文章编号：2096-1472(2021)-11-47-04
DOI:10.19644/j.cnki.issn2096-1472.2021.011.012

电子政务中身份认证技术的研究与实现

刘邦桂[1]，曾思财[2]

(1.广东开放大学人工智能学院，广东 广州 510091；
2.广东云政数据科技有限公司，广东 中山 528400)
✉liubanggui@qq.com; gdyztech@163.com

摘 要：针对电子政务应用中网络自助业务不断增多，用户网络安全意识普遍不高，容易受仿冒服务端发起的网络攻击，导致信息泄露、财产损失等安全问题，以业务中通信数据的完整性、机密性、不可否认性为研究对象，深入研究分析了密码学、数字签名、PKI(Public Key Infrastructure，公共基础设施)、CA(Certificate Authority，证书授权机构)以及证书的工作机制，提出了基于PKI的电子身份认证技术在自助电子政务中的运用方案。利用开源OpenSSL软件包，选用RSA(Rivest Shamir Adleman)签名算法、SHA(Secure Hash Algorithm，安全散列)摘要算法，在目前最新且被市场稳定使用的Red Hat Linux 7.4系统中进行了仿真验证。结果表明，数字证书能够为通信双方提供加密和身份认证服务，结合实名制、生物识别等新网络安全技术，能有效保证自助电子政务业务的安全性，可在实际应用中推广，为解决目前自助电子政务安全难点提供了参考。

关键词：电子政务；数字签名；身份验证；生物识别
中图分类号：TP393.2 **文献标识码**：A

Research and Implementation of Identity Authentication Technology in E-government

LIU Banggui[1], ZENG Sicai[2]

(1.*School of Artificial Intelligence*, *the Open University of Guangdong*, *Guangzhou* 510091, *China*;
2.*Guangdong Yunzheng Data Technology Co*., *Ltd*., *Zhongshan* 528400, *China*)
✉liubanggui@qq.com; gdyztech@163.com

Abstract: With the increasing network self-service business in e-government applications, network users generally have low awareness of network security and they are vulnerable to network attacks from counterfeit servers, which leads to security issues such as information leakage and property loss. Taking the integrity, confidentiality and non repudiation of communication data in business as the research objects, this paper is based on in-depth research and analysis of cryptography, digital signatures, PKI (Public Key Infrastructure), CA (Certificate Authority) and working mechanism of certificates. This paper then proposes an application scheme of electronic identity authentication technology based on PKI in self-service e-government, using open source OpenSSL software package, and selecting RSA (Rivest Shamir Adleman) signature algorithm and SHA (Secure Hash Algorithm) digest algorithm. The simulation verification is carried out in the latest and stable Red Hat Linux 7.4 system. Results show that digital certificate can provide encryption and identity authentication services for both parties of communication. Combined with new network security technologies such as real name system and biometrics, it can effectively ensure the security of self-service e-government business, and can be popularized in practical application, which provides a reference for solving current difficulties of self-service e-government network security.

Keywords: e-government; digital signature; identity verification; biometrics

1 引言(Introduction)

政府部门电子业务办理日趋信息化、自动化，越来越多的政务业务开始逐渐往网络迁移，网络安全也开始与每个人息息相关。然而大部分应用的使用者缺乏网络素养，给网络应用带来越来越多的风险。再者，网络结构的开放性、复杂性，网络应用的多样性，网络终端的虚拟性等特点，使网络

中的信息经常出现“我是谁”“我在哪里”的情况。互联网技术的飞速发展也伴随着网络攻击途径、方式、手段和目的的不断改变和层出不穷。如何做到电子政务网络服务中的攻防平衡是网络安全急需解决的问题。

确保安全使用电子政务网络服务的网络安全技术有很多，比如实名制、加密卡、U盾、动态口令、生物识别、软硬件防火墙等，总结起来无外乎是为了实现信息的机密、完整、不可否认三大特性。密码学技术解决了在不安全的信道中安全传输信息的问题，确保数据的机密性；数字签名技术可以证明信息没有被篡改，实现了信息的完整性；同样利用数字证书身份识别技术实现了信息的不可否认性。然而密码学、数字签名技术均需要在信息的两端互相传输密钥，因此，密钥的管理将是解决网络攻击的核心问题之一。为此我们基于PKI[1]在Linux 7中设计了一种OpenSSL方案，为电子政务的网络应用提供加密和数字签名等密码和数字证书服务管理。

