

推荐性国家标准

《汽车诊断接口信息安全技术要求》

（征求意见稿）

编制说明

标准起草项目组

2022年10月

# 目 次

目 次 .....	2
一、 工作简况.....	3
二、 国家标准编制原则和确定国家标准主要内容.....	6
三、 主要试验（或验证）情况分析.....	7
四、 标准中涉及专利的情况.....	11
五、 预期达到的社会效益等情况.....	11
六、 采用国际标准和国外先进标准的情况.....	11
七、 与现行相关法律、法规、规章及相关标准的协调性.....	12
八、 重大分歧意见的处理经过和依据.....	12
九、 标准性质的建议说明.....	12
十、 贯彻标准的要求和措施建议.....	12
十一、 废止现行相关标准的建议.....	12
十二、 其他应予说明的事项.....	12

# 《汽车诊断接口信息安全技术要求》

## （征求意见稿）编制说明

### 一、 工作简况

#### （一） 任务来源

本项目是根据国家标准委[2021]12号文《关于下达2021年第一批推荐性国家标准计划的通知》（计划项目编号20211169-T-339，标准项目名称《汽车诊断接口信息安全技术要求》）进行制定。

#### （二） 工作过程

##### 1. 项目组工作过程简介

汽标委智能网联汽车分标委组织成立标准起草项目组并征集参与成员单位，经综合考虑，确定中国第一汽车股份有限公司为牵头单位，在此基础上明确了任务和分工，积极开展标准的预研、起草及征求意见等工作。

2018年12月～2019年05月，组织项目组成员专家对标准展开预研工作。

2019年06月～09月，项目组讨论并确定标准制定的指导思想和原则，制定了标准的总体框架和工作计划。

2019年10月～12月，收集、整理并系统地分析了与汽车诊断接口信息安全相关的法规、标准、文献资料等，开展了相关技术研究，并起草标准草案。

2020年01月～02月，经过标准起草项目组的分工编写和反复讨论，形成第一版标准草案。

2020年02月26日，向国家标准委提交立项申请。

2020年03月～2021年04月，经过标准项目组的多次讨论，形成第二版标准草案。

2021年05月07日，国家标准委正式下达了该标准项目计划编号。

2021年06月～2022年07月，经过标准项目组的多次讨论，持续完善标准草案，形成第三版至第六版标准草案。

2022年07月～08月，组织开展标准试验验证工作，根据试验数据，讨论和完善标准文本。

2022年08月，组织专家对标准草案进行研讨和多次修订，形成工作组内征求意见稿，并面向信息安全标准工作组内各成员单位广泛征求意见。

2022年09月，在信息安全标准工作组进行征集意见，收集反馈意见共计227条，并召开意见协调会，65条意见被采纳，57条意见部分采纳，69条意见不采纳，同时解答疑问或问题36条。并根据意见反馈修改形成公开征求意见稿和编制说明。

## 2. 项目组第一次会议

2018年12月20日，项目组在北京召开了“汽车诊断接口信息安全技术要求标准编制项目组第一次工作会议”，正式启动标准制定工作。

会议对各参与单位及主要参与专家的基本情况进行了交流，对标准背景、标准基本内容框架进行了讨论，并围绕标准涉及的内容范围、国内外相关标准和法规现状以及时间安排等多个方面进行了深入讨论。经本次会议讨论，明确了标准的内容与定义，对标准范围进行界定。聚焦通过诊断连接器进行诊断的信息安全，提出接入端和准入端概念，为汽车设计生产厂家和供应商开发诊断接口信息安全与测试验证提供依据。

## 3. 项目组第二次会议

2019年06月04日，项目组在无锡召开了“汽车诊断接口信息安全技术要求标准编制项目组第二次工作会议”，会议明确了标准编制范围包括远程诊断场景以及诊断服务的信息安全要求，不涉及远程诊断的外部服务器等安全要求。会议重点讨论了接入端和准入端的界定范围，明确了标准草案的框架、目录及章节内容范围，制定了初版目录并确定了标准起草组成员，由标准起草组成员分工编写标准文本。

## 4. 起草组提纲讨论会

2019年10月12日，标准起草组通过线上会议方式召开了“汽车诊断接口信息安全技术要求标准编制起草组提纲讨论会议”，会议明确了标准编制范围、标准提纲、标准草案的框架和标准草案各部分的核心内容等问题，标准起草组成员对标准编写框架、目标和内容达成一致，并进行编写分工。

