

基于 WPKI 和虹膜识别的二维码安全管理系统

付钰, 孙连亮, 吴晓平

(海军工程大学信息安全系, 湖北 武汉 430033)

摘要: 针对现有二维码安全技术的不足, 设计并实现了基于 WPKI 和虹膜识别的二维码安全管理系统。该系统通过 WPKI 技术, 利用数字证书对杂凑处理后的信息进行签名, 供用户对二维码的来源进行可信性验证; 通过建立公安户籍管理系统、WPKI/CA 系统、服务端和移动客户端 4 个子系统对二维码的制作和识别进行规范化管理, 并结合生物特征识别技术, 对申请证书的用户进行实名认证, 间接实现数字证书与用户物理身份绑定, 形成一整套责任追究机制。测试结果表明, 该系统能够满足准确性和健壮性要求。

关键词: 二维码; 虹膜识别; WPKI; 数字签名

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018037

QR code security management system based on WPKI and iris recognition

FU Yu, SUN Lianliang, WU Xiaoping

Department of Information Security, Naval University of Engineering, Wuhan 430033, China

Abstract: Aiming at the deficiency of existing QR code security technology, a security management system based on WPKI and iris recognition was designed and implemented. The system uses digital certificates to sign the hashed information for the user to verify the source of the QR code based on WPKI technology. Through the public security household registration management system, WPKI/CA system, server and mobile client four subsystems to standardize the management of the production and identification of QR code, and the application for the certificate of the user real name certification combined with biometric identification technology, indirectly realizing the binding of digital certificates and user physical identities to form a set of accountability mechanisms. Test results show that the system can meet accuracy and robustness requirements.

Key words: QR code, iris recognition, WPKI, digital signature

1 引言

二维码 (QR code), 也称快速响应码, 作为

一种编码方式, 近年来在移动设备上非常流行, 具有存储容量大、可靠性高、保密防伪性强、成本低等优点^[1~3]。二维码既是一种信息载体, 也是

收稿日期: 2018-03-03; 修回日期: 2018-04-15

通信作者: 付钰, 874354471@qq.com

基金项目: 国家自然科学基金资助项目 (No.61100042); 湖北省自然科学基金资助项目 (No.2015CFC867); 信息保障技术国防重点实验室基金资助项目 (No.KJ-13-111)

Foundation Items: The National Natural Science Foundation of China (No.61100042), The National Natural Science Foundation of Hubei Province (No.2015CFC867), The National Laboratory of Information Security Technology (No.KJ-13-111)

搜索信息、存储数据的重要措施和方法。它在物流管理、移动支付和工业自动化等领域有普遍的运用。但是，随着二维码技术的大力推广，其安全问题也日益凸显，特别是在移动支付中的安全问题与每个使用者的切身利益息息相关。针对二维码存在的安全问题，2015年12月29日，商务部中国电子商会与中国质量认证中心联合发布了《二维码安全规范应用评价体系》，举行了战略合作签约仪式，讨论了二维码行业安全标准的发展^[4]。其目的在于从顶层设计层面解读“互联网+”时代的二维码标准规范建设、信息安全及产业发展趋势。

在理论研究方面，国内学者的研究成果主要集中在分布在二维码的机密性方面，对恶意二维码监控技术的研究尚不多见。2016年，蒋溢等^[5]提出一种基于混沌 Z-映射的 QR 码加密机制。通过基于混沌 Z-映射的 QR 码密钥特征算法生成密钥序列，利用密钥对 QR 码的像素矩阵进行加密，实现对 QR 码信息的加密保护。2017年，马峰等^[6]提出了一种将信息隐藏技术应用到二维码中的算法。该算法的核心思想是：通过改变二维码中黑白图像块像素行程的奇偶性来嵌入信息，达到保护二维码内容的目的。在实际应用方面，一些手机提供了对恶意二维码进行监控的安全防护软件，如十分流行的腾讯手机管家、360 手机卫士等，其工作原理主要通过自身的大数据平台，基于黑白名单机制进行匹配，这种模式时效性较差，只能控制危害继续扩大^[7]。综合上述，针对二维码安全问题，目前安全防御技术的研究内容主要分为 2 方面：一是通过密码技术、信息隐藏技术等实现对二维码内容的安全保护；二是通过建立大数据平台，结合安全软件对扫描出来的信息做安全性评估，实现对恶意二维码的检测。以上的研究都不能够验证二维码的来源是否可信，也不能实现事后的责任追究。

