智能卡在WPKI中的应用研究

黄 成,汪海航
(同济大学 计算机科学与技术系,上海 201804)

摘 要:WPKI是在有线PKI基础上进行优化拓展,为无线通信环境提供密钥管理的基础设施。介绍了WPKI体系的结构和PKI智能卡的特点,分析了智能卡在存储能力和处理能力上的局限性。在此基础上,从智能卡本身和WPKI体制的角度,给出了在智能卡上进行密钥管理和证书管理的策略。指出将智能卡安全应用于WPKI体系,智能卡还需相应的安全组件和安全设计,充分保证移动终端的安全。

关键词:WPKI;智能卡;密钥;证书
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2007)12-0154-03

Study on Smart Card Application in WPKI

HUANG Cheng, WANG Hai-hang
(Department of Computer Science & Technology, Tongji University, Shanghai 201804, China)

Abstract: Wireless PKI is an optimized extension of traditional PKI, which concerns the key management for the wireless environment. The architecture of WPKI and the features of PKI based smart card are introduced. The weakness on storage and processing ability of smart card are analyzed. Based on the analysis, the countermeasures for key management and certificate management on smart card are represented by considering the condition of smart card and WPKI. At last, another point that smart card needed when is used in WPKI is indicated as to add some secure component and secure design on smart card to assure the safety on mobile end device.

Key words: WPKI; smart card; key; certificate

0 引 言

随着移动通信技术的迅速发展,人们借助终端设备可以随时随地地接入网络进行交易和数据交换,促进了移动电子商务的发展。移动电子商务作为移动通信应用的一个主要发展方向,其与Internet上的在线交易相比有着许多优点,因此日益受到人们的关注,而移动交易系统的安全是推广移动电子商务必须解决的关键问题。

在有线网络环境中,PKI是网络安全建设的基础与核心,是电子商务安全实施的基本保障。而在无线通信网络中带宽、终端处理能力等方面的限制,使得PKI不能引入无线网络。WPKI(Wireless PKI)就是为满足无线通信安全需求而发展起来的,它可应用于手机、PDA等无线装置,为用户提供身份认证、访问控制和授权、传输保密、资料完整性、不可否认性等安全服务。智能卡拥有优秀的安全性,可以作为WPKI体系当中网络安全客户端很好的接入载体。智能卡有自己的处理器,因而能够在卡内实现密码算法和数字签名,并且能够安全地存储私钥。目前,智能卡已经逐渐应用于公安系统警务查询、税务部门查询、企业移动应用、移动电子商务、移动电子银行等领域,其中包括了基于PKI体系的USB Key以及利用手机短信进行移动业务处理的STK卡等。

1 WPKI与PKI智能卡

WPKI由终端、PKI门户、CA、PKI目录服务器等部分组成密钥管理体系。在WPKI的应用中,还设计WAP网关和数据提供服务器等服务设备。WPKI的基本结构如图1[1]所示。

WPKI中定义了一个PKI中没有的组件,即PKI门户,它负责处理来自终端和网关的请求,PKI门户一般代表RA并且通常和网关集成在一起。RA是连接终端和网关之间的桥梁,它负责接受终端和网关的注册请求,并向CA注册证书,CA一方面需要把生成的证书放到证书目录器(如LDAP服务器),供需要时(如

收稿日期:2007-03-19
基金项目:国家863计划资助项目(2006AA01Z438)
作者简介:黄 成(1983-),男,江苏盐城人,硕士研究生,主要研究方向为计算机网络与电子商务;汪海航,教授,博士生导师,主要研究方向为计算机网络与电子商务。

网关和服务器等设备在需要进行验证时)各实体查询;另一方面要将证书通过 RA 发送到终端和网关。终端包括手机、PDA 等 WAP 设备,而应用于其上的智能卡则用来存储数字证书、密钥等机密信息,实现加解密及进行数字签名的功能。

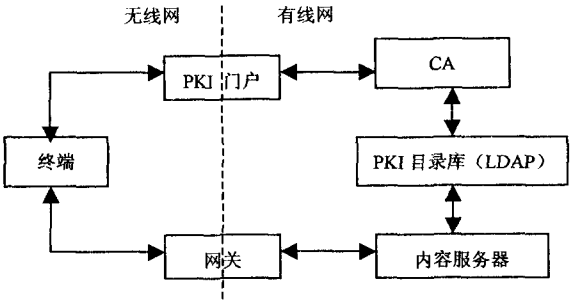

图 1　WPKI 的结构

一张智能卡主要由微处理器(CPU)和存储器以及固化在卡上的操作系统构成,是具有存储能力和计算能力的集成电路芯片卡[2]。PKI 智能卡是将 PKI 技术应用于智能卡的产物,在 PKI 体系中,私有密钥以及第三方认证机构所颁发的数字证书可以存储在极为安全的智能卡上。由于智能卡所携带的微处理器可实现存储、加解密、卡内生成密钥对等功能,因此数字签名可以利用存储在智能卡上的私钥自动计算生成。整个签名过程都是由卡内自动完成,并且签名密钥不可出卡,所以 PKI 智能卡可以有效确保私钥安全和签名的有效性。

