

ICS 43.020
CCS T40



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 44778-2024

**Technical requirements and test methods for cybersecurity of
vehicle diagnostic interfaces**

汽车诊断接口信息安全技术要求及试验方法

Issued on: October 26, 2024

Implemented on: October 26, 2024

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
4 Diagnostic interface architecture
5 Technical requirements...
5.1 General requirements
5.1.2 Authentication algorithm
5.4 Physical connection security requirements
6 Test methods
6.1 Test methods for diagnostic interface information security
6.1.2 Test methods for identity authentication algorithms
6.2 Test methods for information security of diagnostic access units
6.3 Test methods for information security of diagnostic access authentication unit
6.3.1 Test methods for controller information security

1 Scope

GB/T 44778-2024 sets the cybersecurity requirements for vehicle diagnostic interfaces and the methods of testing them. The OBD port is the one deliberate opening into a modern car's internal networks, and it was designed in an era when physical access implied authorisation: through it a device can read and write ECU memory, run routines that move the steering and brakes, and reflash firmware. It is also the port into which fleet trackers, insurance dongles and aftermarket adapters are plugged permanently, several of which carry their own cellular modem. The standard specifies the diagnostic interface security architecture and the technical requirements - the authentication of the tester, the authorisation of diagnostic services, the protection of the communication, the handling of security access and the logging of what was done - and describes the corresponding test methods, with an informative annex giving examples of common diagnostic interface architectures. It applies to M and N category vehicles and took effect on 26 October 2024.

This document specifies the information security architecture and information security technical requirements for vehicle diagnostic interfaces. It describes the corresponding test methods. This document is applicable to M and N category vehicles.

2 Normative references

This document has no normative references.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 diagnostic access unit A device, platform or electronic control unit capable of initiating diagnostic services for a vehicle.

3.2 diagnostic access authentication unit An electronic control unit in a vehicle that processes or responds to diagnostic requests from a diagnostic access unit and determines whether the diagnostic access unit meets the requirements for identity authentication or permission control.

3.3 diagnostic connector A connector used for communication between vehicles and external diagnostic equipment, short-term connection, and can be plugged and unplugged under power. NOTE. It includes a vehicle-side connector socket and an external device-side connector plug. [Source: GB/T 34589-2017, 3.1, modified]

3.4 diagnosed controller An electronic control unit that responds to a diagnostic request message sent by a diagnostic access unit and sends a diagnostic response message to the diagnostic access unit.

3.5 diagnostic gateway An electronic control unit connected between the diagnostic network and the diagnostic subnet to forward and transmit diagnostic request and response messages. NOTE. The diagnostic gateway exchanges diagnostic messages between vehicle subnets by converting the formats of different network protocols between master and slave nodes.

3.6 remote diagnosis controller An electronic control unit with the ability to connect and communicate with a diagnostic server.

3.7 diagnostic interface An interface that connects the diagnostic access unit and the diagnostic access terminal and provides diagnostic services between them.

4 Diagnostic interface architecture

4.1 Overall architecture The automotive diagnostic interface architecture is reflected in different diagnostic network forms. The diagnostic access unit and the diagnostic access authentication unit are important components of the vehicle diagnostic interface architecture. The overall architecture of the vehicle diagnostic interface is shown in Figure 1. Examples of common vehicle diagnostic interface architectures are shown in Annex A. Based on the classification of different diagnostic network architectures, the following are typical diagnostic network architectures.

a) Physical diagnostic interface architecture. the diagnostic device is physically connected

to the diagnostic gateway or the diagnosed controller through a

- b) Remote diagnosis controller. when the remote diagnosis server sends a diagnosis request as a diagnosis access unit, the remote diagnosis controller performs identity authentication or permission control;
- c) Diagnosed controller. the diagnosed controller that performs identity authentication or permission control.

5.1 General requirements

5.1.1 Identity authentication and permission control Meet the following requirements.

a) Conduct the test according to

6.1.1 a). The diagnostic access authentication unit should support opening different access rights for the diagnostic access unit;

b) Conduct the test in accordance with

6.1.1 b). The diagnostic access authentication unit should support identity authentication or permission control for the diagnostic access unit;

c) Conduct the test in accordance with

6.1.1 c). The diagnostic access unit should support identity authentication of the diagnostic access authentication unit.

5.1.2 Authentication algorithm

5.1.2.1 Technical requirements for authentication based on symmetric encryption algorithms Meet the following requirements.

a) Conduct the test in accordance with

6.1.2.1 a). Use a symmetric encryption algorithm for identity authentication. The encryption algorithm should be SM4, AES128, or an algorithm of equivalent strength or higher.

b) Conduct the test in accordance with

6.1.2.1 b). Use a symmetric encryption algorithm for identity authentication. The symmetric key should have a way to update it.

5.1.2.2 Authentication technology requirements based on asymmetric encryption algorithms Conduct the test in accordance with 6.1.2.2. Use an asymmetric encryption algorithm for identity authentication. The encryption algorithm should be SM2, ECC256, or an algorithm of equivalent strength or higher, or an RSA algorithm with a data length of at least 2048 bits.

a) Conduct the test in accordance with

6.3.2.2 a). Access rights to diagnostic services should be divided according to different diagnostic users (e.g., development, production, after-sales, supplier parts development, etc.). Diagnostic services should be grouped by secure access to achieve separation of permissions for different diagnostic users;

b) Conduct the test in accordance with

6.3.2.2 b). The authority setting of the diagnostic user shall follow the principle of minimization defined by the vehicle manufacturer.

5.4 Physical connection security requirements

5.4.1 Physical connection requirements for the diagnostic connector Meet the following requirements.

a) Conduct the test in accordance with

6.4.1 a). The on-board diagnostic connector should not be connected to other communication buses not used for diagnosis;

b) Conduct the test in accordance with

6.4.1 b). For non-communication hard lines connected to the on-board diagnostic connector, only the following functions should be supported. 1) Power supply for the diagnostic access unit; 2) Hard-wired connections required by regulations and standards (e.g., Ethernet activation cable, recovery detonation cable, etc.).

5.4.2 Communication bus requirements for diagnostic connectors Conduct the test in accordance with 6.4.2. The communication bus connected to the on-board diagnostic connector should only be connected to the electronic control unit that performs the functions of diagnostic access authentication unit.

6.1 Test methods for diagnostic interface information security

6.1.1 Test methods for identity authentication and authority control Carry out the test in the following order.

a) Use the test tool to initiate identity authentication or access requests with different permissions to the diagnostic access authentication unit. Check whether the diagnostic access authentication unit passes the request with permission. Reject the request without permission;

b) Initiate an access request to the diagnostic access authentication unit through the test tool. Check whether the diagnostic access authentication unit performs identity authentication or permission control on the requesting device;

c) Initiate an access request to the test tool through the diagnostic access unit. Check whether the diagnostic access unit authenticates the test tool.