因此，如何防范二维码信息被伪造或被篡改、实现对二维码来源的可信性验证、建立一整套的责任追溯机制已成为世界领域专家学者研究的热点课题之一。WPKI (wireless public key infrastructure) 技术遵循移动网络环境中所建立的标

准，是 PKI 技术在无线网络环境中的应用，主要用来管理移动网络环境中使用的公钥和数字证书。WPKI 并不是一个全新的 PKI 规范，它是传统的 PKI 技术应用于无线环境的优化扩展，采用了优化的椭圆曲线加密 (ECC, elliptic curve cryptography) 和压缩的 X.509 数字证书^[8-10]。在 WPKI 中同样采用证书管理公钥，通过第三方的可信任机构——认证中心 (CA, certificate authority) 验证用户的身份。研究表明，采用合适的虹膜识别算法，人的虹膜信息出现误识和错误拒绝的概率相当微小。相比于其他生物特征识别技术，虹膜识别技术的精确度要高出数 10 个数量级。因此，在生物特征识别方面，本文主要就虹膜识别技术展开研究。

2 QR 码编解码原理

QR 码由许多正方形模块组成，结构特征明显，如图 1 所示。

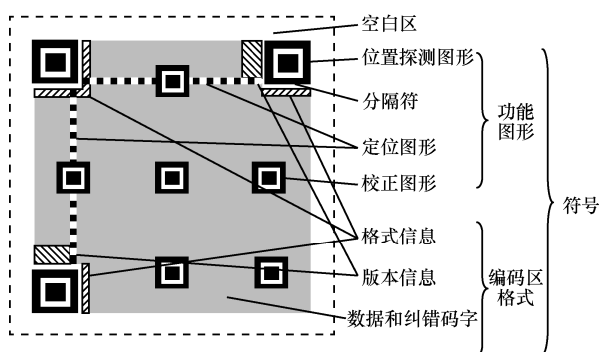


图1 QR 码结构

一个 QR 码由功能图形和编码区格式组成。功能图形的作用是帮助解码程序解码得到编码数据的辅助图形，包括位置探测图形、分隔符、定位图形以及校正图形；编码区格式则包含格式信息、版本信息、数据和纠错码字^[11]。二维码的编码过程分为数据分析、数据编码、纠错编码、码字填充、布置功能图形、添加掩模和添加版本信息 7 个步骤，其流程如图 2 所示。

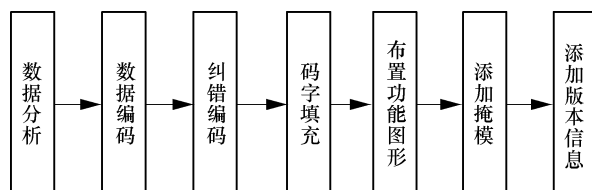


图2 QR 码编码过程

二维码的解码过程主要包括图像预处理、确定位置版本信息、消除掩模、恢复数据和纠错码字、数据码字译码等步骤,具体流程如图3所示。

3 二维码安全管理系统设计

3.1 系统功能设计

从系统的功能出发,将二维码安全管理系统分为公安户籍管理系统、WPKI/CA系统、服务端和移动客户端4个子系统。其中,公安户籍管理系统主要用来提供实名认证服务,WPKI/CA是对二维码来源进行可信性认证的可信第三方,服务端主要用来申请数字证书和制作二维码,移动客户端用来对二维码进行安全识别。系统整体功能模块如图4所示。