2 密码学与数字签名(Cryptography and digital signature)

2.1 密码学

密码学是研究信息系统安全保密的学科。密码编码学主要是指对信息进行编码，实现对信息的隐蔽。密码分析学主要是对加密信息进行破译。在密码学中包含明文、密文、密钥、加密算法、解密算法五个重要的元素，构成了密码学体制[2]，是通信双方能进行加密通信的协议。所以，不管是编码学还是分析学都要用到密钥，它是算法的关键。根据加密和解密过程中密钥是否相同，可以将密码学分为对称密码和非对称密码。对称密码的加解密钥相同；非对称密码的加解密钥不相同，而且相互不能推导。一般情况下，保留在加密方手上不能公开传输的称为私钥；可以在公网上传输的称为公钥，用来解密。因此，在通信双方进行通信前，相互获得共同预定的密钥是整个过程的关键。通常在没有中间人攻击的情况下，需要用到双方都认可的第三方权威机构来进行密钥的分发，才能确保数据的机密性。

2.2 数字签名

日常生活中，一般涉及合同、约定等类型的协议文件都需要签名或者按手印来证明文件的完整性，也就是说没有被伪造或者修改过，简称原件。同样，在网络应用中数字签名也有同样的功能，是手写签名的电子对应物。然而，数字签名中签名同信息是分开的，需要一种方法将签名和消息绑定在一起，而在传统的手写签名中，签名是信息的一部分；数字签名利用一种公开的方法使得任何人都可以对签名进行验证，手写签名是由经验丰富的消息接收者通过以前的签名进行对比来验证真伪的；数字签名可以复制，但其可采用时间戳来防止复制，手写签名则不可以复制。

数字签名包含待签名信息、哈希函数(摘要算法)、签名算法、私钥、验证算法、公钥几个部分[3]。用签名算法和私钥对信息进行加密的过程称为签名，用公钥和验证算法对信息解密的过程称为验证，这和非对称密码体制使用公钥加密和私钥解密刚好相反。

数字签名包含以下几个过程：(1)运用消息摘要算法(哈希函数)对全部信息生成固定长度的哈希值，由于它将任意长度的消息变成固定长度的短消息，因此也称为散列或者杂凑函数。哈希函数是单向的，如果攻击者能够轻易构造出两个不同消息具有相同的摘要，那么这样的哈希函数是不安全的。常用的哈希函数有：MD5(Message Digest)、SHA(Secure Hash Algorithm)等。(2)对生成的摘要运用签名算法和私钥进行签名。常用的签名算法有：DSA(Digital Signature Algorithm)、RSA[4](Ron Rivest、Adi Shamir、Len Adleman发明)。(3)将消息和数字签名发给接收方。(4)接收方选择数字签名中携带的哈希函数对消息进行摘要计算，同时使用数字签名中的公钥对信息的数字签名进行验证，得到发送方计算的摘要，如果两个摘要相同，说明消息完整，没有被修改过。

3 PKI与数字证书(PKI and digital certificate)

3.1 PKI

随着公钥、密钥技术在网络安全领域的应用，用来在非对称密码中加密信息和验证数字签名的公钥都需要在公网中公开传输，非常容易被中间人攻击(如图1所示)，从而顺利被中间人窃取和篡改信息。因为这个过程中通信双方都没有验证对方的身份，所以这是网络安全最重要的一个部分，不仅要获得对方公钥，还需要明确公钥的来源。

