



中华人民共和国国家标准

GB/T XXXXX—XXXX

汽车诊断接口信息安全技术要求

Cybersecurity requirements for vehicle diagnostic interface

(点击此处添加与国际标准一致性程度的标识)

(征求意见稿)

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 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 诊断接口信息安全架构 2

6 技术要求 4

7 试验方法 6

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提出。

本文件由全国汽车标准化技术委员会（SAC/TC114）归口。

汽车诊断接口信息安全技术要求

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 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 34589-2017 道路车辆 诊断连接器

3 术语和定义

GB/T 34589-2017界定的以及下列术语和定义适用于本文件。

3.1

诊断接入端 diagnostic access unit

能够对整车发起诊断服务的设备、系统或平台。

3.2

诊断准入端 diagnostic access control unit

车辆中处理或响应诊断接入端的诊断请求，并确定诊断接入端是否满足身份认证或权限控制的电子控制单元。

3.3

诊断连接器 diagnostic connector

用于车辆和外插诊断设备通信用、短时连接、可带电插拔的连接器，包括两部分：车辆端连接器插座和外插设备端连接器插头。

[来源：GB/T 34589-2017，3.1]

3.4

被诊断控制器 diagnosed controller

响应诊断接入端发送的诊断请求消息，向诊断接入端发送诊断响应消息的电子控制单元。

3.5

诊断网关 diagnostic gateway

连接在诊断网络和诊断子网之间并向车辆子网发送诊断请求消息的电子控制单元。

注：诊断网关通过主从节点间不同网络协议间的格式转换，可以在车辆子网之间进行诊断消息交互。

3.6

远程诊断控制器 remote diagnosis controller

具有与诊断服务器进行连接和通信功能的电子控制单元。

3.7

诊断接口 diagnostic interface

诊断接入端与被诊断控制器之间的通信规则。

3.8

诊断解锁 diagnostic unlock

通过安全手段解除被诊断控制器对于受限功能的访问限制。

4 缩略语

下列缩略语适用于本文件。

CAN	控制器局域网	Controller Area Network
CGW	中央网关	Central Gateway
ECU	电子控制单元	Electronic Control Unit
EOL	生产下线	End of Line
IVI	车载信息娱乐系统	In-Vehicle Infotainment
OBD	车载诊断系统	On-Board Diagnostic
T-BOX	远程终端模块	Telematics Box
UDS	统一的诊断服务	Unified Diagnostic Services

5 诊断接口信息安全架构

5.1 总体架构

诊断网络通常包含被诊断控制器、诊断连接器、控制器之间相互连接的线路以及诊断设备和远程诊断服务器。诊断网络的架构包含从简单的点对点物理连接到复杂的网络架构。

汽车诊断接口信息安全架构由不同的诊断网络形式体现，诊断接入端和诊断准入端是汽车诊断接口信息安全架构的重要组成部分。汽车诊断接口信息安全技术要求包括诊断接口信息安全身份认证和权限控制技术要求、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三个部分。其中：

- a) 诊断接口信息安全身份认证和权限控制技术要求是基于通信或诊断网络实现的诊断准入端对诊断接入端合法身份的认证、鉴权和权限控制要求；
- b) 诊断接入端信息安全技术要求是基于物理连接和远程连接的诊断接入端的信息安全要求；
- c) 诊断准入端信息安全技术要求是汽车内部诊断准入端的信息安全要求。

