ICS 35.240.80
CCS C 07

中华人民共和国国家标准

GB/T 21716.1—2025
代替 GB/Z 21716.1—2008

健康信息学　公钥基础设施 第1部分:数字证书服务综述

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

（ISO 17090-1:2021,MOD）

2025-10-05 发布　　2026-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 21716《健康信息学　公钥基础设施》的第1部分。GB/T 21716已经发布了以下部分：

——第1部分：数字证书服务综述；

——第2部分：证书概要；

——第3部分：认证机构的规范化管理。

本文件代替GB/Z 21716.1—2008《健康信息学　公钥基础设施(PKI)　第1部分：数字证书服务综述》，与GB/Z 21716.1—2008相比，除结构调整和编辑性改动外，主要技术变化如下：

——更改了“医疗保健参与者”“证书”的术语和定义(见3.1.3、3.3.4，2008年版的3.1.3、3.3.4)；

——增加了“组织雇员”的术语和定义(见3.1.6)；

——删除了“支持组织”“标识”“证书管理”“证书验证”的术语和定义(见2008年版的3.1.10、3.2.16、3.3.8、3.3.12)；

——删除了缩略语AA、CA、CP、CPS、CRL、PKC、PKI、RA、TTP(见2008年版的第4章)；

——增加了规范性引用的GB/T 22081(见6.2.1、7.4、8.1.4)。

本文件修改采用ISO 17090-1：2021《健康信息学　公钥基础设施　第1部分：数字证书服务综述》。

本文件与ISO 17090-1：2021的技术差异及其原因如下：

——增加了术语“对等实体鉴别”(见3.2.27)，以便本文件的应用；

——更改了术语“证书”(见3.3.4)，以适应我国国情；

——用规范性引用的GB/T 22081替换了ISO/IEC 27002(见6.2.1、7.4、8.1.4)，以适应我国国情；

——用规范性引用的GB/T 16264.8替换了ISO/IEC 9594-8(见7.2)，以适应我国国情；

——用规范性引用的GB/T 21716.2替换了ISO 17090-2(见8.2)，以适应我国国情；

——用规范性引用的GB/T 21716.3替换了ISO 17090-3(见6.5、9.1)，以适应我国国情。

本文件做了下列编辑性改动：

——删除了术语3.2.16、3.2.20、3.2.24、3.3.13～3.3.15、3.3.18、3.3.19、3.3.21中的来源；

——用资料性引用的GB/T 9387.2替换了ISO 7498-2(见7.3)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国标准化研究院提出并归口。

本文件起草单位：中国标准化研究院、厦门市众科佰联标准化服务有限公司、福建理工大学、青岛华大智造科技有限责任公司、浪潮卓数大数据产业发展有限公司、深圳市卫生健康发展研究和数据管理中心、上海市中医药国际标准化研究院、深圳统标科技有限公司、宜春学院、南京易联阳光信息技术股份有限公司、河南省人民医院、福建省中科标准科技有限责任公司、潮州和德生物技术有限公司。

本文件主要起草人：任冠华、曾小凡、郭欣艳、王萌萌、张帆、陈煌、王志民、李静、吴培凯、王博龙、罗亮、高亮、徐凯程、王淑粉、李柳、宋宝祥、田容、陈湘云。

本文件及其所代替文件的历次版本发布情况为：

——2008年首次发布为GB/Z 21716.1—2008；

——本次为第一次修订。

引　言

GB/T 21716《健康信息学　公钥基础设施》拟由五个部分构成。

——第1部分：数字证书服务综述。目的在于规定医疗保健行业中使用数字证书的基本概念，给出使用数字证书进行健康信息安全通信所需的互操作方案。

——第2部分：证书概要。给出基于国际标准X.509的数字证书的健康专用概要以及用于不同证书类型的IETF/RFC 5280中规定的医疗保健概要。

——第3部分：认证机构的规范化管理。目的在于规定CP的结构和最低要求以及关联认证操作声明的结构。以IETF/RFC 3647的相关建议为基础，确定在健康信息跨国通信的安全策略中所需的原则，规定健康方面所需的最低级别的安全性。

——第4部分：医疗保健文档数字签名。目的在于通过提供生成和验证数字签名及相关证书的最低要求和格式，支持数字签名的可互换性并防止不正确或非法的数字签名。

——第5部分：使用医疗保健PKI凭证进行身份验证。目的在于规定基于GB/T 21716中定义的PKI验证实体凭证的程序要求，用于医疗保健信息系统(包括访问远程系统)。

健康信息学　公钥基础设施
第1部分:数字证书服务综述

1　范围

本文件界定了医疗保健数字证书的基本概念,给出了使用数字证书进行健康信息安全通信所需的互操作方案,进行健康信息通信的主要利益相关方以及使用数字证书进行健康信息通信所需的主要安全服务。

本文件描述了配置医疗保健数字证书所需的公钥密码算法和基本构件,并介绍了不同类型的数字证书(包括标识证书、用于可依赖方的关联属性证书、自签名CA证书)以及CA等级体系与桥接结构。

本文件适用于健康信息安全人员、专门从事健康信息应用软件的设计者和开发者使用。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 16264.8　信息技术　开放系统互连　目录　第8部分:公钥和属性证书框架(GB/T 16264.8—2005,ISO/IEC 9594-8:2001,IDT)

GB/T 21716.2　健康信息学　公钥基础设施　第2部分:证书概要(GB/T 21716.2—2025,ISO 17090-2:2015,MOD)

GB/T 21716.2—2025　健康信息学　公钥基础设施　第2部分:证书概要(ISO 17090-2:2015,MOD)

注:GB/T 21716.2—2025被引用的内容与ISO 17090-2:2015被引用的内容没有技术上的差异。

GB/T 21716.3　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(GB/T 21716.3—2025,ISO 17090-3:2021,MOD)

GB/T 21716.3—2025　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(ISO 17090-3:2021, MOD)

注:GB/T 21716.3—2025被引用的内容与ISO 17090-3:2021被引用的内容没有技术上的差异。

GB/T 22081　网络安全技术　信息安全控制(GB/T 22081—2024,ISO/IEC 27002:2022,IDT)

3　术语和定义

下列术语和定义适用于本文件。

3.1　医疗保健语境术语

3.1.1

应用　application

作为私有加密密钥持有方的、可标识的计算机运行软件程序。

注1:在本语境中,应用可能是医疗保健信息系统中使用的任一软件程序,也包括那些在治疗或诊断中不直接使用的应用。

注2:在一定管辖范围内,包括正规医疗设备软件程序。