

《健康信息学 公钥基础设施 第 2 部分：证书轮廓》

国家标准编制说明

一、工作简况

（一）任务来源

本文件的制订计划由中国标准化研究院提出，经国家标准委批准，正式列入 2023 年推荐性国家标准制修订项目计划，项目编号为 20233185-T-424，采标号为 ISO 17090-2:2015，项目名称为《健康信息学 公钥基础设施 第 2 部分：证书轮廓》。

本文件的标准起草单位包括：中国标准化研究院、中国人民解放军总医院、北京航空航天大学、上海中医药大学、深圳市卫生健康发展研究和数据管理中心、福建省中科标准科技有限责任公司、浙江大学、浙江师范大学、北京信息科技大学、厦门市众科佰联标准化服务有限公司、福建理工大学等。

（二）本文件制定目的和意义

随着经济社会的快速发展，公众对健康的关注不断提升，对多样化的健康服务需求日益增长。健康信息系统作为医疗卫生改革的核心，能够整合社会健康资源，提升服务效率，促进健康服务的形式、流程和内容的根本变革，提高健康资源的可及性和公平性，有效缓解就医难、就医贵的问题。

互联网虽然提供了便捷的信息交换手段，但其不安全性要求我们采取措施保护信息的私密性和保密性。制定一系列基础性、通用性的技术标准至关重要。通过修订《健康信息学 公钥基础设施 第 2 部

分：证书轮廓》，旨在提高公钥基础设施（PKI）的安全性和可靠性，以保护敏感的健康信息不受威胁。通过更新证书轮廓，可以更好地管理和验证数字证书，加强医疗行业中数据传输的安全性，从而保证医疗信息在网络中传输时的加密和身份验证达到最新的安全标准。这对于保护患者的隐私权和个人健康信息至关重要。修订还有助于促进医疗保健行业的互操作性和合作，提高医疗服务的效率和质量。

（三）主要工作过程

3.1 成立起草组，确定标准框架并形成标准草案稿

2024 年 2 月——5 月，在中国标准化研究院的组织下，成立了由中国标准化研究院、中国人民解放军总医院、北京航空航天大学、上海中医药大学、深圳市卫生健康发展研究和数据管理中心、福建省中科标准科技有限责任公司、浙江大学、浙江师范大学、北京信息科技大学、厦门市众科佰联标准化服务有限公司、福建理工大学等单位组织的标准起草组。

因为本文件是修改采用国际标准，所以起草工作小组前期对 ISO 17090-2:2015《健康信息学 公钥基础设施 第 2 部分：证书轮廓》进行了认真的翻译研究工作，并对国际标准中引用到的标准和技术文件逐一进行了查阅和研究，初步确立了本文件的草案第一稿。

在上述工作基础上，起草组在对国内外的健康信息系统建设中的信息安全建设与应用情况进行了资料调研和分析，确立了标准框架和具体内容，形成标准草案正式稿。

3.2 形成征求意见稿

2024 年 6 月——9 月，在确立的草案稿的基础上，起草组内部经过多次讨论后对标准的技术内容进行了充实和完善。同时，起草组多次组织国内相关的专家学者召开研讨会，对标准框架及草案内容提出进行研讨。起草组在广泛听取专家的意见和建议，并经过多次内部的研讨、修改后，于 2024 年 9 月形成了标准的征求意见稿。

二、国家标准编制原则和确定国家标准主要内容的论据

（一）编制原则

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》和 GB/T 1.2—2020《标准化工作导则 第 2 部分：以 ISO/IEC 标准化文件为基础的标准化文件起草规则》的要求，采用翻译法修改采用 ISO 17090-2:2015《健康信息学 公钥基础设施 第 2 部分：证书轮廓》。同时充分考虑到现阶段我国健康信息系统建设情况和实际需求，使其具有可操作性。

（二）标准确定论据

本文件修改采用国际标准 ISO 17090-2:2015《健康信息学 公钥基础设施 第 2 部分：证书轮廓》。

（三）标准主要内容

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要的证书轮廓。还详述了公钥基础设施数字证书在医疗行业中形成的应用，并侧重描述了其中与证书轮廓相关的医疗保健问题。

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

本文件所引用的有关标准、规范、规程均为现行且有效，条文中给出编号，以便于使用时查找。

3 术语和定义

本文件定义的术语包括 GB/T 21716.1 中列出的术语。

4 缩略语

本章定义的缩略语包括：属性机构、认证机构、证书策略、认证操作声明、证书撤销列表、对象标识符、公钥证书、公钥基础设施、注册机构、可信第三方。

5 医疗保健证书策略

本章介绍了医疗保健领域中使用的各类证书及其策略。包括为个人、组织、设备 and 应用发行的标识证书，以及根 CA 证书和从属 CA 证书。还讨论了交叉/桥接证书的概念以及属性证书（AC）和角色证书的使用，这些证书支持基于角色的访问控制，对于医疗保健行业的数字化和信息安全至关重要。

6 一般证书要求

本章介绍了一般证书的要求，包括证书的符合性、通用字段、以及通用字段规范。规定了证书的签名算法、有效性、主体公钥信息等关键要素。提出了各种医疗保健证书类型的发行方和主体字段要求，确保证书在医疗保健领域的适用性和安全性。

7 证书扩展的使用

本章概述了 X.509 第 3 版医疗保健证书中证书扩展的使用。这些扩展提供了证书的额外信息和功能，如机构密钥标识符、主体密钥标识符、密钥使用等。有助于区分密钥、标识公钥、定义密钥用途，并包括了一些可选的扩展，如主体替换名称和机构信息访问。还讨论了专用主体目录属性，如医疗保健角色属性，这对于证书持有者的身份验证和角色指定至关重要。提出了对各种医疗行业证书类型的扩展字段要求，确保证书的适用性和安全性。

三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

本文件的技术内容不涉及试验验证的要求，通过本文件的实施将能够使用数字证书来保护健康信息在领域内部、不同领域之间以及不同辖区之间进行交换。

四、采用国际标准和国外先进标准的程度

本文件修改采用国际标准 ISO 17090-2:2015《健康信息学 公钥基础设施 第 2 部分：证书轮廓》

五、与有关的现行法律、法规和强制性国家标准的关系

本文件符合国家现行法律、法规、规章和强制性国家标准的要求。

六、重大分歧意见的处理经过和依据

本文件在制定过程中未出现重大分歧意见。

七、国家标准作为强制性国家标准或推荐性国家标准的建议

本文件建议作为推荐性标准发布实施。

八、贯彻国家标准的要求和措施建议

本文件作为推荐性标准，建议首先利用报纸、电视、电台及微信、微博等各种新媒体，加大宣传力度，为标准的实施营造良好的社会氛围。其次在有影响力的医疗服务平台中应用实施。同时，将实施过程中出现的问题和好的改进建议反馈给标准起草组，以便未来对本文件的继续修订和完善。

九、废止现行有关标准的建议

本文件不涉及对现行标准的废止。

十、其他

无。

《健康信息学 公钥基础设施 第2部分：证书轮廓》

国家标准起草组

2024年9月