汽车诊断接口信息安全总体架构示例见图1。

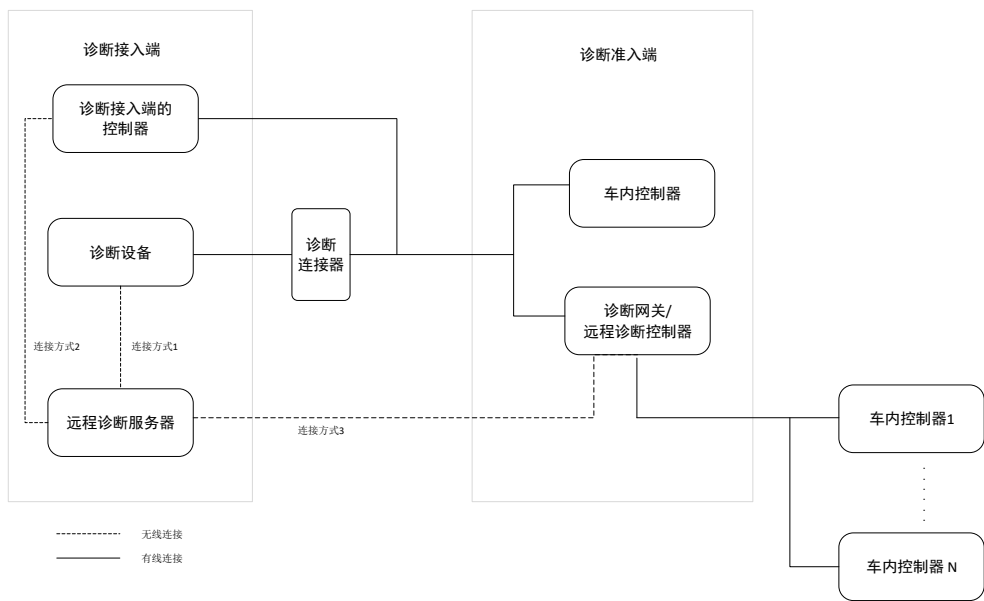


图 1 汽车诊断接口信息安全总体架构示例

根据不同诊断网络，典型诊断网络架构有如下几种：

- a) 诊断设备直接连接被诊断控制器：
——诊断设备通过诊断连接器与车内被诊断控制器物理点对点连接。
- b) 诊断设备非直接连接被诊断控制器：
——诊断设备与车内被诊断控制器不直接连接，而是通过诊断网关进行连接和诊断通信。
- c) 通过远程诊断服务器的远程诊断：
——通过远程诊断服务器向远程诊断控制器发起诊断任务，对车内被诊断控制器进行诊断。

5.2 诊断接入端

下列设备或服务可在诊断过程中归类为诊断接入端：

- a) 诊断设备：能够发起诊断请求的设备，从被诊断控制器获取诊断响应消息，对诊断响应消息进行处理后通过设备的人机界面向用户显示诊断结果。例如：
——用于研发阶段控制器参数标定的标定设备；
——用于生产线下线检测的 EOL 设备；
——用于售后维修服务的售后诊断仪；
——用于 OBD 排放故障检测的检测设备（OBD-II Scan Tool）等。
- b) 远程诊断服务器：能够通过远程联网的方式向车辆提供诊断任务并对诊断任务进行管理、监控，显示车辆诊断任务的执行情况，接收和处理车辆上报的诊断数据并解析和转换为用户可读的语言，同时还可以对数据进行统计分析。
- c) 诊断接入端的控制器：集成诊断客户端功能的车内控制器，具有发起诊断服务的功能，具有类似于诊断设备的功能，该控制器一般为诊断网关或者远程诊断控制器。

5.3 诊断准入端

下列设备可在诊断过程中归类为诊断准入端：

- a) 诊断网关控制器：当执行身份认证或权限控制时，诊断网关控制器作为诊断准入端；

- b) 远程诊断控制器：当远程诊断服务器作为诊断接入端发送诊断请求时，执行身份认证或权限控制的远程诊断控制器作为诊断准入端；
- c) 被诊断控制器：执行身份认证或权限控制的被诊断控制器作为诊断准入端。

6 技术要求

6.1 诊断接口信息安全身份认证和权限控制技术要求

6.1.1 身份认证及权限控制

通过诊断接入端和诊断准入端的身份认证或权限控制实现汽车诊断接口的信息安全，诊断准入端通过身份认证或权限控制结果为诊断接入端开放不同的访问权限：

- a) 按照 7.1.1 a) 进行试验，诊断准入端应支持为诊断接入端开放不同的访问权限；
- b) 按照 7.1.1 b) 进行试验，诊断准入端应支持对诊断接入端进行身份认证或权限控制；
- c) 按照 7.1.1 c) 进行试验，诊断接入端宜支持对诊断准入端进行身份认证。

6.1.2 身份认证算法

6.1.2.1 基于对称加密算法的认证技术要求

应满足以下要求：

- a) 按照 7.1.2.1 a) 进行试验，使用对称加密算法的身份认证过程，加密算法应选择 SM4 或 AES128 及以上强度算法；
- b) 按照 7.1.2.1 b) 进行试验，使用对称加密算法的身份认证过程，对称密钥应具备更新途径。

6.1.2.2 基于非对称加密算法的认证技术要求

按照 7.1.2.2 进行试验，使用非对称加密算法的身份认证过程，加密算法应选择 SM2、RSA2048 或 ECC256 及以上强度算法。

6.1.2.3 摘要算法要求

按照 7.1.2.3 进行试验，进行摘要计算时，算法应选择 SM3 或 SHA256 及以上强度算法。

6.2 诊断接入端信息安全技术要求

6.2.1 安全存储

按照 7.2.1 进行试验，诊断接入端应对身份认证使用的对称密钥、非对称算法私钥进行防篡改保护。

6.2.2 数据使用

应满足以下要求：

- a) 按照 7.2.2 a) 进行试验，诊断接入端应对身份认证使用的对称密钥、非对称算法私钥进行访问控制，防止非法访问；
- b) 按照 7.2.2 b) 进行试验，用于身份认证的对称密钥、非对称算法私钥不应对外传输；
- c) 按照 7.2.2 c) 进行试验，对于非车内电子控制单元的诊断接入端，应具备安全访问控制。