公安户籍管理系统是建立一整套责任追溯机制的重要保障,主要管理公民的身份信息和虹膜特征信息,并且能够通过虹膜识别技术提供实名

认证服务。在系统自身的安全防护方面,本系统设计了基于静态口令的身份认证模块。通过对用户口令和用户信息多次执行 Hash 运算得到认证信息,这种方式既保证了较长的密钥长度,又实现了密钥相对随机和用户口令的加密存储。

WPKI/CA 系统是实现对二维码来源可信性验证的可信第三方,该系统的核心是认证机构 CA 模块,实现对证书的签发、修改、撤销等功能。为了保护私钥的安全,本系统通过基于口令加密(PBE, password based encryption)算法对私钥信息进行加密。PBE 算法并不是简单地直接通过口令对内容进行加密^[12],而是通过某种变换将口令转换成加密的密钥。这个变换过程具体是由 KDF 函数完成的,其实现流程为:首先通过“盐”来扰乱用户口令,产生准密钥,然后用散列函数对准密钥进行多次迭代生成用来加密的密钥,最后利用对称加密算法对数据进行加密,可选择对

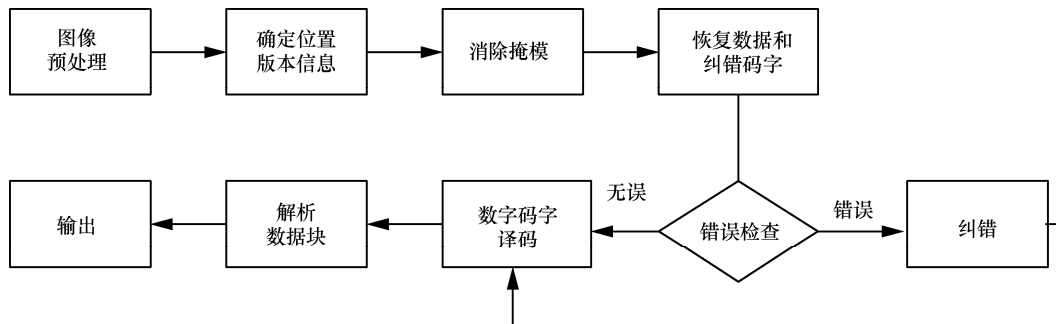


图3 QR 码解码过程

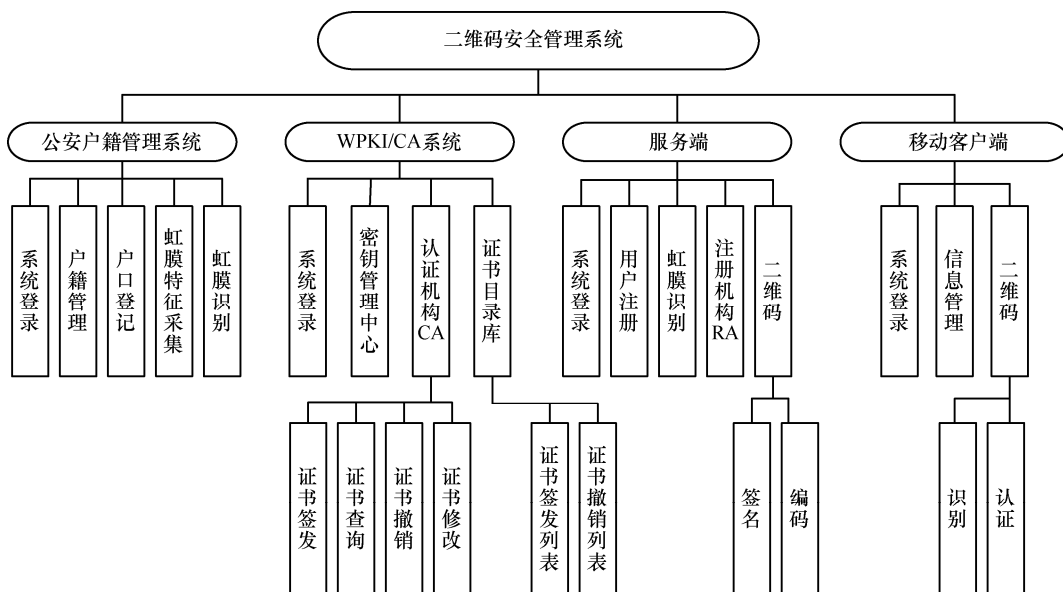


图4 系统功能结构

称加密算法有 DES、3DES、RC5 等。

服务端是整个二维码安全管理系统的核心，是实现责任追究的重要环节。服务端主要实现两大功能。一是扮演注册机构 RA 的角色——向认证机构发送证书申请、修改、撤销的请求，并且能够查询和下载数字证书等；二是利用数字证书制作二维码，供其他用户进行扫描。用户在申请数字证书前，通过虹膜识别进行实名认证，这样做的目的是实现数字证书与用户物理身份信息的间接绑定，从而使虚拟的数字证书能够代替用户的真实身份。同时，服务端保存数字证书与用户物理身份的对应关系。

