Computer Science and Application 计算机科学与应用, 2012, 2, 276-281
http://dx.doi.org/10.12677/csa.2012.25049 Published Online December 2012 (http://www.hanspub.org/journal/csa.html)

Design and Realization of Dynamic Target Tracking and Automatic Close-Up Snapshot*

Ping Sheng[1], Jing Zhang[2], Dongwei Ni[3]

[1]School of Computer Science and Telecommunications Engineering, Jiangsu University, Zhengjiang
[2]School of Electrical and Information Engineering, Jiangsu University, Zhenjiang
[3]Zhengjiang Jiangda Kemao Information System Limited Company, Zhenjiang
Email: pingsheng@ujs.edu.cn

Received: Oct. 13th, 2012; revised: Oct. 27th, 2012; accepted: Nov. 16th, 2012

Abstract: The network security management faces severe challenges currently. To solve the problem that the existing network security model unable to meet the security needs of mobile OA that based on wired or wireless network, we proposed and designed a security model of mobile OA based on the WPKI combined with the security demand characteristics about actual mobile OA. This security model uses digital certificate authentication and authorization mechanism for user identification and access control and provides integrity protection and non-repudiation for information by digital signature. The model unifys wireless and wired authentication system, and it has been applied for Kemao OA system successfully. The running results show that this security model can guarantee communication user identity safety, protect data confidentiality and integrity, and achieves the undeniable for user behavior. The security model we designed meets the mobile office omni-directional security needs completely, and can be widely used in all kinds of mobile information system.

Keywords: Mobile OA; Security Model; WPKI; Digital Certification

基于 WPKI 的移动办公系统安全模型设计及应用*

盛　平[1]，张　净[2]，倪冬玮[3]

[1]江苏大学计算机科学与通信工程学院，镇江
[2]江苏大学电气信息工程学院，镇江
[3]镇江江大科茂信息系统有限责任公司，镇江
Email: pingsheng@ujs.edu.cn

收稿日期：2012 年 10 月 13 日；修回日期：2012 年 10 月 27 日；录用日期：2012 年 11 月 16 日

摘　要：当前网络安全管理问题面临着严峻的考验，针对现有网络安全模型无法满足基于有线网和无线网的移动 OA 安全需求现状的缺陷，结合移动 OA 实际安全需求特点，提出并设计了一种基于 WPKI 的移动 OA 安全模型。采用数字证书的认证与授权机制来实现用户身份确认及访问控制，通过数字签名来提供信息的完整性保护与不可否认性，并实现了无线与有线认证系统的统一，成功应用到科茂 OA 系统中，运行结果表明该安全模型能够很好的保证通信中用户身份安全，保护数据的机密、完整，实现用户行为的不可否认，完全可以满足移动办公的全方位安全需求，可广泛用于各种移动信息系统。

关键词：移动 OA；安全模型；WPKI；数字证书

1. 引言

移动 OA[1]是 OA 发展的一个新阶段，也是 OA 发展的趋势，通过移动 OA 系统，可以有效地提高政府和企业的业务运作能力，优化工作环境。但由于移动 OA 以有线网络和无线网络为承载网络，所以移动 OA

*基金项目：镇江市科技支撑计划——工业(GY2010018)。

面临着有线网络和无线网络通信中的双重安全风险。要成功实现移动 OA，安全问题成为首先必须解决的问题，对于信息系统安全问题的较好的解决方法是根据系统安全需求，建立安全模型。自从 20 世纪 70 年代起，国内外就开始了对信息系统安全模型的研究，提出了 Bell-Lapagula(BLP)、信息流和 Biba 等各种安全模型，但却无法满足基于有线网和无线网的移动 OA 安全需求现状，本系统在分析现有安全模型的基础上，结合实际移动 OA 安全需求特点，提出了基于 WPKI 的移动 OA 安全模型，采用了加密传输和数字签名技术解决了移动 OA 环境中的信任问题，算法成熟可靠安全性高，实现简单易行，从而保证了验证、机密性、完整性和非否认性的有效实施。

