ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 19771-2025

Replacing GB/T 19771-2005

Cybersecurity technology - Public key infrastructure - Specification for minimum interoperability for PKI components

网络安全技术 公钥基础设施 PKI组件最小互操作规范

Issued on: August 1, 2025 **Implemented on: February 1, 2026**

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

Table of Contents

Preface III
1 Scope 1
2 Normative references 1
3 Terms and Definitions 1
4 Abbreviations 2
5 Minimum interoperability basic functional requirements 3
5.1 Overview 3
5.2 CA System 3
5.3 RA System 4
5.4 Certificate Holder 5
5.5 Certificate Verifier 5
5.6 Cryptographic Algorithms 6
6 Interoperability Transaction Data Format Requirements 6
6.1 General Requirements 6
6.2 Registration Request 6
6.3 Certificate Key Update 10
6.4 Revocation Request11 13
6.5 Accessing the Database 13
7 Test and evaluation methods 13
7.1 General test evaluation method 13
7.2 Minimum interoperability basic function test evaluation method 13
7.3 Interoperable Data Format Testing and Evaluation Methods 15

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

This document replaces GB/T 19771-2005 "Information Technology Security Technology - Minimum Interoperability Specifications for Public Key Infrastructure (PKI) Components" Compared with GB/T 19771-2005, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

a) The scope of the document has been changed, the standardization objects and the aspects covered have been redefined, and the applicable Use boundaries (see Chapter 1, Chapter 1 of the 2005 edition);

b) Changed the basic functional requirements of the four components of PKI (see Chapter 5, Chapter 5 of the 2005 edition), added BYOD request Functional requirements for certificates (see 5.3.2, 5.4.2), minimum steps for verifying certificates (see 5.2.2), and requirements for commercial Support for cryptographic algorithms (see 5.6);

c) Changed the requirements for the interoperability transaction data format, including the data structure of digital certificates, certificate extensions, and the format of certificate revocation lists.

The format requirements are modified to comply with GB/T 20518-2018 (see 6.1, 6.2, 6.3 of the 2005 edition); the PKI transaction message The requirements for the format and content have been modified to comply with GB/T 19714-2025 (see 6.1, 6.5 of the 2005 edition); the PKI transaction Message content (see Chapter 6, 6.6 of the 2005 edition);

d) Added test and evaluation methods for CA system, RA system, certificate holder and certificate verifier functions, and added interoperability data.

According to the format test evaluation method (see Chapter 7);

e) Deleted Normative Appendix A, Normative Appendix B, Normative Appendix C, Normative Appendix D (see Appendix A, Appendix D of the 2005 edition) B, Appendix C, Appendix D).

This document is proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260).

This document was drafted by: University of Chinese Academy of Sciences, Beijing Digital Certification Co., Ltd., the Third Research Institute of the Ministry of Public Security, and the Software Research Institute of the Chinese Academy of Sciences.

Software Research Institute, Changchun Jida Zhengyuan Information Technology Co., Ltd., Anhui Xinke Gongchuang Information Security Evaluation Co., Ltd., Tsinghua University, Guangdong Provincial Electronic Commerce Certification Co., Ltd., Shenzhen Electronic Commerce Security Certificate Management Co., Ltd., Asia Information Technology (Shanghai) Co., Ltd., China Science Information Security Common Technology National Engineering Research Center Co., Ltd., China Unicom Online Information Technology Co., Ltd., Beijing Zhongguancun Laboratory, Qi'anxin Wangshen Information Technology (Beijing) Co., Ltd., Shaanxi Information Engineering Research Institute, National Information Technology Security Research Center, Zhongfu Information Co., Ltd., Hangzhou Hikvision Digital Technology Co., Ltd., China Electronics Information Industry Group Co., Ltd. Sixth Research Institute Research Institute, Changyang Technology (Beijing) Co., Ltd.

The main drafters of this document are: Feng Dengguo, Jing Jiwu, Liu Limin, Zheng Yajie, Chen Yan, Ding Zhaowei, Zhang Jianguo, Kou Chunjing, Zhang Liwu, Jia Keting, Zhang Yan, Qin Lingyue, Li Qiang, Chen Shule, Zheng Huitao, Wei Yicai, Hu Jianxun, Liang Bin, Zhao Boxin, Meng Jiaying, An Jincheng, Zhao Xiaorong, Liang Li, Chen Teng, Wang Bin, Wang Long, and Zhao Hua.

The previous versions of this document and the documents it replaces are as follows.

- First published in 2005 as GB/T 19771-2005;

- This is the first revision.

Cybersecurity Technology Public Key Infrastructure Minimum Interoperability Specifications for PKI Components

1 Scope

This document specifies the minimum interoperability requirements and data format requirements for public key infrastructure components, and describes the test and evaluation method.

This document applies to the design, development, testing and application of PKI in activities such as electronic signatures, electronic seals, and identity management.

2 Normative references

GB/T 15852.2

GB/T 19714-2025

GB/T 20518-2018

GB/T 25056-2018

GB/T 32905

GB/T 32907

GB/T 32918.2

GB/T 37092

GB/T 43694

3 Terms and Definitions

The terms and definitions defined in GB/T 25056-2018, GM/Z0001-2013 and the following apply to this document.

3.1

An element of the PKI system that is used to carry out certificate-related activities.

3.2 digital certificatedigitalcertificate

The certificate authority confirms the user's public key and identity information and signs the data with the private key.

Note. Also called public key certificate.

3.3 signaturecertificate

A digital certificate used to authenticate the signing public key. [Source. GM/Z0001-2013, 2.90]