

ICS 35.030
CCS M 10



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

GB/T 47467-2026

**Specification for the security management interface of the
internet of vehicles**

车联网安全管理接口规范

Issued on: April 30, 2026

Implemented on: November 1, 2026

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

Table of Contents

- 2 Normative references
- 4 Internet Protocol version 4 IPv
- 5 Interface Implementation Methods
 - 5.2 Communication Transmission Requirements
 - 5.3 Data Interaction Process
- 6 Internet Protocol version 6
 - 6.1 Data Reporting Interface
 - 6.2 Command Interaction Interface
- 7 Data Reporting Interface Information Format
 - 7.1 Basic Resource Data for Vehicle-to-Everything (V2X)
 - 7.1.2 Vehicle Networking Platform Information
 - 7.3 Network Security Data for Vehicle-to-Everything (V2X)
- 8 Command Interaction Interface Information Format
 - 8.1 Issuance of Commands
 - 8.1.1 Monitoring Instructions
- 9 Interface Verification Methods
 - 9.2 Verification Principles
 - 9.3 Verification Scenarios
 - 9.3.1 Verification Scenario for Reporting Interface Functionality
 - 9.3.2 Interface Communication Verification Scenarios
 - 9.3.3 Command Interaction Interface Verification Scenario

2 Normative references

This document has no normative references.

4. Abbreviations The following abbreviations apply to this document. CNNVD. China National Vulnerability Database of Information Security CNVD. China National Vulnerability Database CVE. Common Vulnerabilities and Exposures FTP. File Transfer Protocol HTTPS. Hypertext Transfer Protocol Secure ICP. Internet Content Provider IDC. Internet Data Center JSON. JavaScript Object Notation NVDB. National Vulnerability Database, a cybersecurity threat and vulnerability information sharing platform. OTA (Over-The-Air) download SFTP. Secure File Transfer Protocol TCP. Transmission Control Protocol TLS. Transport Layer Security UDP. User Datagram Protocol URL. Uniform Resource Locator UTF

8.Variable Length Encoding (8-bit Unicode Transformation Format) VIN. Vehicle Identification Number IP. Internet Protocol IPv

5 Interface Implementation Methods

5.1 Interface Requirements Figure 1 shows a schematic diagram of the vehicle-to-everything (V2X) security management interface. The V2X security management interface includes a data reporting interface and a command interaction interface. The data reporting interface is the channel through which the enterprise-side platform reports data to the national-side platform, while the command interaction interface is the channel between the national-side platform and the enterprise-side platform. The platform's command interaction channel. The command interaction interface is used for data reporting, and should be implemented through different message queues. Currently, data should be transmitted via a secure channel and encrypted.

5.2 Communication Transmission Requirements

5.2.1 Data Reporting Frequency Data should be filled in completely according to the information format described in Chapter 7, and transmitted according to the reporting frequency requirements. The submission of various types of data... The reporting frequency requirements are as specified in Tables 1 and 2.

5.2.2 Data Encoding Format Requirements The data encoding format requirements are as follows:

- a) Data reported by enterprise-side platforms and data distributed by national-side platforms should uniformly use UTF-8 encoding;
- b) Enterprise-side platforms and national-side platforms should use JSON format for data interaction.

5.2.3 Data Security Requirements Data security requirements are as follows:

- a) Enterprise-side platforms and national-side platforms should uniformly use secure communication protocols of TLS 1.2 or higher, or at least equivalent security level. To establish a secure communication connection, TLS certificates should uniformly be those issued by the national platform.
- b) Data reporting from enterprise-side platforms and data distribution from national-side platforms should be conducted using commercial cryptography that conforms to national standards. The encryption algorithm key is generated and provided by the national platform, while each enterprise platform has its own unique key.
- c) Sensitive information such as VIN, longitude, and latitude should be uploaded after security processing without affecting business operations;

- d) Malicious files, traffic files, and evidence files on the enterprise-side platform should be reported to the national-side platform via SFTP. SFTP authentication keys are produced and provided by the national platform, while each enterprise platform has its own unique key.
- e) The confidentiality and integrity of sensitive data such as certificates and keys should be ensured during transmission;
- f) Sensitive data such as certificates and keys should be stored in a secure and trusted storage space.

5.3 Data Interaction Process

5.3.1 Data Reporting The data reporting process is shown in Figure 2, and the requirements are as follows:

- a) Enterprise-side platforms should report data to the national-side platform through data reporting interfaces;
- b) After receiving and parsing the data, the national platform performs data verification to check for errors in the data format. If errors are found, the data verification should fail. The information is sent to the enterprise-side platform;
- c) After receiving a data verification failure message, the enterprise-side platform should ensure that the data meets the requirements before re-uploading.

5.3.2 Command Interaction The instruction interaction process is shown in Figure 3, and the requirements are as follows:

- a) Command information generated by the national platform should be sent to the enterprise platform through the command interaction interface;
- b) When an enterprise-side platform executes instructions, the data generated during the execution process should be reported to the national-side platform (maximum single file size 512MB, if...). If the file size exceeds the limit, it should be split into multiple files for uploading.
- c) During the execution of instructions on the enterprise-side platform, the execution status should be reported to the national-side platform regularly in accordance with the requirements of 8.3.2.

6.1 Data Reporting Interface

6.1.1 Basic Resource Data for Vehicle-to-Everything (V2X) After adding or updating basic vehicle-to-everything (V2X) resource data locally, the enterprise-side platform should report the added or updated data to the national-side platform. Taiwan's basic telecommunications operators should report data including enterprise entity information, while

vehicle-to-everything (V2X) related enterprises should report data including enterprise entity information. Information such as vehicle networking platform information and basic vehicle information.

6.1.2 Networked vehicle operating status data Enterprise-side platforms of connected car manufacturers should promptly report the operational status data of connected vehicles to the national platform.

6.1.3 Vehicle Network Security Data Basic telecommunications operators' enterprise-side platforms should promptly report vehicle-to-everything (V2X) related security data to the national platform, including malicious programs. Information such as sequence information and network attack information. Enterprises involved in the Internet of Vehicles (IoV) should promptly report security data related to their IoV platforms and connected vehicles to the national platform. The platform includes information on malicious programs, cyberattacks, and security vulnerabilities.

6.2 Command Interaction Interface

6.2.1 Issuance of Commands The national platform can generate monitoring instructions and communication log query instructions as needed and send them to the enterprise platform.

6.2.2 Command Status Feedback After receiving monitoring instructions and communication log query instructions from the national platform, the enterprise-side platform should report the execution of the instructions to the national platform. Row status.

6.2.3 Command Result Feedback After receiving monitoring instructions and communication log query instructions from the national platform, the enterprise-side platform should report the execution of the instructions to the national platform. Result.

7.1 Basic Resource Data for Vehicle-to-Everything (V2X)

7.1.1 Enterprise Entity Information Basic telecommunications operators' enterprise-side platforms should report the information of the enterprise entities providing services to the national platform, including information on vehicle-to-everything (V2X) related enterprises. Enterprise-side platforms should report their corporate information to the national platform. Corporate information includes the company name, major industry category, and sub-industry category. Information such as category, registered province, and reporting time is shown in Table 3.

7.1.2 Vehicle Networking Platform Information

7.1.2.1 Basic Information of the Vehicle Networking Platform Enterprise-side platforms of companies involved in vehicle networking should report basic information about their vehicle networking platforms to the national platform, including the platform name and the