示例：常见的安全访问控制措施包括账户登录、动态获取操作权限等。

6.2.3 密钥信息销毁

按照 7.2.3 进行试验，非车内电子控制单元的诊断接入端应具有密钥销毁机制，支持身份认证相关数据的销毁。

6.3 诊断准入端信息安全技术要求

6.3.1 控制器信息安全要求

6.3.1.1 安全存储

按照7.3.1.1 a)、b)进行试验，对于身份认证使用的对称密钥、非对称算法私钥信息，诊断准入端宜使用硬件安全存储机制。对于身份认证使用的身份信息（例如：准入端设备信息等），诊断准入端应进行防篡改防护。

6.3.1.2 权限控制

按照7.3.1.2 a)、b)进行试验，诊断准入端应基于身份认证实现对诊断接入端的权限控制。对于不同的诊断接入端应开放不同的权限，具体权限应由车辆厂商按照诊断功能设计自行定义，开放的功能宜仅用于诊断服务、软件升级等。

6.3.1.3 认证失败处理机制

按照7.3.1.3进行试验，诊断准入端应具备与诊断接入端身份认证失败的处理机制（例如：认证失败延时机制等）。

6.3.2 诊断接口物理安全要求

6.3.2.1 诊断接口物理连接要求

应满足以下要求：

- a) 按照 7.3.2.1 a)进行试验，车载诊断接口不宜连接其他非用于诊断的通讯总线；
- b) 按照 7.3.2.1 b)对于车载诊断接口连接的非通讯类硬线，应仅支持以下功能：
 - 接入端供电；
 - 法规/标准要求连接的硬线，例如：以太网激活线、回收点爆线等。

6.3.2.2 诊断接口通讯总线要求

按照7.3.2.2进行测试，与诊断接口连接的通讯总线，宜仅连接执行诊断准入端功能的电子控制单元。

6.3.3 车内诊断安全要求

6.3.3.1 诊断执行条件

应满足以下要求：

- a) 按照 7.3.3.1 a)进行试验，被诊断控制器应对行车安全相关诊断服务进行安全访问解锁；
- b) 按照 7.3.3.1 b)进行试验，每个被诊断控制器宜使用不同的安全访问密钥；
- c) 按照 7.3.3.1 c)进行试验，被诊断控制器在执行诊断写服务前，宜进行车辆状态检查（例如，车速等），状态条件不满足时，不应执行诊断服务。

示例：如车辆运行状态下执行诊断写服务可能对车辆正常运行和/或驾乘人员安全产生影响。

6.3.3.2 诊断应用场景及诊断权限要求

应满足以下要求：

- a) 按照 7.3.3.2 a)进行试验，应按照不同诊断用户对诊断服务划分应用场景（例如：开发、生产、售后、供应商零部件开发等）；
- b) 按照 7.3.3.2 b)进行试验，应通过安全访问划分诊断服务，实现不同诊断用户的权限分离；
- c) 按照 7.3.3.2 c)进行试验，诊断用户的权限设置应遵循最小化原则。

6.3.3.3 诊断解锁的信息安全要求

应满足以下要求：

- 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；
- b) 按照 7.3.3.3 b) 进行试验，未经安全访问解锁的条件下，车内网关或被诊断控制器应拒绝执行涉及行车安全相关功能暂时或永久禁用的诊断服务。

7 试验方法

7.1 诊断接口信息安全试验方法

7.1.1 身份认证及权限控制试验方法

应满足以下要求：

- a) 通过试验工具对诊断准入端分别发起不同权限的身份认证或访问请求，检查诊断准入端是否通过具有权限的请求，拒绝不具有权限的请求；
- b) 通过试验工具对诊断准入端发起访问请求，检查诊断准入端是否对该请求设备进行身份认证或权限控制；
- c) 使诊断接入端向试验工具发起访问请求，检查诊断接入端是否对该连接设备进行身份认证。

7.1.2 认证算法试验方法

7.1.2.1 基于对称加密算法认证技术要求的试验方法

应满足以下要求：

- a) 针对使用对称加密算法的身份认证，通过监测和解析诊断接入端和诊断准入端之间的身份认证报文数据，正向检查是否使用 SM4 或 AES128 及以上强度的加密算法；
- b) 检查对称密钥是否可以根据提供的密钥安全管理策略或使用场景需求进行更新。

