ICS 35.240
CCS C 07

中华人民共和国国家标准

GB/T XXXXX—XXXX

医疗保障信息平台 便民服务相关技术规范

Information platform of healthcare security-Technical specifications for convenience services

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 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　　录

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。

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。

本文件由全国医疗保障标准化工作组（SAC/SWG 37）提出并归口。

本文件起草单位：

本文件主要起草人：

医疗保障信息平台 便民服务相关技术规范

1 范围

本文件规定了医保码、医保移动支付、医保电子处方、个人医保信息授权查询等4项医保便民服务的接入功能、接入方式、安全和管理要求，及医保业务综合服务终端开发配置要求等。

本文件适用于合作应用渠道接入医疗保障信息平台医保便民服务模块后应实现的相关服务功能，以及应用于医疗保障信息平台医保业务综合服务终端建设。

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 4943.1 音视频、信息技术和通信技术设备 第1部分：安全要求

GB/T 9254.1 信息技术设备、多媒体设备和接收机 电磁兼容 第1部分：发射要求

GB/T 9254.2 信息技术设备、多媒体设备和接收机 电磁兼容 第2部分：抗扰度要求

GB 18030 信息技术 中文编码字符集

GB/T 26237.2 信息技术 生物特征识别数据交换格式 第2部分：指纹细节点数据

GB/T 35742 公共安全 指静脉识别应用 图像技术要求

GA/T 1286 安防虹膜识别应用 图像数据交换格式

GM/T 0028 密码模块安全技术要求

SJ/T 11363 电子信息产品中有毒有害物质限量要求

JR/T 0120.5 银行卡受理终端安全规范 第5部分：PIN输入设备

3 术语和定义

下列术语和定义适用于本文件。

3.1

医保码 healthcare security code

又称医保电子凭证，是国家医疗保障局为参保人、医保经办人员、医护人员、参保机构、定点医药机构、医药机构等在全国统一的医保信息平台颁发的统一信息标识。

3.2

医保移动支付 healthcare security mobile payment

参保人通过医疗保障部门提供的线上移动支付服务完成的费用缴纳。

3.3

合作应用渠道 third party channels

由合作应用机构建设并经医疗保障部门授权接入的，提供医保便民服务的APP、小程序、公众号、生活号等应用路径和方式。

注：合作应用机构包括定点医药机构、合作金融机构、第三方支付机构、国家/地方政务服务部门、其他经医疗保障部门认定的合作机构。

3.4

医保电子处方 healthcare security electronic prescription

定点医疗机构的医保医师在诊疗活动中使用医院管理信息系统为参保人开具,经本机构医保药师审核，能实现存储、管理、传输、重现，可作为用药凭证的数字化医疗文书。

3.5

医保电子签名 healthcare security electronic signature

医疗保障信息平台数字证书加密传输的数据电文中，以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

3.6

医保业务综合服务终端 healthcare security integrated service terminal equipment

医保业务综合服务终端采用医保码及人脸识别技术进行身份核验，基于模块化的软件开发工具，提供医保码、医保移动支付、医保电子处方、个人医保信息查询等的相关业务办理功能。

3.7

生物识别系统 biological recognition system

医疗保障信息平台中用于采集公民个人身份信息、人脸、指静脉、指纹、虹膜等数据，并进行人员信息注册和认证的软件。

3.8

硬件安全模块 hardware security module

用于保护和管理强认证系统所使用的密钥，同时提供相关密码学操作的计算机硬件设备。

4 缩略语

下列缩略语适用于本文件。

APP:应用程序（Application Program）

APN:接入点(Access Point Name)

LDAFAR:活体检测错误接受率（Liveness Detection Attack False Acceptance Rate）

LPFRR:活体检测错误拒绝率（Liveness Presentation False Rejection Rate）

HTTP：超文本传输协议(HyperText Transfer Protocol)

HTTPS：超文本传输安全协议(HyperText Transfer Protocol Secure)

SDK:软件开发工具包（Software Development Kit）

SE:安全单元（Secure Element)

SM2：国家密码管理局发布的椭圆曲线公钥密码算法
SM4：国家密码管理局发布的一种分组密码标准
FTP：文件传输协议（File Transfer Protocol）
SFTP:安全文件传送协议(Secret File Transfer Protocol)
SCP：安全复制协议(Secure copy)
TEE:可信执行环境（Trusted Execution Environment）
TOF:光飞行时间（Time Of Flight）
VPDN:虚拟专有拨号网络(Virtual Private Dial Network)
TPS:每秒传输事务数（Transactions Per Second）
QR码：快速响应码（Quick Response Code）
MAC：报文鉴别码（Message Authentication Code）
WEB：全球广域网（World Wide Web）
VPN:虚拟专有网络（Virtual Private Network）
VPDN:虚拟专有拨号网络(Virtual Private Dial Network)
SSH：安全外壳协议（Secure Shell ）
CPU：中央处理器（Central Processing Unit/Processor）

