

扫码签名在医院电子病历系统中的应用实践

付超 寇斌 魏星

(天津市第四中心医院信息科 天津 300140)

〔摘要〕 以天津市第四中心医院为例,介绍基于U-KEY的电子签名现状以及扫码签名认证系统优点,阐述扫码签名网络架构、工作流程,指出应用扫码签名能够增加签名便利性,提高医护人员工作效率。

〔关键词〕 扫码签名; CA认证; 电子病历; U-KEY认证

〔中图分类号〕 R-056 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2021.01.015

Application of Scan Code and Signature in Electronic Medical Record System of Hospitals FU Chao, KOU Bin, WEI Xing, Department of Information, Tianjin Fourth Central Hospital, Tianjin 300140, China

〔Abstract〕 Taking Tianjin Fourth Central Hospital as an example, the paper introduces the status quo of U-KEY electronic signature and the advantages of the scan code and signature authentication system, expounds the network architecture and workflow of scan code and signature, points out that its application can increase the convenience of signing and improve the working efficiency of medical staff.

〔Keywords〕 scan code and signature; CA certification; Electronic Medical Records (EMR); U-KEY certification

1 引言

由于医疗卫生信息化系统涉及用户隐私信息的授权访问和身份验证、医疗事故责任认定、医疗路径信息监管以及公共卫生体系的安全保障等敏感问题,信息安全问题尤为突出^[1]。为满足电子病历签名身份认证、可靠电子签名以及医疗数据保护等需求,天津市第四中心医院于2015年正式上线CA认证系统,使用U-KEY作为安全介质,U-KEY含有专门密码芯片,将数字证书保存在U-KEY中,近5年使用过程中发现诸多问题。本院对CA认证系统进行全面升级,以扫码签名方式取代U-KEY

密码验证签名。扫码签名在身份、安全验证以及使用便利性方面都有很大提升,提高医护人员工作效率,同时减少CA管理人力成本。

2 电子签名方式

2.1 基于U-KEY的电子签名现状

仅支持Windows环境下电脑端使用CA证书,需安装驱动,插件调用稳定性不佳、用户使用不便利^[2]。每年升级续费需统一上交U-KEY,严重影响医护人员使用,效率低下。医护人员流动性大,U-KEY更换成本高。U-KEY拔插使用频繁,硬件经常损坏,更换时间长,增加使用成本。

2.2 扫码签名认证系统优点

一是便利性。使用手机扫码即可实现电子签名,解决U-KEY丢失或未携带的问题。二是免驱

〔收稿日期〕 2020-05-15

〔作者简介〕 付超,硕士,中级职称,发表论文3篇;通讯作者:魏星,科长。

动。无需额外安装任何插件或驱动，只需下载扫码签 APP 即可，简单易行。三是安全性高。手机人脸识别，与公安网信息系统核对身份信息，保证身份真实有效。

3 扫码签名网络架构

本院网络整体结构可分为 3 个主要区域：外部网络、安全区（Demilitarized Zone, DMZ）以及内部网络。CA 公司服务端提供数字证书签发、验签等服务；扫码签客户端通过防火墙接入安全区，与扫码签服务端进行通信。扫码签服务端、签名服务器、时间戳服务器部署于安全区内，用于与扫码签客户端通信。由负载均衡为安全区域各内部网络组件提供服务，加强网络数据处理能力、提高网络灵活性和可用性；内部网络部署客户应用系统，应用系统通过网闸后主动推送签署请求到安全区的扫码签服务，然后以轮询方式查询签署结果。扫码签业务网络拓扑，见图 1。

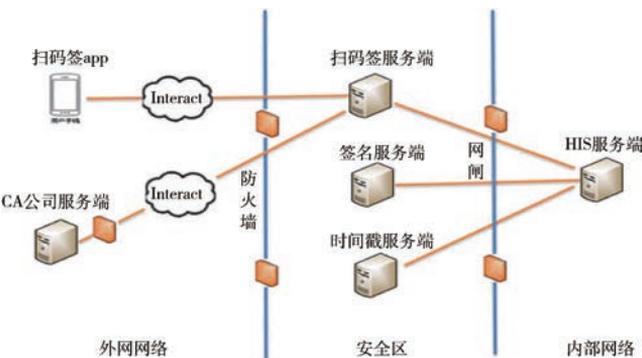


图 1 扫码签名业务网络拓扑

4 扫码签名工作流程

4.1 证书申请

使用证书的人员包括所有电子病历中需要签名的医护人员。必须由医护人员本人申请与其身份相

对应、由 CA 中心签发的数字证书。数字证书常称为密钥，其以介质（USB 接口密钥）方式存在^[3]。扫码签用手机取代传统 USB 介质接口密钥，将密钥存储在手机端，不需要随身携带 U - KEY，方便医护人员随时使用，提高工作效率。