2　智能卡在 WPKI 中应用问题分析

一个安全、可靠的 WPKI 应用系统,其安全性取决于系统的方方面面。将智能卡应用于 WPKI 时,其在客户端的安全中扮演了重要的角色。WPKI 体系根据无线环境与有线网络的种种区别,对 PKI 进行了优化,而当将智能卡应用于其中时,由于智能卡有特殊的环境要求,因此尚需解决一些特殊问题。

在智能卡应用系统中,终端可以支持多个应用系统,终端上的智能卡需要保存所有被其支持的应用系统 CA 公钥,产生密钥并进行加解密运算、数字签名、存储数字证书等[3],因此智能卡上的密钥的安全存储是要解决的重要问题。

在智能卡与终端的交互中,还需要进行相应的信息鉴别,保存交互的信息,以决定智能卡和终端的合法性。

另外智能卡作为一些机密信息的载体,其自身的安全性也是关乎整个系统安全的关键因素,因此在智能卡的设计和选择上需要相应安全策略和安全组件以达到一定的安全级别。

2.1　智能卡密钥管理策略

公钥密码技术已成为现代网络安全保密技术的基石,目前居于核心位置的公钥密码算法有两种,即 RSA算法和椭圆曲线(ECC)算法。智能卡应用于 WPKI 时,不仅要选择计算简单且安全性高的算法,而且对于密钥的管理也非常重要。

2.1.1　算法选择

基于 PKI 的应用中,密钥算法的安全程度也是非常重要的一个环节。目前智能卡芯片通常提供 DES 甚至 Triple - DES 的加密/解密计算能力[4]。DES 算法是一种公开的算法,尽管能破译,但计算既不经济又不实用。例如采用差分分析对一个 16 轮 DES 的最佳攻击需要 2^{47}个选择明文,采用最佳线性攻击平均需要 2^{45}个已知明文。

RSA 算法的优点在于简单易用,缺点是随着安全性要求提高,其所需的密钥长度几乎是成倍增加。目前,一般认为 RSA 密钥至少要 1024bit 以上的长度才有安全保障,但 1024 位的加密运算对于智能卡将是一个沉重的负担。ECC 算法使用较短的密钥就可以达到和 RSA 算法相同的加密强度,它的数论基础是有限域上的椭圆曲线离散对数问题,现在还没有针对这个难题的亚指数时间算法,因而 ECC 算法具有每比特最高的安全强度。由于智能卡在 CPU 处理能力和 RAM 大小的限制,采用一种运算量小同时能提供高加密强度的公钥密码体制对在智能卡上实现数字签名应用是至关重要的。ECC 在这方面具有明显的优势,160 位的 ECC 算法安全性相当于 1024 位的 RSA 算法,而 210 位的 ECC 则相当于 RSA 的 2048 位[5]。

智能卡对秘密数据的加解密都是在卡内完成,攻击者是无法通过智能卡接口取得秘密数据的,因此是比较安全的。

2.1.2　密钥存储

无线识别模块 WIM(Wireless Identity Module)用于存储 WPKI 公钥和用户私钥等密钥信息及相关证书信息,以完成无线传输安全层(WTLS)、传输安全层(TLS)和应用层的安全功能[6]。在对 WIM 的实现中,最基本的要求就是其载体的抗攻击性,也就是有某种物理保护措施,使得任何从 WIM 模块中非法提取和修改信息的操作都不可能成功,智能卡就是一个很好的此类安全载体(目前普遍使用 SIM 卡来实现此模块[1]),而且智能卡有自己的处理器进行加解密和数字签名,更是节省了手机等终端设备的资源。

一般,公钥具有两类用途:数字签名验证和数据加密。因此,终端智能卡需要配置签名密钥对和加密密钥对。这两类密钥对对于密钥管理有不同的要求。

签名密钥对:由终端智能卡生成,公钥发送给认证中心CA,由CA制作证书后再发给用户;私钥则保存在智能卡中,不能由WAP终端设备读取,也不能备份。

加密密钥对:通常情况下,用户端加密密钥由CA中心生成,生成后公钥用户签发证书,解密时要由CA中心加密保存,即做备份处理。在智能卡个人化时,解密私钥以加密方式写入卡中,同时完成加密证书的灌制。

