

ICS 35.240.80
CCS C 07



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

GB/T 21716.1-2025

Replacing GB/Z 21716.1-2008

**Health informatics - Public key infrastructure - Part 1: Overview
of digital certificate services**

健康信息学 公钥基础设施 第1部分：数字证书服务综述
(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	
3.1 Healthcare Terminology	
3.2 Security Service Terminology	
3.3 Public Key Infrastructure Related Terminology	
4 Abbreviations	7.
5 Healthcare Context	
5.1 Healthcare certificate holders and dependents	
5.2 Participant Example	
5.3 Applicability of Healthcare Digital Certificates	
6 Security service requirements in healthcare applications	
6.1 Healthcare Features	
6.2 Digital Certificate Technology Requirements in the Healthcare Sector	
6.3 Healthcare-Specific Requirements and Separation of Data Encryption and Authentication	
6.4 Healthcare Digital Certificate Security Management Framework	
6.5 Policy Requirements for the Issuance and Use of Healthcare Digital Certificates	
7 Public key cryptography	
7.1 Symmetric and Asymmetric Cryptography	
7.2 Digital Certificate	
7.3 Digital Signatures	
7.4 Private Key Protection	
8 Configure digital certificate	
8.1 Required Components	
8.2 Establishing Identification Using Qualification Certificates	
8.3 Establishing professions and roles using identity certificates	
8.4 Using Attribute Certificates for Authorization and Access Control	
9 Interoperability Requirements	
9.1 General Rules	

- 9.2 Options for configuring cross-jurisdictional healthcare digital certificates
- 9.3 Usage of Options
- Appendix A (Informative) Scenario 18 for using healthcare digital certificates
- A.1 Introduction
- A.2 Scene Description
- A.3 Service Examples in Healthcare Scenarios
- A.4 Scene Description
- 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 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 21716.1-2008 "Health Informatics Public Key Infrastructure (PKI) Part 1: Digital Certificate Services".

Compared with GB/Z 21716.1-2008, the main technical changes in the "Description" are as follows, apart from structural adjustments and editorial modifications.

---The terms and definitions for "healthcare participant" and "certificate" have been changed (see 3.1.3, 3.3.4, and 3.1.3 and 3.3.4 in the 2008 edition);

---The term and definition of "organizational employee" have been added (see 3.1.6);

---The terms and definitions of "supporting organizations," "identification," "certificate management," and "certificate verification" have been removed (see section 3.1.10 of the 2008 edition).

3.2.16, 3.3.8, 3.3.12);

---The abbreviations AA, CA, CP, CPS, CRL, PKC, PKI, RA, and TTP have been removed (see Chapter 4 of the 2008 edition);

--- Added normative references to GB/T 22081 (see 6.2.1, 7.4, 8.1.4).

This document is modified to adopt ISO 17090-1:2021 "Health informatics public key infrastructure - Part 1: Overview of digital certificate services".

The technical differences between this document and ISO 17090-1:2021, and the reasons therefor, are as follows.

---The term "peer entity authentication" (see 3.2.27) has been added for the purpose of application in this document;

---The term "certificate" (see 3.3.4) has been changed to suit my country's national conditions;

---ISO/IEC 27002 (see 6.2.1, 7.4, 8.1.4) has been replaced with the normatively referenced GB/T 22081 to adapt to my country's national conditions;

---ISO/IEC 9594-8 (see 7.2) has been replaced with the normatively referenced GB/T 16264.8 to adapt to my country's national conditions;

---ISO 17090-2 (see 8.2) has been replaced with the normatively referenced GB/T 21716.2 to adapt to my country's national conditions;

---ISO 17090-3 (see 6.5, 9.1) has been replaced with the normatively referenced GB/T 21716.3 to adapt to my country's national conditions.

The following editorial changes have been made to this document.

---The sources in terms 3.2.16, 3.2.20, 3.2.24, 3.3.13~3.3.15, 3.3.18, 3.3.19, and 3.3.21 have been removed;

---ISO 7498-2 has been replaced by GB/T 9387.2 (see 7.3), which is cited in the informational reference.

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. Provides a health-specific overview of digital certificates based on the international standard X.509, as well as information on certificates used for different purposes.

The healthcare overview is defined in IETF/RFC5280, a book-type document.

---Part 3: Standardized Management of Certification Bodies. The purpose is to define the structure and minimum requirements of CPs and related certification operations.

The structure of the statement. Based on the relevant recommendations of IETF/RFC3647, it identifies a security strategy for cross-border communication of health information.

The principles required in this context stipulate the minimum level of safety needed in terms of health.

---Part 4: Digital Signatures for Healthcare Documents. The aim is to provide the most efficient way to generate and verify digital signatures and related certificates.

Low requirements and format, supports 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 1: Overview of Digital Certificate Services

1 Scope

This document defines the basic concepts of healthcare digital certificates and outlines the requirements for using digital certificates for secure communication of health information.

Interoperability solutions, key stakeholders for health information communication, and key security requirements for using digital certificates for health information communication.

Full service.

This document describes the public-key cryptographic algorithms and basic components required to configure healthcare digital certificates, and introduces different types of digital certificates.

Certificates (including identification certificates, associated attribute certificates for dependent parties, and self-signed CA certificates) as well as CA hierarchy and bridging structures.

This document is intended for use by health information security personnel, designers and developers specializing in health information application software.