移动客户端是面向扫码用户的二维码安全识别软件，主要用来识别二维码内容，并对二维码来源进行可信性验证。当出现安全问题时，还可以通过查询扫码历史，获取该二维码的签名证书，然后向服务端举报。服务端可以通过查询数字证书与用户身份的对应关系表，查询出该证书的申请者，实现责任追究。

在各子系统之间的保密通信方面，本系统采用基于 PKI 双证书机制的加密传输。双证书包括签名证书和加密证书。签名证书使用在签名中，仅为了验证身份，其中，公钥和私钥由用户自己产生和保管，CA 不负责其保管任务。加密证书用来在传递数据时进行加密，其私钥和公钥由 CA

产生，并由 CA 保存。

3.2 可信性验证功能设计

二维码的可信性验证主要通过 WPKI/CA 系统、服务端和移动客户端 3 个子系统来实现。用户向 WPKI/CA 系统申请到数字证书后，对编码信息进行 Hash 运算，得到 Hash 值；然后利用数字证书的私钥，通过 ECDSA 算法对 Hash 值进行签名，得到签名值，最后将信息、签名值和数字证书一起制作成 QR 码，供其他用户扫描。

用户通过移动客户端对 QR 码进行扫描，得到扫码信息，并对扫码信息进行分割，提取其中的信息、签名值和数字证书。然后对证书进行 4 个方面的验证：QR 码图片中有没有加入证书、证书是否过期、证书有没有被撤销、证书上的签名是否正确。只有这 4 个方面的验证都通过，才能证明证书有效。之后利用证书上的公钥完成对签名的验证，如果验证通过，则认为 QR 码的来源是可信的；否则认为 QR 码来源不可信。二维码可信性验证流程如图 5 所示。

3.3 责任追究机制设计

责任追究的关键是实现数值证书与用户物理身份的绑定，因此在用户申请数字证书过程中需要通过虹膜识别进行实名认证。实名认证流程如图 6 所示，将身份信息（姓名、身份证号）、虹膜特征信息和时间参数一起用签名证书和加密证书

