医保网络安全和信息化标准

医保业务综合服务终端（III类）技术规范（V2.1）

2022-10-31 发布　　2022-10-31 实施

国家医疗保障局网络安全和信息化领导小组办公室　发布

目 录

前 言

本规范按照 GB/T 1.1-2020 相关规则起草。

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这些专利的责任。

本标准由国家医疗保障局网络安全和信息化领导小组办公室提出并归口。

本标准起草单位：国家医疗保障局网络安全和信息化领导小组办公室。

医保业务综合服务终端技术规范

1. 范围

本规范规定了医保业务综合服务终端通用模型、要求、试验方法、质量评定程序以及标志、包装、运输、贮存等，适用于医保业务综合服务终端的生产、检验、验收等。

2. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 191 包装储运图示标志

GB 4943.1 信息技术设备 安全 第1部分：通用要求

GB/T 9969 工业产品使用说明书 总则

GB/T 13543 数字通信设备环境试验方法

GB/T 18455 包装回收标志

GB/T 38671-2020 信息安全技术 远程人脸识别系统技术要求

AIMC 0001-2006 条码阅读设备通用技术规范

GA 450-2013 台式居民身份证阅读器

GA 1153-2014 手持式居民身份证阅读

GA/T 1212-2014 安防人脸识别应用 防假体攻击测试方法

GM/T 0054-2018 信息系统密码应用基本要求

SJ/T 11363-2006 电子信息产品中有毒有害物质的限量要求

SJ/T 11364-2014 电子信息产品有害物质限制使用标识要求

SJ/T 11608-2016 人脸识别设备通用规范

XJ-G01.1-2019 医疗保障信息平台生物识别数据规范 第1部分：人脸识别数据规范

GB/T 9254.1-2021 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 9254.2-2021 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

《关于印发<全国医疗保障系统核心业务区骨干网络建设指南>的通知》医保网信办〔2019〕40号

3. 术语和定义

下列术语和定义适用于本文件。

人脸图像 face image

包含人脸的数字图像。

模板 template

已经人脸注册并登记入库的人脸图像数据。

人脸注册 face enrollment

采集身份证件号码和姓名等个人身份信息，采集人脸图像，注册人脸特征等人脸相关数据的过程。

人脸活体检测 face liveness detection

人脸图像采集认证过程中，对采集对象进行人脸的活体检测。

人脸识别 face recognition

利用可更新人脸参考进行个体识别的过程，包括人脸认证和人脸辨认。

人脸识别设备 face recognition equipment

具备人脸识别功能并能通过人脸识别确认用户身份的设备，包括但不限于桌面式、手持式、外接式及大屏壁挂式终端等形态。

硬件安全模块 hardware security module

是一种用于保护和管理强认证系统所使用的密钥，并同时提供相关密码学操作的计算机硬件设备。硬件安全模块一般通过扩展卡或外部设备的形式直接连接到电脑或网络服务器。

4. 缩略语

下列英文缩略语适用于本文件。

APP：应用程序（Application Program）

FAR：错误接受率（False Acceptance Rate）

FRR：错误拒绝率（False Rejection Rate）

IR：红外线（Infrared Radiation）

JTAG：联合测试工作组（Joint Test Action Group）

REE：普通执行环境（Rich Excecution Environment）

SDK：软件开发工具包（Software Development Kit）

SE：安全单元（Secure Element）

SN：序列号（Serial Number）

SWD：串行调试（Serial Wire Debug）

TEE：可信执行环境（Trusted Execution Environment）

TOF：光飞行时间（Time Of Flight）

UART：通用异步收发传输器（Universal Asynchronous Receiver/Transmitter）

5. 设备通用模型

医保业务综合服务终端通过专线或者 VPDN 的方式接入医保核心业务区网络，不能同互联网连接。终端采用医保电子凭证及人脸识别技术进行身份核验，基于模块化的各类 SDK，提供基于医保电子凭证的医保支付结算等相关业务的办理功能。为了保障设备本身、应用及 SDK 的安全性，要求设备提供基于国产密码技术的安全加固功能。同时，医保业务综合服务终端须接受国家及属地医保部门的监控管理。终端通用模型如图 1 所示。

图 1　设备通用模型

终端设备的通用模型可分为设备硬件层、系统层、SDK 层和应用层。

终端硬件层主要包括人脸采集装置、显示设备、通讯模块、硬件安全模块、条码阅读模块，支持扩展模块如身份证、银行卡受理模块等。

系统层应分为基于 REE 实现的普通执行环境、基于 TEE 或 SE 实现的可信执行环境。REE 为上层应用提供设备的所有功能,基于操作系统实现应用隔离；TEE 或 SE 提供更高安全级别的可信执行环境。

SDK 层为应用层提供专用的接口服务，主要包括专用于人脸识别逻辑处理的人脸 SDK、专用于设备安全防护的安全 SDK 以及专用于设备及应用监控管理的监控 SDK。

人脸 SDK 主要功能包含人脸检测、人脸采集、人脸质量判断、人脸活体检测、人脸比对等，主要实现前端设备有效的数据采集、质量控制及活体检测，即在采集设备的拍摄范围内，采集用户的人脸图像，准确标定出人脸的位置和大小，进行图像质量评估，验证用户采集过程中是否为本人操作，进行人脸比对。前端设备采集的照片需上传国家医保信息平台并符合其照片库要求，同时，其人脸设备端算法需要