5 概述

5.1 医疗保障信息平台便民服务功能采取统一设计、统一标准、统一技术架构、统一业务规范的方式进行建设。系统架构见图 1。

5.2 便民服务功能主要包括医保码、医保移动支付、医保电子处方和个人医保信息授权查询；通过医保码实现参保人在各医保业务场景中展示本人医保码或代已绑定亲情账户关系的亲友展示医保码完成业务办理；通过医保移动支付实现参保人医保基金和个人自费或自付资金的线上支付；通过医保电子处方实现线下就诊开方或线上复诊开方、个人电子处方授权查询、电子处方流转、线下就近取药、线上送药到家等服务；通过个人医保信息授权查询实现在参保人授权前提下查询使用参保人医保信息；合作应用渠道通过互联网或专线方式接入便民服务功能模块实现相应的便民服务功能。

5.3 医保业务综合服务终端作为实现医保便民服务功能的载体，通过专线或者 VPDN 方式接入医疗保障信息平台核心业务区。

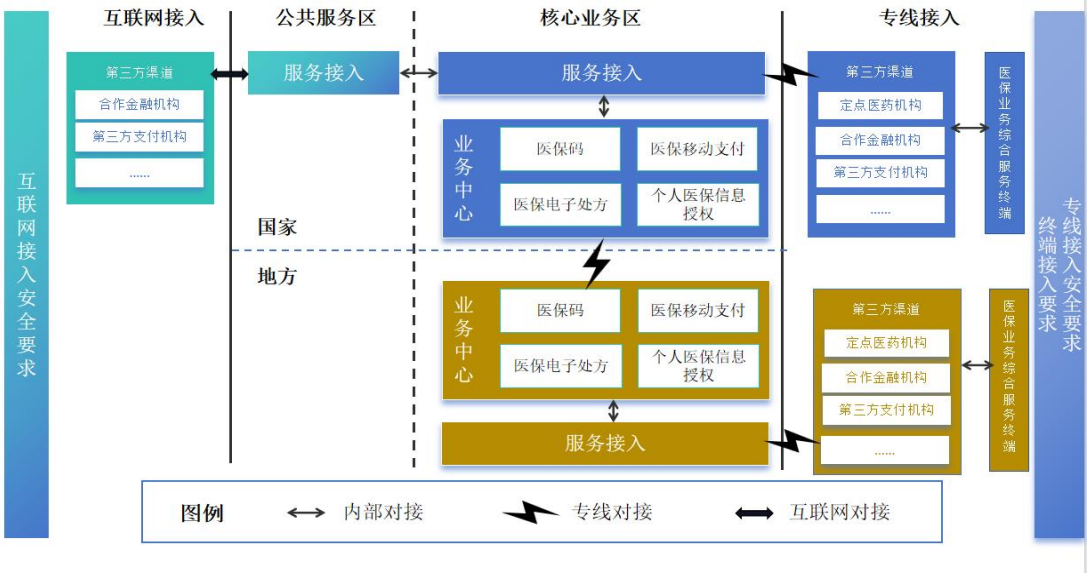

图 1　医保便民服务系统架构图

6　医保便民服务接入要求

6.1　接入功能要求

6.1.1　医保码接入功能要求

6.1.1.1　定点医药机构接入功能要求

定点医药机构接入医疗保障信息平台医保码服务后应实现在医保结算环节和需核验医保参保身份信息的业务支持使用医保码。

6.1.1.2　其他合作应用渠道接入功能要求

除定点医药机构外的合作应用渠道接入医疗保障信息平台医保码服务后应实现的功能包括但不限于：

a)　医保码激活授权；
b)　医保码二维码展示。

6.1.2　医保移动支付接入功能要求

6.1.2.1　定点医药机构接入功能要求

定点医药机构接入医疗保障信息平台医保移动支付服务后应实现的功能包括但不限于：

a）　支付：费用明细上传、支付下单、医保订单信息同步或银行卡支付下单、医保退费等；
b）　查询：医保订单结算结果查询；
c）　通知：医保结算结果通知；
d）　撤销：费用明细上传撤销。

6.1.2.2　合作金融机构接入功能要求

合作金融机构接入医疗保障信息平台医保移动支付服务后应实现的功能包括但不限于：

a)　支付：订单支付、订单退款、订单冲正等；
b)　查询：商户查询、绑卡查询、交易查询、冲正查询、退款查询等；
c)　通知：商户入网通知、绑卡结果通知、大额支付结果通知、银行文件通知等；
d)　协议：金融绑卡、解除绑卡、商户信息上传等。

