医疗电子认证系统设计与应用

刘振峰

（安徽省肿瘤医院 合肥 230001）

〔摘要〕 介绍各电子签名方案特点及选择方法，阐述基于手机盾的电子签名系统架构设计、手机盾认证系统技术原理及应用，为相关研究提供参考。

〔关键词〕 手机盾；电子认证；电子签名

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2021.10.014

Design and Application of Medical Electronic Authentication System *LIU Zhenfeng, Anhui Provincial Cancer Hospital, Hefei 230001, China*

〔**Abstract**〕 The paper introduces the characteristics and selection methods of various electronic signature schemes, expounds the architecture design of electronic signature system based on mobile phone shield, the technical principle of mobile phone shield authentication system and the application of the system, and provides references for related study.

〔**Keywords**〕 mobile phone shield; electronic authentication; electronic signature

1 引言

2018 年 7 月 31 日国务院印发《关于加快推进全国一体化在线政务服务平台建设的指导意见》，就电子政务服务平台“一网通办”做出部署，针对“统一身份认证”要求试点地区、部门于 2019 年底前完成，全国范围 2020 年完成[1]。在此背景下移动身份认证方案关注度不断升高。医疗卫生信息化系统涉及患者隐私信息访问授权和身份认证、医疗事故责任认定以及公共卫生系统安全保障等问题，保障医疗卫生行业信息安全尤为重要[2]。目前医疗行业解决信息安全问题的通用方案是以公钥基础设施/认证机构（Public Key Infrastructure/Certification Authority，PKI/CA）为基础的安全防护和网络可信认证方案，基于该方案的硬件 USB Key 数字证书认证系统为各类业务系统提供身份认证、电子签名等服务，是目前医疗领域使用较为普遍的数字证书认证方式。但是传统 USB Key 存在携带不便、易丢失、硬件投入大等弊端[3]，随着移动互联网技术发展以及智能移动终端普及，越来越多医疗信息系统终端从台式计算机扩展至移动设备。针对移动互联网业务需求特点、电子签名技术发展趋势以及电子签名法的要求，基于手机盾的移动身份认证系统为电子签名提供新的解决方案，为低成本使用电子签名以及相关安全认证技术提供可靠手段。

2 电子签名方案对比与选取

2.1 电子签名方案比较（表 1）

2.1.1 USB Key（硬件数字证书载体） 使用 USB Key 存放代表用户唯一身份的数字证书和用户

〔修回日期〕 2021－01－27

〔作者简介〕 刘振峰，工程师，发表论文 2 篇。

私钥。此方案基于 PKI 体系，用户私钥在高安全度 USB Key 内产生且终身不可导出到 USB Key 外部。在数字签名应用中，交易数据数字签名均在 USB Key 内部完成并受到 USB Key 个人识别号码（Personal Identification Number，PIN）保护。

2.1.2 *动态口令* 最安全的身份认证技术之一，根据专门算法生成一个不可预测的随机数字组合，每个密码只能使用 1 次，被广泛运用于网络银行、电信运营商、电子商务、企业等领域。

2.1.3 *基于手机盾的移动签名方案* 基于手机芯片 TEE 和 SE 实现的移动终端高安全性解决方案，支持将传统盾（Key）转化到移动终端（手机），保证安全性和便捷性。

表 1 电子签名方案比较

特点	基于手机盾移动签名	USBKey	动态口令
安全级别	具有独立的安全认证通道和过程，安全级别高；有国家相关政策支持	硬件加密，安全级别高；有国家相关政策支持	存在安全漏洞，容易被钓鱼攻击，安全级别较弱无国家相关政策支持
适用范围	可实现跨平台的认证；服务于多个业务应用	仅适用于 IE 浏览器业务应用；1 个 USKey 服务 1 个行业	可以实现跨平台的认证；1 个动态口令令牌服务 1 个业务
市场拓展	移动签名可实施产品标准化，市场拓展空间大，存在成熟的产品	已在银行和企业内部使用，有一定的市场	在安全级别要求不高的行业有一定的需求；不能实现认证的产品标准化，安全级别太低，不具有推广价值
成本情况	用户开通成本最低，使用成本最低	用户开通成本较低，使用成本可以忽略	用户使用成本较高，每 3 ~ 5 年需要进行 1 次更换成本
使用便捷性	仅需手机安装 APP 就可以实现多个业务的身份认证	需要携带 USKey 设备，仅能在 Windows 操作系统上使用	需要携带动态口令牌设备，在规定时间内输入动态口令