与国家医保信息平台后台服务端算法的认证结果保持一致且算法应符合国家医疗保障信息平台生物识别相关规范和要求。

安全 SDK 提供密钥预置、硬件安全模块管理操作、设备接入认证、业务签名、业务加解密等功能，以实现终端设备本身及其业务运行的安全。

监控 SDK 提供设备基本属性采集、设备基本状态采集、设备性能采集、设备模组信息采集、设备通讯状态采集等功能，以实现医保部门对设备运行状态和运行风险的监控。

电子凭证 SDK 主要提供医保电子凭证激活服务。设备实现医保电子凭证激活服务应符合《国家医疗保障信息平台电子凭证技术规范》要求，统一使用电子凭证中心提供的电子凭证 SDK 进行接入。

应用层主要是结合不同应用场景提供医保电子凭证及医保支付相关业务的办理功能。

6. 终端通用要求

6.1. 操作系统要求

终端操作系统应使用主流操作系统，运行内存不小于 2GB，机身储存内存不小于 32GB，空余存储空间不小于 16GB。CPU 进行人脸数据处理的处理单元规格不低于 ARM 1GHz 4 核或等效计算能力。

6.2. 接入网络要求

医保业务综合服务终端通过专线或者 VPDN 的方式接入医保核心业务区网络，不能同互联网连接。终端设备通过调用医保核心区电子凭证中心服务完成医保业务办理。终端连接网络时须符合国家医保局《全国医疗保障信息系统核心业务区骨干网络建设指南》要求，在系统中提供快捷 APN 设置功能。

6.3. 终端的分类

Ⅰ类：仅支持扫码应用终端；

Ⅱ类：支持扫码应用和刷脸应用终端；

Ⅲ类：支持扫码应用、刷脸应用和医保支付终端。

本技术规范主要针对Ⅲ类终端，Ⅰ类和Ⅱ类终端技术规范另行制定。

6.4. 外观与结构

外观和结构要求如下：

a) 外观及结构无明显的异常，如凹痕、裂缝、飞边、缩水、应力痕、变形等；

b) 表面涂镀层应均匀，不应有明显色差、起泡、皱皮、掉漆、龟裂等；

c) 标签打印应清晰、完整，贴附无气泡、起翘等。

6.5. 功能与配置

6.5.1. 设备功能

设备应具备电源、接口、人脸识别及安全、信息显示、信息输入与输出、条码识读、设备及系统安全、系统环境、SDK、医保应用等功能。

6.5.2. 设备功能配置

设备功能配置如表 1：

表 1 设备功能配置

序号	功能	模块名称	要求
1	电源	电源模块	电源适配器工作电压范围：AC110V～220V；工作频率 50/60Hz，终端应能正常工作
2	接口	接口模块	具体要求见 6.6
3	人脸识别及安全	摄像头模块	人脸识别应基于 3D 结构光摄像头或者 3D TOF 摄像头
		人脸识别及安全模块	具体要求见 6.7
4	信息显示	显示/触摸屏模块	桌面式终端不小于 8 英寸；手持类终端不小于 5.5 英寸；大屏壁挂式终端不小于 21 英寸，应根据使用场景满足较好的交互体验
5	信息输入与输出	喇叭模块	50cm 距离响度不低于 83dB，且谐波失真< 10%
		键盘模块	支持 USB 或蓝牙方式连接外接键盘
		接口模块	≥1 个 USB 口；总输出电流≥1A；单独一个口工作时，输出电流≥1A
6	通讯	通讯模块	应满足国家相关标准要求，应支持 VPDN 相关通讯协议
7	位置	物理位置模块	支持基于基站进行定位
8	计算处理	处理芯片	性能不低于 4 核 1.0GHz
9	识读身份证件（选配）	身份证件读取模块	支持身份证读取功能，能够读取二代身份证（选配）
10	银行卡受理（选配）	银行卡受理模块	支持可扩展磁卡阅读、IC 卡阅读、非接触卡阅读（选配）
11	条码识读	条码阅读模块	具体要求见 6.8
12	设备安全	物理、系统及数据、应用及 SDK 安全模块	具体要求见 6.9

序号	功能	模块名称	要求
13	系统环境	系统环境要求	系统层应分为基于 REE 实现的普通执行环境、基于 TEE 或 SE 实现的可信执行环境
14	SDK	人脸 SDK	包含人脸检测、人脸采集、人脸质量判断、人脸活体检测、人脸比对等
		安全 SDK	提供密钥预置、硬件安全模块管理操作、设备接入认证、业务验签名、业务加解密等功能
		监控 SDK	提供设备基本属性采集、基本状态采集、设备性能采集、设备模组采集、设备位置采集、设备通讯状态采集
		电子凭证 SDK	提供医保电子凭证激活服务
15	应用	医保业务	提供医保电子凭证及医保支付相关业务的办理功能