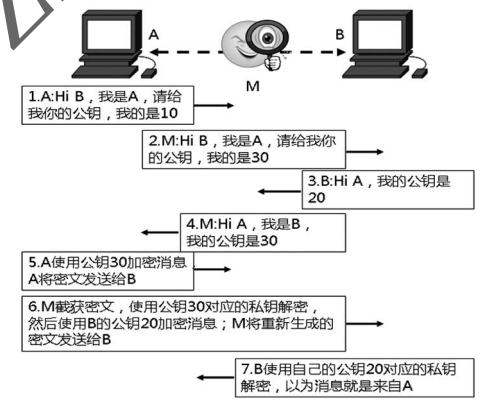

图1 中间人攻击

Fig.1 Man-in-the-middle attack

公钥基础设施PKI能够完成以上任务，它是一种遵循既定标准的公共密钥管理平台，是利用公钥理论和技术建立的提供安全服务的基础设施，也是数字证书管理平台。其关键技术是通过数字签名提供不可否认业务；将公钥和个人身份建立联系，并对公钥进行集中管理。

3.2 数字证书

数字证书[5]是互联网中用来证明自己和识别对方身份的一种权威性电子文档，也是网络中的“居民身份证”。它是一种树状层次结构，其格式遵循国际电信联盟制定的数字证书标准X.509[6]，目前为版本4。它包含证书授权中心CA(Certificate Authority)，是可信的第三方机构，负责证书的发放、废除以及查询；证书注册机构RA(Registration Authority)，是用户和CA的中间人，负责用户注册信息的收集、验证，密钥对生成和管理以及作废的请求管理等。

数字证书的工作流程有以下几个步骤：(1)用户利用软件或者其他途径生成公私钥对，其中公钥交给RA注册，私钥由用户自己保管；(2)用户在程序生成向导中利用自己的注册信息包括地理信息及联系方式等生成证书申请，提交给RA；(3)RA收到请求后验证用户的身份以及与证书请求对应的公私钥对的正确性，在无误的情况下将请求提交给CA；(4)CA收到证书申请后，为注册用户信息签名，生成数字证书，并将证书拷贝存放在证书目录中。

数字证书已经将公钥和身份信息绑定，验证了证书的有效性就是认可了对方的身份。除了公钥，证书里面提供了相关的摘要算法、加密算法、签名算法。客户端验证证书分为两个步骤：第一，使用证书携带的摘要算法对证书的客户信息进行摘要计算；第二，运用证书携带的公钥对证书中的摘要进行解密，如果与第一步计算的摘要相同，说明证书有效，否则无效。具体通信过程如图2所示。

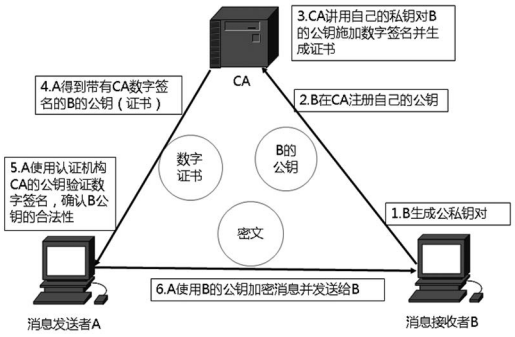

图2 证书加密机制

Fig.2 Certificate encryption mechanism

数字证书在使用过程中可能会因为私有密钥的泄露，使用时间、应用范围变更而被撤销，证书撤销列表CRL(Certificate Revocation List)就形成了。

4 OpenSSL技术(OpenSSL technology)

OpenSSL是开放源代码的软件包，由加拿大人Eric A. Young和Tim J. Hudson采用C语言编写而成，目前比较完善，能支持多种平台，包括密码算法库、SSL协议库和应用程序三大部分。具体有以下重要功能：(1)提供八种对称加密算法，其中有AES、DES、IDEA、RC2、RC5、CAST、Blowfish等七种分组加密算法，一种流加密算法RC4。(2)提供DH算法、RSA算法、DSA算法和椭圆曲线算法(EC)四种非对称加密算法。(3)实现了MD2、MD4、MD5、MDC2、SHA等五种信息摘要算法。(4)包含密钥和证书管理机制。(5)具备OpenSSL透明地使用第三方提供的软件硬件加密设备进行加密的Engine机制。(6)封装有内存访问、文件访问及Socket等I/O接口机制。

