第 33 卷 第 1 期 计 算 机 工 程 2007 年 1 月
Vol.33 No.1 Computer Engineering January 2007
·安全技术· 文章编号：1000—3428(2007)01—0145—03 文献标识码：A 中图分类号：TP393

移动网络报税系统的轻量级安全解决方案

周 强[1]，林国恩[1]，李建彬[2]
(1. 清华大学软件学院，北京 100084；2. 国家税务总局，北京 100038)

摘 要：针对移动网络报税系统有关安全性和可用性的要求，提出了一个符合《电子签名法》规定的轻量级端到端安全解决方案。该方案集成了公钥密码系统和简单密码认证，用可靠性较高的公钥密码系统来保证动态密钥交换安全，又通过简单密码认证来减少运算时间，使得系统达到安全和效率之间的平衡，从而保证了移动网络报税系统的安全有效运行。

关键词：移动网络；报税系统；端到端安全；轻量级

Lightweight Security Scheme for Mobile Online Tax Returns System

ZHOU Qiang[1], LAM Kwokyan[1], LI Jianbin[2]
(1. School of Software, Tsinghua University, Beijing 100084; 2. State Administration of Taxation, Beijing 100038)

【Abstract】 On-line tax returns systems are inevitably subject to security exposures and risks of the global Internet. This paper presents a security design for tax returns system that supports mobile end user devices. The proposed approach is designed to address new security requirements due to the electronic signature law which aims to provide a legal basis for electronic transactions. The design makes use of and combines the advantages of PKI mechanism and simple password authentication. It is a lightweight security approach that can operate efficiently on resource-scarce mobile devices.

【Key words】 Mobile network; Tax returns system; End-to-end security; Lightweight

1 概述

网络报税系统就是借助计算机网络开展网上纳税服务，它可以规范税收管理、提高办事效率和方便纳税人办理涉税事宜。特别是 2005 年 4 月 1 日《电子签名法》的实施，更为网络报税系统的使用提供了法律保障，也对电子交易系统提出了安全需求。同时，该法就电子数据作为证据的真实性、可靠性、完整性和不可抵赖性也做了明确的规定。

近些年来随着摆脱空间限制的移动网络得到越来越广泛的应用，移动电子政务也成为政府部门信息化建设的一个新方向。使用手机等这类普及面极广的移动计算设备作为网络报税系统的终端平台，不仅能方便纳税人纳税，还可以为纳税服务拓展一个很好的新平台。

但是，移动网络比有线网络更容易受到干扰、窃听和攻击。当前移动网络普遍采用 WAP 协议作为无线网络通信的标准，但该协议只能保证移动终端到 Web 服务器这段安全通道上传输安全，数据在 Web 服务器被解密并以明文的形式存在。由于 Web 服务器很容易受到攻击，因此在 Web 服务器上存放数据明文是极大的安全隐患；同时也不符合法律对电子交易的要求，很大程度上威胁着移动网络报税系统的安全。此外，移动终端具有内存少、主频低、显示屏幕小和电池能源有限的特点，尽管目前的技术使得移动终端具备独立编程能力，但移动终端的安全依然在很大程度上受到计算资源的约束，传统基于 PC 机的安全措施在移动计算设备环境下并不适用。

可见，要保障移动网络报税系统的安全，必须从实效出发建立一套既能满足《电子签名法》安全需求，又能适应移动设备运算环境的安全解决方案。

然而，传统的PKI技术必须依靠复杂的计算来实现数据的安全，在移动计算设备上运行此类算法是不够实际的。此外，WMLScript[1]技术尽管可以实现移动设备上的数据安全，但由于它是在WAP协议的应用层上实现的，而且脚本语言本身的运算效率比较低，因此对移动终端的计算承受能力是个考验。

本文针对移动网络报税系统中的安全需求，提出一种基于移动计算设备平台的符合《电子签名法》安全需求的轻量级安全解决方案。该方案在保证移动报税系统的数据交换和事务处理安全的同时，充分考虑到移动计算设备的资源约束，将对数据进行加解密所耗费的时间控制在使用者所能承受的范围内。

2 移动报税系统安全需求

2.1 端到端安全需求

《电子签名法》的出台使电子数据获得了与传统数据同等的法律效力，也解决了推行移动报税系统所面临的电子数据的法律效应问题；同时，该法对电子交易过程中电子数据的传输和存储有明确的安全要求。如果在网络报税过程中出现纠纷，确保能够认定法律责任，保证国家税款不受流失。其中，该法第 8 条规定，审查数据电文作为证据的真实性，应当考虑以下因素：