6.1.2.3　第三方支付渠道接入功能要求

第三方支付渠道接入医疗保障信息平台医保移动支付服务后应实现的功能包括但不限于：

a)　查询：医保订单信息查询、现金支付通知结果查询、现金退款通知结果查询等；
b)　通知：现金支付结果通知、现金退款结果通知、医保退费结果通知等。

6.1.2.4　其他合作应用渠道接入功能要求

除定点医药机构、合作金融机构、第三方支付渠道外的其他合作应用渠道接入医疗保障信息平台医保移动支付服务后应实现的功能包括但不限于：

a）　医保码激活授权；
b）　医保移动支付订单页展示。

6.1.3 医保电子处方接入功能要求

6.1.3.1 定点医药机构接入功能要求

定点医药机构包括定点医疗机构和定点零售药店。定点医药机构接入医疗保障信息平台医保电子处方服务后应实现的功能包括但不限于：

a) 电子处方线下或线上流转授权；
b) 电子处方下载；
c) 电子处方信息核验；
d) 电子处方药师审方信息上传；
e) 药品销售出库明细上传及撤销；
f) 电子处方流转结算取药；
g) 药品配送信息同步及签收确认。

除此之外，定点医疗机构还应实现以下功能：

a) 电子处方上传预核验；
b) 电子处方医保电子签名；
c) 电子处方医院上传；
d) 电子处方撤销；
e) 电子处方信息查询；
f) 电子处方取药结果查询及反馈；
g) 电子处方审方结果查询及反馈。

6.1.3.2 医保电子处方合作应用渠道接入功能要求

医保电子处方合作应用渠道包括具备开展互联网医药服务相关资质的定点医药机构渠道和其他经医疗保障部门认定可开展医保电子处方相关业务的合作应用渠道。医保电子处方合作应用渠道接入医疗保障信息平台医保电子处方服务后应实现的功能包括但不限于：

a) 电子处方个人信息渠道应用访问授权；
b) 电子处方个人信息查询；
c) 电子处方二维码展码；
d) 电子处方线上流转授权；
e) 电子处方药品配送信息及状态同步；
f) 电子处方状态消息通知。

6.1.4 个人医保信息授权查询接入功能要求

合作应用渠道接入医疗保障信息平台个人医保信息授权查询服务应实现的功能包括但不限于：

a) 授权业务：个人医保信息授权、查询参保人授权信息、授权操作记录信息等；
b) 个人医保信息查询。

6.2 接入方式

6.2.1 医保码接入方式

医保码接入方式为：

a) 定点医药机构采取专线接入方式；
b) 除定点医药机构外的其他合作应用渠道采取互联网接入方式。

6.2.2 医保移动支付接入方式

医保移动支付接入方采取专线接入方式。

6.2.3 医保电子处方接入方式

医保电子处方接入方式为：

a) 定点医药机构采取专线、有线 VPN、无线 VPDN 等接入方式；
b) 医保电子处方合作应用渠道采取互联网接入方式。

6.2.4 个人医保信息授权查询接入方式

合作应用渠道接入医疗保障信息平台个人医保信息授权查询服务，授权业务采取互联网接入方式，查询业务采取专线接入方式。

6.3 安全要求

6.3.1 网络环境要求

接入方的网络环境应满足如下要求：

a) 信息安全等级保护三级标准，并提供三级等保测评报告；
b) 提供专线接入网络环境及设备信息。

6.3.2 信息传输协议要求

信息传输协议应满足如下要求：

a) 采用 HTTP、HTTPS 进行传输，医保码和医保移动支付可采用 FTP、SSH、SFTP、SCP 进行文件传输；
b) 协议应保证传输的保密性和完整性；
c) 每年对传输协议的证书进行有效性审定。

6.3.3 数据传输完整性要求

数据传输完整性应遵循如下要求：

a) 传输时支持信息完整性校验机制,根据 SM2 算法签名报文管理数据、鉴别信息，实现敏感信息、业务数据等传输完整性保护；
b) 具有通信延时和中断处理功能；
c) 使用符合要求的国产安全加密技术对报文进行加签处理；
d) 检测到传输完整性遭到破坏时恢复或重新获取数据。

6.3.4 数据传输保密性要求

数据传输保密性应满足如下要求：

a) 业务数据、鉴别信息数据采用 SM4 国密算法进行数字信封加密，确保数据以加密形式传输；
b) 建立会话连接前，对发送方和接收方进行身份鉴别，利用数字证书认证机制进行会话验证；
c) 会话连接过程中，会话标识应随机且唯一，并全程保持认证状态；
d) 针对批量或高频登录异常行为，利用 IP 地址、终端设备标识等信息进行综合识别，及时采取附加验证、拒绝请求等手段。