5 方案设计与实现(Scheme design and implementation)

目前电子政务网站、电子邮件安全的威胁主要有两个方面，一方面是非法的访问端，主要是攻击网站服务器，以盗取信息或文件；另一方面是非法的服务器端，主要以盗取客户账号和密码来牟取不合法利益为目的，比如钓鱼网站、仿冒网站(仿冒对象以各大银行、12306、网上商城等尤为突出)。解决以上问题，有经验的客户可以通过记住官网网址来实现，但对于绝大部分网络素养不高的客户来说，数字证书就是最有效的方式之一了。

以服务器端为例，当客户端访问网站时，客户端鉴定该网站是否合法，即Web服务器需要向可信CA申请服务器证书并安装绑定到Web站点。客户端与该可信CA建立信任关系后，客户端与服务器之间便建立起信任的证书链关系，客户端将认为该Web站点是可信任的。由于CA证书服务器是根据Web服务器的证书请求文件来颁发证书的，因此要首先在Web服务器上产生自己的公私钥文件，并且根据公私钥文件来生成证书的请求文件。方案拓扑如图3所示。

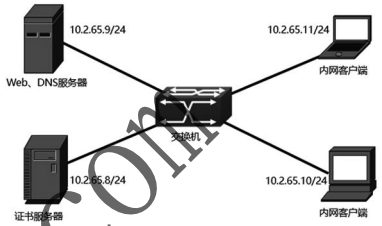

图3 网络拓扑图

Fig.3 The network topology diagram

该方案需要一个客户端和服务器端都认可的第三方可信任机构即CA来负责密钥和证书的管理。为了达到在客户端和服务端都能互相信任，需要在客户端、服务器端安装可信任机构的根证书，所以接下来的应用部署过程中，需要制作三个证书，分别是根证书、客户端证书、服务端证书并应用到网站中。

5.1 信任机构的部署

证书服务安装在Red Hat Linux 7.4中，一般情况下系统默认已经安装。由于安装过程中有比较多的软件包且它们之间有依赖关系，我们在配置好安装源后采用yum安装OpenSSL相关软件包：

[root@cadnswgs yum.repos.d]# yum install -y openssl

5.2 根证书的申请

配置证书的系统文件内容：

[root@cadnswgs tls]vi /etc/pki/tls/openssl.cnf

文件中有CA_default节点、policy_match节点、req_distinguished_name节点，一般将policy_match节点中的countryName、stateOrProvinceName、organizationName由match改为optional，以备与根证书在不同地区的用户申请和使用证书。在/etc/pki/CA目录下面包含certs、crl、newcerts、private四个文件，分别用来指定已经生成的证书的默认目录、证书撤销列表的默认目录、新签发证书的默认目录、存放CA证书服务器自身的私钥和证书文件的目录。另外还需要自己创建用来保存已经签发证书的文本数据库文件和签发证书时使用的序列号文件。

生成CA自身的私钥文件：

[root@cadnswgs CA]# openssl genrsa -out /etc/

pki/CA/private/cakey.pem 2048

利用私钥生成CA证书，此证书可以导出到客户机使用：

[root@cadnswgs CA]#openssl req -new -x509 -key /etc/pki/CA/private/cakey.pem -out /etc/pki/CA/cacert.pem -days 3650

5.3 网络应用服务证书的申请

电子政务网络应用可以是Web或者电子邮件等应用，这里以Web服务为例。在此之前需要在服务器中安装httpd服务，在/etc/httpd目录中新建一个certs目录用来存放服务器的私钥文件、证书申请文件和获得的证书文件。

Web服务端运用openssl命令利用私钥生成请求文件并发给CA申请证书：

[root@webwgs certs]# openssl req -new -key httpd.key -out httpd.csr

在CA中利用证书请求文件给Web服务颁发证书：

[root@cadnswgs CA]# openssl ca -in certs/httpd.csr -out certs/httpd.crt

5.4 利用证书构建安全的Web站点

Web服务器有了自己的私钥和证书，接下来利用证书搭建一个安全Web站点访问。需要将客户端访问Web站点的方式由HTTP升级为HTTPS，启动SSL证书，把服务器证书和安全的Web站点关联起来。为此，需要用到mod_ssl软件模块：