本文针对现有移动 OA 安全特点，在现有安全模型[2-4]的基础上，提出并设计了一种基于 WPKI 的移动 OA 安全模型，更好地适应无线环境下的使用。该模型提出了双重密钥对的解决方案，将加密密钥对与签字密钥对分开，并采用 U 盘保存私钥，使用了软硬结合的强双因子认证模式，很好的解决了安全性与易用性之间的矛盾；同时设计和实现了基于 WPKI 的新型证书系统，使整个认证系统有线无线融合在一起，实现统一无缝连接。

2. 移动 OA 安全模型设计

随着网络技术和信息技术的发展，移动办公成为可能，并在一些单位得以实施，但是，隐藏在这些移动 OA 表面下的安全问题同样不可小视。移动 OA 中的安全问题，归纳起来包括以下几个方面：身份假冒、信息泄漏、破坏信息完整性、行为抵赖。

2.1. 移动 OA 的安全目标

针对移动 OA 中的安全问题及安全需求，在移动 OA 中，必须从技术上保证在移动环境中能够实现身份认证、用户权限控制、安全传输、不可否认性、数据完整性。由于数字证书认证技术采用了加密传输和数字签名，能够实现上述要求，因此采用基于 WPKI 的安全模型解决移动 OA 中的安全问题。

总体目标为：

1) 通过基于数字证书的认证方法来确认用户身份；

2) 提供基于数字证书[5,6]的授权控制来实现对信息资源及应用的访问控制；

3) 采用加密技术来保护信息的机密性；

4) 通过对消息摘要和数字签名[7,8]的验证来提供完整性保护；

5) 采用数字签名来提供不可否认。

2.2. 基于 WPKI 的移动 OA 安全模型

在移动 OA 环境下，建立一个基于 WPKI 的移动 OA 安全模型，模型结构如图 1 所示。

从图 1 中可以看出，基于 WPKI 的移动 OA 安全模型由用户、认证中心、注册中心、数字证书库、证书作废处理系统、密钥备份及恢复系统等几部分组成。

2.3. 主要模型各部分功能

1) 终端用户：终端用户包括有线终端和无线终端，它既是证书的持有者，也是证书的验证者。持有者是证书的拥有者，使用证书向对方证实自己的身份，从而获得相应的权力。验证者通是授权方，只有在成功鉴别之后才可授权对方。无线终端通过 RA 注册机构向 CA 中心申请数字证书，CA 中心审核用户身份后签发数字证书给用户，用户将证书、私钥存放在 UIM 卡中。

2) 认证中心 CA：CA 是 PKI 的核心执行机构，是 WPKI 的主要组成部分。CA 负责将公钥和终端用户的身份捆绑起来。CA 在对用户的真实身份进行验证之后，对一个包含身份信息和一个公钥的数据结构进行数字签名，以将用户公钥和用户身份捆绑起来。这样的数据结构称为公钥证书，或简称证书；CA 还

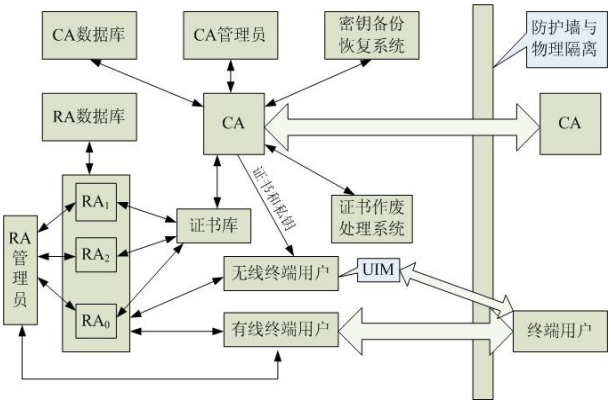

Figure 1. Security model of mobile OA
图 1 移动 OA 安全模型

负责签发证书撤销表(CRL)。CA 是保证移动应用环境、电子商务、电子政务、网上银行、网上证券等网上操作的权威性、可信任性和公正性的第三方机构。

3) 注册中心 RA：数字证书注册审批机构。代替 CA 确认终端实体的身份，代表终端用户启动和 CA 的认证过程，生成代表用户的密钥资料，还可以执行一些密钥和证书生存周期管理功能(例如产生撤销请求)。RA 系统是整个 CA 中心得以正常运营不可缺少的一部分。

