

ICS 35.030

CCS M 10



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

GB/T 47325-2026

**Security technical requirements and test methods for
over-the-air updates in the internet of vehicles**

车联网在线升级安全技术要求与测试方法

Issued on: March 31, 2026

Implemented on: October 1, 2026

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

Table of Contents

Foreword...	3
1 Scope...	4
2 Normative references...	4
3 Terms and definitions...	4
4 Abbreviated terms...	6
5 Internet of vehicles over-the-air update architecture...	6
6 Security technical requirements...	7
6.1 Update package...	7
6.2 Internet of vehicles over-the-air update platform...	8
6.3 Communication link...	9
6.4 Over-the-air update applications...	10
7 Test methods...	11
7.1 Update package security testing...	11
7.2 Internet of vehicles over-the-air update platform security testing...	12
7.3 Communication link security testing...	14

1 Scope

GB/T 47325-2026 is the Chinese national standard covering updating a car over the air without opening a way in - the signing and verification of the package, the protection of the transfer, the conditions under which an update may be installed, the rollback and the record of what a vehicle is running. First edition, in force since 1 October 2026, with GB/T 47324-2026 on platform security. It was issued on 31 March 2026 and takes effect on 1 October 2026, as a first edition. This page is published from the official record of the 2026 edition; the clause text of a standard this recent is not yet in circulation, and the figures, limits and tables it contains are those of the document itself, delivered in full with the English translation.

This document specifies the security technical requirements related to over-the-air update packages, over-the-air update platforms, communication links, and over-the-air update applications during the over-the-air update process of internet of vehicles, and describes the corresponding test methods. This document is applicable to guiding the security design, research and development, testing, and operation of internet of vehicles over-the-air update platform, communication links, and over-the-air update applications.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 25069-2022, Information security techniques - Terminology

GB/T 39412-2020, Information security technology - Audit specification of code security

GB/T 47324-2026, Cyber security protection requirements for internet of vehicles platform

YD/T 2359-2011, Terminal technical requirement for download over the air YD/T 2910-2015,

Technical requirements of LTE/SAE security YD/T 4958-2024, 5G mobile telecommunication network - Technical requirement of 5G security (Phase 2)

3 Terms and definitions

For the purposes of this document, the following terms and definitions, as well as those given in GB/T 25069-2022, apply.

3.1 over-the-air update; OTA update Software update that is transferred to the vehicle wirelessly rather than using cables or other local connections.

Note 1. "Over-the-air update" is also called "remote update".

Note 2. "Local connection" generally refers to the physical connection made through the on-board diagnostics (OBD) interface, universal serial bus (USB) interface, etc. [Source: GB 44496-2024, 3.3]

3.2 update package Software package used for software update. [Source: GB 44496-2024, 3.6]

3.3 internet of vehicles over-the-air update platform Information system or platform that collects, stores, uses, processes, and provides data and related equipment data generated during the over-the-air update service of non- commercial motor vehicles (excluding special-purpose vehicles) during the operation phase, as well as system or platform that aggregates and manages the aforementioned data in a unified manner. Note

1. Motor vehicles refer to wheeled vehicles that are driven or towed by a power unit and travel on roads for the purpose of carrying passengers or goods or carrying out special engineering operations. They do not include combination vehicles, motorcycles, wheeled special machinery vehicles, trailers, trolley buses, trams, tractors and tractor transport units, nor do they include motorized wheelchairs for the disabled and electric bicycles that meet the relevant national standards in terms of maximum design speed, unladen mass, and external dimensions, even if they have a power unit. Note

2. Special-purpose vehicles include police vehicles, fire trucks, ambulances, engineering

rescue vehicles, and other vehicles used for special transportation tasks or special operations, as well as other special purposes.

3.4 smart mobile terminal A terminal that can access the mobile communication network, has an operating system that provides application programmers development interfaces, and has the ability to install, load, and run application software. [Source: YD/T 3228-2023, 3.4]

3.5 vehicle smart mobile terminal An electronic device installed in a vehicle, equipped with computing, storage, and input/output interfaces, and capable of supporting over-the-air update applications.

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply. CAVD. China Automobile Vulnerability Database NVDB. National Vulnerability DataBase TLCP. Transport Layer Cryptography Protocol TLS. Transport Layer Security 4G. 4th Generation Mobile Communication Technology 5G. 5th Generation Mobile Communication Technology

5 Internet of vehicles over-the-air update architecture

The internet of vehicles over-the-air update architecture is shown in Figure 1, mainly including over-the-air update packages, over-the-air update platforms, communication links, and over-the-air update applications. The internet of vehicles over-the-air update platform is responsible for over-the-air update process management, update package and source code storage, update package encryption, signature and verification, etc.; the communication link is responsible for identity authentication, command interaction, update package and related data transmission between the internet of vehicles over-the-air update platform and the over-the-air update application; the over-the-air update application is responsible for over-the-air update requests and confirmations, update package download and reception, update package decryption and verification, update process execution, update interactive operations, etc. Figure 1 - Over-the-air update architecture diagram

6 Security technical requirements

6.1 Update package The detailed requirements are as follows:

- a) It shall have mechanisms to protect authenticity and integrity;
- b) It shall not contain hard-coded sensitive information (e.g. private keys) or code debugging information;
- c) The update package shall be checked for hidden debugging interfaces to ensure it does not contain debugging sections, symbol tables, or similar content.
- d) Debugging interfaces and debugging log outputs shall be disabled by default;

e) It shall not contain any unremediated vulnerabilities rated as high severity or above that have been disclosed more than six months earlier by authoritative vulnerability platforms.

Note

1.The vulnerability risk severity levels are specified in relevant national standards such as GB/T 30279. Note

2.Authoritative vulnerability platforms include National Vulnerability DataBase (NVDB), China Automobile Vulnerability Database (CAVD), which are recognized by the competent authorities.

f) It should incorporate code protection mechanisms, such as anti-decompilation measures;

g) It should undergo code security audit and comply with the requirements specified in GB/T 39412-2020.

6.2 Internet of vehicles over-the-air update platform

6.2.1 General requirements The detailed requirements are as follows:

a) It shall comply with the Level 3 security-related requirements specified in GB/T 47324-2026.

b) It shall verify the authenticity of update packages and associated files (e.g. update package release notes).

c) It shall verify the integrity of update packages and associated files (e.g. update package release notes), and shall provide timely alerts when integrity is compromised.

d) It shall be capable of verifying the authenticity of the identity of over-the-air update applications to prevent spoofed over-the-air update applications from obtaining update packages and associated files. If verification of the authenticity of an over-the-air update application's identity fails, it shall promptly terminate the service response and record the abnormal information.

6.2.2 Access control The detailed requirements are as follows:

a) An access control mechanism shall be set up to configure access control policies for update packages on the internet of vehicles over-the-air update platform and prevent unauthorized access to update packages;

b) A privilege separation mechanism shall be set up to allow for independent update and operation permissions for different vehicle models and different update packages, thereby preventing unauthorized updates;

c) A security management and control mechanism shall be provided to configure account and session policies and mitigate the risks of privilege abuse and insufficient traceability;

d) Different update permissions should be assigned to different vehicles to prevent