

ICS 43.020
CCS T 04



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

GB/T 47001-2025

**General specification for the digital identity and authentication
of intelligent and connected vehicles**

智能网联汽车数字身份及认证通用规范

Issued on: December 31, 2025

Implemented on: July 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...	5
4 Abbreviations...	5
5 Digital Identity Encoding...	6
6 Carrier...	6
6.1 Without External Power Supply...	6
6.2 With External Power Supply...	6
7 Identity Authentication...	7
7.1 General Requirements...	7
7.2 Symmetric Encryption Algorithm-based Mechanism...	8
7.3 Digital Signature Technology-based Mechanism...	8
8 Test Methods...	8
8.1 Test Conditions...	8
8.2 Test Configuration...	9
8.3 Test without External Power Supply...	9

1 Scope

GB/T 47001-2025 is the Chinese national standard covering the cryptographic identity of a vehicle - how a car proves to the infrastructure, to other vehicles and to its manufacturer's cloud that it is the vehicle it claims to be, with the certificates, their lifecycle and the privacy problem of an identity that can also be used to track. First edition, under the Ministry of Public Security, with the traffic facility identity standard GB/T 46999-2025. It was issued on 31 December 2025 and has been in force since 1 July 2026, as a first edition. The document is under the responsibility of the Ministry of Public Security. This page is published from the official record of the 2025 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 requirements for digital identity encoding, carrier and authentication of intelligent and connected vehicles, and describes the corresponding test methods. This document applies to the design of digital identity authentication processes and the development and testing of the carrier of intelligent and connected vehicles.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 2423.1 Environmental Testing for Electric and Electronic Products - Part

3 Terms and Definitions

The following terms and definitions are applicable to this document.

3.1 digital identity of intelligent and connected vehicle A combination of numbers and letters that associate vehicle attribute information and uniquely identify a vehicle in an Internet of Vehicles application environment.

3.2 carrier of digital identity A chip or module used to store the digital identity, keys, digital certificates and vehicle attribute information of an intelligent and connected vehicle, possessing authorized access mechanisms and cryptographic operation functions.

3.3 registration identity certificate A digital certificate used to identify and prove the legitimacy of the digital identity of an intelligent and connected vehicle operating on the road.

3.4 V2X enrolment certificate A digital certificate that is used to prove the legitimacy of an identity during the V2X pseudonym certificate application process.

3.5 V2X pseudonym certificate A digital certificate that is used to prove the legitimacy of an identity during V2X communication and to anonymize the identity.

4 Abbreviations

The following abbreviations are applicable to this document. CA. Certificate Authority EAL. Evaluation Assurance Level GPIO. General-Purpose Input/Output OBU. On Board Unit OID. Object Identifier USB. Universal Serial Bus V2X. Vehicle to Everything

5 Digital Identity Encoding

The digital identity of intelligent and connected vehicles (hereinafter referred to as digital identity) consists of OID encoding, vehicle identification number, vehicle type, and vehicle usage nature. The encoding rules shall comply with the requirements of Appendix A.

6 Carrier

6.1 Without External Power Supply It shall comply with the requirements of GB/T 35789.1.

6.2.1 Classification and basic requirements

6.2.1.1 In accordance with whether V2X communication applications are supported, it is classified into Class I and Class II.

6.2.1.2 Class I carriers shall meet the following requirements.

- a) Support registration identity applications and more than two extended applications.
- b) Digital signature count is greater than or equal to 100 times per second, and digital signature verification count is greater than or equal to 200 times per second.
- c) Encryption/decryption throughput is greater than or equal to
- d) Total storage capacity is greater than or equal to 512 kB. The capacity of the registration identity application storage area is greater than or equal to 128 kB, and the capacity of each extended application storage area is greater than or equal to 64 kB.

6.2.1.3 Class II carriers shall meet the following requirements.

- a) Support registration identity applications, V2X communication applications, and at least one extended application.
- b) Digital signature count is greater than or equal to 100 times per second, and digital signature verification count is greater than or equal to 2,500 times per second.
- c) Encryption/decryption throughput is greater than or equal to
- d) Total storage capacity is greater than or equal to 512 kB. The capacity of the registration identity application storage area is greater than or equal to 128 kB, the capacity of the V2X communication application storage area is greater than or equal to 128 kB, and the capacity of the extended application storage area is greater than or equal to 64 kB.

6.2.2 Physical properties The following requirements shall be met.

- a) Ambient operating temperature. 40 C ~ 105 C;
- b) Data retention time is greater than or equal to 20 years;

7 Identity Authentication

7.1 General Requirements The following requirements shall be met.