4) 证书库：证书库是 CA 颁发证书和撤消证书的集中存放地，是一种公共信息库，可供公众进行开放式查询。证书库有多种实现方式，实际中主要用数据库或 LDAP 服务器实现。证书库必须是稳定可靠的、规模可扩充的。

5) 证书作废处理系统：当出现密钥介质丢失、认证证书被破坏或用户身份变更等详细情况时，证书在 CA 为其签署的有效期内也需要作废。作废证书一般通过将证书列入作废证书表(CRL)来完成。通常，在系统中由 CA 负责创建并维护一张及时更新的 CRL，由用户在验证证书时负责检查该证书是否在 CRL 之列。证书的作废处理必须在安全及可验证的情况下进行，系统还必须保证 CRL 的完整性。

6) 密钥备份及恢复：密钥备份及恢复是密钥管理的主要内容，用户由于某些原因将解密数据的密钥丢失，从而使已被加密的密文无法解开。为避免这种情况的发生，WPKI 提供了密钥备份与密钥恢复机制：当用户证书生成时，加密密钥即被 CA 备份存储；当需要恢复时，用户只需向 CA 提出申请，CA 就会为用户自动进行恢复。

3. 安全模型实现技术

3.1. 密钥生成

本系统由可信的第三方，为用户产生两种密钥对，即用于数字签名/验证的签名密钥对和用于数据加密/解密的加密密钥对，利用密钥管理中心 KMC 生成密钥对确保了密钥对的机密性、完整性和可验证性。而使用双重密钥对，将加密密钥对与签字密钥对分开，这样用户有两种证书，一种用于数字签名，另一种用于加密。每位用户可以用有两种或一种证书。签名证书主要用于对用户信息进行签名，以保证信息的不可否认性。加密证书主要用于对用户传送的信息进行加密，以保证信息的真实性和完整性。这两种密钥用途不同，生成的方式，管理的方式也不一样，这样分开设置可以提高系统的安全性。

3.2. 密钥管理与身份认证技术

本文采用 U 盘进行密钥存储和身份认证，存储密钥安全可靠，方便简单，用户的签名密钥对的生成可以在优盘进行，做到私钥不出盘；同时采用“口令 + U 盘”双因子身份认证的方式提高了安全性。

采用 USB 接口密钥管理器，私钥的产生、加密和解密运算均在密钥管理器内完成，不会被读入计算机的内存里，绝对安全；可直接与 USB 接口相连，无需读卡器之类的专用外设，即插即用。

利用 USB 接口密钥管理器中内置的密码算法实现 USB Key 认证，采用软硬件相结合、一次一密的强双因子认证模式。每个 USB Key 硬件都具有用户 PIN 码，以实现双因子认证功能。USB Key 内置单向散列算法(MD5)，预先在 USB Key 和服务器中存储一个证明用户身份的密钥，当需要在网络上验证用户身份时，先由客户端向服务器发出一个验证请求。服务器接到此请求后生成一个随机数并通过网络传输给客户端(此为冲击)。客户端将收到的随机数提供给插在客户端上的 USB Key，由 USB Key 使用该随机数与存储在 USB Key 中的密钥进行带密钥的单向散列运算并得到一个结果作为认证证据传送给服务器(此为响应)。与此同时，服务器使用该随机数与存储在服务器数据库中的该客户密钥进行 HMAC-MD 5 运算，如果服务器的运算结果与客户端传回的响应结果相同，则认为客户端是一个合法用户，原理如图 2 所示。

图中“N”代表服务器提供的随机数，“Key”代表密钥，“X”代表随机数和密钥经过 HMAC-MD5 运算后的结果。通过网络传输的只有随机数“N”和运算结果“X”，用户密钥“Key”既不在网络上传输