## 5. 项目组第三次会议

2019年11月07日，项目组在杭州召开了“汽车诊断接口信息安全技术要求标准编制项目组第三次工作会议”，会议重点审阅了标准初稿、讨论了标准草案部分章节的内容，会议明确：目录框架内容达成一致意见；将5.4、5.5、5.1相关章节进行整合，认证方式与认

证算法整合，明确要求的算法强度；标准编写行文格式要遵循 GB/T 1.1-2020 的要求。

## 6. 起草组意见处理会议

2020 年 06 月 29 日，标准起草组通过线上会议方式召开了“汽车诊断接口信息安全技术要求标准编制起草组意见处理讨论会议”。会议对标准各章节内容及项目组第三次会议遗留问题等多方面进行了深入讨论。会后，针对意见问题完成对标准草案的修改。

## 7. 项目组第四次会议

2020 年 10 月 22 日，项目组在北京组织召开“汽车诊断接口信息安全技术要求标准编制项目组第四次工作会议”。会议对标准题目、接入端和准入端的场景分析、认证算法描述等多方面进行了深入讨论。会议同时欢迎各成员单位更多专家踊跃参与到标准编制工作中，充分征询各方意见和建议，提高标准的广泛性。

## 8. 项目组第五次会议

2021 年 04 月 27 日，项目组在天津组织召开“汽车诊断接口信息安全技术要求标准编制项目组第五次工作会议”。会议对最新的标准草案进行逐章逐条的详细讨论，包括全文范围、缩略语、术语和定义、诊断接口信息安全架构、诊断信息安全认证技术要求、诊断接入端信息安全技术要求、诊断准入端信息安全技术要求、诊断服务安全技术要求、测试和验证方法九个章节的修改建议，并讨论了后续标准编制工作的时间计划，按照会议结论，进一步修订和完善标准草案。

## 9. 项目组第六次会议

2022 年 5 月 26 日，项目组通过线上会议组织召开“汽车诊断接口信息安全技术要求标准编制项目组第六次工作会议”。会议对修改后的标准草案进行讨论，形成如下意见：

- 1) 诊断接口信息安全架构章节，示意图需要进行调整；
- 2) 诊断信息安全认证技术要求章节，原数据安全要求，内容定义不清晰、题目过大，需删除原数据安全要求；
- 3) 诊断接入端信息安全技术要求章节，数据销毁要求细化修改；
- 4) 诊断准入端信息安全技术要求章节，对于车辆诊断接口连接的通讯总线的要求、总线连接控制器的要求、双因子验证的要求等需要调整；

5) 诊断服务安全技术要求章节,测试环境准备、待测对象要求未单独明确;测试内容与需求内容未关联;示意图不准确;

6) 测试和验证方法章节,缺少示例性描述语句、架构图不准确。

会议同意在完成个别条文的修订后,进行工作组内征求意见。

## 10. 工作组内部征求意见情况

2022年08月12日至09月09日,进行了汽车信息安全标准工作组内征求意见。工作组内部征求意见稿发出后,共收到227条的反馈意见和建议。根据反馈意见的内容,项目组进行讨论并给出结论,其中,65条意见被采纳,57条意见部分采纳,69条意见不采纳,同时收到疑问或问题36条,项目组逐一进行了解答。

项目组根据以上意见对标准进行了修改,形成公开征求意见稿。

### (三) 主要参加单位和工作组成员及其所做的工作等

本标准由十余家单位共同起草。在本标准的制定过程中,多次组织行业专家进行了研讨,并开展了验证试验,得到了相关单位的支持、协助与配合,取得了大量建设性意见、建议。

## 二、 国家标准编制原则和确定国家标准主要内容

### (一) 标准编制原则

- 1) 本标准编写符合 GB/T 1.1-2020《标准化工作导则》的要求;
- 2) 在项目组内对标准内容广泛征求意见,并在工作组会议上充分讨论;
- 3) 起草过程充分考虑了车辆厂商、零部件厂商和信息安全解决方案提供商的意见,在当前行业技术水平的基础上前瞻性地考虑技术发展方向;
- 4) 起草过程充分考虑国内外现有相关标准的统一和协调。

### (二) 标准主要内容

#### 1. 范围

本文件规定了汽车诊断接口的信息安全架构、信息安全技术要求与试验方法。

本文件适用于 M 类、N 类汽车,其他类型车辆可参照执行。

#### 2. 术语和定义

标准的术语和定义参考了GB/T 34589-2017《道路车辆 诊断连接器》中的部分术语和定义，并对标准最主要的“诊断接入端”“诊断准入端”“被诊断控制器”“诊断网关”“远程诊断控制器”“诊断接口”“诊断解锁”等术语进行了标准化定义。