4.2 身份认证

在手机端下载扫码签 APP，首次登录需要注册信息、上传身份证照片。输入身份证信息后，系统自动调用公安网身份核查系统，通过人脸识别和视频录音的方式进行身份认证，确保本人身份真实、有效。身份认证的前提是在扫码签服务端已经存在此身份信息。该申请人必须是本院登记的医护人员才能注册扫码签 APP，否则无法完成注册。

4.3 扫码登录

医护人员在电子病历系统中点击登录发送登录请求，电子病历系统服务端调用 CA 扫码签服务端请求授权接口，将登录请求关键信息发送给 CA 扫码签服务端。CA 扫码签服务端收到医院信息系统（Hospital Information System, HIS）服务端发送的请求登录信息，然后返回随机数至 HIS 服务端。HIS 将随机数以二维码形式展示到电脑端。医护人员使用手机扫码签 APP 扫描 PC 上二维码，确认后点击授权登录，然后扫码签 APP 与 CA 服务端进行握手确认。电子病历系统服务端在 PC 上显示二维码后会定时循环调用 CA 服务端检查授权状态接口，获取授权处理状态。此时扫码签 APP 和 CA 服务端已完成握手，会返回授权处理状态至电子病历服务端（成功时同时返回 HIS 用户 ID 等信息）。电子病历服务端根据授权状态返回的用户 ID 确定该 ID 对应的用户在使用手机进行登录操作，转发登录信息给 PC 端。扫码登录流程，见图 2。

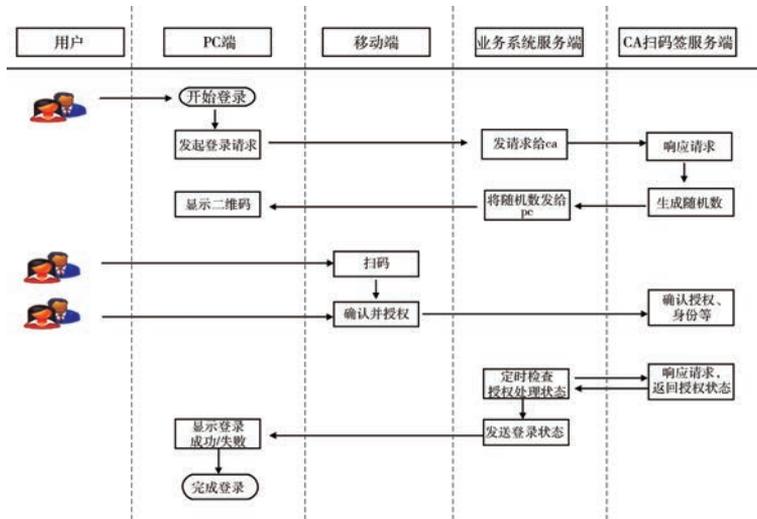


图 2 扫码登录流程

4.4 扫码签名

使用手机扫二维码进行身份、证书验证，最后实现签名，医护人员在电子病历系统 PC 端点击签署。电子病历系统将签署请求相关信息发给其服务端，服务端收到用户签署确认内容后先进行 hash 摘要运算，然后调用 CA 扫码签服务端的请求授权接口，将签署请求相关信息（用户 ID、hash 摘要等）发送至 CA 服务端。CA 扫码签服务端收到电子病历服务端发送的请求签署信息，根据用户 ID 找到对应的手机，将请求授权信息推送到手机端。医护人员扫码签 APP 上收到授权签署的请求信息，用户确认后点击授权。然后扫码签 APP 进行电子签名，和 CA 服务端进行握手确认。电子病历系统服务端发送签署请求后会定时循环调用 CA 服务端检查授权状态接口，获取授权处理状态。此时扫码签 APP 和 CA 服务端已完成握手，会返回授权处理状态、用户 ID、签名结果、证书信息等。