2.2 方案选择

2.2.1 *基本情况* 互联网医院移动电子签名平台建设方案应支撑电脑端和移动端的互联网电子签名业务，结合微信、企业微信账户安全体系为医护人员、患者提供在线刷脸实名认证、移动 CA 数字证书签发、在线诊疗和电子处方电子签名、电子病历电子签名等安全应用技术支撑。互联网医院移动电子签名平台可满足互联网医疗信息系统在微信、企业微信、APP 和电脑端系统中的各类应用需求。

2.2.2 *应用案例* 中国科学技术大学附属第一医院为省级大型三级甲等综合性医院，由 4 个院区构成，开放床位 4 672 张，日均门诊约 20 000 人次。2016 年医院推行基于硬件 USB Key 的个人 CA 电子签章系统，门诊和住院电子病历只需在电脑上使用 USB Key 签名即可，无需在纸质病历上手写签名。个人 CA 推行后日均签名数量达到 30 000 次，在提高医生诊疗效率的同时，也暴露出使用场景单一、不易携带、维护成本较高等问题。需要应用一款多场景、方便携带、低成本的移动电子签名认证系统，结合医院实际需要最终选择基于手机盾的移动签名方案。

3 手机盾认证系统架构设计

3.1 系统整体架构（图 1）

基于手机盾的电子签名系统包含移动身份认证系统、数字签名服务器、移动电子签章系统和时间戳服务系统，可提供在线移动实名身份认证、数字签名、数据加密、时间戳、电子签章等服务，从可信身份、行为、数据、时间 4 个范畴搭建互联网医院移动电子签名平台，从而真正实现互联网医疗信息系统的可信业务环境建设需求。

