ICS 11.020
CCS C 07

WS

中华人民共和国卫生行业标准

WS/T 847—2024

医学电子文档数字签名技术标准

Technical standard for medical electronic document digital signature

2024－10－28 发布　　2025－04－01 实施

中华人民共和国国家卫生健康委员会　发布

前　言

本标准为推荐性标准。

本标准由国家卫生健康标准委员会卫生健康信息标准专业委员会负责技术审查和技术咨询，由国家卫生健康委统计信息中心负责协调性和格式审查，由国家卫生健康委规划发展与信息化司负责业务管理、法规司负责统筹管理。

本标准起草单位：国家卫生健康委统计信息中心、首都医科大学附属北京天坛医院、安徽医科大学第一附属医院、北京大学人民医院、中国医科大学附属第一医院、首都医科大学附属北京胸科医院、河南省新乡市第一人民医院、黑龙江省医院、四川大学华西医院、兰州大学第二医院、青岛大学附属医院、新疆自治区人民医院。

本标准主要起草人：胡建平、李岳峰、王韬、白波、汤学军、董方杰、杨慧清、洪建、沈雷、王方非。

医学电子文档数字签名技术标准

1 范围

本标准规定了医学电子文档应用数字签名时的通用、对象、格式、验证、存储和应用等要求。

本标准适用于全国各级各类医疗卫生单位医学电子文档的数字签名。医疗卫生单位可依据本标准对医疗卫生信息系统厂商、第三方电子认证服务机构提出建设要求。

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标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 25061 信息安全技术 公钥基础设施 XML数字签名语法与处理规范

GB/T 25064 信息安全技术 公钥基础设施 电子签名格式规范

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 35291 信息安全技术 智能密码钥匙应用接口规范

GB/T 36322 信息安全技术 密码设备应用接口规范

GM/T 0015 基于SM2密码算法的数字证书格式规范

GM/T 0019 公钥密码基础设施应用技术体系 通用密码服务接口规范

GM/Z 4001 密码术语

卫生系统数字证书格式规范（试行） 原卫生部办公厅 2010年

卫生系统数字证书介质技术规范（试行） 原卫生部办公厅 2010年

卫生系统数字证书应用集成规范（试行） 原卫生部办公厅 2010年

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用本标准。

3.1

数字签名数据 digital signature data

经数字签名后得到的结果，包括数字签名值、时间戳、摘要值以及数字签名人的数字证书。

3.2

数字签名服务系统 digital signature service system

能够独立完成数字签名功能的服务系统。

3.3

医学电子文档 electronic medical document

医学服务提供人员在医学服务活动过程中，使用医疗卫生信息系统生成的文字、符号、图表、图形、数字、影像等数字化信息,并能实现存储、管理、传输和重现的医疗记录，包括医学服务对象健康状况记录及相关医学服务活动的信息记录等。

3.4

时间戳 time stamp

基于权威可靠时间和第三方电子认证服务，对签名对象进行数字签名产生的数据，以证明原始文件在签名时间之前已经存在，签名对象包括原始文件信息、签名时间、签名记录等信息，是一种特定形式的数字签名。

4 缩略语

下列缩略语适用于本文件。

ES-T 带时间戳的电子签名（Electronic Signature with Timestamp）

XML 可扩展标记语言（Extensible Markup Language）

5 通用要求

5.1 数字证书

数字签名时使用的数字证书应满足如下要求：

a) 签发数字证书的第三方电子认证服务机构应符合《中华人民共和国电子签名法》、《卫生系统电子认证服务管理办法（试行）》等相关条件要求，应建立全面、规范、安全、高效的运行服务体系，满足医疗卫生信息系统在身份认证、授权管理、责任认定等方面的信息安全需求；