2.2 证书存储

在无线环境中,由于网络带宽窄、稳定性差,以及终端设备受存储能力和处理能力的限制,因此要将智能卡应用于WPKI体系,必然对证书大小有严格的要求。

WPKI支持WTLS和X.509两种证书[1]。IETF PKIX工作组定义了一种新的证书格式——WTLS证书格式,它是标准PKI证书的子集,保证了这些PKI标准互操作的可能性,但更小,更简化。智能卡中的容量通常比较小,一般只有2~32kB,而X.509证书代码可多达10k,这将影响到智能卡功能的发挥。在WPKI中,除了使用WTLS证书格式外,还有一个解决方案:只在智能卡中存放一个指针,由指针指出完整证书的位置,而这个指针往往是一个URL地址(HTTP URL或LDAP URL[7])并且由PKI门户或(网关)服务器负责解析。这个URL地址往往只有几个字节,既适应了无线环境的特点,又能与现有PKI设施兼容。

在PKI系统中,客户端最大负荷在于验证对方的证书,这项任务可由两种方式完成。一是证书注销清单CRL,它是证书吊销的一个列表,用户将CRL下载到本地后进行验证,这样开销比较大;另一种是在线证书状态协议OCSP方式,OCSP服务器对外公开证书状态查询端口,收到查询请求包后,在系统证书状态表中检查证书是否作废,将查询结果按OCSP协议生成响应包后回送客户端。因定期下载CRL所需要的时间和费用以及无线带宽限制等原因,上述两种方法不适合WPKI。目前WPKI中采用短生命周期的网关证书,这种证书使用短的有效期,当CA想撤回网关或服务器证书,只要停止发放短期证书就可以了,客户因为得不到有效证书也会停止认为这个服务器或网关是有效的。

在PKI应用中,当智能卡插入到终端时将卡中的用户个人证书导入到终端系统的证书存储区,这样终端就可以使用用户证书进行身份验证和接入应用了。当智能卡从终端拔出时,终端需要将证书存储区中的证书信息删除以保证安全性。在证书导入、导出的过程中,需要验证此用户是否为合法经授权的用户,因此,可以结合用户的个人密码来提高安全性。

3 智能卡安全

智能卡中存储了WPKI所需的证书、密钥等机密信息,这些信息不仅在使用时确保其安全性,在存储中时也要确保防盗、防篡改。智能卡的安全在硬件方面通常是添加一些安全组件来保证的,在软件方面包括构造安全的卡片操作系统、安全的应用程序及相应的文件结构。

3.1 卡片安全组件

智能卡应用于WPKI时需保证存储于其中的信息的安全,因此卡自身的安全变得非常重要,为智能卡添加安全组件则是常用的一些方法,主要有硬件加解密、随机数发生器、内存管理单元以及安全检测与防护等模块组成。

安全的身份认证:智能卡采用PIN码进行保护,持卡人只有同时具备卡和其PIN码才可正常使用卡。卡与终端采用互认证,即不仅终端要验证卡的身份,而且卡也要验证终端的身份,以避免潜在的攻击、信息外泄。

卡片抵御攻击能力:智能卡在设计阶段就应采取有针对性的安全检测和防护手段。通过优化或增加一些硬件保护组件抵御入侵式或者非入侵式的硬件攻击,如通过产生干扰信号、抵御SPA[2]等攻击手段。卡片操作系统的良好设计也能避免被植入木马等程序而导致密钥等机密信息泄露的情形。

硬件加解密:密钥和加解密算法是系统中非常机密的信息,由于采用软件进行加解密操作有被盗取信息的可能性,而采用硬件实现则将机密信息屏蔽,外界很难探测到重要信息,具有更高的安全性。对于用来生成密钥的随机数来说,更是需要采用硬件随机数发生器(白噪声技术)来提高安全性。

安全的内存管理:实现逻辑地址的分区管理以及物理地址与逻辑地址的映射,保证用户程序代码和数据在存储区中的不连续存放。这样,即使芯片被解剖分析,攻击者也无法读出正确的数据。

3.2 卡片安全访问权限

智能卡中往往存储了机密信息,在卡片正式使用之前,须对卡片进行应用规划:建立相关的文件结构、建立相应的访问权限、写入相关数据和密钥。公钥算法中的签名私钥则只能在卡内生成,并且私钥只允许设置修改权和使用权,即私钥不出卡。用户的私有信息(如私钥、证书、PIN码等)由用户密码进行保护,并

(下转第160页)

2.3 TreeView 控件的拓展使用

在本系统的新闻模块里，系统实现了用户在发布新闻时可以选择新闻信息发布的对象(某一部门或者某一员工可看，或者所有人均可看)。这一功能的实现主要是借助于对 TreeView 控件数据绑定方法的改写。TreeView 控件是一种树型导航控件，它可以自动绑定网站的地图文件，一般用于网站的导航。在这里，系统利用了 TreeView 控件具有多层节点，并且每层节点都可以绑定数据的特点，将 TreeView 控件设为三层节点，同时对每一层节点，手动写代码分别绑定不同的数据源，从而实现了利用一个 TreeView 控件就可以将旅行社内部的所有部门以及部门下的所有员工显示出来的效果。从而实现了选择新闻信息发布对象的作用。如图 4 所示，整个 TreeView 控件分为三层：根节点是整个旅行社；二级子节点绑定的是旅行社下属的所有部门；三级子节点绑定的是各个部门下的员工。