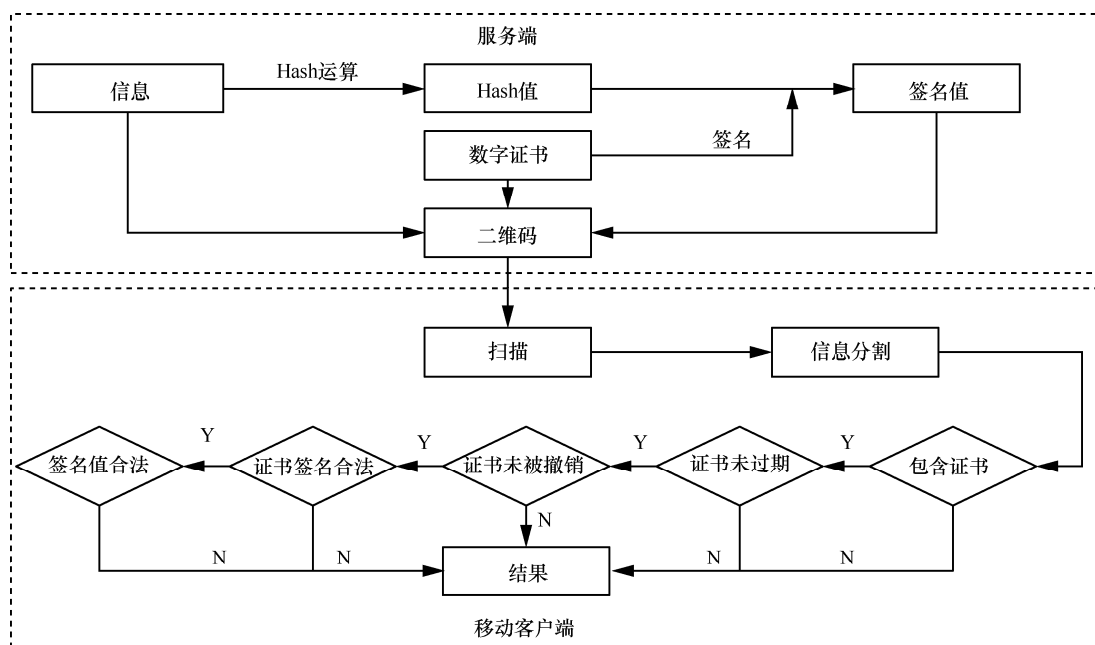


图 5 QR 码可信验证流程

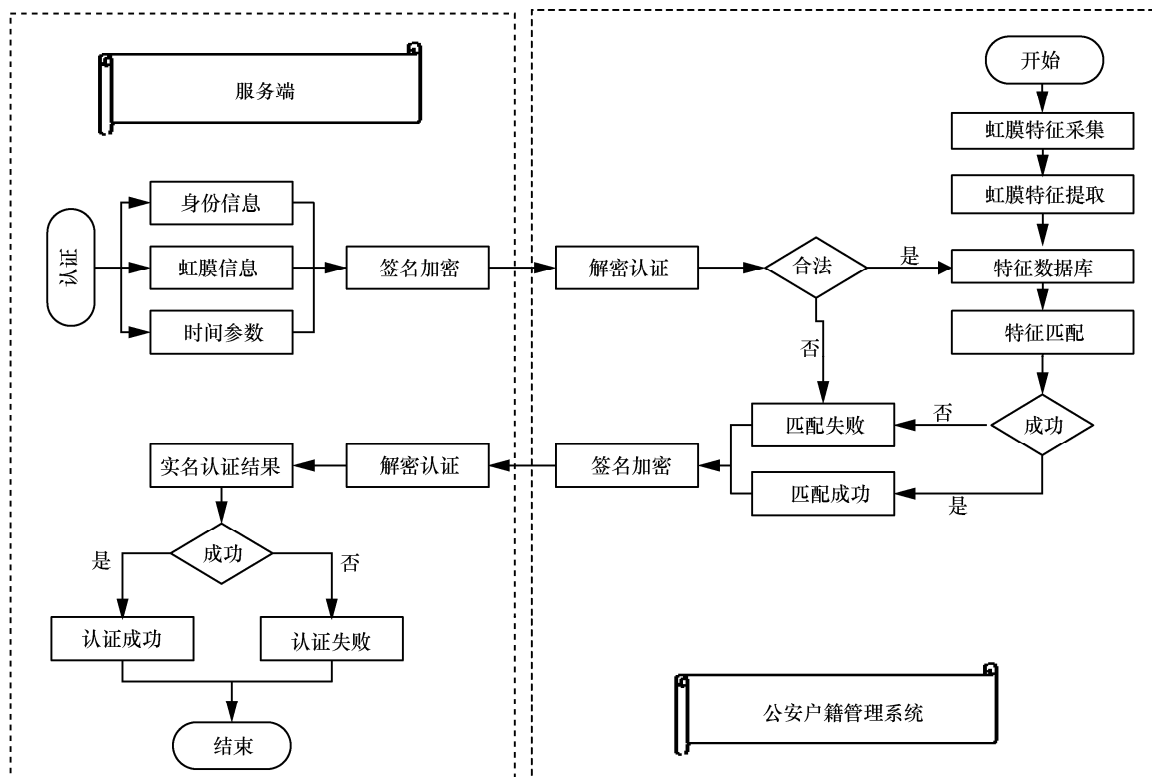


图6 实名认证流程

进行签名加密，然后发送给公安户籍管理系统。公安户籍管理系统接收到信息后，进行解密认证，然后查询生物特征数据库进行特征匹配，将匹配结果反馈给服务端。通过实名认证后服务端才向 WPKI/CA 系统申请数字证书。用户通过移动客户端对 QR 码进行识别，如果经过 5 个方面的验证（具体内容在 4.3 节中介绍）仍然出现安全问题，就可以通过查询扫码历史获提取该 QR 码，并向服务端发出举报请求，要求服务端索赔损失。服务端接收到请求后，经验证该 QR 码存在安全问

题，就会提取 QR 码中的数字证书，查询数据库中数字证书与用户身份的对应关系表，获取该证书的申请者，然后向有关部门进行举报，为打击二维码网络犯罪提供第一手资料。

4 二维码安全管理系统实现

4.1 公安户籍管理系统实现