b) 数字证书算法应采用SM2商用密码算法，符合GB/T 32918的相关要求；

c) 数字证书格式应符合GM/T 0015、《卫生系统数字证书格式规范（试行）》的相关要求。

5.2 数字证书介质

数字签名时使用的数字证书介质应满足如下要求：

a) 应符合《中华人民共和国电子签名法》、《卫生系统数字证书介质技术规范（试行）》的相关要求；

b) 数字证书及签名私钥应在符合国家密码主管部门相关要求的介质中产生、存放和使用；

c) 应具备独立的数字证书及其密钥的存储安全保障机制，确保签名私钥不能以任何形式获取或从介质中导出；

d) 应具备数字证书持有人的身份校验机制，应采用生物识别、PIN码验证、设备指纹等一种或多种组合的认证方式确保数字证书及其密钥仅属于数字签名人专有和控制，无法复制和伪造；

e) 执行数字签名时，应保证签名私钥仅由数字签名人控制，不能集中托管在服务器端。采取以手机、PAD等智能移动终端为存储介质的签名私钥应采用密钥分割等技术，应由私钥存储介质和签名服务端共同作用完成数字签名。

5.3 数字签名算法

医学电子文档的数字签名算法应满足如下要求：

a） 非对称算法：应采用SM2商用密码算法，符合GB/T 32918的相关要求；

b） 摘要算法：应采用SM3商用密码算法，符合GB/T 32905的相关要求。

5.4 数字签名服务系统

用于实现数字签名的数字签名服务系统应满足如下要求：

a） 应符合 GB/T 35276、GB/T 35291、GB/T 36322、GM/T 0019、《卫生系统数字证书应用集成规范（试行）》等标准的相关要求；
b） 应具备国家密码管理局发放的《商用密码产品认证证书》；
c） 应能够在接收到医疗卫生信息系统数字签名/签名验证、时间戳/时间戳验证请求时，输出符合本标准要求的数字签名数据，或数字签名、时间戳验证结果。

6 对象要求

医学电子文档数字签名对象应为医学电子文档的全部内容以及医学服务主体、服务对象的标识信息，标识信息包括但不限于：单位编号、医学电子文档编号、医学服务提供人员编号、医学服务对象的姓名以及医学服务对象在医疗卫生信息系统的唯一标识（如病案号、身份证件号码）等。

7 格式要求

7.1 数据格式

医学电子文档数字签名数据格式应采用符合GB/T 25064要求的带时间戳的电子签名（ES-T），且应采用GB/T 25061中定义的XML数字签名语法要求的XML格式。

7.2 数据结构

数字签名数据说明见表1。

在应用本标准时，应将GB/T 25061中的附录文件存放在医疗卫生信息系统可以访问的位置。示例见图1。

表1 数字签名数据说明

元素名称	基数	约束	类型	说明与描述
SignatureValue	1…*	R	字符	数字签名值
Signcertificate	1…*	R	字符	数字证书
TimeStamp	1…*	R	字符	时间戳
DigestValue	1…*	R	字符	摘要值

示例：本标准中假定存放在http://127.0.0.1/2000/09/xmldsig中，可根据实际情况调整存放位置，数字签名数据结构如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://127.0.0.1/2000/09/xmldsig#">
  <! -- 数字签名数据 -->
  < SignedInfo >
```