6.6. 接口

6.6.1. 硬件接口

应用终端应具备串口双向通讯功能，应内置相关接口。

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。

6.6.2. 软件接口

软件接口应符合医疗保障信息平台有关标准的要求。

6.7. 人脸识别及安全

6.7.1. 人脸识别

6.7.1.1.人脸图像采集

人脸图像采集应满足 XJ-G01.1-2019 第 5 章的相关技术要求；应支持活体检测，防范常见假体攻击；需采取安全措施防范活体检测中人脸对象与人脸识别过程中人脸对象不一致的情况。

6.7.1.2.性能要求

人脸辨识性能指标应满足当 FAR 为 0.00001%时，FRR 应≤2%。

6.7.2. 人脸识别安全

6.7.2.1.人脸采集安全

应设置人脸图像采集超时处理机制，即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时，模块自动退出运行；

应采用密码技术对采集到的用户人脸图像进行保护，防止被非法窃取或者篡改；应结合安全单元（SE）或可信执行环境（TEE）对人脸采集过程中涉及到的密钥进行安全保护。

6.7.2.2.人脸传输安全

应满足如下要求：

a) 传输时应采取加密措施，保证数据传输的机密性；

b) 在本地软件其他进程间传输时应采取加密措施，保证数据传输的机密性；

c) 终端应采取安全措施如报文鉴别码（MAC）以确保数据传输的完整性。

6.7.2.3.人脸活体检测

在获取图像数据的过程中应进行人脸活体检测，人脸活体检测应满足 XJ-G01.1-2019 第 8 章的相关技术要求，应防范二维和三维假体攻击，防范二维和三维假体攻击次数比例为 9:1 时，性能指标应满足当 LDAFAR 为 0.1%时，LPFRR≤1%。

6.8. 条码识读

应满足如下要求：

a) 应符合 AIMC 0001-2006 条码阅读设备通用技术规范的要求；

b) 可识读一维条码和二维条码；

c) 可以是内置或外接条码扫描设备；

d) 在满足以上要求的情况下，尽量利用现有设备资源。

6.9. 终端安全要求

6.9.1. 物理安全

应符合如下要求：

a) 应符合 GB 4943.1 要求；

b) 结合机具物理特征的唯一标识及硬件安全模块唯一标识，防止被篡改或者伪造；

c) 人脸识别应基于 3D 结构光摄像头或者 3DTOF 摄像头,具体可根据不同的应用场景要求进行选择，高安全级别的场景应选用 3D 摄像头；

d) 终端应具备软硬件电路防护机制（如防拆开关、斑马条、mesh 电路等），在上电或断电情况下防止被加装非法电路或改造，终端的外置部件或分体部件应防止恶意拆除；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至少 16 分，实施攻击分值至少 8 分；

e) 终端应具备取得商用密码产品认证证书的国产密码算法安全模块。

6.9.2. 系统及数据安全

终端应满足国家医保局对数据安全传输控制方面的要求，在与医保信息系统对接过程中应遵守严格的系统安全保密机制，保证医保业务系统安全、稳定、可靠，具体要求如下：

a) 终端入网前应通过国家医保局指定的具备相关资质的检测机构检测；

b) 终端应预制全国医保统一的数字证书，保证终端真实、合法、唯一；

c) 证书的存储和交易信息的加密/解密应在硬件加密设备中进行；

传输数据应满足如下保密性要求：

a) 业务数据、鉴别信息数据采用国密算法进行数字信封加密，保证数据以加密形式传输；

b) 对发送方和接收方在建立会话前，应进行身份鉴别；

c) 在建立会话连接前，利用数字证书认证机制进行会话验证；

d) 会话标识应随机并且唯一，会话过程中应维持认证状态；

e) 终端应支持设备标识、IP 地址上送。

系统数据安全应满足如下要求：

a) 应采用数字签名等技术手段保证交易信息的完整性，支持信息完整性校验机制,根据国密算法签名报文实现管理数据、鉴别信息、敏感信息、重要业务数据等重要数据的传输完整性保护；

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) 使用硬件签名服务器对报文进行加签处理，防止数据被伪造、篡改；

d) 在检测到完整性遭到破坏时采取措施来恢复或重新获取数据；

e) 应具有防范暴力破解的保护措施；

f) 应进行代码审查，防范应用程序中不可信数据被解析为命令或查询语句；

g) 应使用安全的接口，防范接口被攻击和非授权调用；

h) 应通过自动化工具对应用程序进行检查；

i) 同时应启动相关安全机制防止系统被入侵。

设备固件更新，应采用密码技术确保固件真实性和完整性。且具备固件审核机制，确保固件中不含隐藏或非法功能。

对于搭载智能操作系统的终端，应对操作系统进行安全加固，对已经公开的 CNCVE 漏洞进行修复，仅包含必要的组件和服务，并运行于最小特权模式，包括但不限于：系统加载安全、固件安全认证、提权保护机制等，防止系统漏洞导致的敏感信息泄露。