公安户籍管理系统是使用 Eclipse 开发的 Java 项目，顶层设计包如图 7 所示。

其中，com.gahj.dao 包放置的是访问数据库的

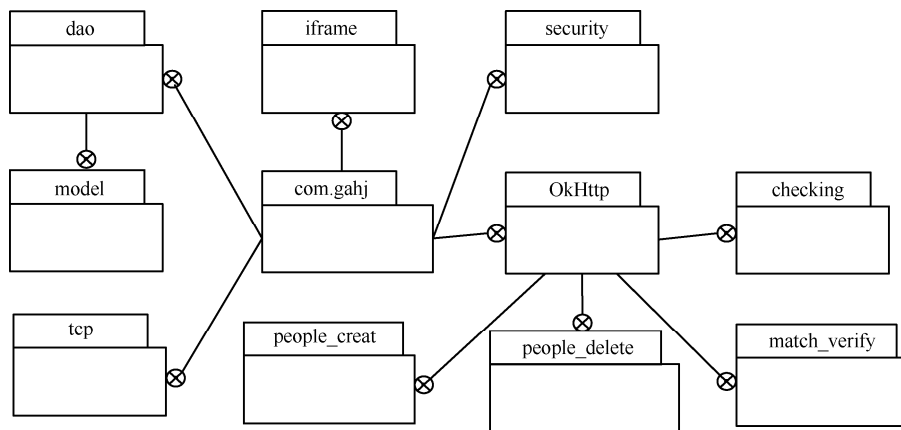


图7 公安户籍管理系统顶层包

方法，同时管理数据库的链接和关闭；com.gahj.dao.model 包中放的是数据模型公共类，它们对应数据库中不同的数据表；com.gahj.iframe 包放的是内部窗体类，包括系统登录、户口登记、户籍管理和虹膜识别窗体；com.gahj.security 包中放置的是 ECC 加解密以及 ECDSA 签名认证程序，主要用来实现与服务端之间的安全通信；com.gahj.tcp 包放置的是利用 ServerSocket 类编写双向通信类程序；com.gahj.OkHttp 包中放置的是实现虹膜识别的方法，checking 类检测图片（Image）中的虹膜（Iris），match_verify 类进行虹膜识别，people_creat 类创建用户，people_delete 类删除用户。