```
        <SignatureValue>数字签名值</SignatureValue>
        <Signcertificate>数字证书</Signcertificate>
        <TimeStamp>时间戳</TimeStamp>
        <DigestValue>摘要值</DigestValue>
    </SignedInfo >
</Signature>
```

图 1　数字签名数据结构 XML 示例

7.3　数字签名数据与医学电子文档的关联关系

应确保数字签名数据与医学电子文档一一对应的关联关系，见图2。

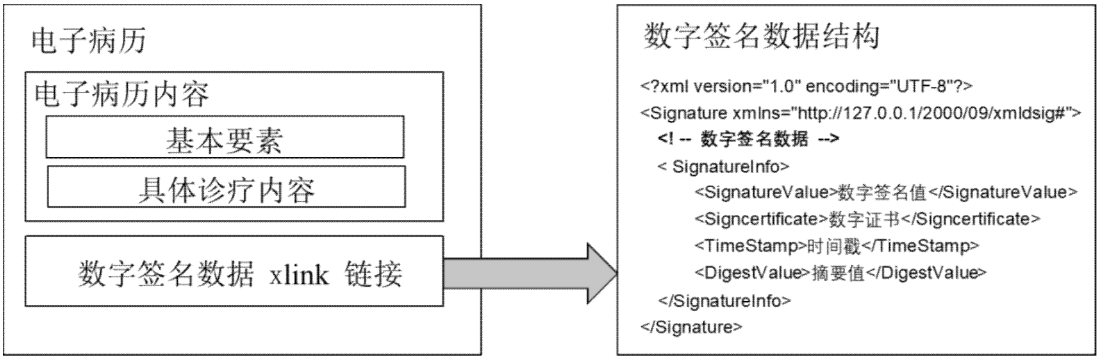

图 2　数字签名数据与医学电子文档的关联关系

8　验证要求

医学电子文档数字签名验证应满足如下要求：

a)　应验证数字证书在数字签名生成时刻的数字证书持有人和颁发者名称链的正确性、数字证书有效期和吊销列表的有效性；应比对医学电子文档原文和数字签名值在验证中产生的两个摘要信息是否一致；应验证时间戳和时间信息的有效性等内容；

b)　在数字签名验证失败时，应提示明确的验证失败反馈信息；

c)　跨机构、跨网络环境等场景下验证数字签名时，应采用密码技术保障签名数据在传输过程中的安全性。

9　存储要求

医学电子文档及其数字签名数据存储应满足如下要求：

a)　应采用 XML、版式文件等开放文档格式存储；

b)　存储内容应包括医学电子文档原文、数字签名数据、医学服务主体及服务对象的标识信息、数字签名流水号等；

c)　存储内容应能够通过数字签名验证；

d)　应独立于医疗卫生信息系统存储医学电子文档数字签名日志，包括：数字签名流水号、医学电子文档原文的唯一序列号、医学服务主体及服务对象的标识信息、医学电子文档原文摘要值、摘要算法标识、数字证书序列号、数字签名数据等信息，并可实现对数字签名日志的数字签名。

10 应用要求

10.1 医学电子文档生成

10.1.1 医学服务提供人员数字签名

医学服务提供人员在医学电子文档生成时执行数字签名应满足如下要求：

a) 应先对医学服务提供人员进行基于数字证书的身份认证，确认其真实可信身份；
b) 应先校验数字证书的有效性和合法性，校验内容包括：数字证书的有效期、颁发者证书链、吊销列表等，校验失败时，则不可进行数字签名；
c) 医疗卫生信息系统应提供具有完整语义的医学电子文档原文，由医学服务提供人员本人持有的数字证书执行数字签名；
d) 执行数字签名时，时间戳应同时执行，确保一一对应，有效证明电子数据和数字签名的有效产生时间；
e) 数字签名成功时，医疗卫生信息系统应当以适当方式标记显示医学服务提供人员已完成数字签名；
f) 数字签名失败时，医疗卫生信息系统应提示明确的验证失败反馈信息；
g) 应具备数字签名超时机制，即医学服务提供人员无任何操作的时间超过设定的时长后，应重新进行身份认证操作。

10.1.2 医学服务对象数字签名

知情同意类医学电子文档在生成时，需要执行医学服务对象数字签名的，应采用与医学服务提供人员数字签名应用要求一致的数字签名方式，或选择事件型数字证书数字签名方式。

医学服务对象在医学电子文档生成时执行事件型数字证书数字签名应满足如下要求：

a) 应先鉴别医学服务对象的有效身份信息，身份鉴别应采用两种或两种以上的组合鉴别方式，鉴别方式包括但不限于：身份证识别、指纹、人脸影像、手机短信验证等；
b) 医疗卫生信息系统应提供具有完整语义的医学电子文档原文，由医学服务对象使用事件型数字证书进行数字签名；事件型数字证书中应固化签署过程事件的信息数据，包括但不限于医学服务对象的身份鉴别信息、医学电子文档摘要值、签署行为（如手写签名笔迹数据）等；