人脸识别设备应对上送的敏感信息进行保护，要求如下：

a) 应采用国家密码管理部门核准的密码算法，保证敏感信息的完整性和机密性；

b) 发送的报文应对关键要素（如人脸图像、时间等）进行加密和签名，保证交易的真实性和抗抵赖性；

c) 在交易结束或异常终止时终端设备应及时清除终端内的敏感数据，包括人脸信息等。

6.9.3. 应用及 SDK 安全

应用软件完整性要求包括：

a) 应对医保业务综合服务终端设备应用软件进行签名，表明软件的来源和发布者，保证所下载的应用软件来源于所信任的机构；

b) 应用软件应支持 SSL 传输层安全协议，保障数据传输安全，客户端和服务端应采用 HTTPS 协议通讯；

c) 应用软件启动和更新时，应采用密码技术进行真实性和完整性校验，防范应用软件被篡改。

d) 终端应用上线前应进行安全检测，包括但不限于恶意代码扫描、漏洞扫描等；

应用软件运行安全要求包括：

a) 从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力；

b) 能监测并向后台系统反馈医保业务综合服务终端设备环境安全状况，作为风控策略的依据；

c) 应防止消耗过多的系统资源而使系统崩溃；

d) 软件安装于自助式医保业务综合服务终端设备时应具备防崩溃机制及防退出机制，避免非授权人员对系统进行操作。

应用软件合法性应满足：

a) 应对医保业务综合服务终端应用软件进行签名，表明软件的来源和发布者，保证所下载的应用软件来源于所信任的机构；

b) 应用软件启动和更新时，应进行真实性和完整性校验，防范应用软件被篡改。

c) 应采取安全加固措施提升自身安全防护，包括：

d) 在运行时应具备运行环境的检查能力，在发现运行环境异常时应具备相应处理措施；

f） 支持远程更新以支持漏洞修复；

g） 模块更新时，服务端应对待更新的模块进行签名，表明软件的来源和发布者，终端对模块进行验证，保证所下载的模块来源于所信任的机构。

6.9.4. SDK 接口安全

应符合如下要求：

a） SDK 接口在被调用时应验证调用方的身份合法性；

b） 不允许任何敏感数据、安全相关数据通过公开或无权限控制的接口进行传输、处理。

c） 所有接入支付的应用应取得支付授权许可；

d） 终端应用支付业务发起时进行安全分析，并由相应的异常处置机制；

e） 应对终端应用发起支付业务的权限和应用进行隔离，防止出现越权。

6.9.5. 调试接口

出厂设备应关闭所有调试接口，防止攻击者通过调试接口进行攻击。如果必须留有接口用于后续维护及本地升级等，需制定合理的访问控制策略，并对接口开关增加验证。

6.9.6. 证书管理要求

应满足以下要求：

a） 设备证书应由国家医保信息平台统一 PKI/CA 体系生成，并通过安全通道下发到设备中；

b） 设备证书应确保一机一证书；

c） 终端应保证相关 CA 根证书都经过终端安全保存且不可篡改和替换；

d） 终端使用证书时，应保证相关证书是未经篡改和替换的，使用 CA 根证书逐级校验证书；

e） 终端应用应检查用到证书的有效性和正确性，包括证书域名、证书链等；

f） 应使用国家密码管理部门核准的密码算法；

g） 硬件安全模块的证书制作和发放应与终端设备生产相独立，医保部门掌控终端设备的证书制作与发放等关键环节。

6.9.7. 硬件密码模块

应满足如下要求：

a） 密码模块应符合《GM/T 0028-2014 密码模块安全技术要求》，密码模块等级为安全二级及以上；

c） 硬件安全密码模块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；

d） 硬件安全模块应使用安全 SDK 接口，通过终端 USB 串口或 HID 写入证书，证书写入时间应在 1 分钟内完成。

e） 医保业务加密的平台应为硬件密码模块，实现医保相关加解密功能，其他加密操作功能可在可信执行环境中/SE中执行，但需符合相关行业安全标准。

f） 应使用安全单元（SE）或可信执行环境（TEE）对密钥和人脸数据进行保护，防止通过渗透攻击或监控辐射（包括能量波动）的方法来识别人脸数据及相关密钥。防攻击强度分值计算方式应符合 JR/T 0120.5 的要求，对密钥的攻击总分值至少 26 分，实施攻击分值至少 13 分。

终端使用的安全模块性能应满足医保业务相关要求，包括但不限于：

a） 具备高速加解密功能；

b） 支持商用密码 SM2/SM3/SM4 等算法；

c） 具备真随机源，能提供安全可靠的随机数；

d） 安全模块平台对密钥提供安全保护，加密算法应具备抵抗侧信道、故障注入等芯片级别的抗攻击能力，能够满足医保业务对于模块算法安全及性能的要求；

6.10. 终端授权激活

厂商应提供有效且可行的管理手段保证授权激活操作的安全性，防止不受控制的激活行为。仅当完成授权激活后，受理终端才能进入正常状态。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） 应对授权人员进行身份认证，可通过专用设备（如授权激活卡）识别叠加后台联机认证等方式实现；