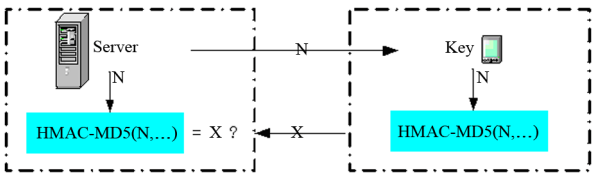

Figure 2. USB Key principle of authentication
图 2. USB Key 身份认证原理

也不在客户端电脑内存中出现，网络上的黑客和客户端电脑中的木马程序都无法得到用户的密钥。由于每次认证过程使用的随机数“N”和运算结果“X”都不一样，即使在网络传输的过程中认证数据被黑客截获，也无法逆推获得密钥。这就从根本上保证了用户身份无法被仿冒。

本模式可以保证用户身份不被仿冒，却无法保护用户数据在网络传输过程中的安全。我们通过数字证书认证方式可以有效保证用户的身份安全和数据安全。数字证书是

由可信任的第三方认证机构颁发的一段包含用户身份信息，用户公钥信息以及身份验证机构数字签名等数据，身份验证机构的数字签名可以确保证书信息的真实性，用户公钥信息可以保证数字信息的不可否认性。

从表 1 中可以看出，USB Key 具有安全可靠，便于携带、使用方便、成本低廉的优点，加上 WPKI 体系中数字证书完善的数据保护机制，我们选择 USB-Key 存储数字证书的身份认证方式，具体部署如图 3 所示。

3.3. WPKI 技术

WPKI 即“无线公开密钥体系”，它是将有线网中 PKI 安全机制引入到无线网络环境中的一套遵循既定标准的密钥及证书管理平台体系，用它来管理在移动网络环境中使用的公开密钥和数字证书，有效建立安全和值得信赖的无线网络环境，以解决无线终端的安全认证问题。WPKI 基本上是 PKI 在无线环境下的扩展，WPKI 系统结构如图 4 所示。

WPKI[9,10]对 PKI 的优化主要有三个方面：WPKI 协议、证书格式、密码算法和密钥。我们重点研究证书格式方面，WPKI 证书格式的制定者力图减小证书的大小，使之需要更少的存储空间。方法之一就是定义一个新的服务器证书格式(WTLS 证书格式)，这样与标准的 X.509 证书尺寸(大小约 2 k)相比，WTLS 格式证书的长度有很大的减小，也是 PKIX 证书格式的一个子集。因此，它们的证书之间可以互用。这样在本系统中就可以考虑将无线和有线网络认证的系统统一起来，采用将现有线认证中心扩展到无线领域的方式来构建认证中心 CA。具体建设方案如图 5 所示。

Table 1. Comparison of authentications
表 1. 身份验证比较

认证技术	特点	应用	主要产品
用户名/密码方式	简单易行	保护非关键信息	嵌入软件中
智能卡认证	安全可靠	需专用读卡器	智能加密卡
动态口令	一次一密	可能有新的漏洞	动态令牌
生物特征认证	安全性最高	技术不成熟	质问认证
USB Key 认证	安全可靠，成本低	依赖硬件的安全性	IKEY2000

