ICS 43.020
CCS T40

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 vehicle cryptography application

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

（本草案完成时间：2026.07.24）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

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

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和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，车端实现密码功能的相关零部件可参照实施。

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 44495—2024 汽车整车信息安全技术要求

GB/T 37092—2018 信息安全技术 密码模块安全要求

GM/T 0008—2012 安全芯片密码检测准则

GB/T XXXX 汽车芯片信息安全技术规范

GB/T 32915—2026 信息安全技术 二元序列随机性检测方法

3 术语和定义

GB/T 25069—2022、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

指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

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。

[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

密钥管理 key management

在密钥全生存周期，根据安全策略，对密钥的生成、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等进行管理。

[来源:GB/T 25069—2022,3.401]

3.5

根证书 root certificate

根证书机构向自身签发的自签名证书，是一个公钥基础设施系统中所有证书链的终节点。

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。

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的关键密钥的安全，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。

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。

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

重要系统密码应用要求如下：

a) 应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、获取或删除自动驾驶数据记录系统的操作实体身份真实性；

b) 应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。

5.2.2 安全启动密码应用要求

涉及远程控制系统、车载软件升级系统、自动驾驶数据记录系统以及经风险评估识别确需安全启动的系统，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。

5.2.3 软件升级密码应用要求

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。

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

车辆与 TSP 平台、OTA 平台等云平台通信密码应用要求如下：

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。

5.3.2 远程控制密码应用要求

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。

5.3.3 授权的第三方应用密码应用要求

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。

5.3.4 诊断接口密码应用要求

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。

5.3.5 V2X 直连通信密码应用要求

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。

5.3.6 外部无线通信密码应用要求

车辆与外部设备进行无线通信密码应用要求如下：
a) 使用密码技术保护时，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验证通信实体的真实性；
b) 使用密码技术保护时，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、来源真实性、完整性，并采取有效手段防止重放攻击；
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。

5.3.7 车内通信密码应用要求

使用密码技术保护汽车内部设备之间通信时要求如下：
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通信实体的真实性；
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障通信数据的完整性；
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。

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

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。

5.4.2 保护重要数据密码应用要求

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。

5.4.3 保护车辆身份识别数据密码应用要求

使用密码技术保护存储在车内的VIN等用于车辆身份识别的数据时要求如下：

a) 应验证车辆身份识别数据删除和修改操作实体的身份真实性；
b) 在车端产生的密钥应符合 5.1.3 的要求；
c) 如在车端存储密钥，应保障密钥存储的安全性；
d) 不应以明文方式导出对称密钥、私钥；
e) 使用数字证书保护车辆身份识别的数据安全时，数字证书应满足 5.3.1 g)的要求。

5.4.4 保护关键数据密码应用要求

使用密码技术保护存储在车内的关键数据时要求如下：

a) 应验证关键数据删除和修改的操作实体身份真实性；
b) 在车端产生的密钥应符合 5.1.3 的要求；
c) 如在车端存储密钥，应保障密钥存储的安全性；
d) 不应以明文方式导出对称密钥、私钥；
e) 使用数字证书保护存储在车内的关键数据安全时，数字证书应满足 5.3.1 g)的要求。

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、自动驾驶系统运行信息、行车环境信息等自动驾驶、辅助驾驶数据以及其他车辆运行过程中产生的可能影响行车安全的数据。

5.4.5 保护安全日志密码应用要求

使用密码技术保护存储在车内的安全日志密码应用时要求如下：

a） 应对安全日志的删除操作实体进行身份真实性验证；

b） 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安全日志的完整性；

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。

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，从6.3-6.6中选择适配的方法开展测试，确认车辆满足第5章技术要求。车辆密码应用方案包括待测车辆的密码功能及调用接口、选用的密码算法、配用的密钥种类和用途、密钥全生命周期技术要求、选用的密码模块或安全芯片的安全机制说明及检测报告或认证证书等。

