

《健康信息学 公钥基础设施 第1部分：数字证书服务 综述》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年国家标准制修订项目计划，项目计划号为20233531-T-424。采标号为ISO 17090-1:2021，采标名称为《健康信息学 公钥基础设施 第1部分：数字证书服务综述》。

本文件的起草单位包括：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

本文件的制定旨在指导医疗卫生行业如何利用数字证书技术来保护患者的健康信息安全，实现在不安全的网络环境下对敏感数据的安全交换。通过正确配置数字证书，保证个人健康记录的安全访问和传输，满足临床和管理方面的需求。

此外，数字证书的互操作性和信任框架的建立也是本文件的重要目标，实现不同组织和不同国家之间的数字证书有效交换和认证，从而促进国际医疗保健信息的安全传输和共享。通过本文件的制定和实施，帮助医疗保健行业提高对数字证书技术的应用水平，保护患者隐

私和数据安全，促进医疗信息的互联互通，提高医疗卫生服务的效率和质量。

在纸质处理向自动化电子处理转变这一背景下，本文件的制定也有助于降低医疗卫生行业的费用 and 成本，推动新的医疗保健模式的发展，满足专业医疗保健提供者之间共享患者信息的需求。通过采用数字证书技术，医疗卫生行业可以以经济实用的方式对互联网中传输的数据进行适当的保护，降低未经授权访问的风险，为医疗保健系统的信息安全提供可靠的保障。

综上，通过修改采用 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》，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，优化跨国医疗健康信息安全系统和医疗效率，推动医疗健康信息学的发展。

（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成的标准起草组。

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 17090-1:2021《健康信息学 公钥基础设施 第 1 部分：数字证书服

务综述》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，初步确定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 17090-1:2021《健康信息学 公钥基础设施 第1部分：数字证书服务综述》。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 17090-1:2021《健康信息学 公钥基础设施 第1部分：数字证书服务综述》。

（三）标准主要内容

1. 范围

本文件定义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。本文件还给出了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。

本文件简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，并进一步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、自签名认证机构（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

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：医疗保健语境术语、安全服务术语、公钥基础设施相关术语。

4 缩略语

本章给出了 2 项缩略语：ECG：心电图（Electrocardiogram）；HER：电子健康记录（Electronic Health Record）。

5 医疗保健语境

本章规定了医疗保健语境的医疗保健证书持有方和可依赖方、参与者示例、医疗保健数字证书的适用性等内容。

6 医疗保健应用中的安全服务需求

本章规定了医疗保健应用中的安全服务需求的医疗保健特征、医疗保健领域中的数字证书技术需求、医疗保健具体需求与数据加密和身份验证的分离、医疗保健数字证书安全管理框架、医疗保健数字证书发行和使用的策略要求等内容。

7 公钥密码算法

本章规定了公钥密码算法的对称密码算法与非对称密码算法、数字证书、数字签名、保护私钥等内容。

8 配置数字证书

本章规定了配置数字证书的必备组件、使用资质证书建立标识、使用身份证书建立专业和角色、使用属性证书进行授权和访问控制等内容。

9 互操作性要求

本章规定了互操作性要求的概述、配置跨辖区的医疗保健数字证书的选项、选项的用法等内容。

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。优化跨国医疗健康信息安全系统和医疗效率，推动医疗健康信息学的发展。

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 17090-1:2021 《健康信息学 公钥基础设施 第 1 部分：数字证书服务综述》。

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机构中应用实施。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 1 部分：数字证书服务综述》

国家标准起草组

2024 年 9 月