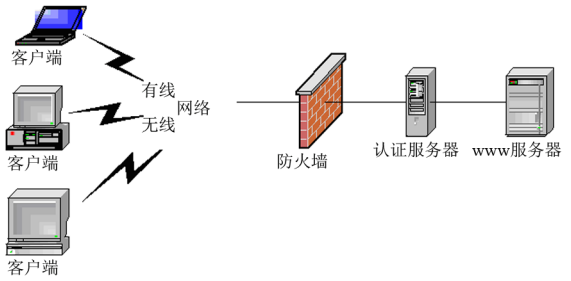

Figure 3. Deploy of authentication
图 3. 身份认证部署图

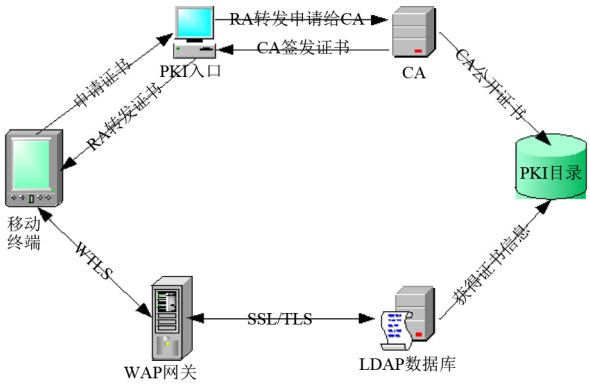

Figure 4. WPKI system structure
图 4. WPKI 系统结构

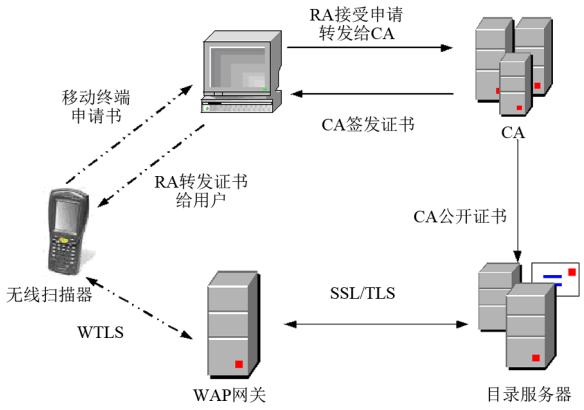

Figure 5. WPKI constructing scheme
图 5. WPKI 建设方案

在上图中可以看出：

1) 存在只为移动终端服务的申请登记中心(RA)服务器。它负责向移动终端提供证书申请、证书/密钥下载、证书注销申请、证书查询、证书吊销列表下载申请等服务。

2) 用无线应用协议网关连接无线传输层安全认证服务器与安全套接层认证服务器，无线应用协议网关起着两种协议转换的桥梁作用。

3) 有线认证中心可以与无线认证中心交互，它们的证书之间可以互用，这是有线认证中心与无线认证中心能共享数据的基础。

在此建设方案中，硬件投入基本没有额外增加，软件方面可以很好的将目前的有线 CA 部分共享，减少开发成本，也使整个认证系统有线无线融合在一起，实现统一，无缝连接，为以后更多无线需求奠定基础。

4. 移动 OA 系统构架与安全设计

4.1. 移动 OA 系统构架

移动 OA 系统由多个功能模块组成，各个功能模块紧密结合。移动 OA 系统的系统框架模型如图 6 所示。

移动设备(如笔记本、PDA、智能手机)与通信塔通信，通信塔将信息无线的传给有线网络，无线网关 PDSN 接收数据，并通过线缆将数据转发给有线网络。移动 OA 系统后台服务器通过自己的数据池同传统办公系统数据池交换数据，在传统 OA 基础上开发出一个工作引擎，代替前端移动设备处理复杂的业务流程，实现与传统 OA 的无缝交互。

4.2. 移动 OA 安全设计与主要模块

移动 OA 系统的安全功能模块由两大部分组成，分为用户功能模块和系统功能模块。其中用户功能模块主要包括：证书注册申请审核、撤消证书审核、证书更新、证书查询、证书下载、证书撤消、证书验证、CRL 查询、和密钥备份及恢复。系统功能模块主要包括：CA 初始化、日志管理、密钥管理和权限管理等。

证书签发模块：将通过审核的证书上传给 CA 服务器，然后 CA 服务器从证书申请表中读取已经通过审核的证书申请信息。对应每条证书申请信息，CA 首先为申请人生成双重密钥对，并将私钥用户提供的密码加密后写入密钥库的密钥表中：再由 CA 为申请人生成证书请求；接着 CA 为申请人生成 X.509V3 格式证书，并将证书保存在证书库的证书表中，同时将证书的一个副本发布到 LDAP 目录服务器。证书签发数据流程如图 7 所示。

证书下载模块：用户登录 RA 服务器，填写其证书序列号，个人 PIN 值，并提供私钥保护密码。RA 服务器审核用户身份，审核通过后，向 CA 服务器提出请求，CA 服务器将加密后(用户设定的密码加密)的用户私钥和该用户的数字证书合在一起，生成格式文件，返回给用户，用户进入证书下载界面，将 RA 服务器已颁发的证书下载到 U 盘保存，用于实现本系统用户的身份认证。