6.3.5 接入性能要求

6.3.5.1 业务吞吐量

业务吞吐量要求如下：

a) 医保码和个人医保信息授权查询接入方应根据用户规模进行定向评估；

b) 医保移动支付接入方支撑的最大业务吞吐量应满足以下要求：

1)定点医药机构、第三方支付渠道和合作金融机构应根据用户规模进行定向评估；

2)第三方支付渠道吞吐量≥5000TPS。

6.3.5.2 业务处理成功率

排除人为因素、网络因素等非系统处理环节导致的异常交易后，业务处理成功率应≥99.9%。

6.3.5.3 业务处理耗时

业务受理并完成应答的平均耗时应满足以下要求：

a) 医保码和医保移动支付业务处理耗时满足：

1）业务高峰时段业务处理耗时<5s；

2）非业务高峰时段业务处理耗时<3s。

b) 医保电子处方业务处理耗时满足：

1）业务高峰时段业务处理耗时<1s；

2）非业务高峰时段业务处理耗时<0.5s。

c) 个人医保信息授权查询业务处理耗时应满足：

1）业务高峰时段业务处理耗时<3s；

2）非业务高峰时段业务处理耗时<1s。

6.3.6 敏感数据安全防护要求

敏感数据主要包括个人账户信息、身份信息、隐私信息、密码密钥等。敏感数据安全防护应满足如下要求：

a) 征得个人用户同意授权；

b) 不应以明文的形式显示或存储。

6.4 管理要求

6.4.1 管理机构及团队

接入方应配置专门的管理机构及团队，全面负责对接和管理工作。具体要求如下：

a) 接入方负责人：负责整体接入流程的协调、管理，并承担对接过程中及后续运维阶段的全面管理责任；

b) 技术团队：接入方应配备专门的技术团队，负责系统接入后的持续稳定运行，并制定详细的应急处置方案以应对系统稳定性问题和突发的业务中断，在系统出现问题或业务中断的情况下，及时进行应急处置。

6.4.2 技术支持和运维

接入方技术支持和运维服务包括但不限于：

a) 实时监测系统状态，故障发生时能迅速定位并高效处理，将影响降至最低；

b) 持续开展性能优化，保障系统稳定运行，按时推进系统更新升级，修复既有问题。

6.4.3 验收要求

接入方应针对6.3.1、6.3.5相关要求提供相应的证明材料。

7 医保业务综合服务终端配置要求

7.1 操作系统要求

终端设备操作系统应满足以下要求：

a) 运行内存≥2GB；
b) 机身储存内存≥16GB；
c) CPU 进行人脸数据处理单元规格≥ARM 1GHz 4 核或等效计算能力。

7.2 接入网络要求

终端通过专线或者VPDN的方式接入，终端连接网络时应在系统中提供快捷APN设置功能。

7.3 外观和结构要求

外观和结构要求如下：

a) 外观及结构无明显异常；
b) 表面涂镀层均匀；
c) 标签打印清晰、完整，贴附无气泡、起翘等。

7.4 硬件和软件要求

7.4.1 接口要求

7.4.1.1 硬件接口

终端应具备串口双向通讯功能，内置相关接口：

a) 串行通讯接口（RS232 等）；
b) USB 接口；
c) 以太网通讯接口；
d) WIFI 通讯接口；
e) 蓝牙通讯接口；
f) 4G 及以上无线网络通讯接口；
g) 其他必要接口。

7.4.1.2 软件接口

软件接口应符合 6 接入要求。

7.4.2 生物识别

7.4.2.1 人脸识别

具备人脸识别能力的终端应满足：

a) 人脸采集安全

1) 设置人脸图像采集超时处理机制，在设置的有效时长内，如无法采集到符合质量要求且通过活体检测的人脸图像，模块自动退出运行；
2) 采用密码技术对采集到的用户人脸图像进行保护；
3) 结合SE或TEE对人脸采集过程中涉及到的密钥进行安全保护。

b) 人脸传输安全
1) 传输时采取加密措施，确保数据传输的机密性；
2) 采取安全措施，确保数据传输的完整性。

c) 人脸活体检测
1) 宜采用非配合式；
2) 防照片检测：应能检测或防止使用照片伪造识别人脸图像；
3) 假体检测：应能检测或防止使用人脸面具的防冒行为；
4) 应按附录A所列方法进行检测，满足LDAFAR为1%时，LPFRR≤1%。

7.4.2.2 其他生物识别

具备其他生物识别能力的终端应满足相应的生物识别性能及安全要求，其中：

a) 指纹识别满足 GB/T 26237.2 的要求；
b) 指静脉识别满足 GB/T 35742 的要求；
c) 虹膜识别满足 GA/T 1286 的要求。

7.4.3 条码识读

条码识读应满足：

a) 可内置或外接条码扫描设备；
b) 可正确识读标准 QR 码、PDF417 码、CODE128 码和 EAN13 码等码制的条码；
c) 单次识读后输出的信息，应具有唯一性和可重复性；输出数据信息的表达应没有歧义，若包含汉字，汉字编码字符集应符合 GB 18030 等；
d) 可识读最高精度不超过 0.251mm（10mil）的标准纸质条码和最高精度不超过 0.381mm（15mil）的标准电子条码；
e) 识读单个解码能力范围内条码的时间≤1s;
f) 识读解码能力范围内条码的出错率应≤10^{-4}。

