XXXXXXX
XXXX

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WS XXX—201X

电子健康卡技术规范 第5部分:客户端应用软件接入检测

Technical specification for electronic health card Part 5:

Client application software access testing

（征求意见稿）

201X-XX-XX 发布　　201X-XX-XX 实施

国家卫生健康委员会 发布

目　次

1 范围 1
2 规范性引用文件 1
3 术语和定义 1
3.1 电子健康卡客户端软件 1
4 检测概述 1
5 功能检测 1
6 安全检测 2
6.1 APP 自身安全检测 2
6.2 用户安全鉴别检测 2
6.3 数据安全检测 3
6.4 二维码安全检测 3
6.5 SDK 安全检测 4
7 接口检测 4
8 UI 检测 4
9 稳定性检测 5
10 性能效率检测 5
11 测试结果判定准则 5

前　言

本标准由卫生部卫生信息标准专业委员会提出。

本标准主要起草单位：国家卫生健康委员会，

本标准主要起草人：

电子健康卡技术规范 第5部分：客户端应用软件接入检测

1 范围

本规范规定了电子健康卡客户端软件的测试内容、测试方法及步骤和测试结果判定准则等。

本规范适用于对接入电子卡管系统的电子健康卡客户端软件从自身安全要求、用户安全鉴别、数据安全、二维码安全、SDK安全、基本功能流程、接口、UI界面、稳定性和性能等十个方面进行的接入测试，以保证接入电子卡管系统的客户端软件的安全可靠运行。

2 规范性引用文件

下列文件对于本规范的应用是必不可少的。凡是注日期的引用文件，其随后所有的修改单(不包括刊物的内容)或修订版均不适用于本规范，然而，鼓励根据本规范达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本规范。

GB/T 9386-2008　　计算机软件测试文档编制规范

GB/T 20158-2006　　信息技术软件生存周期过程配置管理

3 术语和定义

下列术语和定义适用于本规范。

3.1 电子健康卡客户端软件

设备中运行的完整的且包含虚拟化功能的APP应用程序。**类型包括手机、微信公众号、自主终端及其他类型的终端。**

4 检测概述

测试内容包括客户端软件的自身安全要求测试、用户安全鉴别测试、数据安全测试、二维码安全测试、SDK安全测试、基本功能流程测试、接口测试、UI测试、稳定性测试和性能测试共十个方面。

检测项包括必测项、选测项和条件必测项。必测项为指定测试项；选测项为可选测试项；条件必测项为如具备该功能则必测，如不具备该功能则不做要求。

5 功能检测

编号	检测项	检测方法及步骤	检测说明
1	实名制注册功能	验证应用软件是否具备用户实名制注册功能及相应的操作流程。	必测项
2	用户身份认证功能	验证应用软件是否提供多种用户身份认证功能，如静态口令身份验证功能、动态口令身份验证功能、生物识别身份验证功能、基于密钥身份认证功能等。	必测项
3	就诊卡账户绑定功能	验证应用软件是否具备就诊卡账户绑定功能（如无此功能，则为不适用）。	条件必测项

4	就诊信息查询	验证应用软件是否具备就诊信息查询功能（如无此功能，则为不适用）。	条件必测项
5	二维码申请功能	验证应用软件是否具备二维码申请功能。	必测项
6	二维码接收功能	验证应用软件是否具备二维码接收功能。	必测项
7	二维码生成功能	验证应用软件是否具备二维码生成功能。	必测项
8	交易结果通知功能	验证应用软件是否具备交易结果通知功能。	必测项
9	用户注销功能	验证应用软件是否具备用户注销功能。	必测项

6 安全检测

6.1 APP 自身安全检测

编 号	检测项	检测方法及步骤	检测说明
1	软件更新	验证通过客户端软件的更新流程。	必测项
2	客户端签名	检查开发文档中关于客户端软件的反编译要求和实现机制。 尝试进行反编译操作，验证是否成功。	必测项
3	应用软件的自检	检测应用软件启动时是否执行自检程序及检查软件运行时所必须的条件 。	必测项
4	合法性认证和风险控制	1. 检查开发文档中关于安全协议层的安全认证要求。 2. 检查开发文档中客户端软件是否提供会话超时重鉴别功能，确认其超时阈值。 3. 尝试空闲操作达到设置阈值，验证是否提供重鉴别功能。 增强要求： 4. 查看服务端对客户端的身份认证方式，包括提供对手机号码绑定或移动终端标识符绑定等认证方式，并验证其有效性。 5. 查看客户端对服务器端的身份认证方式，包括提供服务器证书，并验证其有效性。	必测项