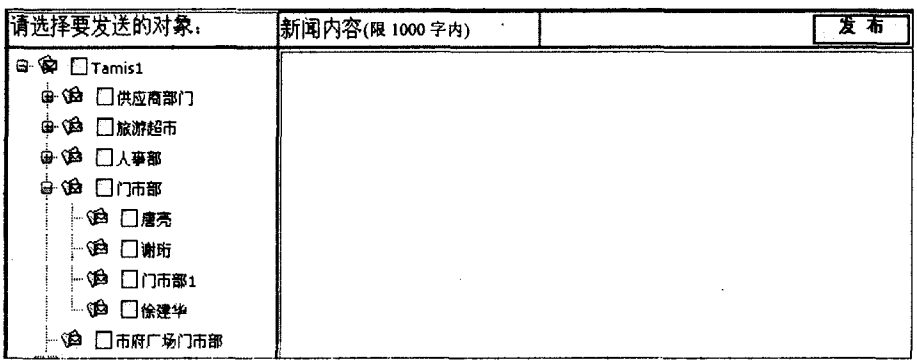

图 4 新闻模块里的 TreeView 控件

3 结 论

利用 ASP.NET 2.0 技术开发的基于 B/S 架构的旅行社管理信息系统，无论是从开发过程的效率上还是从系统的稳定性上来说，都大大优于之前的 Web 技术。系统较好地解决了当前旅行社管理信息系统所面临的一些问题，适用于中小型旅行社。而第三方列表控件、TreeView 控件和自定义查找控件等技术的使用，更是提高了系统操作上的方便性，完善了系统的功能。

同时本系统还具有一定的扩展空间，在提供必要的 Web 服务接口的情况下，可以向“电子交易平台”升级，因而具有比较广阔的应用前景。

参考文献：

[1] 马 军. 精通 ASP.NET 2.0 网络应用系统开发[M]. 北京：人民邮电出版社，2006.

[2] 徐新华. 精通 ASP.NET 2.0[M]. 北京：机械工业出版社，2006.

[3] 郝 刚. ASP.NET 2.0 开发指南[M]. 北京：人民邮电出版社，2006.

[4] 彭 征，廖和平，黄易禄，等. 旅行社旅游信息系统研究[J]. 西南师范大学学报：自然科学版，2006，31(3)：130－133.

[5] 陈 旭，张学杰. 基于 ASP.NET 技术的 Web 人事管理信息系统的设计与实现[J]. 计算机应用研究，2004(11)：217－219.

[6] 王 恒，韩作振，毛善君，等. 基于 B/S 结构的矿产资源管理信息系统设计[J]. 中国矿业，2006，15(7)：17－19.

(上接第 156 页)

且设置密码的错误次数上限，一般限制为 3 次，即密码核实三次出错，卡片锁死，且只能到指定地点进行解锁。

4 结束语

随着移动通信技术的发展，基于 WPKI 体系的应用也会越来越广泛，而智能卡则在这些应用系统中保证了客户端的安全。从技术和现实的角度讨论了将智能卡应用于 WPKI 体系中的一些问题，分析了如何根据智能卡的特点突破这些局限性，并对智能卡的存储安全和使用安全的相关策略进行了探讨。然而不同的应用系统可能会对智能卡有不同的要求，因此应根据需要采用不同的使用策略。

参考文献：

[1] 赵 文，戴宗坤. WPKI 应用体系架构研究[J]. 四川大学学报：自然科学版，2005，42(4)：725－730.

[2] 张志红. 智能卡安全技术及在 PKI 中的应用[J]. 网络安全技术与应用，2005(6)：10－12.

[3] 曹化工，梁宗炼，高小新，等. 基于智能卡的 PKI 体系实现框架[J]. 小型微型计算机系统，2003，24(6)：1004－1008.

[4] Hendry M. 智能卡安全与应用[M]. 杨义先等译. 北京：人民邮电出版社，2002.

[5] 刘 杰，王春萌，范春晓. 移动电子商务及 WPKI 技术[J]. 北京邮电大学学报，2002，25(2)：1－7.

[6] 刘志强. 智能卡在无线交易中的应用[J]. 信息安全与通信保密，2006(1)：53－57.

[7] 路 纲，余 堃，周明天，等. WPKI 与 PKI 关键技术对比[J]. 计算机应用，2005，25(11)：2505－2508.