7.4.4 硬件密码模块

硬件密码模块应满足以下要求：

a) 符合 GM/T 0028 的要求，等级为安全二级及以上；
b) 应使用国家密码管理部门核准的密码算法，并取得商用密码产品认证证书；
c) 应使用安全 SDK 接口，通过终端 USB 等接口写入证书，证书写入时间应在 1min 内完成；
d) 应实现医保交易信息加解密功能；
e) 使用 SE 或 TEE 对密钥和人脸数据进行保护；防攻击强度分值计算方式符合 JR/T 0120.5 的要求，对密钥的攻击总分值≥26 分，实施攻击分值≥13 分。

7.4.5 终端授权激活

终端授权激活应由授权人员进行操作，并具备相应的安全机制，包括但不限于：

a) 对授权人员进行身份认证；
b) 保留授权激活的操作日志。

7.4.6 地理位置信息上送

受理终端具备地理位置信息获取和上送功能，对地理位置信息进行有效保护。

7.4.7 电源适应能力

终端应能在交流电压AC110V～220V，工作频率50/60Hz条件下正常工作。

7.4.8 电磁兼容性

电磁兼容性应满足GB/T 9254.1-2021、GB/T 9254.2-2021的要求。

7.4.9 气候环境适应性

气候环境适应性应满足表1要求。

表 1 气候环境适应性

气候条件		要求
温度	工作	0℃～50℃各 2h
	贮存运输	-40℃～70℃各 16h
相对湿度	工作	20%～90%(40℃、非凝露态)
	贮存运输	20%～93%(40℃、非凝露态)
大气压		86kPa～106kPa

7.5 安全要求

7.5.1 物理安全

物理安全应符合以下要求：

a) 符合 GB 4943.1 要求；
b) 终端应具有医保唯一序列号；
c) 人脸识别应基于 3D 结构光摄像头或 3D TOF 摄像头；
d) 具备防探测或监控报警功能，终端在上电或关机情况下被攻击后立即进入不可用状态，并立即清除终端中的敏感信息；
e) 终端的防攻击强度分值计算方式应符合 JR/T 0120.5 的要求，对人脸图像的攻击总分值≥16 分，实施攻击分值≥8 分。

7.5.2 系统安全

系统安全应满足以下要求：

a) 终端入网前应通过具备相关资质的检测机构检测；
b) 预制全国医保统一的数字证书，确保终端真实、合法、唯一；
c) 保证操作系统的加载安全，防止非法的操作系统在终端上运行，包括但不限于对操作系统分区进行真实性和完整性校验，未通过校验的分区无法加载运行；具备开机后能启动逐级校验保护的机制，从可信根开始，逐级校验各级固件；若校验失败，终端无法正常启动；
d) 用户不得刷机及非法升级，对更新的系统进行完整性和真实性验证，不得使用系统开放环境或开源社区的默认密钥来签名系统；

e） 定期对系统漏洞进行检查与修复；
f） 对系统的外部访问接口进行限制；
g） 不得提供具有 root 权限提升功能的相关接口或服务程序；
h） 在交易过程中禁用截屏录屏功能；
i） 应采用国家密码管理部门核准的密码算法；
j） 应采取网站页面防篡改措施，应具备对 Web 后门进行检测和报警的能力；
k） 在交易结束或异常终止时及时清除终端内的敏感数据。

7.5.3 传输数据安全

传输数据应满足以下要求：
a） 应确保网络传输中数据的机密性，包括但不限于采用安全的加密算法和密钥长度；
b） 应确保网络传输中数据的完整性，包括但不限于采用 MAC 或数字签名；
c） 应能鉴别后台服务器的身份；
d） 应能监测信息重放等攻击行为，并对异常情况进行处理。

7.5.4 系统数据安全

系统数据安全应满足以下要求：
a） 确保交易信息的完整性，支持信息完整性校验；
b） 具有通信延时和中断处理功能,配合终端进行完整性保证；
c） 在检测到完整性遭到破坏时采取措施恢复或重新获取数据；
d） 具有防范暴力破解的保护措施；
e） 进行代码审查，防范应用程序中不可信数据被解析为命令或查询语句；
f） 启动安全机制防止系统被入侵。

7.5.5 应用软件安全

应用软件应满足以下要求：
a） 对终端设备应用软件进行签名，表明软件的来源和发布者；
b） 安装和更新时，采用密码技术进行真实性和完整性校验；
c） 上线前进行安全检测，包括但不限于恶意代码扫描、漏洞扫描等；
d） 提升安全防控能力，包括但不限于木马病毒防范、信息加密保护、运行环境可信等；
e） 监测并向后台系统反馈终端设备环境安全状况；
f） 防止消耗过多的系统资源导致系统崩溃；
g） 软件安装于自助式终端设备时具备防崩溃机制及防退出机制；
h） 应建立完善的交易验证机制，每次处理的客户信息均以服务器端数据为准，当服务器端检测到客户提交的信息被篡改时，应及时中断交易，并对客户请求指令的逻辑顺序进行合理控制；
i） 应对 API 接口行为进行分析，识别数据爬取等行为。