6.2 测试条件

测试样件包括整车及涉及的零部件，应满足以下要求：

———测试样件可正常运行；

———汽车密码应用相关功能处于开启状态。

6.3 通用技术要求测试

6.3.1 密码算法测试

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5.1.1的要求：

a） 车辆使用给定的密钥和明文经对称密码算法加密，测试人员比对加密结果和给定密文是否完全相同；

b） 车辆使用给定的密钥和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；

c） 车辆使用给定密钥和公钥密码算法对给定明文加密，测试人员采用对应公钥密码算法及密钥解密，解密结果与原始明文是否完全相同；

d） 车辆使用给定密钥和公钥密码算法对明文完成“先加密-再解密”全流程操作，最终解密结果与原始明文是否完全相同；

e） 车辆使用给定密钥和公钥密码算法对目标消息签名，测试人员采用对应公钥密码算法及公钥验签，验签结果是否通过；

f） 车辆使用给定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；

g） 车辆使用给定的密钥和密钥协商参数，调用公钥密码算法的密钥协商算法，与测试人员的检测工具完成密钥协商，比对协商生成的密钥是否一致。

h） 车辆使用给定消息调用密码杂凑算法计算杂凑值，测试人员比对结果是否和给定杂凑值完全相同；

i） 车辆使用给定消息和参数调用密码杂凑算法计算杂凑值，测试人员比对结果是否和给定杂凑值完全相同；

j） 测试人员应使用密码分析工具，在设定的计算资源条件下，根据密码应用场景及算法类型开展脆弱性分析，检测是否通过脆弱性测试。

6.3.2 密码模块/安全芯片测试

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。

6.3.3 随机数测试

测试人员应按照以下测试方法依次开展测试，判定车辆是否满足 5.1.3 要求：

a) 采集车辆产生的连续 1000000 比特的随机数，检测是否符合 GB/T 32915-2026 中 A.2 的随机性检测要求；
b) 检测随机数生成功能，样本长度不低于 256 比特，应采用 GB/T 32915-2026 中规定的扑克检测，扑克检测参数 m=2，如果检测未通过，允许重复检测 1 次；
c) 应查看随机数上电自检日志，检查随机数检测的检测项、检测结果、判定车辆是否满足 5.3 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依次开展测试，判定车辆是否满足5.2.1要求：

a) 测试人员尝试以伪造的身份访问、获取、删除自动驾驶数据记录系统数据，检测系统是否采用密码技术校验操作实体身份真实性；
b) 测试人员尝试篡改自动驾驶系统、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的存储数据，检测系统是否采用密码技术校验记录数据完整性；
c) 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.2.1 c)要求；
d) 测试人员尝试导出密钥，检测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固件、引导程序、操作系统、关键应用软件等启动组件镜像，上电启动车辆，检测车辆系统是否具备逐级安全启动校验流程，能否采用密码技术识别并拦截不真实、被篡改的启动组件，判定车辆是否满足5.2.2的要求。

6.4.3 软件升级密码应用要求测试

测试人员应按照以下测试方法依次开展测试，判定车辆是否满足5.2.3的要求：

a) 若使用车载软件升级系统，测试人员尝试篡改或伪造接收到的升级包，检测车载软件升级系统是否校验升级包的真实性和完整性；
b) 若不使用车载软件升级系统，测试人员尝试篡改或伪造接收到的升级包，检测被升级的控制器是否校验真实性和完整性；
c) 测试人员尝试伪造车辆信任的密钥，检测车辆是否校验密钥的完整性；
d) 测试人员尝试导出密钥，检测导出的密钥是否为明文。

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

测试人员应按照以下测试方法依次开展测试，判定车辆是否满足5.3.1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，检测协议是否实现正确，是否满足 5.3.1 a)的要求；
b) 测试人员尝试与伪造云平台通信，检测车辆是否校验通信实体的真实性；
c) 测试人员尝试篡改通信数据，检测车辆是否校验通信数据的完整性；
d) 测试人员获取车辆存储和向外传输的重要数据，检验车辆是否对重要数据进行机密性保护；
e) 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.3.1 e)要求；
f) 测试人员尝试导出密钥，检测导出的密钥是否为明文；
g) 测试人员尝试修改根证书，检测车辆是否满足 5.3.1 g) 1)的要求；
h) 测试人员使用工具抓取车辆生成的证书申请数据，检测车辆是否满足 5.3.1 g) 2)的要求；
i) 测试人员使用证书分析工具抓取证书申请数据，检测车辆证书申请数据传输过程是否满足 5.3.1 g) 3)的要求；
j) 测试人员分别导入非车端可信证书信任链签发的数字证书、证书密钥与车端存储的私钥不匹配的数字证书，检测车辆是否满足 5.3.1 g) 4)和 5)的要求；
k) 测试人员依次使用与业务系统不匹配的证书和过期的证书执行相关业务操作，检测车辆是否满足 5.3.1 g) 6)的要求；
l) 测试人员检测是否可撤销证书，如可撤销，则尝试使用已撤销的数字证书执行业务操作，检测车辆是否满足 5.3.1 g) 7)的要求。

6.5.2 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依次开展测试，判定车辆是否满足5.3.2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，检测车辆是否校验远程控制信息的真实性；
b) 测试人员尝试篡改远程控制指令信息，检测车辆是否校验远程控制信息的完整性；
c) 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.3.2 c)要求；
d) 测试人员尝试导出密钥，检测导出的密钥是否为明文。