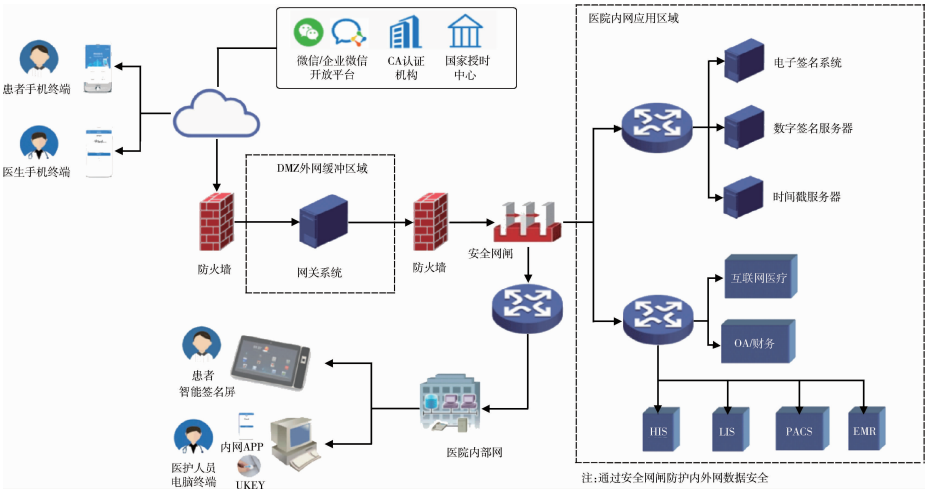

图 1 手机盾认证系统整体架构

3.2 移动端认证系统架构

3.2.1 整体情况 移动端身份认证系统通过应用程序接口（Application Programming Interface，API）和医院信息系统（Hospital Information System，HIS）对接。针对浏览器/服务器（Browser/Server，B/S）系统，业务应用系统通过手机盾提供的安全超文本传输协议（Hyper Text Transfer Protocol Secure，HTTPS）接口进行交互，浏览器端利用微信二维码和手机盾交互。针对医院现有移动 APP 应用，手机盾直接提供软件开发工具包（Software Development Kit，SDK）给现有 APP 应用程序使用，应用程序通过 SDK 方式调用手机盾。

3.2.2 手机盾框架功能组成 （1）展现层。可视化手机盾界面，提供用户登录、口令输入、指纹验证、修改口令、二维码扫码等界面操作。（2）接口层。分两种类型接口，应用第 3 方 SDK 接口向第 3 方应用提供相关服务。（3）核心层。手机盾核心服务层，提供密钥运算、签名、加解密、安全键盘、获取设备信息等核心业务。（4）安全区。采用可信执行环境（Trusted Execution Environment，TEE）标准接口，手机盾设备密钥、设备信息等存储在安全区域，操作系统对其无法操作和修改[4]。（5）安全加固。手机盾采用反编译安全加固技术，具有一定抗逆向工程以及抗调试与篡改能力，防止恶意程序或攻击者绕过用户身份认证机制[5]。手机盾架构，见图 2。

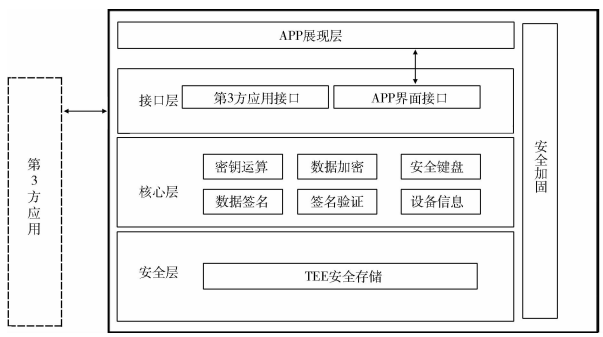

图 2 手机盾架构

3.3 移动身份认证系统架构

认证系统后台架构，见图 3。（1）接口层。提供手机盾调用和管理端接口，管理端接口为系统管理界面提供服务。（2）业务层。安全审计：对系统所有操作和接口调用进行详细记录，非授权人员不可篡改记录；系统及服务监控：对系统服务进行监控，授权管理员查看设备运行状态；账户管理：对手机盾账户进行管理、统计、查询，维护账户状态，存储账户对应的设备公钥信息等；管理员管理：对系统操作管理员进行添加、删除、修改以及授权，只有授权管理员才能登录系统进行操作。（3）应用管理。添加应用，对应用进行授权。（4）密码接口层。实现与密码模块交互，包括密钥生成、数据签名、数据加密接口等操作。

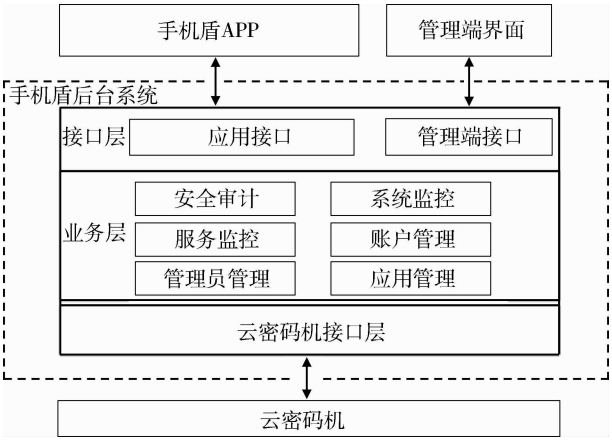

图 3 认证系统后台架构

4 系统技术原理

4.1 证书管理

电子认证系统应为各项业务系统用户颁发软数字证书并进行动态管理，包括证书申请、发放、吊销、更新、解锁等。数字证书管理情况记入日志文件，保留管理操作痕迹，实现数字证书管理痕迹可查、可溯源[6]。系统提供数字证书管理情况查询统计功能接口，方便医院业务系统调用数字证书管理情况。