(1)生成、储存或者传递数据电文方法的可靠性；

(2)保持内容完整性方法的可靠性；

基金项目：国家自然科学基金资助项目(90412007)；国家“863”计划基金资助项目(2001AA414220)

作者简介：周 强(1975－)，男，硕士生，主研方向：系统安全，无线网络；林国恩，教授、博导；李建彬，硕士、研究员

收稿日期：2006-04-30 **E-mail：**zhouq04@mails.tsinghua.edu.cn

(3)用以鉴别发件人方法的可靠性；

(4)其他相关因素。

依照《电子签名法》规定，在实施移动网络报税系统时必须考虑以下几个方面的安全问题：(1)报税数据从纳税人端到税务局端的传输安全；(2)报税数据到达税务局端的存储安全；(3)能够确定数据发送方的真实身份。

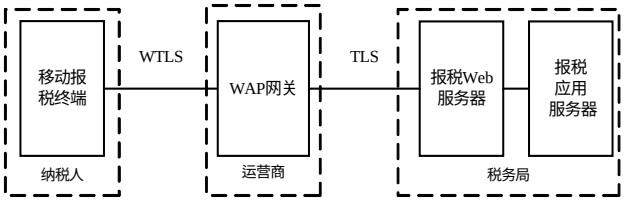

图 1 移动报税系统架构

如图 1 所示，在移动网络报税系统中，一般存在 3 类实体：纳税人，移动网络运营商和税务局。纳税人端移动设备通过移动通信网络与税务局端服务器连接。目前移动网络普遍使用 WAP 网关技术与有线网络实现互联，在传输层上以数据转发的形式提供安全通道。以 WAP 网关为界，移动终端到 Web 服务器之间的数据通道被分为两个部分：无线部分和有线部分。这两个部分分别用 WTLS 和 SSL 安全协议来保证安全。数据在无线环境下被封装在 WTLS 安全连接中，在有线环境下则被 SSL 所保护，在这两个区域内数据是安全的。

但是，WTLS[2]和SSL分别建立在WTP和TCP协议之上，二者之间无法保持无缝安全连接。为了接收和发送数据，WAP网关必须将数据从WTLS解密，然后再加密进入SSL，从而导致传输的数据明文会在WAP网关暴露。另外，WAP2.0 里规定了整个传输通道上将一致使用TLS安全协议(TLS协议是SSL协议的后续发展)。但是即使WAP2.0 得到了全面应用，TLS的安全保护也仅限于移动终端到Web服务器之间；也就是说，虽然数据可以很安全地从客户端传送到Web服务器，但是在Web服务器上被解密并以明文的形式存在，而Web服务器在互联网中是最容易受到攻击的。

显然，这种系统架构的安全性不符合《电子签名法》关于数据传输可靠性、内容完整可靠性和鉴别可靠性的规定。所以，为了规避数据明文暴露在 Web 服务器的风险，应该采用一定的措施保证数据在 WAP 网关和 Web 服务器时保持加密状态，而且要把数据解密和明文数据存储等工作放在安全性更高的应用服务器上进行。这就需要在移动网络报税系统上实现端到端安全来满足《电子签名法》要求和保证系统交易安全。

2.2 轻量级安全需求

相对固定网络，移动网络使得上网更加便利，它不受接入端口限制，只要在无线信号覆盖的地点都能实现上网。新一代手机如 Pocket PC 和 Palm top 等有着重量轻、体积小、高移动性等特点，也就成为移动网络用户的首选。

但是，更高的安全需求不可避免地会牺牲事务处理的效率。和传统 PC 相比，移动终端的资源要少得多。因此，在移动计算设备上的安全需求也和一般 PC 终端不同。对移动网络报税系统来说，需要在可用性方面满足以下的具体安全需求：

(1)保证数据在传输过程中的安全可靠；

(2)安全机制容易实现；

(3)考虑移动计算设备的低配置，在进行加密解密运算时要求耗费内存要少、计算量要小、速度要快；

(4)合适的密钥管理，移动计算设备属于便携式设备，容易丢失，要考虑密钥的安全存储问题；

(5)必要的用户身份认证。

公钥基础设施(PKI)[3]是目前使用最广泛的网络安全机制，它一般采用RSA加密算法，有着复杂的密钥管理。但是，如果在移动终端上运行RSA等公钥算法，必然导致计算时间过长甚至内存溢出，同时也将移动网络服务的优势全部抵消。所以不能简单地把PKI应用移植到移动网络平台，要在保证移动网络事务交易安全的前提下，考虑移动终端设备CPU和内存等的承受能力。