c) 事件型证书的签名私钥应仅用于当次签署过程事件，完成数字签名值计算后应立即销毁，确保数字签名私钥不被用于其他事件的数字签名；
d) 执行数字签名时，时间戳应同时执行，确保一一对应，有效证明电子数据和数字签名的有效产生时间；
e) 数字签名成功时，医疗卫生信息系统应显示带有医学服务对象身份鉴别信息的数字签名，且其身份鉴别信息应与医学电子文档内容建立绑定关系并不可用于其它医学电子文档中；
f) 数字签名失败时，医疗卫生信息系统应提示明确的验证失败反馈信息。

10.1.3 医疗卫生单位数字签名

医疗卫生单位在医学电子文档生成时执行数字签名应满足如下要求：

a) 应先对医疗卫生单位数字证书持有人进行身份认证，确认其真实可信身份；
b) 应先校验数字证书的有效性和合法性，校验内容包括：数字证书的有效期、颁发者证书链、吊销列表等，校验失败时，则不可进行数字签名；
c) 医疗卫生信息系统应提供具有完整语义的医学电子文档原文，由医疗卫生单位持有的数字证书进行数字签名；

d) 执行数字签名时，时间戳应同时执行，确保一一对应，有效证明电子数据和数字签名的有效产生时间；
e) 数字签名成功时，医疗卫生信息系统应当显示医疗卫生单位的数字签名或反馈数字签名成功的信息；
f) 数字签名失败时，医疗卫生信息系统应提示明确的验证失败反馈信息。

10.2 医学电子文档归档

医疗卫生单位在医学电子文档归档时执行数字签名应满足如下要求：

a) 医学电子文档归档前应通过数字签名服务系统验证待归档医学电子文档中所含数字签名数据的有效性，保障医学电子文档内容的真实性、完整性；
b) 数字签名验证成功时，医疗卫生信息系统应提示明确的验证成功反馈信息，并由医疗卫生单位对符合归档标准的医学电子文档执行数字签名和时间戳；
c) 数字签名验证失败时，医疗卫生信息系统应提示明确的验证失败反馈信息。

10.3 医学电子文档复制

医疗卫生单位在医学电子文档复制时执行数字签名应满足如下要求：

a) 应验证复制部分的医学电子文档的数字签名数据的有效性；
b) 数字签名验证成功时，医疗卫生信息系统应提示明确的验证成功反馈信息，并由病案管理部门对复制部分的医学电子文档执行数字签名和时间戳；
c) 数字签名验证失败时，医疗卫生信息系统应提示明确的验证失败反馈信息。

10.4 医学电子文档封存

医疗卫生单位在医学电子文档封存时执行数字签名应满足如下要求：

a) 应验证待封存部分的医学电子文档的数字签名数据的有效性；
b) 数字签名验证成功时，医疗卫生信息系统应提示明确的验证成功反馈信息，并应由医患双方对待封存部分的医学电子文档分别执行数字签名和时间戳，把产生的数字签名数据和封存部分的医学电子文档内容存储在独立安全可靠的存储介质中；
c) 数字签名验证失败时，医疗卫生信息系统应提示明确的验证失败反馈信息。

10.5 医学电子文档共享

医疗卫生单位在医学电子文档共享时执行数字签名应满足如下要求：

a) 发送单位在医学电子文档共享前应先验证医学电子文档数字签名数据的有效性，通过验证后才能共享医学电子文档；
b) 发送单位应对共享的医学电子文档执行数字签名和时间戳；
c) 接收单位在接收到共享的医学电子文档时应先验证医学电子文档数字签名数据的有效性，确保医学电子文档在共享过程中的真实性、完整性。

参 考 文 献

[1] 中华人民共和国电子签名法
[2] 卫生系统电子认证服务管理办法（试行）（卫办发〔2009〕125号）
[3] WS/T 482 卫生信息共享文档编制规范
[4] WS/T 483 健康档案共享文档规范
[5] WS/T 500 电子病历共享文档规范