

ICS 35.030
CCS L 80



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

GB/T 47679.1-2026

**Cybersecurity technology - Security requirements, test and
evaluation methods for quantum key distribution - Part 1:
Requirements**

网络安全技术 量子密钥分发的安全要求、测试和评估方法 第1部分：要求
(English Translation)

Issued on: May 25, 2026

Implemented on: December 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.
5 The theoretical aspects of the QKD protocol	
5.1 General Instructions	
5.2 Principle	
5.3 Classification	
5.4 Structure	
6 Implementation modules of the QKD protocol	
6.1 General Instructions	
6.2 External Interfaces of the QKD Module	
6.3 Internal Structure of the QKD Module	
6.4 The TOE range of the QKD module is 13.	
6.5 General Workflow of the QKD Module	
7 Security Issues Analysis of the QKD Module	
7.1 General Notes	
7.2 Safety Assumption	
7.3 Asset Analysis	
7.4 Threats to Traditional Network Components	
7.5 Threats to Quantum Optical Components	
8 Extended security function components implemented using QKD	
8.1 General Notes	
8.2 Extended Security Features for Trusted Path/Channel Class (FTP)	
9 Safety Function Requirements for QKD Modules	
9.1 General Notes	
9.2 General Requirements for Traditional Network Components in QKD Modules	
9.3 General Requirements for QKD Protocol Implementation	
9.4 General Requirements for Quantum Optics Components in QKD Modules	
10 Compliance Statements	

10.1 General Notes

10.2 Statement of Compliance with Security Issues

10.3 Statement of conformity to safety function requirements

Appendix A (Informative) Guidelines for the Preparation of Protection Profiles for QKD Modules

A.1 General Explanation

A.2 Protection Profile Introduction

A.3 Declaration of Conformity and Statement of Conformity

A.4 Security Issues

A.5 Safety Purpose

A.6 Extended Security Function Component Definitions

A.7 Safety Requirements

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 1 of GB/T 47679 "Security Requirements, Test and Evaluation Methods for Quantum Key Distribution in Network Security Technology".

GB/T 47679 has published the following parts.

---Part 1: Requirements;

---Part 2: Testing and Evaluation Methods.

This document is equivalent to ISO/IEC 23837-1:2023 "Information security - Security requirements, test and evaluation methods for quantum key distribution".

Part 1: Requirements.

The following minimal editorial changes have been made to this document.

---To align with existing standards, the standard's name has been changed to "Security Requirements, Testing, and Evaluation for Quantum Key Distribution in Cybersecurity Technology".

Methods Part 1: Requirements;

---To align with existing standards, Chapter 1 includes additional information clarifying the scope of this document.

---The URL for Chapter 3, the ISO and IEC terminology database, has been removed.

---To improve the readability of this document, the abbreviation FUN_KM has been added to Chapter 4.

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

GB/T 47679 "Security Requirements, Test and Evaluation Methods for Quantum Key Distribution in Network Security Technology" is based on GB/T 18336 (all parts).

Within the framework of (), the security requirements for quantum key distribution (QKD) are established, and corresponding testing and evaluation methods are given. This document mainly regulates A set of common baseline safety functional requirements (SFRs) for QKD modules was defined.

GB/T 47679 is proposed to consist of two parts.

---Part 1: Requirements. The aim is to establish a general framework for the security assessment of QKD modules and to provide a general basis for QKD modules.

Line SFR set.

---Part 2: Testing and Evaluation Methodology. The aim is to establish testing and evaluation methods for QKD security assessment, and to provide specific methods for...

The evaluation method for the QKD protocol, the quantum optical components in the QKD module, and the SFRs of traditional network components constituted by the test and evaluation system.

The assessment activities should be evaluated, and supplementary assessment activities should be provided to meet the security requirements of the corresponding assurance level QKD.

In theory, QKD is a technique for generating long symmetric keys using a pre-shared key, and its security does not depend on the attacker's computing power;

The generated key can then be used in cryptographic applications such as building secure communication channels.

Although the theoretical security of the QKD protocol has been proven under a strict security model (assuming that the communicating parties share a security key in advance) However, discrepancies between theoretical models and engineering implementations often occur at various stages of the QKD module's lifecycle. These discrepancies may lead to...

This has led to security vulnerabilities in actual QKD systems. Among these vulnerabilities, a serious side-channel attack has been identified and demonstrated in QKD hacking experiments.

There are some principle-based verification demonstrations. Like traditional cryptographic modules and network devices, the QKD module is expected to undergo rigorous testing before being deployed in practical applications.

Rigorous security testing and evaluation are conducted to prevent information leakage risks caused by security attacks. Before QKD gained widespread industry recognition, meticulous and rigorous [security measures] were implemented.

A safety assessment is an essential step.

To this end, GB/T 47679 provides QKD module manufacturers with strict and unified safety specifications. manufacturers can develop QKD-based products in accordance with these specifications.

This technology enables IT products to be evaluated and assessed by assessors, thereby effectively reducing the risk of security function failures during QKD system operation.

The risks involved. This document adopts the standardized model and description language in GB/T 18336 (all parts), and specifies the general requirements for QKD modules.

Using a baseline SFR set, this paper covers the full implementation of QKD protocols, from traditional network components to quantum optical components. Appendix A provides QKD...

The protection profile development guidelines for the module. Part 2 of GB/T 47679 specifies the requirements for the QKD module to achieve the expected assessment protection level.

Specific safety assessment activities.

Note: This document describes the Extended Security Features (ESF) components (see 8.2) and SFRs (see Chapter 9) in terms of security feature families, component structure, and text format (i.e., bold and bold text).

The bold text and other aspects are consistent with the safety function components in GB/T 18336.2-2024, and these styles are in accordance with the conventions of GB/T 18336.2-2024.

This description is provided to distinguish certain terms from other text. This descriptive approach facilitates understanding for users familiar with GB/T 18336 (all parts).

Evaluation documentation for the QKD module is prepared using extended security features components and SFRs.

Quantum key distribution, a network security technology Safety requirements, testing and