本系统在实现虹膜识别时主要利用天诚盛业公司提供的生物识别云服务平台。借助于 OkHttp 库发送 HTTP 请求，获取虹膜识别的返回结果。首先，需要创建一个 OkHttpClient 的实例和一个 RequestBody 对象来存放待提交的参数。其次，需要创建一个 Request 对象，用来发起一条 HTTP 请求。之后，调用 OkHttpClient 的 newCall() 方法来创建一个 Call 对象，并调用它的 execute() 方法发送请求并获取服务器返回数据^[12]。发送虹膜识别请求的具体代码如下所示。

```
public void sendVerifyRequest(final String
Base64image ,final String username) {
    new Thread(new Runnable() {
        @Override
        public void run() {
            try {
                OkHttpClient client = new OkHttpClient();
                RequestBody requestBody = new
                FormBody.Builder()
                    .add("app_id", eyekey_appid)
                    .add("app_key", eyekey_appkey)
                    .add("img", Base64image) //图
                    片的 base64 编码
                    .add("people_name", username)
                    .build();
                Request request = new Request.
                Builder()
                    .url(Match+"/match_verify")
```

```
.post(requestBody)
                .build();
                Response response = client.new
                Call(request).execute();
                String responseData = response.
                body().string();
                showResponse(responseData);
            } catch (Exception e) {
                e.printStackTrace();
            }
        }
    }).start();
}
```

4.2 WPKI/CA 系统实现

WPKI/CA 系统主要利用 OpenSSL 来实现证书的签发。OpenSSL 是一个开放源代码软件包，是最常用的证书管理工具。利用 OpenSSL 签发数字证书首先要建立 CA，即签发自签名证书。然后产生密钥和证书请求，由根证书根据证书请求签发证书。

首先，要创建根证书。然后，利用 openssl ecparam 命令生成 ECDSA 密钥；利用 openssl req 命令产生证书请求，证书请求用来生成证书（其中，请求信息包括国家、城市、组织名、主题名等）；最后，利用 openssl x509 命令签发数字证书。

签发用户证书和创建根证书一样，只是在执行 openssl 命令时签名私钥为根证书的私钥。

4.3 服务端实现

服务端的实名认证功能主要通过安全通信模块向公安户籍管理系统发送虹膜识别请求，实现程序与 com.gahj.tcp 和 com.gahj.security 相同。在二维码制作方面，先通过 PBECoder 类中的 decrypt() 方法对加密后的私钥进行解密，然后利用 ECDSACoder 类中的 sign() 方法对要编码内容进行签名，最后利用 CreateQRCode 类中的 encoder() 方法将要编码内容、签名值、数字证书的 Base64 编码值一起制作成二维码图片。

4.4 移动客户端实现

移动客户端是使用 Android Studio 开发的 Android 项目。该项目主要实现对二维码的识别并进行可信性验证。扫描 QR 码解码数据的基础工作是利用 Google 的开源包 ZXing 来实现的，扫

码过程在 `CaptureActivity` 中进行。该类中启动了二维码识别编码线程 `DecodeThread`、相机获取焦点及相机预览回调的一个循环过程，直至返回二维码识别的结果，得到识别结果后对二维码来源进行可信性验证。

移动客户端对扫码得到的数据做了5个方面的验证。

- 1) 扫码方通过分割数据判断是否含有证书。
- 2) 利用 `CertUtils` 类中的 `checkValidity()` 方法判断证书是否过期。
- 3) 向服务器发送 `request` 请求，设置该证书的序列号，利用 `getRevokedCertificate()` 方法，查看该证书是否在证书撤销列表中。
- 4) 利用 `getPublicKey()` 方法，获取根证书中的公钥信息，然后利用 `verify()` 方法验证证书中的签名是否正确。
- 5) 同样利用 `getPublicKey()` 方法，获取数字证书中的公钥信息，然后利用 `verify()` 方法验证二维码的签名是否正确。

当这5个方面的验证全部通过后，即可认为该QR码安全可靠。

5 结束语

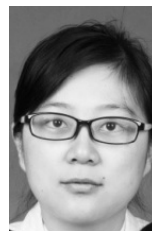
本文设计并实现了基于WPKI和虹膜识别的二维码安全管理系统，该系统能通过对二维码来源进行可信性验证确保扫码安全，避免安全隐患，即使出现安全问题，也能够实现责任追究，实现对二维码的安全管理，促进了二维码技术的安全推广与健康发展。然而，责任追究机制的建立还需要公安局等部门的配合，以及法律法规的保障。为更好地促进该系统的应用与推广，一方面需要虹膜识别技术的进一步发展，另一方面可以采用较为成熟的指纹识别或人脸识别技术。