6.5.3 授权的第三方应用密码应用要求测试

测试人员应按照以下测试方法依次开展测试，判定车辆是否满足5.3.3的要求：

a) 测试人员安装非授权的第三方应用，检测车辆是否校验第三方应用的真实性；
b) 测试人员尝试安装篡改的已授权第三方应用，检测车辆是否校验第三方应用的完整性。

6.5.4 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5.3.4的要求：

a） 测试人员尝试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，检测车辆是否校验通信实体的真实性，判定车辆是否满足要求；

b） 测试人员尝试伪造诊断信任的密钥，检测车辆是否校验密钥的完整性；

c） 测试人员尝试导出密钥，检测导出的密钥是否为明文。

6.5.5 V2X 直连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5.3.5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，检测车辆是否校验 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，检测车辆是否校验 V2X 直连通信消息的完整性；

c） 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.3.5 c)要求；

d） 测试人员尝试修改、删除存储在车端的密钥，检测车辆是否能保护存储的密钥的安全性；

e） 测试人员依次使用 6.5.1 g) - k)的测试方法，检测车辆是否满足 5.3.5 d)的要求。

6.5.6 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 5.3.6 的要求：

a） 测试人员尝试以伪造的身份与车辆进行外部无线通信，检测车辆是否校验外部无线通信实体的真实性；

b） 测试人员尝试发送篡改的外部无线通信数据，检测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外部无线通信数据，检测车辆是否满足 5.3.6 c)的要求；

d） 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.3.6 d)要求；

e） 测试人员尝试修改、删除存储在车端的密钥，检测车辆是否能保护存储的密钥的安全性；

f） 测试人员尝试导出密钥，检验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

测试人员应按照以下测试方法开展测试，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通信数据，检测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全量交互报文数据，检测是否具备完整性功能，然后测试人员尝试发送篡改的车内通信数据，检测车辆是否校验车内通信数据的完整性；

c） 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.3.7 c)要求；

d） 测试人员尝试修改、删除存储在车端的密钥，检测车辆是否能保护存储的密钥的安全性；

e） 测试人员尝试导出密钥，检测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

测试人员应按照以下测试方法依次开展测试，判定是否满足5.4.1的要求：

a） 测试人员尝试以伪造身份访问敏感个人信息，检测车辆是否校验身份真实性；

b） 测试人员获取车辆存储的敏感个人信息，检测车辆是否对存储的敏感个人信息进行机密性保护；

c） 测试人员采集车辆向外传输的敏感个人信息，解析通信报文数据，检测车辆是否对向外传输的敏感个人信息进行机密性保护；
d） 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.4.1 d)要求；
e） 测试人员尝试修改、删除存储在车端的密钥，检测车辆是否能保护存储的密钥的安全性；
f） 测试人员尝试导出密钥，检验导出的密钥是否为明文；
g） 使用数字证书时，测试人员依次使用 6.5.1 g) - l)的测试方法，检测车辆是否满足 5.4.1 g)的要求。

6.6.2 保护重要数据密码应用要求测试

测试人员应按照以下测试方法依次开展测试，判定是否满足5.4.2的要求：
a） 测试人员尝试以伪造身份访问重要数据，检测车辆是否校验身份真实性；
b） 测试人员获取车辆存储的重要数据，检测车辆是否对存储的重要数据进行机密性保护；
c） 测试人员采集车辆向外传输的重要数据，解析通信报文数据，检测车辆是否对向外传输的重要数据进行机密性保护；
d） 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.4.2 d)要求；
e） 测试人员尝试修改、删除存储在车端的密钥，检测车辆是否能保护存储的密钥的安全性；
f） 测试人员尝试导出密钥，检验导出的密钥是否为明文；
g） 使用数字证书时，测试人员依次使用 6.5.1 g) - l)的测试方法，检测车辆是否满足 5.4.2 g)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依次开展测试，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车辆身份识别数据，检测车辆是否校验身份真实性；
b） 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.4.3 b)要求；
c） 测试人员尝试修改、删除存储在车端的密钥，检测车辆是否能保护存储的密钥的安全性；
d） 测试人员尝试导出密钥，检验导出的密钥是否为明文；
e） 使用数字证书时，测试人员依次使用 6.5.1 g) - l)的测试方法，检测车辆是否满足 5.4.3 e)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依次开展测试，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车内的关键数据，检测车辆是否校验身份真实性；
b） 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.4.4 b)要求；
c） 测试人员尝试修改、删除存储在车端的密钥，检测车辆是否能保护存储的密钥的安全性；
d） 测试人员尝试导出密钥，检验导出的密钥是否为明文；
e） 使用数字证书时，测试人员依次使用 6.5.1 g) - l)的测试方法，检测车辆是否满足 5.4.4 e)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依次开展测试，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，检测车辆是否校验身份真实性；
b） 测试人员尝试篡改安全日志，检测车辆是否校验安全日志完整性；
c） 测试人员依照 6.3.3 a)的测试方法检测产生的密钥是否满足 5.4.5 c)要求；
d） 测试人员尝试修改、删除存储在车端的密钥，检测车辆是否能保护存储的密钥的安全性；
e） 测试人员尝试导出密钥，检测导出的密钥是否为明文。

7 同一型式判定

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；

——车辆保护与云平台通信、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。

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。

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。