6.2 用户安全鉴别检测

编 号	检测项	检测方法及步骤	检测说明
1	用户标识	1. 测试当进入客户端时，是否先需要进行标识（如建立账号），而没有进行标识的用户不能进入系统。 2. 测试新建立一个账号，其用户标识为已有用户的标识（如用户名），查看是否不会成功。	必测项
2	手势密码	1. 检查开发文档中客户端软件是否提供手势密码的点长度要求。 2. 尝试在添加手势密码时，添加短于或长于要求的长度，验证是否给出相应提示。 3. 检测在应用软件启动手势密码时，是否检查手势密码的界面安全。	必测项
3	重验证机制	1. 检查在执行密码重置前，是否对用户身份进行重新验证。 2. 检查开发文档中客户端软件是否提供会话超时重鉴别功能，确认其超时阈值。 3. 尝试空闲操作达到设置阈值，验证是否提供重验证功能。	必测项

4	验证信息（密码）保护	1. 检查确认客户端软件关于用户身份认证信息的存储情况。 2. 确认数据的加解密方式、加密密钥长度及密钥管理方式。 3. 尝试截获远程敏感数据的传输，验证其是否采取安全加密措施。 4. 检查口令的长度、复杂度及更改周期等。 5. 检查开发文档中是否提供密码可重复使用的次数限制。 6. 尝试在客户端验证密码可重复使用的次数限制。	必测项
5	失败的验证	1. 查看客户端是否限制无效验证次数。	必测项
6	短信验证码	1. 检查用户预留手机号码信息是否保存于服务端数据库中。 2. 检查短信验证码的长度及随机性，验证短信验证码是否仅可使用一次和有效时间。 3. 验证是否限制单个用户一定时间内的使用频次。	必测项

6.3 数据安全检测

编 号	检测项	检测方法及步骤	检测说明
1	数据的输入	1. 检查开发文档中关于敏感信息显示的规定。 2. 查看用户通过客户端软件登录时输入的登录密码是否以明文的方式显示。 3. 查看用户通过客户端软件进行支付操作时，输入的支付密码是否以明文方式显示。 4. 若客户端软件中存在其它需要用户输入的敏感数据，则查看是否以明文的方式显示。	必测项
2	数据的传输	1. 检查开发文档中关于安全协议层的安全认证要求。 2. 查看是否采取了有效措施以确保敏感数据的保密性。 3. 尝试截获远程敏感数据的传输，验证其是否采取安全加密措施。 增强要求： 4. 查看服务端对客户端的身份认证方式，包括提供对手机号码绑定或移动终端标识符绑定等认证方式，并验证其有效性。 5. 查看客户端对服务器端的身份认证方式，包括提供服务器证书，并验证其有效性。	必测项
3	数据的加密	1. 确认数据的加解密方式、加密密钥长度及密钥管理方式。	必测项
4	数据的存储	1. 检查开发文档中关于移动终端操作系统敏感数据的保留情况，保留的空间和时间是否进行限制，并明确保留的位置。 2. 检查确认客户端软件关于敏感数据的存储情况。	必测项
5	残余信息保护	1. 检查开发文档中客户端软件防止内存中残留敏感信息的措施。 2. 在移动终端上输入敏感信息并完成相应功能的操作后，测试验证敏感信息的残留情况。	必测项

6.4 接入安全检测

编 号	检测项	检测方法及步骤	检测说明
1	基本授权	1. 检查 APP 是否在电子健康卡 SDK 授权管理系统进行注册，并下载 app_secret。 2. 检查 APP 调用 SDK 时是否符合本规范第 2 部分 5.4.2SDK 验证流程。	必测项
2	附加授权	1. 检查 APP 是否在电子健康卡 SDK 授权管理系统进行注册，并下授权码文件。 2. 检查 APP 所调用的 SDK 是否是经电子健康卡 SDK 授权管理系统进行注册发布的标准 SDK。	必测项