参考文献:

- [1] 王飞, 贾玉文. 二维码在移动信息服务中的应用探析[J]. 学理论, 2013(35): 72-73.
WANG F, JIA Y W. Application of two-dimensional code in mobile information service[J]. Theory, 2013 (35): 72-73.
- [2] 杨森. 二维码应用及安全分析[J]. 信息安全与技术, 2015, 6(8): 64-65.
YANG S. Application and security analysis of two dimensional code[J]. Information Security and Technology, 2015, 6 (8): 64-65.
- [3] 张丰, 施勇, 薛质. 二维QR码在电子商务中应用的安全性研究[J]. 计算机技术与应用, 2017, 27(3): 131-135.

- ZHANG F, SHI Y, XUE Z. Research on the security of two-dimensional QR codes in electronic commerce[J]. Computer Technology and Development, 2017, 27 (3): 131-135.
- [4] 马文生. 我国发布首个二维码安全规范应用评价体系[J]. 中国防伪报道, 2016(3): 45.
MA W S. Releases the first releases code safety standard application evaluation system in China[J]. China Anti-Counterfeiting Report, 2016(3): 45.
- [5] 蒋溢, 刘雨龙, 罗宇豪. 基于混沌 Z-映射的 QR 码加密机制[J]. 计算机工程与设计, 2016, 37(9): 2361-2365.
JIANG Y, LIU Y L, L Y H. QR code encryption mechanism based on chaotic Z-map[J]. Computer Engineering and Design, 2016, 37(9): 2361-2365.
- [6] 马峰, 张硕. 一种基于信息隐藏的安全二维码技术[J]. 科学技术创新, 2017(32): 83-84.
MA F, ZHANG S. A secure two-dimensional code technology based on information hiding[J]. Science and Technology Innovation, 2017(32): 83-84.
- [7] 逯全芳, 唐杰, 文红. Android 移动智能终端操作系统安全机制的安全性评估[J]. 信息安全与技术, 2013, 4(8): 54-58.
QUAN Q F, TANG J, WEN H. Android mobile intelligent terminal operating system security mechanism security assessment[J]. Information Security and Technology, 2013, 4 (8): 54-58.
- [8] 张举. WPKI 在移动电子商务中的应用研究[J]. 现代信息科技, 2017, 1(4): 99-100.
ZHANG J. WPKI applied research in mobile electronic commerce[J]. Modern Information Technology, 2017, 1 (4): 99-100.
- [9] 明海波. 移动商务安全工作模式中 WPKI 技术的应用[J]. 电脑知识与技术, 2016, 12(35): 43-45.
MING H B. Application of WPKI technology in mobile commerce security work mode[J]. Computer Knowledge and Technology, 2016, 12(35): 43-45.
- [10] 徐晓宁. WPKI 关键技术的设计与实现[D]. 西安: 西安电子科技大学, 2015.
XU X N. Design and implementation of the key technology of WPKI[D]. Xi'an: Xidian University, 2015.
- [11] 伊恩泽, 佟新, 魏震, 等. Android 智能终端二维码安全检测系统的设计与实现[J]. 电脑知识与技术, 2017, 13(8): 61-64.
YI E Z, TONG X, WEI Z, et al. Design and implementation of Android intelligent terminal QR code security detection system[J]. Computer Knowledge and Technology, 2017, 13(8): 61-64.
- [12] 梁栋. Java 加密与解密的艺术[M]. 北京: 机械工业出版社, 2014.
LIANG D. Java encryption and decryption art[M]. Beijing: Mechanical Industry Press, 2014.

[作者简介]



付钰(1982-), 女, 湖北武汉人, 博士, 海军工程大学副教授, 主要研究方向为信息安全风险评估。

孙连亮(1995-), 男, 山东济宁人, 海军工程大学硕士生, 主要研究方向为信息安全。

吴晓平(1961-), 男, 山西新绛人, 博士, 海军工程大学教授, 主要研究方向为系统分析与决策。