ICS 35.240.60
CCS L 73

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 44130.5-2025

Charging and battery swap service information exchange for electric vehicles - Part 5: Data transmission and security

电动汽车充换电服务信息交换 第5部分：数据传输及安全

Issued on: August 29, 2025 **Implemented on: March 1, 2026**

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

Table of Contents

1 Scope

This document specifies the data transmission and security requirements for the charging and battery swap service information exchange for electric vehicles, including authentication requirements, data transmission security requirements, and data transmission communication requirements for charging and battery swap service information exchange.

This document applies to charging and battery swap service information exchange between charging and battery swap service platforms of different operators, information exchange between electric vehicle charging and battery swap service platforms and third-party services and management platforms, and information exchange between charging and battery swap equipment within the charging and battery swap infrastructure and charging and battery swap service platforms. Other parts of the charging and battery swap infrastructure may refer to this document for further information.

2 Normative References

GB/T 9387.1

GB/T 17901.1-2020

1 Framework

GB/T 19027 Quality Management - Guidance on Statistical Techniques for GB/T 19001-2016 GB/T 19596 Terminology of Electric Vehicles GB/T 20271 Information Security Technology - Common Security Techniques Requirement for Information System GB/T 22239-2019 Information Security Technology - Baseline for Classified Protection of Cybersecurity

3.1 Terms and Definitions

The terms and definitions defined in GB/T 19596, GB/T 25056, GB/T 25069, GB/T 29317, GB/T 44130 and GB/T 19027, and the following are applicable to this document.

3.1.1 Platform authentication

The process of verifying the legitimacy of a platform's identity to ensure its trustworthiness, security and reliability.

3.1.2 Distributed authentication

An authentication process conducted collaboratively across multiple nodes or systems to improve the system's trustworthiness, security and reliability.

3.1.3 Central exchange authentication

A mode where authentication services are provided by a unified authentication service provider.

NOTE. in this mode, the operator and the central authentication service provider negotiate and determine the operator identifier, operator key and message key. The authentication mode is jointly determined by each operator and the authentication service provider.

3.1.4 Symmetric encryption technique

A cryptographic technique that uses the same key for encryption and decryption.

[source. GB/T 25069-2022, 3.133]

3.1.5 Asymmetric cryptographic technique

A cryptographic technique that uses different keys for private key operations and public key operations. One key (public key) can be made public, while the other key (private key) shall be kept secret, and it is computationally infeasible to solve the private key from the public key.

[source. GB/T 25069-2022, 3.150, modified]

3.1.6 Certificate

Data about an entity, issued by a certification authority using its private key or secret key, and cannot be counterfeited.

[source. GB/T 25069-2022, 3.779]

3.1.7 Certificate verification

MAC. Message Authentication Code MQTT. Message Queuing Telemetry Transport NONCE. Number once PKCS. Public Key Cryptography Standards RFC. Request For Comments RSA. Rivest-Shamier-Adleman Algorithm SM2.SM2 cryptographic algorithm SM3.SM3 cryptographic algorithm SM4.SM4 cryptographic algorithm SN. Serial Number TLCP. Transport Layer Cryptographic Protocol TLS. Transport Layer Security VPN. Virtual Private Network

4.1 System Architecture

The process of charging and battery swap service information exchange for electric vehicles is a bidirectional exchange of data between electric vehicle charging and battery swap service platforms, and between charging and battery swap infrastructure and third-party services and management platforms. The system architecture for electric vehicle

charging and battery swap data transmission is shown in Figure 1.The transmitted data shall include the status information of the electric vehicle charging and battery swap infrastructure, user identity information, charging and battery swap operation records, etc. The main components of data transmission shall encompass the charging and battery swap infrastructure, charging and battery swap service platforms, third-party services and management platforms, and user client-side, etc. Data interaction between platforms or between platforms and facilities shall be conducted through specified interfaces, while maintaining confidentiality, integrity, availability and non- repudiation of data, and preventing the leakage of sensitive information.

NOTE. inter-platform information exchange includes the bidirectional exchange process between electric vehicle charging and battery swap service platforms and between charging and battery swap infrastructures and third-party services and management platforms. Platforms include charging and battery swap service platforms and third-party services and

5.1 Basic Requirements

The basic authentication requirements are as follows.

a) Charging and battery swap service information exchange for electric vehicles shall comply with the technical requirements for secure computing environment design specified in GB/T 25070-2019 and the requirements for secure communication network specified in GB/T 22239-2019.

b) The authentication requirements in this document shall include application layer authentication requirements between charging and battery swap infrastructure and charging and battery swap service platforms, and between charging and battery swap service platforms and third-party services and management platforms.

c) Platforms participating in the charging and battery swap service information exchange for electric vehicles shall have authentication service function. Before information exchange, platforms shall complete platform authentication to acquire the capability of secure data transmission. The basic requirements for data transmission security are as follows.

1) Both parties of information exchange shall adopt secure transmission protocols to ensure confidentiality, integrity and non-repudiation of data during transmission;

2) Authentication protocols shall employ an anti-replay attack mechanism and should use timestamps, sequence numbers, and other verification mechanisms to ensure the uniqueness of received valid messages;

3) The information exchange platform shall have access control policies to allow or deny users from establishing session connections based on user identity, access address, time range, and other security attributes;