

ICS 35.240.80
CCS C 07



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

GB/T 21716.3-2025

Replacing GB/Z 21716.3-2008

**Health informatics - Public key infrastructure - Part 3: Policy
management of certification authority**

健康信息学 公钥基础设施 第3部分: 认证机构的规范化管理

(English Translation)

Issued on: October 5, 2025

Implemented on: May 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 Standardized Management Requirements for Digital Certificates in the Healthcare Context	
5.1 General Rules	
5.2 High-level guarantee	
5.3 Trust at the Senior Management Level	
5.4 Infrastructure Availability	
5.5 Internet Compatibility	
5.6 CP Assessment and Comparison	
6 Structure of Healthcare CP and CPS	
6.1 General Requirements for CP	
6.2 CPS General Requirements	
6.3 Relationship between CP and CPS	
6.4 Applicability	
7 Minimum requirements for healthcare CP	
7.1 Basic Requirements	
7.2 Responsibilities for Release and Storage	
7.3 Identification and Marking	
7.4 Certificate Lifecycle Operation Requests	
7.5 Physical Control	
7.6 Technical security controls	
7.7 Certificates, CRL, and OCSP Outline	
7.8 Compliance Audit	
7.9 Other Business and Legal Issues	
8 PKI publicly declared model	
8.1 Overview	
8.2 Declaration of Structure 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 3 of GB/T 21716 "Public Key Infrastructure for Health Informatics". GB/T 21716 has published the following...

part.

---Part 1: Overview of Digital Certificate Services;

---Part 2: Certificate Summary;

---Part 3: Standardized Management of Certification Bodies.

This document replaces GB/Z 21716.3-2008 "Public Key Infrastructure (PKI) for Health Informatics - Part 3: Policies for Certification Authorities".

Compared with GB/Z 21716.3-2008, the main technical changes in the "Management" standard, apart from structural adjustments and editorial modifications, are as follows.

---The abbreviations "AC" and "OCSP" have been added (see Chapter 4);

---Service availability and operational features have been removed (see 7.4.10.2 and 7.4.10.3 in the 2008 versions);

---The general rules have been amended (see 5.1, 2008 version 5.1);

---The content of the higher-level trust requirements has been changed (see 5.3, 5.4 in the 2008 version);

---Changes have been made to the information regarding infrastructure availability (see 5.4, 5.3 from the 2008 version);

---The relationship between CP and CPS has been changed (see 6.3, 2008 version 6.3);

---The rules for interpreting the name format have been changed (see 7.3.1.4, 2008 version 7.3.1.4);

---The content regarding personal identification has been changed (see 7.3.2.3, 2008 version 7.3.2.3);

---The certificate application processing time has been changed (see 7.4.2.3, 2008 version 7.4.2.3);

---Changes have been made to the availability of the service (see 7.4.10.2, version 7.4.10.2 from 2008);

---The CA representation and warranty have been revised (see 7.9.6.2, 2008 version 7.9.6.2);

---Changes have been made to the declaration types, declaration descriptions, and CP requirements in the PKI public declaration model (see 8.1, 2008 version 8.1).

This document is modified to adopt ISO 17090-3:2021 "Health informatics - Public key infrastructure - Part 3: Standardization of certification authorities".

manage".

This document has undergone the following structural adjustments compared to ISO 17090-3:2021.

---7.6.1.2 corresponds to 7.6.1.2~7.6.1.4 of ISO 17090-3:2021;

---Sections 7.4.9.2 to 7.4.9.18 correspond to sections 7.4.9.1 to 7.4.9.17 of ISO 17090-3:2021;

--- Table 1 in 8.1 corresponds to Table 1 in 8.2 of ISO 17090-3:2021.

The technical differences between this document and ISO 17090-3:2021, and the reasons therefor, are as follows.

---The abbreviations "AC" and "OCSP" (see Chapter 4) have been added to simplify the expression;

---The resulting information has been changed to a note (see 5.3) to simplify the description;

---ISO 17090-1 (see Chapter 3) has been replaced with the normatively referenced GB/T 21716.1-2025 to adapt to my country's national conditions;

---ISO 17090-2 (see 7.3.1.1, 7.3.2.6, 7.7) has been replaced with the normatively referenced GB/T 21716.2 to adapt to my country's national standards.

National conditions;

---ISO/IEC 27002 (see 7.2.1, 7.5, 7.6, 7.9.14) has been replaced with the normatively referenced GB/T 22081 to adapt to my country's national standards.

National conditions;

---USFIPS 140-2 (see 7.6.6.2, 7.6.6.12) has been replaced with the normatively referenced GM/T 0028-2024 to adapt to my country's national standards.

National conditions.

The following editorial changes have been made to this document.

---The reason for removing the archiving of certificate creation or revocation requests in section 7.5.6.3 of ISO 17090-3:2021.

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 China National Institute of Standardization.

Introduction

GB/T 21716 "Public Key Infrastructure for Health Informatics" is proposed to consist of five parts.

---Part 1: Overview of Digital Certificate Services. The purpose is to define the basic concepts of digital certificate use in the healthcare industry and provide...

Interoperability solutions are needed for secure communication of health information using digital certificates.

---Part 2: Certificate Overview. The purpose is to provide a health-specific overview of digital certificates based on the international standard X.509 and their application.

Healthcare overview as specified in IETF/RFC5280 for different certificate types.

---Part 3: Standardized Management of Certification Bodies. The aim is to define the structure and minimum requirements of the Certificate Policy (CP) and its related aspects.

The structure of the certification operation statement. Based on the relevant recommendations of IETF/RFC3647, it identifies the aspects of cross-border communication of health information.

The principles required in a security strategy define the minimum level of security needed in terms of health.

---Part 4: Digital Signatures for Healthcare Documents. This section provides minimum requirements for generating and verifying digital signatures and related certificates.

The format supports the interchangeability of digital signatures and prevents incorrect or illegal digital signatures.

---Part 5: Authentication using healthcare PKI credentials. The purpose is to specify authentication methods based on the definitions in GB/T 21716.

PKI verification of entity credentials is a procedural requirement for healthcare information systems (including access to remote systems).

Health Informatics Public Key Infrastructure Part 3: Standardized Management of