b） 应保留授权激活的操作日志。

6.11. 地理位置信息上送

受理终端应具备地理位置信息获取和上送能力，应对地理位置信息进行有效保护，防止被篡改。

6.12. 电源适应能力

应能在电源输入 100~240 V 交流电压，50~60Hz 交流电条件下正常工作。

6.13. 气候环境适应性

要求见表 2：

表 2 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		86～106kPa

6.14. 电磁兼容性

满足 GB/T 9254.1-2021、GB/T 9254.2-2021 标准要求。

~~6.16.~~ 6.15. 限用物质

除电路板组件铅含量外，应符合 SJ/T11363-2006 的要求。

~~6.17.~~ 6.16. 终端开发要求

医保业务综合服务终端开发要求见附录。

~~6.18.~~ 6.17. 终端界面标准

终端界面标准应符合如下要求：


中国医疗保障
XXX市第一人民医院
医保业务综合服务终端


中国医疗保障
医保定点药店
医保业务综合服务终端

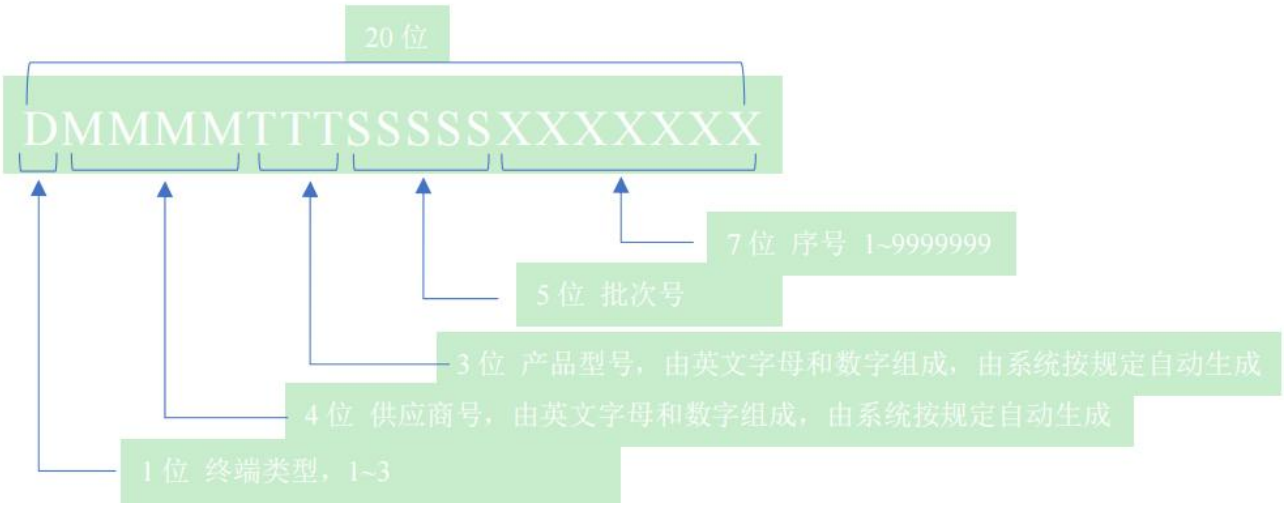

中国医疗保障
医保电子凭证
官方认证
国家医保局监制
使用方便
就医购药不用卡
安全放心
刷脸安全有保障
去激活
点击按钮即表示同意《终端用户服务协议》


选择医保账户
若查询不到参保地账户，即该地区尚未开通
厦门市
福州市
漳州市

图 2 终端界面

~~6.19.~~ 6.18. 终端序列号编码

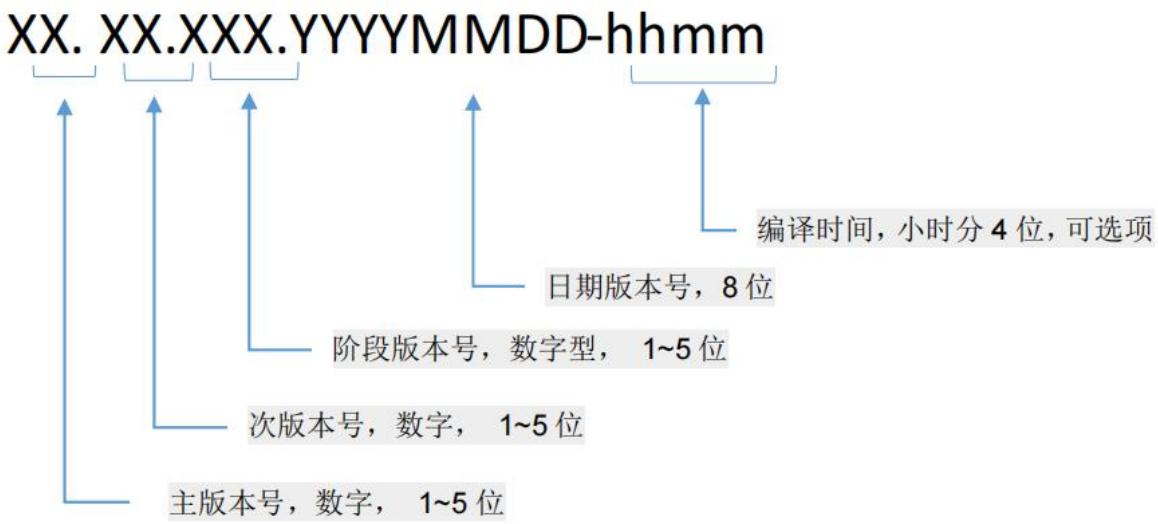
~~6.19.1.~~ 6.18.1. 终端序号编码规则



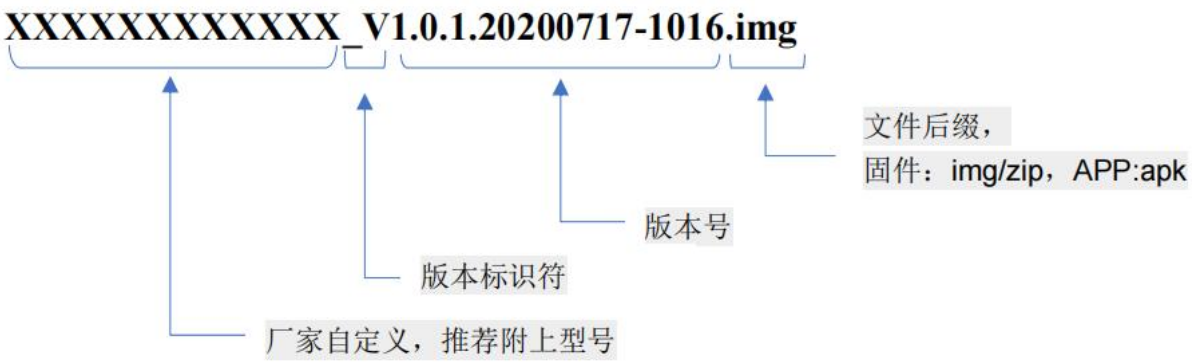
终端编码说明

终端类型	说明	编码值
Ⅰ 类	支持医保电子凭证扫码应用终端	1
Ⅱ 类	支持医保电子凭证扫码应用和刷脸应用终端	2
Ⅲ 类	支持医保电子凭证扫码应用、刷脸应用和医保支付终端	3

~~6.19.2.~~6.18.2. 版本命名规则



~~6.19.3.~~6.18.3. 固件或 APP 文件命名规则



~~6.19.4.~~6.18.4. 人脸识别 VendorID 编码规则

XXXXXX 数字，6 位

7. 质量评定程序

7.1. 一般规定

产品在研发阶段和生产过程中应按本文件和产品规范中的补充规定进行检验，并符合相关规定的要求。

7.2. 检验分类

本部分规定的检验分为：

a） 研发测试；

b） 生产测试。各类检验项目和检测分类情况如表 3：

表 3 检验分类

