；
c) 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文；
d) 使用数字证书时，测试人员依次按照 6.5.1.3 的测试方法，测试车辆是否满足 5.4.4.4 的要求。

6.6.5 保护安全日志密码应用要求测试

测试人员应按照以下测试方法开展测试，判定是否满足5.4.5的要求：

a) 测试人员尝试以伪造身份删除安全日志，测试车辆是否校验真实性；
b) 测试人员尝试篡改安全日志，测试车辆是否校验安全日志完整性；

c） 测试人员尝试修改、删除存储在车端的与保护安全日志相关的密钥，测试车辆是否能保护其安全性；
d） 如支持密钥导出功能，测试人员尝试导出密钥，测试导出的密钥是否为明文；
e） 使用数字证书时，测试人员依次按照 6.5.1.3 的测试方法，测试车辆是否满足 5.4.5.4 的要求。

7 同一型式判定

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。

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。

8 标准的实施

对于新申请型式批准的车型，自本文件实施之日起开始执行。

对于已获得型式批准的车型，自本文件实施之日起第25个月开始执行。

附 录 A
（规范性）
确定测试对象的方法

A.1 测试人员需对照车辆密码应用方案逐项确认各个条款的测试对象。

A.2 对于 6.4.3.2、6.6.1～6.6.5，测试人员需采用如下方法确定测试对象：

a) 对待测车辆涉及 6.4.3.2、6.6.1～6.6.5 的控制器进行梳理，使用表 A.1 进行记录，标注各控制器与对应条款关联情况；

表 A.1 控制器清单

控制器名称	是否涉及 6.4.3.2	是否涉及 6.6.1	是否涉及 6.6.2	是否涉及 6.6.3	是否涉及 6.6.4	是否涉及 6.6.5
示例 1：控制器名称:依次填写 6.4.3.2、6.6.1～6.6.5 涉及的控制器名称，控制器名称需与铭牌信息保持一致。 **示例 2**：是否涉及 6.4.3.2：是/否。 **示例 3**：是否涉及 6.6.1：是/否。 **示例 4**：是否涉及 6.6.2：是/否。 **示例 5**：是否涉及 6.6.3：是/否。 **示例 6**：是否涉及 6.6.4：是/否。 **示例 7**：是否涉及 6.6.5：是/否。 **注**：若待测车辆有多个涉及6.4.3.2、6.6.1～6.6.5的控制器可自行增补行数，若待测车辆功能不涉及 6.4.3.2、6.6.1～6.6.5，可删除对应的列。						

b) 测试人员从控制器清单中选择待测控制器 1，确认待测控制器 1 覆盖的条款；

c) 若待测控制器 1 能覆盖 6.4.3.2、6.6.1～6.6.5，则使用待测控制器 1 执行测试；若待测控制器 1 不能覆盖 6.4.3.2、6.6.1～6.6.5，则继续从控制器清单中选择待测控制器 2，并确认待测控制器 1 和待测控制器 2 覆盖的条款；

d) 若待测控制器 1 和待测控制器 2 能覆盖 6.4.3.2、6.6.1～6.6.5，则使用待测控制器 1 和待测控制器 2 执行测试；若待测控制器 1 和待测控制器 2 不能覆盖 6.4.3.2、6.6.1～6.6.5，重复上述选择动作，直至所选择的控制器能覆盖 6.4.3.2、6.6.1～6.6.5，流程示意图见图 A.1。

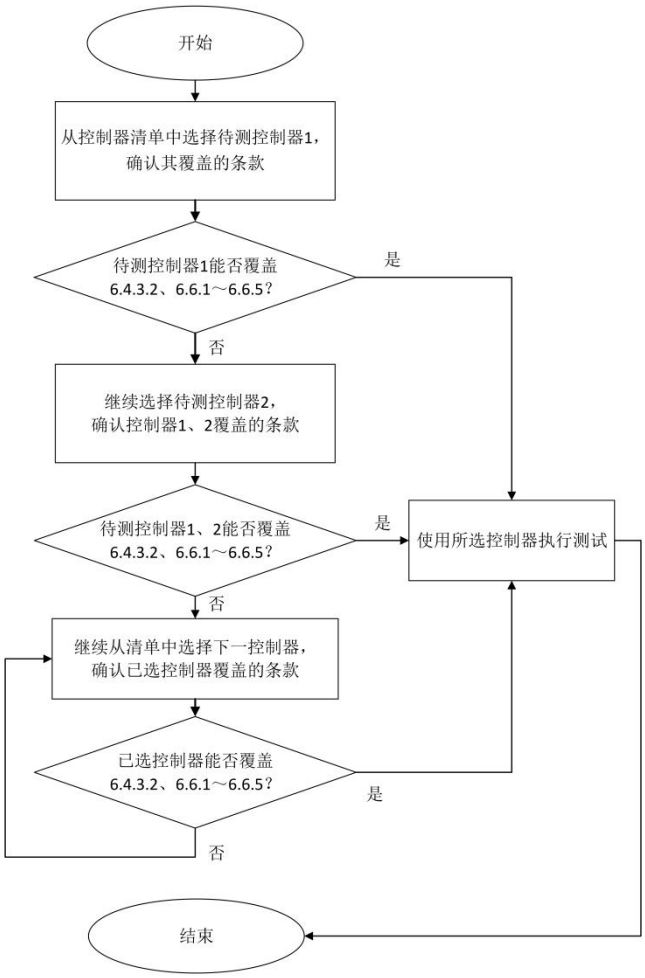


图 A.1　确定测试对象流程示意图

A.3　测试人员应记录选择待测控制器的过程并形成可追溯的原始记录。