

ICS 35.240.80
CCS C 07



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

GB/T 21716.2-2025

Replacing GB/Z 21716.2-2008

**Health informatics - Public key infrastructure - Part 2:
Certificate profile**

健康信息学 公钥基础设施 第2部分：证书概要
(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 Use of Healthcare Certificates	
5.1 Type 2 of Healthcare Certificates	
5.2 CA Certificate	
5.3 Cross-connect/Bridging Certificate	
5.4 End-Entity Certificate	
6 General Certificate Requirements	
6.1 Certificate Compliance	
6.2 Common Certificate Fields	
6.3 General Field Specifications	
6.4 Requirements for Healthcare Certificate Types	
7 Use of Certificate Extensions 9.	
7.1 Overview	
7.2 General Extension	
7.3 Dedicated Main Directory Attributes	
7.4 Qualification Certificate Declaration	
7.5 Requirements for Medical Industry Certificate Types	
Appendix A (Informative) Certificate Summary Example	
A.1 Overview	
A.2 Consumer Certificate Summary	
A.3 Summary of Non-Regular Health Professional Certificates	
A.4 Summary of Certified Healthcare Professionals (CHP)	
A.5 Summary of Certificates for Trusted Healthcare Providers	
A.6 Summary of Supporting Organization Employee Certificates	
A.7 Organizational Certificate Summary	
A.8 AC Summary	
A.9 CA Certificate Summary	

A.10 Bridging Certificate Summary

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 2 of GB/T 21716 "Public Key Infrastructure for Health Informatics". GB/T 21716 has already published the following parts.

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

---Part 2: Certificate Summary;

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

This document replaces GB/Z 21716.2-2008 "Public Key Infrastructure (PKI) for Health Informatics - Part 2: Certificate Outlines", and is consistent with...

Compared with GB/Z 21716.2-2008, apart from structural adjustments and editorial changes, the main technical changes are as follows.

---The abbreviation "OID" has been added (see Chapter 4);

---Added the section on establishing a trust chain in the "Root CA Certificate" section (see 5.2.1);

---Added the section on "Subordinate CA Certificates" used together with other certificates to establish a chain of trust (see 5.2.2);

---Added "Award Recipients" (see 5.4.1);

---Change the normative reference to IETF/RFC3281 to an informative reference (see 5.4.6, 5.4.5 of the 2008 edition);

---Changed the requirements for the extended fields in the medical industry certificate type section to include both mandatory and optional applications (see 7.5, 2008 version).

This document is modified to adopt ISO 17090-2:2015 "Health informatics public key infrastructure - Part 2: Certificate summary".

This document has undergone the following structural adjustments compared to ISO 17090-2:2015.

---5.4.2~5.4.7 correspond to 5.4.1~5.4.6 of ISO 17090-2:2015.

The technical differences between this document and ISO 17090-2:2015, and the reasons therefor, are as follows.

---The abbreviations CPS and TTP (see Chapter 4) have been removed because they are not used in the main text;

---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;

---The standard GB/T 21716.3-2025 (see 7.2.5) has been replaced with the normatively referenced GB/T 21716.3-2025 to adapt to my country's national conditions.

The following editorial changes have been made to this document.

---Added note (see 6.3.2);

---The reason why email addresses are optional in the subject name field has been removed (see 6.3.6 of ISO 17090-2:2015);

---A heading has been removed (see 7.5.1 of ISO 17090-2:2015);

---Change the examples in Appendix A to relevant Chinese names.

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. 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 2: Certificate Summary

1 Scope

This document specifies the CA (Certificate Authority) required for the exchange of healthcare information within an individual organization, between different organizations, and across jurisdictional boundaries.

This standardizes the structure, field requirements, and certificate extension usage for healthcare certificates such as book, client entity certificates, and attribute certificates. It also regulates public key infrastructure.

The application of digital certificates in the healthcare industry is illustrated with examples.

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

2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included.

For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies.

This document.

GB/T 21716.1-2025 Public Key Infrastructure for Health Informatics - Part 1: Overview of Digital Certificate Services (ISO 17090-1.

2021, MOD)

GB/T 21716.3-2025 Public Key Infrastructure for Health Informatics - Part 3: Standardized