证书验证模块：验证证书是否由 CA 签发，具体是检验发行者的 CA 公钥能否正确解开用户实体证书中的“发行者的数字签名”；检查证书是否在有效期内或者是否已被撤消。

结合所讨论安全模型的各个功能模块，本文构建一个满足移动 OA 用户要求的端到端安全传输模型，并且可以保证传输过程中数据的保密性、完整性、不可否认性，并完成通信双方的身份认证，同时实现了无线有线无缝融合。

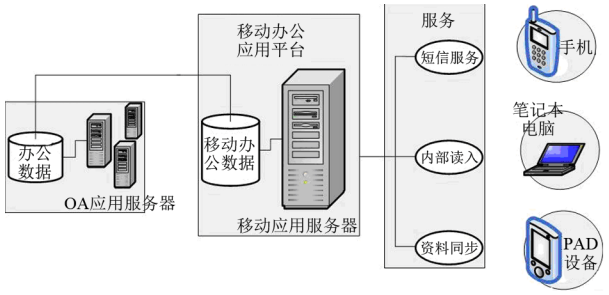

Figure 6. Frame model of mobile OA system
图 6. 移动 OA 系统框架模型

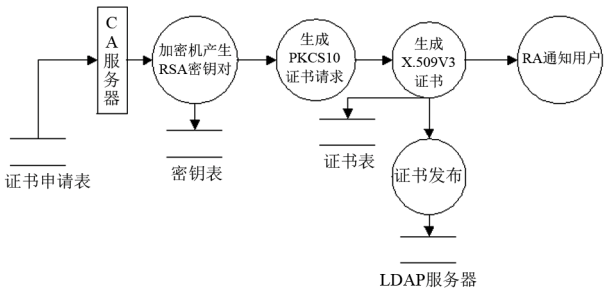

Figure 7. Digital flow diagram of certification issuance
图 7. 证书签发数据流程图

5. 结语

针对现有移动 OA 的安全需求现状，在现有安全模型的基础上，提出了一种基于 WPKI 的移动 OA 安全模型，能够很好的实现整个安全系统有线无线融合。系统运行结果表明本文的 OA 安全系统完全可以满足移动办公的全方位安全需求，实现了移动 OA 环境下的身份认证，保证数据的机密、完整和行为的不可抵赖，可广泛用于各种移动信息系统。未来可考虑椭圆曲线密码算法与 WPKI 证书设计等降低对计算量和网络带宽的限制。

参考文献 (References)

[1] 宋岐国, 张诗珊, 尚文利. 基于移动办公的烟草企业协同办公系统[J]. 制造业自动化, 2011, 33(10): 78-81.

[2] C. Cheng, A. Rasliid. Iaernel particle filter for visual tracking. IEEE Signal Processing Letters, 2005, 12(3): 242-245.

[3] S. Hyung-Ah. Breaking the short certificate less signature scheme. Information Sciences, 2009, 179(3): 303-306.

[4] 李风华, 卜巍, 马建峰等. 基于行为的访问控制模型及其行为管理[J]. 电子学报, 2008, 3(10): 1881-1890.

[5] H. Saripan, Z. Hamin. The application of thedigital signature law in securing internet banking: Some preliminary evidence from Malaysia. Procedia Computer Science, 2011, 3: 248-253.

[6] B. Miller. Electronicgovernment, concepts, methodologies, tools, and applications. Government Information Quarterly, 2010, 27(1): 109-110.

[7] 杨浩淼, 孙世新, 徐继友. 一种无随机预言机的高效可验证加密签名方案[J]. 软件学报, 2009, 20(4): 1069-1076.

[8] K. A. Shim. An ID-based aggregate signature scheme with constant pairing computations. The Journal of Systems and Software, 2010, 83(10): 1873-1880.

[9] T. Kwon. Privacy preservation with X. 509 standrd certificates. Information Sciences, 2011, 181(13): 2906 -2921.

[10] 厉京运, 赵卓. 基于WPKI的移动OA安全平台的研究与设计[J]. 计算机工程与设计, 2010, 31(3): 472-475.