可见，在设计移动网络报税系统安全构架时，需要在《电子签名法》的安全需求框架下权衡安全和效率之间的关系，并在充分考虑移动网络报税系统实际应用环境的基础上，设计出一种针对移动终端设备的轻量级安全解决方案。

为此，本文提出了适用于移动网络报税系统的端到端轻量级安全解决方案。主要致力于实现以下两个目标：(1)实现移动网络报税系统的端到端安全性，保证在传输途中不暴露数据明文；(2)考虑移动计算设备的资源限制，实现轻量级的安全机制。

3 轻量级安全解决方案

3.1 移动报税系统安全架构

选择图 2 所示的系统架构来构建移动网络报税系统的端到端安全体系。

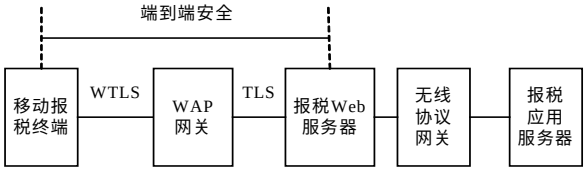

图 2 满足端到端安全性的移动报税系统架构

该架构在 Web 服务器和应用服务器之间引入一个无线协议网关。无线协议网关是一个税务局端网络上的服务器，其主要功能是对移动报税终端提交的登录账号进行身份认证，在认证通过后，它将作为移动报税终端在有线网络上的代理，提供一个接点让移动报税终端连接到税务局端的网络，然后代表移动报税终端与应用服务器实行信息交互和事务处理。从终端用户到 WAP 网关，从 WAP 网关到 Web 服务器分别有 WTLS、SSL 进行安全保护，而 Web 服务器与无线协议网关之间一般采用 HTTP 通信协议与 HTML 格式。寻求在这些安全协议的基础上构建一个从移动报税终端到无线协议网关的安全协议，使得数据明文不会暴露在 WAP 网关和 Web 服务器上，确保移动网络报税系统的端到端安全性。

这个网络架构可以有效保障移动网络报税系统的安全。此外，针对移动网络报税系统的轻量级安全需求，本文在移动终端和无线协议网关之间引入一个符合端到端安全需求的轻量级安全认证协议[4]。

3.2 端到端安全协议

在这个安全协议中，一个通信过程开始于客户端向服务器发出身份认证请求，接下来客户端和服务器之间将进行以下消息交换过程。

(1)服务器→客户端： R_a

服务器发给客户端一个随机数 R_a，用以标识不同的会话。

(2)客户端→服务器： $EK_S[R_a, R_{b1}, PIN]$， $EK_S[R_a, R_{b2}, SK]$

客户端发给服务器两个信息：密码验证和密钥交换。这两个信息都经服务器公钥 EK_S 加密后发送到服务器。密码验证消息包含用户密码 PIN，附加随机数 R_a 用以标识会话，附加随机数 R_{b1} 用以保证加密数据不被暴力破解；密钥交换消息包含一个客户端临时生成的对称密钥 SK，附加随机数 R_a 用以标识会话，附加随机数 R_{b2} 用以在下一步确认服务器收到密钥 SK。

(3)服务器→客户端： $E_{SK}[SN, R_{b2}]$

用客户端发送过来的密钥 SK 加密随机数 R_{b2} 并发送回客户端，客户端解密后与原有数据对比，如果一致，说明动态密钥 SK 交换成功，可以进行数据传输。

3.3 系统实现

如图 3 所示，移动网络报税系统可以分为 3 个部分：纳税人终端，移动通信网络和税务受理平台。由于搭建一个移动通信系统需要大量的人力物力，大多数的应用系统都是使用移动运营商提供的 WAP 网关。这样使得 WAP 网关不在税务端控制范围内，暴露明文显得更加不安全，也更加凸现了端到端安全的重要性。移动网络报税系统利用移动运营商提供的通信网络和 WAP 网关作为传输通道,在税务端搭建 Web 服务器和无线协议网关服务器，并使用防火墙等安全手段杜绝互联网访问内部数据。

