

ICS 35.030
CCS L 80



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

GB/T 25068.6-2025

**Information technology - Security techniques - Network
security - Part 6: Securing wireless IP network access**

信息技术 安全技术 网络安全 第6部分：无线网络访问安全

(English Translation)

Issued on: December 2, 2025

Implemented on: July 1, 2026

Issued by: State Administration for Market Regulation

Table of Contents

Preface
Introduction
1 Scope
2 Normative References
3 Terms and Definitions
4 Abbreviations
5 Overview
5.1 Wireless Network Access Technology
5.2 Wireless Network Security Principles
6 Security Threats
6.1 Overview
6.2 Unauthorized Access
6.3 Packet Sniffing
6.4 Malicious Wireless AP
6.5 DoS attack
6.6 Bluetooth Hijacking
6.7 Bluetooth Vulnerability Attack
6.8 Ad-hoc cyber threats
6.9 Other Threats
7 Security Requirements 6.
7.1 Overview
7.2 Confidentiality
7.3 Integrity
7.4 Availability
7.5 Identity Verification
7.6 Authorization
7.7 Verifiability
8 Safety Controls 7.
8.1 Wireless Security Policy
8.2 Encryption Control and Implementation
8.3 Integrity Assessment
8.4 Identity Verification

- 8.5 Access Control
- 8.6 Defense against DoS attacks
- 8.7 DMZ isolation
- 8.8 Vulnerability Management
- 8.9 Continuous Monitoring of Wireless Networks
- 9 Safety Design
 - 9.1 Safety Design Planning
 - 9.2 WLAN
 - 9.3 WMAN
 - 9.4 Bluetooth
 - 9.5 Other Wireless Technologies
- References

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents".

Drafting.

This document is Part 6 of GB/T 25068 "Information Technology Security Technology - Network Security". GB/T 25068 has been published.

The following section.

- Part 1: Overview and Concepts;
- Part 2: Guidelines for Cybersecurity Design and Implementation;
- Part 3: Threats, Design Techniques, and Controls for Network Access Scenarios;
- Part 4: Security Protection for Internet Communication Using Security Gateways;
- Part 5: Security Protection for Cross-Network Communication Using Virtual Private Networks;
- Part 6: Wireless Network Access Security;
- Part 7: Network Virtualization Security.

This document is modified to adopt ISO/IEC 27033-6:2016 "Information technology security techniques - Network security - Part 6: Wireless networks" Access security.

This document has undergone the following structural adjustments compared to ISO/IEC 27033-6:2016.

---Chapter 5 of ISO/IEC 27033-6:2016 has been deleted;

---Chapter 5 corresponds to Chapter 6 of ISO/IEC 27033-6:2016, where 5.1 and 5.2 are derived from ISO/IEC 27033-6:2016.

The content of Chapter 6 was broken down and organized;

Annex A of ISO/IEC 27033-6:2016 has been deleted.

The technical differences between this document and ISO/IEC 27033-6:2016, and the reasons therefor, are as follows.

---Added normative reference to GB/T 25069 (see Chapter 3), and removed the terms "wireless access point," "wireless base station," and "Bluetooth." "Home base station", "machine-to-machine", "power ratio", "wireless access network", "wireless network controller", "wireless network", "wireless ad hoc" "Wireless networks" and "wireless hotspots" (see ISO/IEC 27033-6:2016, 3.1-3.3, 3.5, 3.7-3.12) should be used to adapt to my country's national conditions and...

Chinese context;

---The description of wireless communication networks has been revised (see 5.1) to conform to the current state of technological development in my country and the needs of practical application scenarios;

---Changes were made to the WLAN-related technical aspects of the security design, including the addition of a WAPI security mechanism and modifications to the confidentiality and integrity protocols.

The document also outlines the security configuration of WLAN devices (see 9.2) to adapt to the published mandatory national standards and my country's national conditions;

---The Bluetooth-related technical content in the security design has been modified (see 9.4) to conform to the standardized document writing specifications in the Chinese context, adding...

Highly readable.

The following editorial changes have been made to this document;

---The abbreviations "AES", "BYOD", "3GPP", "CCM", "PEAP-GTC", "SIG", "TTLS", and "UEA1" have been removed.

The terms "WRAN" and "WWAN" have been expanded to include "2FA", "4G", "5G", "Ad-hoc", "RAP", and "WAP3" (see Chapter 4) to better suit various needs.

my country's national conditions;

---Packet sniffing (see 7.3 of ISO/IEC 27033-6:2016) and authentication (see ISO/IEC 27033-6:2016) have been removed.

The examples in section 8.5) are used to enhance the document's conciseness and readability;

---The headings of clauses 9.1, 9.5.1, and 10.1 in ISO/IEC 27033-6:2016 have been changed to conform to the standardization document formatting requirements in the Chinese context.

Write guidelines to enhance readability.

Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents.

This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260).

Introduction

The purpose of GB/T 25068 is to provide detailed guidance on security aspects for the management, operation, use, and interconnection of information system networks.

This standard is designed to facilitate the adoption of security-related personnel (e.g., cybersecurity personnel) within an organization to meet their specific needs. It consists of seven parts, each...

The main objectives are as follows.

---Part 1: Overview and Concepts. Defines and describes concepts related to cybersecurity and provides management guidance.

---Part 2: Guidelines for Cybersecurity Design and Implementation. Provides organizations with guidance on how to plan, design, and implement high-quality cybersecurity architectures.

Provide guidance.

---Part 3: Threats, Design Techniques, and Controls for Network Access Scenarios. This section lists specific threats, design techniques, and controls relevant to typical network access scenarios.

Body risk, design technology and control.

---Part 4: Security Protection for Internet Communication Using Security Gateways. Provides guidance on implementing, operating, monitoring, and auditing networks using security gateways.

Guidelines on safety control related issues.

---Part 5: Security Protection for Cross-Network Communication Using Virtual Private Networks. Defines the procedures for establishing secure connections using Virtual Private