### 3. 条款 5 诊断接口信息安全架构

本条款对诊断接口信息安全架构进行了说明。

### 4. 条款 6.1 诊断接口信息安全认证和权限控制技术要求

本条款主要对在诊断接入端和准入端间进行的身份认证及权限控制两个方面提出了标准化要求。

### 5. 条款 6.2 诊断接入端信息安全技术要求

本条款主要从安全存储、数据使用、密钥信息销毁三个方面对诊断接入端提出了标准化要求。

### 6. 条款 6.3 诊断准入端信息安全技术要求

本条款主要从控制器信息安全、诊断接口物理安全、车内诊断安全3方面对诊断准入端提出了标准化要求。其中：

条款6.3.3.3 a)：按照7.3.3.3 a) 进行试验，应通过对被诊断控制器安全访问解锁后，执行与行车安全相关参数的诊断写服务。

说明：

行车安全相关参数包括但不限于制动功能和转向功能的关键参数等，非预期的诊断写服务会使这些参数发生变化而引起车辆行为的异常改变，影响行车安全。要求对于涉及行车安全相关参数功能的诊断写服务需要经过安全访问（例如：诊断27服务）后才可被执行。

### 7. 条款 7 信息安全试验方法

根据本标准“6. 技术要求”中各项信息安全技术要求，逐一对应提出了试验方法。

## 三、 主要试验（或验证）情况分析

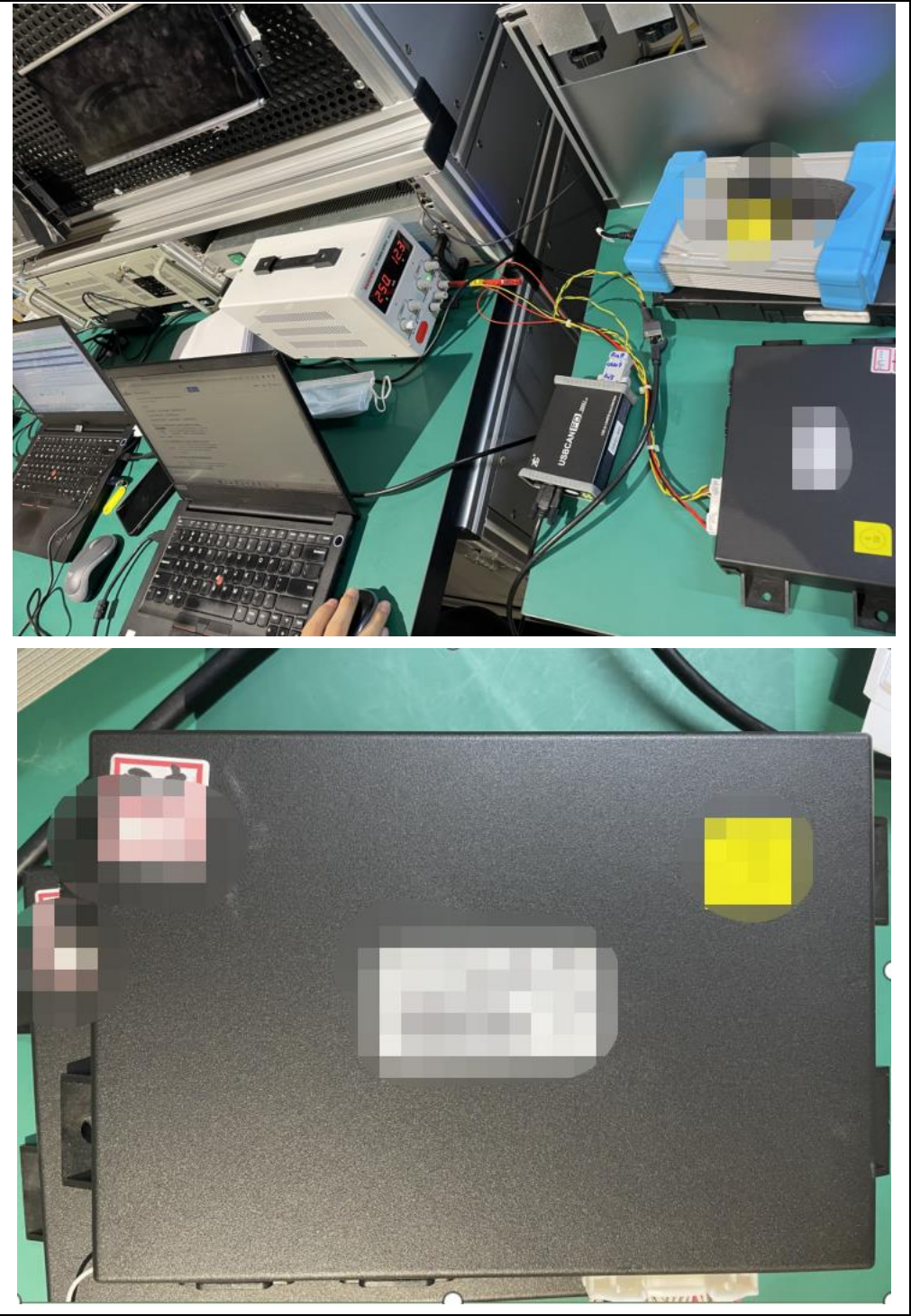
### （一） 试验概况

试验时间：2022年07月至08月

试验地点：长春 一汽红旗

试验单位：中汽研软件测评（天津）有限公司

试验目标物:	网关
试验环境:	根据标准文稿搭建测试
试验方法:	根据标准文稿规定的测试方法编制具体测试用例。



(二) 试验内容



## 1. 试验工具

在标准试验中，使用了以下试验工具设备：

工具名	作用