4.2 身份认证流程

提供 CA 身份认证功能，电子病历系统通过调用电子认证服务系统相关接口，能够利用数字证书进行用户身份认证。个人电脑端和移动 APP 身份认证基于同一数字证书（每个用户只分配 1 个数字证书）。提供数字证书与用户账号绑定功能，提高证书安全性。个人电脑端 Web 应用调用手机盾签名相关业务流程如下：应用系统调用手机盾 API，申请认证或签名二维码，返回二维码统一资源定位符（Uniform Resource Locator，URL）地址；应用系统发送二维码到浏览器，浏览器展现二维码图片；用户打开手机盾，点击扫码；用户输入密钥保护口令或指纹，获取密钥操作权限；提交认证处理信息；手机盾和云密码机配合完成密钥协同计算[7]；推送签名或认证结果到应用系统，见图 4。

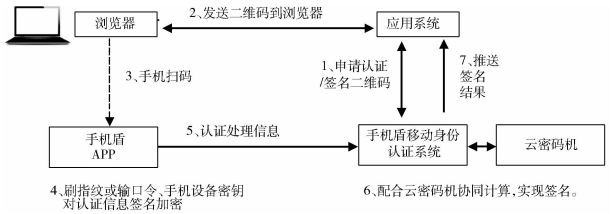

图 4 身份认证流程

4.3 电子签章

通过签章接口，电子病历系统用户能够使用签名预设、更改、现场签名、补签名等功能，可在监督检查、风险分级登记以及其他业务操作产生的电子文件指定位置进行手写签名和加盖单位签章。电子签章提供事务证书功能，为监管人员提供临时数字签名，方便其在电子文书上手写签名确认。电子签名功能保证签名图片原笔迹不变形、不失真。签名数据需加密传输，对已签名的电子文件进行加密存储，以防止恶意篡改。

4.4 签章验证

对于已签章的电子文件，电子认证系统提供文件签章有效性验证接口（具备单个和批量文件在线验证功能）和验证工具软件（对单个或批量文件线下验证）[8]，电子病历系统通过调用批量验证接口能够及时发现被篡改电子文件。签章文件验证功能提供直观的验证结果展示，方便用户查看。

5 系统应用

5.1 数字证书申请

对于申请开通手机电子认证权限的医生，信息维护人员在手机盾后台维护医生基本信息，包含工号、科室、身份证号和手机号等。可进行单人信息维护，也可通过 Excel 将信息批量导入系统中。医生首次申请数字证书流程为：使用微信扫描二维码，弹出手机盾登录界面后输入手机号，只有通过手机盾后台维护的手机号才能收到登录验证短信；登录后系统进行人脸识别实名认证；通过手机进行手写签名采集。

5.2 认证流程

已经在手机盾申请证书的用户可使用微信扫描

二维码登录，通过手机授权登录医院信息系统。系统默认授权时间为 5 小时，授权期间登录医院信息系统签署的文件无需在手机上进行授权操作，超时后授权自动取消。

5.3 后台数据管理

手机盾具有可视化后台管理界面，通过管理界面可进行用户添加删除、查看文件签署日志、服务器资源消耗情况以及签章管理等操作。例如中国科学技术大学附属第一医院全院申请手机盾的用户数量为 5 465 人，在全院执业医师中占比 95% 以上，执业医师只需通过手机即可进行文件签署，平均每日使用手机盾签署文件数量约 10 000 份，较以往 USB Key 故障率和报修次数大幅下降。