序号	试验项目	要求章条号	研发测试	生产测试
1	外观与结构	6.4	●	●
2	功能与配置	6.5	●	●
3	接口	6.6	●	○
4	人脸识别与安全	6.7	●	●
5	设备安全	6.9	●	●
6	电源适应能力	6.12	●	○
7	环境适应性	6.13	●	○
8	电磁兼容性	6.14	●	○
9	限用物质	6.15	●	—
注 1：●表示应进行试验的项目；○表示试验的项目可选；—表示不必进行试验的项目； 注 2：在生产测试中，安全检验仅作接地连续性、接触电流和抗电强度三项。				

7.3. 研发测试

研发测试由制造单位质量检测部门负责进行。在设备的主要设计、工艺、原材料、元器件及零部件变更时进行，主要是为研发设计把关，通过充分验证的产品方可进入量产。

7.4. 生产测试

工厂制程环节为了保证输出产品质量达标，整个生产过程中，需要对产品一致性进行充分验证，包含线前入料测试，在线功能测试，线后烧机测试等。通过相关生产良率指标监控，确保生产各环节产品质量处于受控状态，若存在超出指标的情况，将启动工厂相关应急预案，对产品或制程进行专项分析，找到根因并有效解决后方可恢复生产，保证工厂输出到市场产品满足产品质量要求。

8. 标志、包装、运输、贮存

8.1. 标志

8.1.1. 产品标志

凡在中华人民共和国境内使用的设备应具有相应的中文标志与提示，并应在设备醒目的位置设置产

品铭牌。内容包括：产品名称、型号、产品标准编号、制造厂名称、地址、出厂日期、商标等项，其标志应简明、清晰、端正和牢固。

产品中有毒有害物质含量的标识应符合 SJ/T 11364 中的要求。

8.1.2. 包装标志

包装箱外应标有产品名称、产品型号、制造厂名称、出厂日期、毛重、包装箱尺寸，并喷刷或粘贴符合 GB/T 191-2008 规定的“易碎物品”、“怕雨”、“向上”、“禁止滚翻”、“禁止堆码”等储运图示标志。包装箱外喷刷或粘贴的标志不应因运输条件和自然条件而褪色。

产品包装的回收标志应符合 GB/T 18455-2010 的要求。

8.2. 包装

包装箱应符合防潮、防尘、防震的要求，包装箱内应有装箱清单、检验合格证及有关的随机文件。产品说明书应符合 GB/T 9969 的要求。

产品包装应符合 GB/T 13384 中的有关规定。

所有随机文件应有中文文本，其中产品使用说明书的编写应符合 GB/T 9969 的有关规定。

8.3. 运输

包装后的设备应能以任何交通运输工具和方式运送到任何地点，在长途运输时不得装在敞篷的船舱和车厢，中途转运不得存放在露天仓库中，不允许与易燃、易爆、腐蚀性的物品同车装运，设备不允许经受雨、雪、液体物质的淋袭与机械损伤。