7.5.6 SDK 接口安全

SDK接口安全应满足以下要求：
a） 被调用时验证调用方的身份合法性；
b） 敏感数据、安全相关数据不得通过公开或无权限控制的接口进行传输、处理；
c） 接入支付的应用应取得支付授权许可；
d） 支付业务发起时进行安全分析，并建立异常处置机制；

e） 对发起支付业务的权限和应用进行隔离。

7.6 证书管理要求

证书管理应满足以下要求：

a） 由国家医疗保障信息平台统一 PKI/CA 体系生成，通过安全通道下发到设备中，一机一证书；
b） CA 根证书安全保存且不可篡改和替换；
c） 使用证书时，确保证书未经篡改和替换，使用 CA 根证书逐级校验证书；
d） 检查证书的有效性和正确性；
e） 使用国家密码管理部门核准的密码算法；
f） 硬件安全模块的证书制作和发放与终端设备生产相独立。

7.7 限用物质要求

除电路板组件铅含量外，应符合SJ/T 11363的要求。

7.8 编码与命名规则

7.8.1 终端序号编码规则

终端序号编码规则如图2所示：

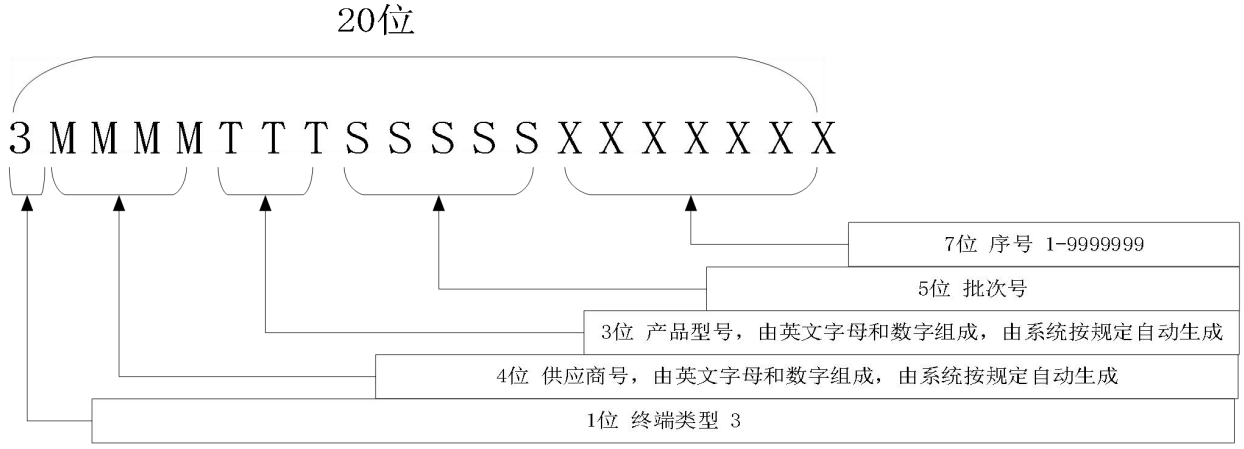

图 2 终端序号编码规则

7.8.2 版本命名规则

版本命名规则如图3所示：

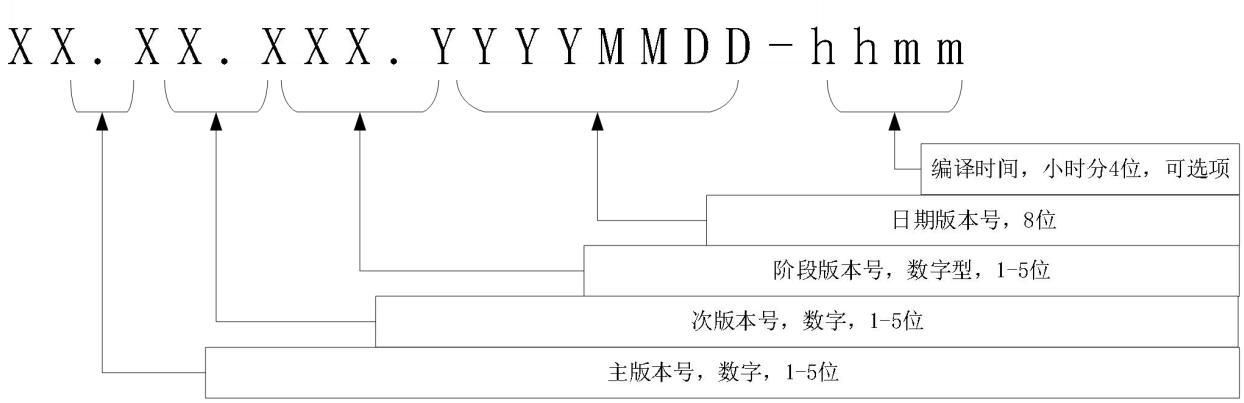

图 3　版本命名规则

7.8.3　固件或 APP 文件命名规则

固件或APP文件命名规则如图4所示：

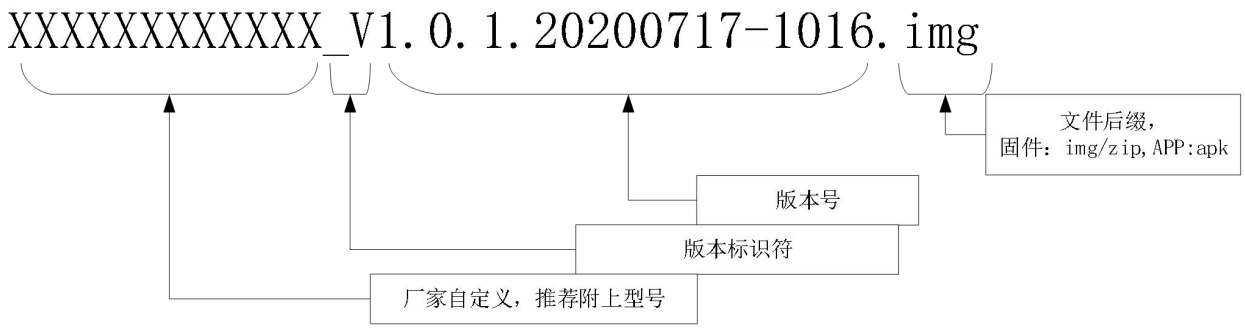

图 4　固件或 APP 文件名命名规则

附 录 A
（规范性）
活体检测评估方法

A.1 假体攻击类型

活体检测应能防范的假体攻击类型包括二维假体攻击和三维假体攻击，其中二维假体攻击包括但不限于二维静态纸质图像攻击、二维静态电子图像攻击、二维动态图像攻击等；三维假体攻击包括但不限于三维面具攻击、三维头模攻击等。

a) 二维静态纸质图像攻击，样本应考虑的因素包括但不限于：