6.5 二维码安全检测

编 号	检测项	检测方法及步骤	检测说明
1	二维码申请	检查移动终端从后台服务器获取条码时，后台是否对用户身份和移动终端进行身份验证。	必测项
2	二维码显示	1. 查看二维码是否包含敏感信息，是否采用加密技术对条码关键信息进行保护。 2. 验证是否二维码显示界面进行防截屏保护。	必测项

6.6 SDK 安全检测

编 号	检测项	检测方法及步骤	检测说明
1	SDK 接口安全	1. 检查是否提供 SDK 的接口调用手册（如应用软件以 SDK 形式提供给第三方的，为必测项）。 2. 检查 SDK 是否在电子健康卡 SDK 授权管理系统进行注册。 3. 如果是原生 APP 调用的 SDK，还需要检查 SDK 是否内置自动调用 SDK 授权验证函数。	条件必测项

7 接口检测

编 号	检测项	检测方法及步骤	检测说明
1	与虚拟化管理系统接口测试	验证应用软件是否正确实现与系统的接口交互，具备异常处理能力。	必测项
2	接口数据完整性测试	验证应用软件是否提供保障接口数据的完整性和异常检查能力。	必测项
3	接口报文功能性测试	验证应用软件是否正确实现报文交互和解析功能。	必测项
4	不同网络环境适配测试	验证应用软件是否具备在不同网络状态下的正常处理能力。	必测项

8 UI 检测

编 号	检测项	检测方法及步骤	检测说明
1	二维码识别精度测试	验证应用软件是否按照适当的精度展示二维码，最高表示精度不应超过 0.381mm（15mil）。	必测项
2	二维码展示亮度测试	验证应用软件是否在主流手机屏幕上展示二维码时，采用一致的亮度进行展示，保证二维码适度体验的一致性。	必测项
3	居民健康卡标识展示测试	验证应用软件是否将二维码与居民健康卡标识（LOGO）相结合，展现居民健康卡品牌性。	必测项
4	界面 UI 布局、功能	验证应用软件 UI 界面是否在主流手机屏幕上可以正常展示及实现正确的用户交互操作。	必测项
5	账户信息完整性测试	验证应用软件是否在主流手机屏幕上可以完整展示用户账户信息。	必测项
6	就诊信息完整性测试	验证应用软件是否在主流手机屏幕上可以完整展示就诊信息（如无此功能，则为不适用）。	条件必测项

9 稳定性检测

编 号	检测项	检测方法及步骤	检测说明
1	启动可靠性测试	验证应用软件是否在主流手机上可以正确启动。	选测项
2	操作流畅性测试	验证应用软件是否在主流手机上可以实现与用户的流程交互，无严重卡顿、无响应现象。	选测项
3	健壮性测试	验证应用软件是否正确处理各类异常，在大量多次操作下，无强制关闭、异常崩溃、应用无法关闭、弹窗无法关闭等严重问题。	选测项

10 性能效率检测

编号	检测项	检测方法及步骤	检测说明
1	安装耗时	查看应用软件在典型配置的手机上的安装耗时。	必测项
2	启动耗时	查看应用软件在典型配置的手机上的启动耗时。	必测项
3	CPU 占用率	查看应用软件的运行时的 CPU 占用率，均值应低于 30%。	必测项
4	内存占用率	查看应用软件的运行时的内存占用率。	必测项
5	关键操作耗时	验证应用软件的关键操作（生成二维码）的整体耗时不超过 3 秒。	必测项

11 测试结果判定准则

每个检测项满足检测方法和步骤要求的所有内容（不包括增强要求）则判定为“通过”，否则为“不通过”。增强要求为补充要求，是否实现对判定结果无影响。

条件必测项如具备该功能，则进行结果判定；如不具备该功能，则判定为“不适用”。

所有必测项和条件必测项测试结果均为“通过”或者“不适用”，则判定测试结果为通过；否则测试结果判定为“不通过”。