8.4. 贮存

贮存时应放在原包装箱内，存放设备的仓库环境温度应为 0℃～40℃，相对湿度为 30%～85%。仓库内不能有各种有害气体、易燃、易爆的产品及有腐蚀性的化学物品，并应无强烈的机械振动、冲击和强磁场的作用。包装箱应垫离地面至少 10cm，距墙壁、热源、冷源、窗口、空气人口至少 50cm。若无其他规定时，贮存期一般应为 6 个月。若在生产厂存放超过 6 个月者，则应重新进行逐批检验。

附录

医保业务综合服务终端应用开发要求

1. 总体原则

医保业务综合服务终端（以下简称“终端”）提供统一的桌面应用，随系统启动后强行“霸屏”，终端提供的所有业务 APP 必须通过桌面应用启动，实现终端业务一体化、标准化、规范化。

终端出厂后系统需预置终端管理 APP、终端自检 APP 及终端业务 APP。终端自检 APP、终端业务 APP 由厂商自行开发安装，终端自检 APP 需厂商按本文要求开发，终端管理 APP 由国家医保局统一提供。终端在业务检测前需预置所有的 APP 及服务，实现“开箱即用、通电过检”。

2. 终端自检 APP

2.1. 设备信息

终端支持可查看设备基础信息。界面要求如下：

2.2. 终端检测

2.2.1. 一键自检

终端需支持一键自动检测功能，检测网络和刷脸服务是否正常。界面要求如下：


医保终端检测
一键检测
极速 当前为WiFi网络，信号强度55rssi
网络检测
刷脸检测
扫码检测
身份证检测
硬件检测
设备信息

2.2.2. 手动检测

2.2.2.1. 网络检测

终端网络检测功能需支持设置服务端 IP 地址和端口，支持设置循环调用时间间隔，支持设置请求时长，默认请求时长为 72 小时，记录网络测试请求次数、请求时间、成功次数和成功率，将测试数据记录到终端本地文件。

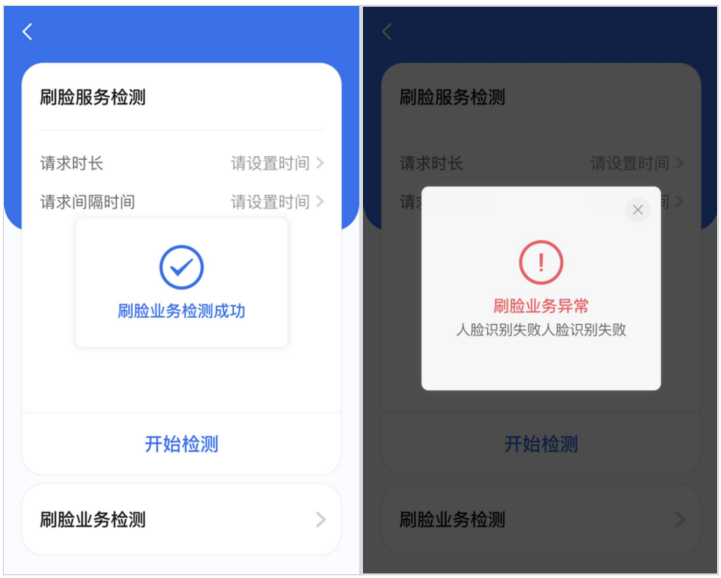
界面要求如下：

2.2.2.2. 刷脸接口检测

终端需支持自动循环检测刷脸服务是否成功，并记录接口耗时时间、请求次数、成功次数。注：不需要用户实际刷脸。

界面要求如下：

终端需支持唤起摄像头，检测是否能够成功识别人脸。界面要求如下：



2.2.2.3. 扫码检测

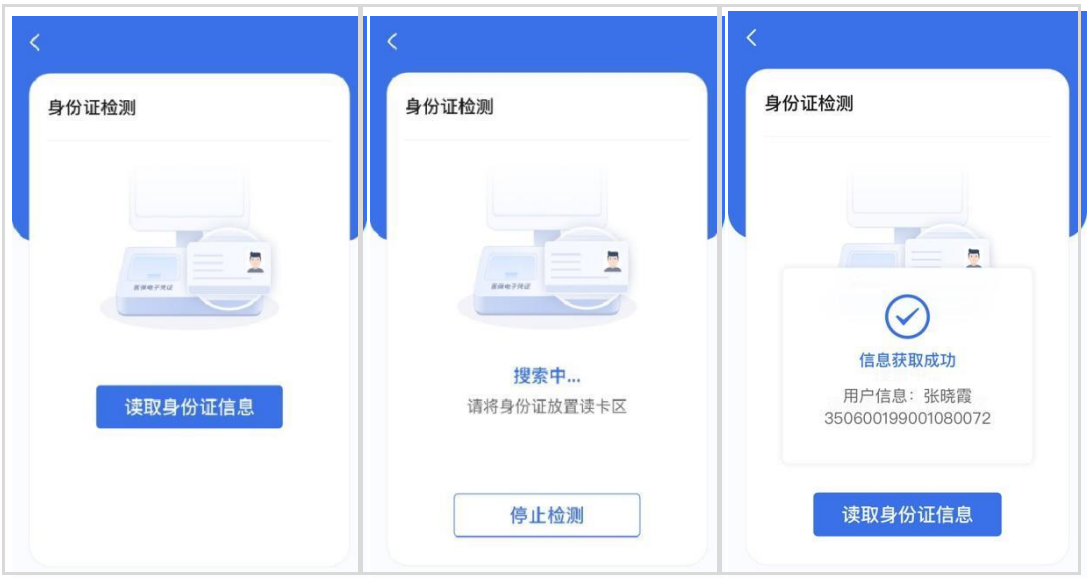
终端需支持唤起扫码墩功能，检测是否能够正确识读一维码和二维码，并将具体内容显示到终端页面上。