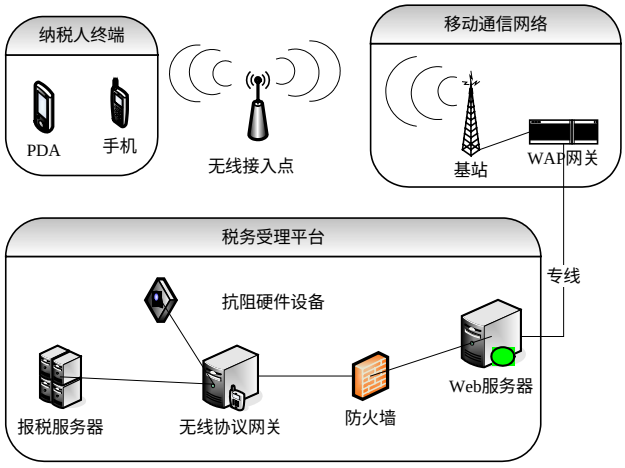

图 3 移动网络报税系统部署

在移动报税终端和无线协议网关服务器之间应用前文提及的端到端安全协议，使用J2ME平台来实现移动网络报税的数据安全传输[5]。

移动网络报税系统的工作流程如下：

(1)纳税人在客户端填写申报数据，形成要传送的数据文件；

(2)向服务器发出传送数据请求；

(3)移动报税终端和无线协议网关服务器之间依照安全协议产生密钥 SK ;此后移动终端与服务器之间的信息交换都是通过使用密钥 SK 来完成安全传输；

(4)移动报税终端用密钥 SK 加密申报数据后发送到无线协议网关服务器，无线协议网关服务器解密收到的数据并将其提交应用服务器；

(5)应用服务器返回申报结果信息给无线协议网关服务器，无线协议网关服务器用密钥 SK 加密数据后发送到移动报税终端；

(6)移动报税终端解密数据得到反馈信息。

4 安全分析与讨论

本文引入的端到端安全协议通过结合非对称加密和对称加密技术来实现移动计算设备和无线协议网关之间的相互认证授权，从而建立起安全的数据传输通道。这个协议有以下几个特点：(1)客户端的认证是通过简单的密码认证，但是这个密码是用服务器端的公钥加密的。而对一般的公钥密码系统如 RSA，公钥加密的运算量要比私钥解密低很多。因此该协议可以很大程度降低客户端的运算时间。(2)客户端不需要进行私钥解密和数字签名操作，大大减少了客户端的计算负荷。(3)共享一个密钥，这个密钥是客户端临时创建的，而且只有服务器知道。这种“一次一密”的密钥安全性能会更高，还可以依此鉴别数据发送方的身份。(4)客户端只需保存服务器的公钥，从而对客户端本身没有存储安全的要求。

这个轻量级安全解决方案集成了公钥密码系统和简单密码认证，用可靠性较高的公钥密码系统来保证系统安全，又通过简单密码认证来减少运算时间，它是符合移动网络报税系统的安全需求的。

此外，还需要采取必要的安全措施来保证无线协议网关和应用服务器的安全。特别是作为端到端安全机制边界的无线协议网关服务器还承担着对终端用户连接的身份认证和保存服务器私钥的任务。因此，必须保证服务器私钥的安全保存和用户密码以加密方式存储，并严格控制密钥和密码的访问权限，确保包括系统管理员在内的任何非授权用户都不能对密钥和密码进行任何操作。在实际应用中，可以采用图 3 所示的抗阻硬件设备[6]来保证密钥存储、密码存储和验证的安全。

5 结论

本文在《电子签名法》的安全需求框架下，结合移动网络报税系统的特点，提出了一个移动网络报税系统安全解决方案。该方案将数据加密后发送出去，到了无线协议网关服务器才被解密，从而实现系统的端到端安全需求；该方案使用的安全协议在客户端部分的计算量很小，只进行对称密钥的加解密和公钥加密操作，符合系统的轻量级安全需求。总而言之，该方案能够保证数据传送的安全可靠和内容完整，能够有效识别数据来源，符合《电子签名法》对移动网络系统的安全要求。

参考文献

1 WAP Forum. WMLScript Crypto Library[Z]. 2001. http://www.openmobilealliance.org/tech/affiliates/wap/wap-161-wmlsscriptcrypto-20010620-a.pdf.

2 WAP Forum. Wireless Transport Layer Security Specification[Z]. 2001. http://www.openmobilealliance.org/tech/affiliates/wap/wap-261-wtls-20010406-a.pdf.

3 Andrew N, William D, Celia J. 公钥基础设施(PKI)实现和管理电子安全[M]. 张玉清, 译. 北京: 清华大学出版社, 2002.

4 Lam Kwokyan, Chung Siuleung, Gu Ming, et al. Lightweight Security for Mobile Commerce Transactions[J]. Computer Communications, 2003, 26(18): 2052-2060.

5 Gupta V, Gupta S. Securing the Wireless Internet[J]. Communications Magazine, IEEE, 2001, 39(12): 68-74.

6 Wullems C, Looi M, Clark A. Enhancing the Security of Internet Applications Using Location: A New Model for Tamper-resistant GSM Location[J]. Computers and Communication, 2003, 2(1): 1251-1258.