[root@webwgs Packages]# yum install -y mod_ssl

使用yum方式安装mod ssl，在/etc/httpd/conf.d目录下自动生成一个SSL配置文件ssl.conf，修改证书和私钥文件的路径：

[root@webwgs conf.d]# vi ssl.conf

SSLCertificateFile /etc/httpd/certs/httpd.crt //设置使用的证书

SSLCertificateKeyFile /etc/httpd/certs/httpd.key //设置证书的私钥

5.5 客户端验证

基于SSL协议的安全站点已经架设完成，客户机需要通过浏览器进行访问验证。由于客户机访问时Web服务器的证书是自己搭建的证书服务器，不是受信任机构颁发的安全证书，要正常访问，需要在客户机上将CA和Web服务的证书都下载过来并安装添加到受信任机构中，如图4和图5所示。

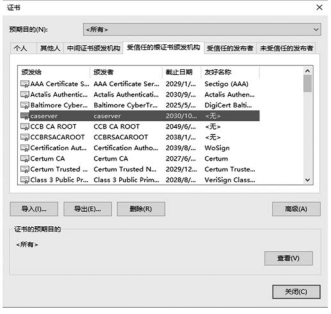

图4 添加根证书

Fig.4 Adding a root certificate

图5 证书路径

Fig.5 Certificate path

6 结论(Conclusion)

PKI技术是信息安全技术的核心，也是目前电子政务[7]、电子商务以及企业网络安全的关键技术。基于纯文本协议的HTTP协议存在明文传输容易被窃听、没有验证容易被中间人攻击进而篡改数据等安全威胁，破坏了网络安全的机密性、完整性等。数字证书经过CA确认、签名并颁发，对于全球性的网站服务，增强了网站服务的信誉度。利用SSL协议来提供公钥和身份绑定的数字证书验证机制，实现了具有加密通信、身份验证以及完整性保护功能的HTTPS，使得传统的Web服务得到了安全保障。随着软件自定义网络、活动目录、VPN等技术的交错深入发展，在鉴别身份之后提供对应权限的PMI技术开始紧密地与PKI结合使用起来[8]，为电子政务以及网络环境中的各种应用提供了统一的授权管理和访问控制机制，这将是未来网络安全发展的趋势之一。

参考文献(References)

[1] 刘那仁格日乐,王郝日钦.基于PKI技术的用户身份数据转发认证算法仿真[J].计算机仿真,2020,37(9):373-375.

[2] 牛淑芬,杨喜艳,李振彬,等.基于异构密码系统的混合签密方案[J].计算机工程与应用,2019,55(3):61-67.

[3] 彭春燕,杜秀娟,李梅菊,等.基于格的数字多签名体制[J].微电子学与计算机,2016,33(8):50-53.

[4] KURYAZOV D M. Development of electronic digital signature algorithms with compound modules and their cryptanalysis[J]. Journal of Discrete Mathematical Sciences and Cryptography, 2021, 24(4):1085-1099.

[5] 韩水玲,马敏,王涛,等.数字证书应用系统的设计与实现[J].信息网络安全,2012(9):43-45.

[6] 王开轩,滕亚均,王琼霄,等.隐式证书的国密算法应用研究[J].信息网络安全,2021(5):74-81.

[7] 张一梅.电子政务网络安全威胁及应对措施研究[J].网络安全技术与应用,2021(8):112-113.

[8] 任兴元,王佳慧,马利民,等.基于PKI与PMI的海洋政务服务系统安全解决方案的设计与实现[J].计算机应用与软件,2020,37(12):68-75.

作者简介：

刘邦桂(1983-)，男，硕士，讲师.研究领域：服务器技术，网络安全技术.

曾思财(1993-)，男，本科，工程师.研究领域：电子政务，智能信息处理研究.