6 结语

手机可作为电子证书介质，较 USB Key 硬件介质使用更为方便。手机盾应用系统充分发挥移动互联网优势，医护人员可有效利用零散时间进行电子病历审核和签名，实现医疗过程移动化、便利化。基于手机证书的医院电子认证系统针对移动互联网业务需求特点、电子签名技术发展趋势以及电子签名法的法律要求设计新的电子签名解决方案，为低成本使用电子签名以及相关安全认证提供可靠技术手段。

参考文献

1 王琎. 我国电子认证服务业发展现状、趋势及建议［N］. 中国计算机报，2019 - 04 - 01（12）.
2 戴宇飞. 医院网络与信息安全策略研究［J］. 数码世界，2020（7）：208.
3 吕尧，周千荷. 电子认证服务行业发展分析［J］. 网络空间安全，2020，11（9）：94 - 103.
4 朱佳伟，喻梁文，关志，等. Android 权限机制安全研究综述［J］. 计算机应用研究，2015，32（10）：2881 - 2885.
5 甘佳，张茂凡，周志寰，等. 基于反编译技术的 Android 应用自动化测试方案［J］. 西南科技大学学报，2019，34（1）：74 - 79.
6 杨文清. 浅谈数字签名与数字证书［J］. 计算机产品与流通，2020（11）：286.
7 任良钦，王伟，王琼霄，等. 一种新型云密码计算平台架构及实现［J］. 信息网络安全，2019（9）：91 - 95.
8 李强，高超航，何智，等. 一种基于区块链的电子签章验证平台设计［J］. 信息安全研究，2019，5（12）：1089 - 1095.

（上接第 63 页）

18 中国青年网. “智慧养老”越来越近［EB/OL］.［2020 - 04 - 26］. https：//baijiahao. baidu. com/s? id = 1665014464741729372.
19 郑思思，郭华玲，张夏天，等. 可穿戴设备在中医药健康管理中的应用与展望［J］. 世界科学技术 - 中医药现代化，2019，21（12）：2678 - 2683.
20 上海中医药大学. “中医智能舌诊系统研发”项目获得国家重点研发计划立项资助［EB/OL］.［2018 - 04 - 16］. http：//www. shutcm. edu. cn/2018/0416/c221a14701/page. htm.
21 搜狐. 又一项中医国际标准！舌诊仪舌色苔色获取表示方法国际标准发布［EB/OL］.［2019 - 01 - 14］. https：//www. sohu. com/a/288938695_ 456034.
22 樊瑛，唐晓笛. 全科医生结合物联网社区慢病管理模式初探［J］. 中国继续医学教育，2020，12（19）：166 - 168.
23 史心傲，张帆，常乐，等. 日本养老产业的精细化、专业化与人性化——2018 日本国际福祉机器展及日本养老设施考察记［J］. 家具与室内装饰，2018（12）：116 - 118.
24 陈言. 日本人工智能养老模式：大数据与机器人［N］. 中国经济导报，2017 - 09 - 16（B03）.
25 中国中医药报. 智能针灸机器人应用于临床还待时日［EB/OL］.［2018 - 12 - 17］. http：//paper. cntcm. com. cn/html/content/2018 - 12/17/content_ 604487. htm.
26 百度. 中医推拿按摩人才缺口大，AiTreat 让机器人做他们的下代“接班人”［EB/OL］.［2018 - 11 - 23］. https：//baijiahao. baidu. com/s? id = 161788540545009 9001.
27 小阳科技速报. 机器人中医看病？让你脑洞大开！［EB/OL］.［2020 - 05 - 21］. https：//baijiahao. baidu. com/s? id = 1667279887941015631.
28 上海道生医疗科技有限公司. 智能中医机器人正是针对中医的痛点［EB/OL］.［2020 - 04 - 03］. http：//www. daosh. com/about - details - 111. html.
29 王素娟，李会，王淑君，等. 大数据背景下居家养老云服务平台构建研究［J］. 合作经济与科技，2020（13）：188 - 190.