诊断工具	用于收发报文，向网关发送攻击报文、正常报文并接收 CAN 网关转发的报文。
数据抓包工具	用于读取诊断接入端和诊断准入端通过 DoIP 交互的数据报文。
证书分析工具	用于读取、分析、修改证书。
密码分析工具	用于分析认证过程中使用的密码算法、协议、证书、随机数等。

## 2. 试验方法

试验类别	使用的试验方法	试验目的
身份认证试验	身份认证分析试验	1、检测是否具有身份认证要求； 2、检测身份认证流程一致性； 3、检测身份认证设计、实现的安全性。
认证算法试验	算法正确性验证试验 算法参数验证试验	1、检测认证过程使用算法是否安全； 2、检测使用算法的正确性、一致性； 3、检测算法的椭圆曲线方程。
安全存储试验	接入端安全存储访问试验	1、检测安全存储区域是否能被非授权访问、篡改和销毁等。
数据使用试验	接入端权限控制试验 密钥安全试验	1、检测不同权限的用户是否具有访问关键安全参数的能力； 2、检测认证交互过程是否有敏感密钥。
涉密数据销毁试验	数据销毁试验	1、检测接入端是否具备数据销毁的功能，以及被销毁的数据是否能够恢复。
控制器信息安全试验	准入端安全存储访问试验 准入端权限控制试验 认证失败处理试验	1、检测安全存储区域是否能被非授权访问、篡改和销毁等； 2、检测准入端对不同权限的请求是否响应不同； 3、检测诊断准入端是否只能进行诊断和车载软件更新功能的服务。
诊断接口物理安全试验	诊断接口物理安全试验 网络拓扑检查试验	1、检测诊断接口引脚是否有非诊断用通信总线和非通信类硬线是否只有接入端供电硬线和法规、标准要求连接的硬线； 2、检测诊断接口连接的通信总线是否仅有一个电控单元。
车内诊断安全试验	诊断条件检查试验 拒绝服务试验 诊断解锁信息安全试验	1、检测诊断执行条件是否符合要求； 2、检测不同场景、权限访问的应答是否不同； 3、检测诊断解锁是否符合要求。