- 样本材质：包括不限于打印纸、亚光相纸、高光相纸、绒面相纸、哑粉、光铜等；
- 样本质量：包括但不限于分辨率、清晰度、大小、角度、光照条件、完整度等；
- 样本呈现方式：包括但不限于距离、角度、移动、弯曲、折叠等；
- 样本剪裁方式：图像是否扣除眼部、鼻子、嘴部等。

b) 二维静态电子图像攻击，样本应考虑的因素包括但不限于：
- 显示设备类型：包括不限于平板电脑、手机、电脑显示器等；
- 显示设备性能：包括不限于分辨率、亮度、对比度等；
- 样本质量：包括不限于分辨率、清晰度、大小、角度、光照条件、完整度等；
- 呈现方式：包括但不限于距离、角度、移动等。

c) 二维动态图像攻击，样本应考虑的因素包括但不限于：
- 二维动态图像类型，包括但不限于录制视频、合成视频等；
- 显示设备类型：包括不限于平板电脑、手机、电脑显示器等；
- 显示设备性能：包括不限于分辨率、亮度、对比度等；
- 样本质量：包括不限于分辨率、清晰度、帧率、人脸大小比例等；
- 呈现方式：包括但不限于距离、角度、移动等。

d) 三维面具攻击，样本应考虑的因素包括但不限于：
- 样本材质：包括不限于塑料面具、三维纸张面具、硅胶面具等；
- 呈现方式：包括但不限于距离、角度、移动等；
- 光线条件：包括但不限于正常光、强光、弱光、逆光等；
- 剪裁方式：面具是否扣除眼部、鼻子、嘴部等。

e) 三维头模攻击，样本应考虑的因素包括但不限于：
- 样本材质：包括但不限于泡沫、树脂、全彩砂岩、石英砂等；
- 呈现方式：包括但不限于距离、角度、移动等；
- 光线条件：包括但不限于正常光、强光、弱光、逆光等。

A.2 测试样本选取

活体检测中假体人脸测试样本中：

——男性占 40%至 60%，女性占 40%至 60%；

——年龄小于 18 岁占 5%至 10%，18 岁至 29 岁占 10%至 20%，30 岁至 39 岁占 10%至 20%，40 岁至 49 岁占 20%至 30%，50 岁至 65 岁占 20%至 30%，大于 65 岁占 10%至 20%；