4.5 扫码签验证

由明文电子病历信息验签和盖戳时间明文验证^[4]，保证电子病历系统签名数据的真实性。电子病历系统服务端调用签名验签服务器验签接口，将扫码签相关签名数据作为参数传入（包括原文、签名结果、证书信息）。签名验签服务器对传入的签名数据进行验签，返回验证结果。验证成功后电子病历系统将保存扫码签执行过程中的相关数据，包括用户签署确认内容、签名结果、证书信息等，以备日后查验。

4.6 盖时间戳

电子病历系统将扫码签系统执行过程中的签名原文和结果拼在一起，作为时间戳签名原文，调取时间戳服务进行签名；调用时间戳服务的验签和解析接口对时间戳数据进行验证和解析；对时间戳结果验签和解析成功后，保存相关数据，包括即将盖时间戳的原文（即扫码签系统执行过程中的签名原文和结果拼在一起的字符串）、盖时间戳的结果，以备日后查验。扫码签名、签名验证、盖时间戳流程，见图 3。

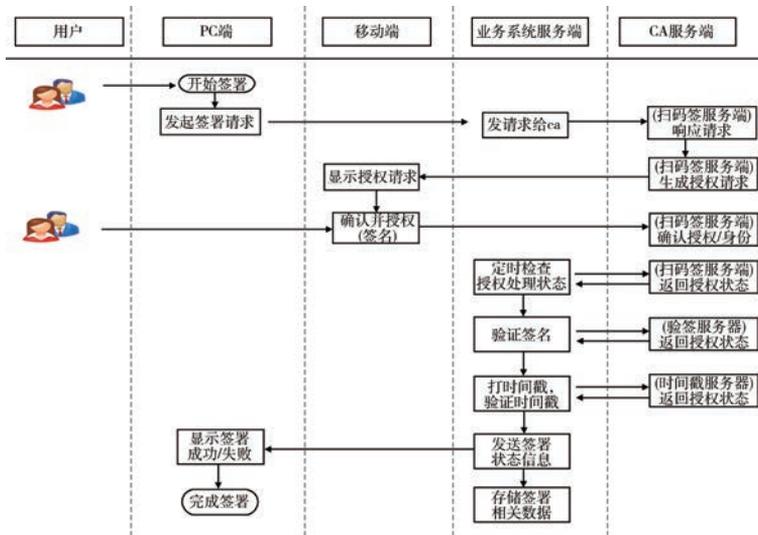


图3 扫码签名、验证签名、盖时间戳流程

4.7 病历归档批量电子签章

病历审核通过后完成归档。对归档病历的电子签章是指对整份电子病历盖医院公章，可实现患者自助打印病历，提高医院病案室整体工作效率，改善患者就医体验，提升医院医疗服务整体水平。

5 结语

医师电子签名并非只是简单地将纸质病历手写签名转变为CA认证数字签名，而是从提高医院管理水平与医护诊治工作效率入手，进一步实现医院医疗管理模式中流程的优化、安全保障^[5]。手机扫码签名的认证方式不依赖于任何平台，解决了U-KEY介质携带、损坏的问题，减少医院U-KEY管理成本，提高医院管理效率。下一步将医院业务信

息系统与扫码签认证系统对接，患者端使用手写版签字加指纹验证方式实现医院电子病历无纸化，全闭环使用电子签名。

参考文献

- 1 刘浩, 邹玲. 手机证书在医院电子认证系统中的应用 [J]. 中国数字医学, 2018, 13 (11): 80-82.
- 2 王飞龙, 尹青, 郭玉东, 等. 基于USB Key的身份认证系统设计与实现 [J]. 信息工程大学学报, 2016, 17 (1): 65-70.
- 3 王颖, 徐宝元, 李亚丽, 等. 护理病历数字认证技术的设计与实现 [J]. 中国数字医学, 2017, 12 (6): 27-29.
- 4 杨齐成, 王锦, 胡北辰. 数字证书在网络安全中的应用分析 [J]. 江汉大学学报: 自然科学版, 2017, 45 (3): 278-282.
- 5 史森中. 医院电子病历电子签名需求分析及实施方案 [J]. 医学信息学杂志, 2019, 40 (3): 48-51.

敬告作者

《医学信息学杂志》网站现已开通，投稿作者请登录期刊网站：<http://www.yxxxx.ac.cn>，在线注册并投稿。

《医学信息学杂志》编辑部