## 3. 试验结果

试验方法	试验结果
------	------

身份认证分析试验	1、搭载正常诊断设备环境，OBD 身份认证通过； 2、搭载第三方诊断设备环境，OBD 身份认证失败； 3、采用非授权的诊断设备和诊断软件链接，诊断接入端认证设备失败。 测试结果：通过。
算法正确性验证试验	1、算法对比符合目前国家标准要求； 2、进行加密、解密、签名、验签验证，算法正确性验证通过。 测试结果：通过。
算法参数验证试验	将参数带到方程组中进行验证，满足曲线参数要求。 测试结果：通过。
接入端安全存储访问试验	尝试访问、修改、删除诊断接入端的存储的身份认证密钥信息的位置，无法访问。 测试结果：通过。
接入端权限控制试验	1、使用非授权用户尝试访问、修改、删除诊断接入端端的存储的身份认证密钥信息的位置，无法访问； 2、使用用户合法管理工具尝试访问、修改、删除诊断接入端的存储的身份认证密钥信息的位置，可以访问、修改、删除； 测试结果：通过。
密钥安全试验	1、通过监听身份认证过程数据，提取出证书进行对比，与接入端证书一致； 2、证书包含公钥信息，是否需将标准改为只针对对称密钥或私钥，未通过。 测试结果：未通过。
数据销毁试验	对诊断接入端涉密数据进行销毁，无法恢复；
准入端安全存储访问试验	尝试访问、修改、删除诊断准入端的存储的身份认证密钥信息的位置，无法访问。 测试结果：通过。
准入端权限控制试验	1、使用非授权诊断仪发送诊断服务请求，一般服务应答，特殊服务无应答； 2、使用授权诊断仪发送诊断服务请求，一般服务应答，特殊服务应答； 测试结果：通过。
认证失败处理试验	使用非授权诊断仪认证失败，准入端拒绝认证。 测试结果：通过。
诊断接口物理安全试验	检查测试件接口定义，无非诊断用通信总线和非通信类硬线是否只有接入端供电硬线和法规、标准要求连接的硬线。 测试结果：通过。
网络拓扑检查试验	1、检查网络拓扑结构图，只有网关一个电控单元； 2、测试环境非整车环境，未进行整车验证。

	测试结果：未测到。
诊断条件检查试验	1、使用授权诊断设备，可认证通过； 2、使用非授权诊断设备，认证不通过； 3、使用授权设备，可通过安全访问； 4、使用非授权设备，无法无法通过安全访问； 5、依据诊断设计文档，模拟不满足合理性条件时工况向被诊断控制器发送诊断服务请求，发送否定响应； 6、测试环境无远程通信功能，未测试。 测试结果：远程诊断未测到，其余通过。
拒绝服务试验	1、向被测样件发送不符合应用场景的诊断服务请求，发送否定响应； 2、向被测样件发送不符合安全等级的诊断服务请求，检查是否发送否定响应； 3、具备使车辆信息安全相关的功能永久丧失的诊断服务请求，未通过； 4、无远程诊断环境，未测试。 测试结果：未通过。
诊断解锁信息安全试验	1、向被测样件发送安全相关参数的诊断服务请求，被诊断控制器处于未安全解锁状态接收到请求报文无响应，未通过； 2、向被测样件发送读写诊断内部存储的服务请求，被诊断控制器处于未安全解锁状态接收到该请求报文后发送否定响应。 测试结果：未通过。

#### （四）试验总结分析

- 1) 验证试验中，合计试验项31个，其中通过24个，未通过的4个，未测试的3个，其中未测试到的内容为环境不支持。针对上述情况，经过项目组讨论，将标准中关于身份认证密钥信息安全要求进行修改。
- 2) 通过试验验证，确认本标准的技术要求均能够落地实施，不存在技术壁垒。
- 3) 通过试验验证，确认本标准的试验方法均可实际操作。

#### 四、标准中涉及专利的情况

本标准不涉及专利问题。

#### 五、预期达到的社会效益等情况

诊断接口作为车辆诊断网络的核心节点，承载了车辆刷写及控制等重要指令功能的执行，其安全性不言而喻。推进诊断接口信息安全标准的广泛应用，可以大幅降低整车信息安全风险，具有巨大的安全价值与社会效益。本标准的制定和实施，将为零部件厂商和汽车整车生产企业提供安全开发的技术支撑，引导车辆及相关产品满足行业信息安全要求，进而提升车辆的信息安全技术水平。

#### 六、采用国际标准和国外先进标准的情况

本标准没有采用国际标准。

本标准制定过程中未查到同类国际、国外标准。

#### **七、 与现行相关法律、法规、规章及相关标准的协调性**

本标准与我国现行有关法律、法规和强制性国家标准不矛盾。

#### **八、 重大分歧意见的处理经过和依据**

无。

#### **九、 标准性质的建议说明**

建议本标准的性质为推荐性国家标准。

#### **十、 贯彻标准的要求和措施建议**

1. 本次编制的《汽车诊断接口信息安全技术要求》不仅与汽车整车生产企业有关，而且与系统部件企业、安全厂商、检测机构等相关。对于标准使用过程中容易出现的疑问，起草单位有义务进行必要的解释。

2. 可以针对标准使用的不同对象，如整车生产企业、系统部件企业、安全厂商等相关部门，有侧重点地进行标准的培训和宣贯，以保证标准的贯彻实施。

#### **十一、 废止现行相关标准的建议**

无。

#### **十二、 其他应予说明的事项**

无。