界面要求如下：

2.2.2.4. 身份证读取检测

如设备配备身份证读取模块，需支持调用身份证读卡器功能，检测是否能够正确识读身份证，并且将身份证号和姓名等信息显示在终端页面上。

界面要求如下：



2.2.2.5. 硬件检测

终端需支持 LED 灯检测、蜂鸣检测功能等硬件检测功能。界面要求如下：

2.2.2.6. 安全环境检测

安全环境检测需支持数据加解密、数据签名验签。

密钥位置支持：1-8 密钥类型支持：SM4_ECB、DES_ECB、AES_ECB、SM4_CBC、DES_CBC、AES_CBC、SM2、RSA1024、RSA2048

哈希类型支持：SM3、SHA256；

密钥位置支持：1-8，密钥类型支持：SM2、RSA1024、RSA2048

2.3. 必要条件

APP 入口界面需要在 intent-filter 新增一个 action 和 category，如下：

```
<activity
    android:name=".MainActivity"
    android:theme="@style/AppTheme.NoActionBar">
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />

        <category android:name="android.intent.category.LAUNCHER" />

        <action android:name="android.intent.action.chs.process" />
        <category android:name="android.intent.category.chs.process" />
    </intent-filter>
</activity>
```

医保桌面 APP 启动时会扫描系统 APP，通过过滤 action、category 展示出对应的 APP，由医保桌面 APP 统一导航。

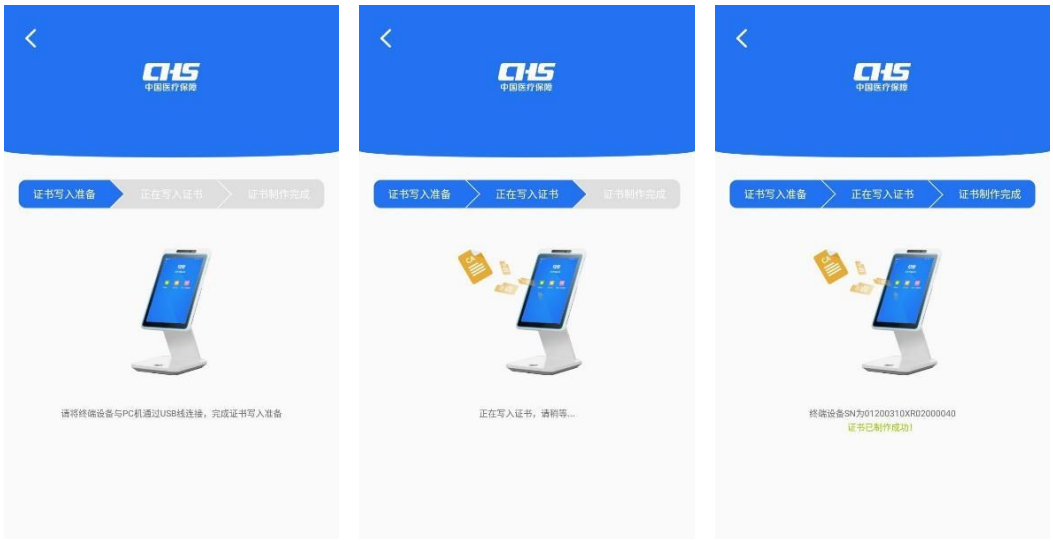
终端自检 APP 需统一在左上角设计统一的返回按钮，图片尺寸 24x44px，边距 5dp。

```
<ImageView
    android:id="@+id/img_back"
    android:layout_width="wrap_content"
    android:layout_height="match_parent"
    android:layout_centerVertical="true"
    android:layout_marginStart="10dp"
    android:background="?android:attr/selectableItemBackground"
    android:padding="5dp"
    android:scaleType="centerInside"
    android:src="@drawable/back" />
```

3. 终端管理 APP

3.1. 证书写入

终端设备在出厂前，需要由厂商完成终端证书写入，只有正确写入证书后，才能激活并正常使用。首先将设备通过 USB 口与终端证书写入工具连接，在终端桌面点“终端管理”、“证书写入”，启动证书写入应用后系统自动开始写入。



3.2. 终端激活

设备开机后会自动连接医保专网，在终端桌面点击“终端激活”APP。

勾选“阅读并同意《终端用户服务协议》”，点击“马上激活”，输入定点医药机构代码，系统会默认带出“单位名称”、“联系电话”、“单位地址”，其中“单位名称”不可编辑。

点击“安装地址”，可以调整设备真实安装地址，点击激活，完成设备激活。

再次核对激活信息后，点击“确认”，开始远程激活终端。

激活成功！

3.3. 终端设置

在终端桌面点击“终端管理”、“终端设置”可以对系统启动后默认拉起的业务主应用进行设置。