ICS 35.240.80
CCS C 07

中华人民共和国国家标准

GB/T 21716.2—2025
代替 GB/Z 21716.2—2008

健康信息学　公钥基础设施
第2部分：证书概要

Health informatics—Public key infrastructure—Part 2: Certificate profile

（ISO 17090-2:2015，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2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 21716.2—2008《健康信息学　公钥基础设施(PKI)　第2部分：证书轮廓》，与GB/Z 21716.2—2008相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了缩略语“OID”(见第4章)；

——增加了“根CA证书”中建立信任链部分内容(见5.2.1)；

——增加了“从属CA证书”中与其他证书一起被用来建立信任链部分内容(见5.2.2)；

——增加了“颁发对象”(见5.4.1)；

——将规范性引用的IETF/RFC 3281更改为资料性引用(见5.4.6，2008年版的5.4.5)；

——更改了医疗行业证书类型扩展字段的要求中扩展必备的和可选的应用(见7.5，2008年版的7.5)。

本文件修改采用ISO 17090-2：2015《健康信息学　公钥基础设施　第2部分：证书概要》。

本文件与ISO 17090-2：2015相比做了下述结构调整：

——5.4.2～5.4.7对应ISO 17090-2：2015的5.4.1～5.4.6。

本文件与ISO 17090-2：2015的技术差异及其原因如下：

——删除了缩略语CPS、TTP(见第4章)，因正文未使用；

——用规范性引用的GB/T 21716.1—2025替换了IS0 17090-1(见第3章)，以适应我国国情；

——用规范性引用的GB/T 21716.3—2025替换了IS0 17090-3(见7.2.5)，以适应我国国情。

本文件做了下列编辑性改动：

——增加了注(见6.3.2)；

——删除了电子邮件在主体名称字段中可选的原因(见ISO 17090-2：2015的6.3.6)；

——删除了条标题(见ISO 17090-2：2015的7.5.1)；

——将附录A中示例更改为我国相关名称。

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、福建省中科标准科技有限责任公司、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、汕头市信德嘉生物科技有限公司、福建省标准化服务行业协会、杭州砺盈科技有限公司、康知己医药(潮州)有限公司。

本文件主要起草人：任冠华、李静、王志民、吴培凯、王萌萌、陈煌、高亮、徐凯程、田容、曾小凡、郭欣艳、魏川梅、宋宝祥、刘湘怡、张振、周利、顾迎旦、李锦轩。

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 21716.2—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。目的在于给出基于国际标准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。目的在于规定证书策略(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2部分:证书概要

1　范围

本文件规定了在单独组织内部、不同组织之间和跨越管辖界限时,医疗保健信息交换所需的CA证书、端实体证书、属性证书等医疗保健证书的结构、字段要求及证书扩展的使用。规范了公钥基础设施数字证书在医疗行业中的应用,并提供了示例说明。

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 21716.1—2025　健康信息学　公钥基础设施　第1部分:数字证书服务综述(ISO 17090-1:2021,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 17090-3:2008[1)]被引用的内容没有技术上的差异。

IETF/RFC 5280　互联网X.509公钥基础设施　证书和证书吊销列表(CRL)轮廓[Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile]

IETF/RFC 5755　用于授权的互联网属性证书规范(An Internet Attribute Certificate Profile for Authorization)

3　术语和定义

GB/T 21716.1—2025界定的术语和定义适用于本文件。

4　缩略语

下列缩略语适用于本文件。

AA:属性机构(Attribute Authority)

AC:属性证书(Attribute Certificate)

CA:认证机构(Certification Authority)

CP:证书策略(Certificate Policy)

CRL:证书撤销列表(Certificate Revocation list)

OID:对象标识符(Object Identifier)

1)　ISO 17090-3:2008已被ISO 17090-3:2021代替。