7.1.2.2 基于非对称加密算法的认证技术要求的试验方法

针对使用非对称加密算法的身份认证，通过监测和解析诊断接入端和诊断准入端之间的身份认证报文数据，正向检查是否使用 SM2、RSA2048 或 ECC256 及以上强度的加密算法。

7.1.2.3 摘要算法试验方法

通过监测和解析诊断接入端和诊断准入端之间的身份认证报文数据，正向检查摘要算法是否使用 SM3 或 SHA256 及以上强度。

7.2 诊断接入端信息安全试验方法

7.2.1 安全存储试验方法

通过试验工具尝试修改或删除诊断接入端存储的身份认证使用的对称密钥、非对称算法私钥信息，检查其是否可以被篡改。

7.2.2 数据使用试验方法

应满足以下要求：

- a) 分别使用不同的用户身份对诊断接入端中存储的身份认证使用的对称密钥、非对称算法私钥进行访问，检查是否仅具有访问权限的用户可以成功访问，其他用户无法使用或访问；
- b) 监测解析诊断接入端发出的报文数据，检查数据中是否有身份认证涉及的对称密钥、非对称算法私钥的明文信息；

- c) 对于非车内电子控制单元的诊断接入端，检查是否仅具有访问控制的方式（例如：账户登录、动态获取操作权限等）。

7.2.3 密钥信息销毁试验方法

对于非车内电子控制单元的诊断接入端，检查是否其具有密钥销毁机制，可以销毁身份认证相关数据。

7.3 诊断准入端信息安全试验方法

7.3.1 控制器信息安全试验方法

7.3.1.1 安全存储试验方法

应满足以下要求：

- a) 审查信息安全设计相关文档，检查诊断准入端是否使用硬件安全存储机制存储身份认证使用的对称密钥、非对称算法私钥信息；
- b) 通过试验工具尝试访问、修改或删除诊断准入端的存储的身份认证使用的信息，检查其是否实现安全存储。

7.3.1.2 权限控制试验方法

应满足以下要求：

- a) 通过试验工具分别模拟不同的诊断接入端对诊断准入端发送诊断服务请求，检查诊断准入端是否对权限范围内的请求发送肯定响应，对非权限范围内的请求发送拒绝访问响应；
- b) 根据诊断服务设计文档，检查诊断准入端是否只开放了用于诊断和车载软件更新功能的服务。

7.3.1.3 认证失败处理机制试验方法

通过试验工具向诊断准入端发起无效的身份认证请求，检测诊断准入端是否有认证失败处理机制。

7.3.2 诊断接口物理安全试验方法

7.3.2.1 诊断接口物理连接试验方法

应满足以下要求：

- a) 审查诊断接口引脚定义文档，检查是否有非诊断用通信总线；
- b) 审查诊断接口各引脚定义文档，检查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。

7.3.2.2 诊断接口通讯总线试验方法

根据设计的网络拓扑图，检查诊断接口连接的通信总线是否仅有具备诊断接入端功能的电控单元。

7.3.3 车内诊断安全试验方法

7.3.3.1 诊断执行条件试验方法

应满足以下要求：

- a) 通过试验工具向车内被诊断控制器发起行车安全相关诊断服务请求，检查该控制器是否进行安全访问解锁；
- b) 通过试验工具使用被诊断控制器对应的密钥发起安全访问请求，检查被诊断控制器是否通过安全访问，以及不同的被诊断控制器是否使用不同的密钥；
- c) 审查诊断服务设计文档，检查是否设置诊断服务执行前合理性条件检查，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，检查是否发送否定响应。

7.3.3.2 诊断应用场景及诊断权限试验方法

应满足以下要求：

- a) 审查诊断服务设计文档，检查诊断服务定义是否按照不同诊断用户划分应用场景。通过试验工具向被测样件发送不符合应用场景的诊断服务请求，检查是否发送否定响应；
- b) 审查诊断服务设计文档，检查诊断服务是否定义对应的安全访问等级。通过试验工具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；
- c) 通过试验工具使用不同诊断用户权限分别发起诊断请求，检查其访问权限是否满足最小权限原则。

7.3.3.3 诊断解锁的信息安全要求试验方法

应满足以下要求：

- a) 通过试验工具向被测样件发送行车安全相关功能的诊断写服务请求，检查被诊断控制器处于未安全解锁状态接收到该请求报文后是否无响应或发送否定响应；
 - b) 通过试验工具在未经安全访问解锁的条件下向车内网关或被诊断控制器发起能够使车辆行车安全相关的功能暂时和/或永久丧失的诊断服务请求，检查被测样件是否无响应或发送否定响应。
-