——二维和三维假体样本攻击次数比例应为 9:1。

A.3 性能指标

活体检测性能评价指标包括LDAFAR和LPFRR：

$$LDAFAR = \frac{\text{假体攻击阶段被错误判定为活体的尝试次数}}{\text{假体攻击阶段总尝试次数}} \quad (A.1)$$

$$LPFRR = \frac{\text{活体验证阶段被错误判定为假体的尝试次数}}{\text{活体验证阶段总尝试次数}} \quad (A.2)$$

参 考 文 献

[1] GB 13000 信息技术 通用多八位编码字符集（UCS）
[2] GB/T 13543 数字通信设备环境试验方法
[3] GB/T 18455 包装回收标志
[4] GB/T 20518 信息安全技术 公钥基础设施 数字证书格式
[5] GB/T 20520 信息安全技术 公钥基础设施 时间戳规范
[6] GB/T 26237.4 信息技术 生物特征识别数据交换格式 第4部分：指纹图像数据
[7] GB/T 26237.5 信息技术 生物特征识别数据交换格式 第5部分：人脸图像数据信息技术公用生物特征识别交换
[8] GB/T 26237.6 信息技术 生物特征识别数据交换格式 第6部分：虹膜图像数据
[9] GB/T 28826.1 信息技术 公用生物特征识别交换格式框架 第1部分：数据元素规范
[10] GB/T 28826.2 信息技术 公用生物特征识别交换格式框架 第2部分：生物特征识别注册机构操作规程
[11] GB/T 32905 信息安全技术 SM3密码杂凑算法
[12] GB/T 32918（所有部分）信息安全技术 SM2 椭圆曲线公钥密码算法
[13] GB/T 33135 信息技术 指静脉识别系统 指静脉采集设备通用规范
[14] GB/T 33190 电子文件存储与交换格式
[15] GB/T 33560 信息安全技术 密码应用标识规范
[16] GB/T 33767.4 信息技术 生物特征样本质量 第4部分：指纹图像数据
[17] GB/T 35273 信息安全技术 个人信息安全规范
[18] GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范
[19] GB/T 35276 信息安全技术 SM2密码算法使用规范
[20] GB/T 35291 信息安全技术 智能密码钥匙应用接口规范
[21] GB/T 35678 公共安全 人脸识别应用 图像技术要求
[22] GB/T 35736 公共安全 指纹识别应用 图像技术要求
[23] GB/T 37076 信息安全技术 指纹识别系统技术要求
[24] GB/T 38540 信息安全技术 安全电子签章密码技术规范
[25] GB/T 38671 信息安全技术 远程人脸识别系统技术要求
[26] GB/T 41988 公共安全 虹膜识别应用 图像技术要求
[27] GA 450 台式居民身份证阅读器
[28] GA 461 居民身份证制证用数字相片技术要求
[29] GA/T 893-2010 安防生物特征识别应用术语
[30] GA/T 1011居民身份证指纹采集器通用技术要求
[31] GA 1153 手持式居民身份证阅读器
[32] GA/T 1235 居民身份证指纹信息采集本地系统功能与技术规范
[33] GA/T 1212 安防人脸识别应用 防假体攻击测试方法
[34] GA/T 1429 安防虹膜识别应用图像技术要求
[35] GM/T 0015 基于SM2密码算法的数字证书格式规范
[36] GM/T 0034 基于SM2密码算法的证书认证系统密码及其相关安全技术规范
[37] GM/T 0054 信息系统密码应用基本要求
[38] SJ/T 11608 人脸识别设备通用规范

[39] 《国务院办公厅关于印发“十四五”全民医疗保障规划的通知》（国办发〔2021〕36号）
[40] 《关于医疗保障信息化工作指导意见的通知》（医保发〔2019〕1 号）
[41] 《关于开展医疗保障信息化建设试点工作的通知》（医保发〔2019〕22 号）
[42] 《关于积极推进“互联网+”医疗服务医保支付工作的指导意见》(医保发〔2020〕45号)
[43] 《国家医疗保障局关于加强网络安全和数据保护工作的指导意见》（医保发〔2021〕23号）
[44] 《关于建立完善国家医保谈判药品“双通道”管理机制的指导意见》（医保发〔2021〕28号）
[45] 《国家医疗保障局关于优化医保领域便民服务的意见》（医保发〔2021〕39号）
[46] 《国家医疗保障局办公室关于实施医保服务十六项便民措施的通知》（医保办发〔2023〕16号）
[47] 《关于开展医保电子凭证应用工作的通知》（医保网信办发〔2019〕39 号）
[48] 《医院处方点评管理规范（试行）》（卫医管发〔2010〕28号）
[49] 《医疗机构处方审核规范》（国卫办医发〔2018〕14号）
[50] 《关于印发互联网诊疗管理办法（试行）等3个文件的通知》（国卫办医发〔2018〕25号）
[51] 《关于印发长期处方管理规范(试行)的通知》（国卫办医发〔2021〕17号）