面向电子政务应用的电子签章中间件设计与实现*

丁惠春，谷建华，张　凡，刘　刚
(西北工业大学 计算机学院，陕西 西安 710072)

摘　要：电子签章中间件作为电子政务系统中的一个重要组成部分,为电子政务系统提供功能服务,主要解决电子文件的签字盖章问题,用于辨识电子文件签署者的身份,保证文件的真实性、完整性、机密性和不可抵赖性。基于公开密钥基础设施(PKI),给出了完整的电子签章中间件安全解决方案,并详细分析了电子签章中间件的设计和实现。

关键词：电子政务；电子签章；公开密钥基础设施；中间件
中图法分类号：TP309.2　　**文献标识码**：A　　**文章编号**：1001-3695(2005)03-0135-03

Design and Realization of Electronic Seal Middleware Oriented E-Government

DING Hui-chun, GU Jian-hua, ZHANG Fan, LIU Gang
(College of Computer, Northwestern Polytechnical University, Xi'an Shanxi 710072, China)

Abstract: As an important component of E-Government system, electronic seal middleware provides the function service for E-Government System, and basically solves the problem of stamping the seal and signature in electronic document, distinguish the identity of operation, ensure the electronic document authenticity, integrality, confidentiality and cannot denying. This paper brought forward the safety solution of electronic middleware based on public key infrastructure, and analysed the design and realization of electronic seal middleware in detail.

Key words: E-Government; Electronic Seal; Public Key Infrastructure(PKI); Middleware

在政务管理自动化的过程中,以往政府办公主要以书面文件形式完成,文件的效力是以上级主管部门或领导签字盖章作为依据;目前政府办公流程是先在计算机中将文件整理好,打印出来交由领导审阅盖章,再批、转、发给其他部门,以供查阅。这样做一方面增加了办公环节,无法及时处理一些紧急文件;另一方面增加了工作人员的劳动强度,电子政务的优越性不能充分体现。最重要的是无法保证签章的安全性,任何人都可以盗用、仿制签章。这样,如何实现网上盖章与公文认证成为电子政务普及亟待解决的问题。

1　电子签章中间件

电子签章是电子政务时代的印章和印信。电子签章中间件作为电子政务系统的功能部件,使用户可以在电子文件上完成签字盖章,并通过网络安全、可靠地传输文件。此外,收件人可以轻松地验证出发件人的身份和签章的真实性,以及文件的原文在传输过程中是否被窜改,即电子签章中间件需要提供以下安全服务:

(1) 身份认证服务。建立一种信任及信任验证机制,用于确认参与电子政务业务的实体的身份,通过身份认证,保证身份的真实性。

(2) 信息保密服务。采用密码技术,对传输中需要保密的信息进行加/解密处理,防止信息的非授权泄漏。

(3) 数据完整性服务。文件的接收者应能验证在传送的过程中文件是否被窜改,使入侵者不可能用假文件代替合法文件。

(4) 不可否认性服务。保证签章签署者和文件发送者在事后无法否认他们所做的操作,为解决电子政务中的争议提供法律证据。

收稿日期：2004-04-12；修返日期：2004-05-27
基金项目：国家“863”计划资助项目(2003AA1Z2560)

2　电子签章中间件的安全解决方案

近年来,在提供分布式网络安全服务机制中,公开密钥基础设施(PKI)作为一种重要的安全机制在我国得到很大发展,它是利用公钥体制提供安全服务的具有通用性的支撑性基础设施,通过自动管理密钥和证书为用户建立起一个安全的网络运行环境。在 PKI 提供的框架中,各种各样的构建、应用、策略等组合起来为网络应用提供认证、访问控制、机密性、完整性和不可抵赖性服务[1]。根据电子签章中间件的安全需求特点,给出如下基于 PKI 的安全解决方案。

2.1　身份认证服务

目前,在分布式网络应用的身份认证中,最常见的是基于口令的认证机制,这是一种弱认证方式,口令在开放网络环境中传输时可能被嗅探、劫持,或被重放攻击,不适用于安全性较高的场合,而且其认证是单向的。

安全电子签章中间件通过使用由可信证书机构(CA)颁发的数字证书,结合对应的私钥,完成对实体的单向或双向身份认证,克服了传统的口令认证的弊端,大大提高了身份认证的安全水平。在系统中,用户登录需要提供数字证书,以确认身份,保证用户的真实性和合法性;同时,用户也可以获取服务器的数字证书,并对其进行认证,保证服务器的可信性。

2.2 信息保密服务

传输在网络上的敏感、机密信息和数据有可能在传输过程中被非法用户截取或恶意窜改,安全电子签章中间件使用公钥密码技术来提供信息保密服务,保证交互信息的机密性。然而,公钥密码的计算是很慢的,为了提高处理效率,结合对称密钥,在电子签章中间件中采用如下过程实现信息保密服务:

(1) 加密过程:①用随机生成的对称密钥来加密数据;②接着用授权接收者的公钥来加密这个对称密钥。

(2) 解密过程:①授权接收者用他的私钥来解出对称密钥;②接着用对称密钥进行解密获得原始数据[2]。

2.3 不可否认性和数据完整性服务

电子签章中间件需要保证公文的签字盖章者事后不会否认,以及加盖过签章的电子公文在流转过程中不被窜改。通过数字签名技术可以实现电子签章中间件中的不可否认服务和数据完整性服务。

数字签名操作是一个两步过程:

(1) 签名者通过杂凑函数把数据变成固定大小。

(2) 签名者把杂凑后的结果用于私钥操作。

验证操作也是一个两步过程:

(1) 验证者通过杂凑函数把数据变成固定大小。

(2) 验证者检查杂凑后的结果、传输来的签名、签名实体的公钥(如果签名与公钥和杂凑结果相匹配,签名就被验证了;否则,验证失败)[2]。

通过数字签名技术,可以为原始信息的真实性和完整性提供有力的证明,同时数字签名技术在提供不可抵赖性的服务中起到了至关重要的作用。由于非对称密码体制的安全性,只要保证签名方私钥信息的秘密性,即能够保证任何其他人都无法对签名进行伪造,任何人都不能对发送者的原始信息进行任何窜改,因为任何窜改都可以导致签名的无效。

3 电子签章中间件的设计与实现

3.1 电子签章中间件的流程设计

通过对电子政务系统总体运行环境和电子签章的工作流分析,设计电子签章的操作流程如下:

(1) 用户登录系统,进行身份认证。保证只有合法用户才能进入系统。

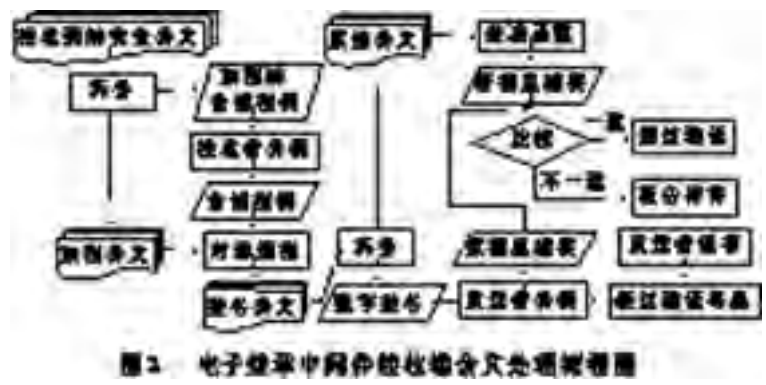
(2) 合法用户获得其有权使用的签章。合法用户进入系统后,可以获得其有权使用的电子签章列表。为了使用其中某个电子签章,签章使用者必须向 CA 申请他的电子签章。只有申请签章通过后,CA 才能下发电子签章并交付使用者使用。

(3) 加盖电子签章。签章者对电子公文进行签章操作,这里包括两个方面的内容:①前台界面的处理,使用户可以获得在文档上加盖签章的视觉效果;②还需在后台进行数字签名操作。

(4) 发送电子公文。利用发送者的私钥对电子公文进行数字签名,将签名结果和电子公文合成(称之为签名公文);然后采用对称密钥对其进行加密(称之为加密公文),该对称密钥是一个随机产生的会话密钥,它由接收者的公钥加密保护(生成加密的会话密钥)。发送前,将加密后的加密公文和加密的会话密钥进行合成,形成发送端的安全公文进行发送,从而实现了电子公文的数字签名和加密。发送端的处理流程如图 1 所示。

这里,原始公文是已经加盖签章完毕后的公文,在公文中每个签章对应于一个独立的数字签名,在加盖签章的操作过程中,每个签章加盖时,都会产生一个加盖者的签名信息,在接收端可以分别进行验证。

(5) 接收方进行验证。接收方收到发送方的数据之后,将其拆分,从中提取出加密的会话密钥,然后通过自己的私钥恢复出会话密钥,再通过会话密钥将加密公文恢复成签名公文,接着再对签名公文进行拆分,得到原始公文和数字签名。再把由原始公文通过杂凑函数计算出来的新消息摘要和由数字签名通过发送方公钥恢复出来的原数字签名进行比较,如果一致则通过验证;否则不能通过验证,并报告异常。图 2 给出了电子签章中间件接收端公文处理流程。



基于公开密钥基础设施之上构造电子签章中间件具有很高的安全性,实现了对电子公文的机密性、完整性保护,以及签章的真实性和不可否认性服务。

3.2 电子签章中间件功能模块设计

电子签章中间件可以分为以下四个模块(图 3):

(1) 用户管理模块。它包含用户身份认证和用户权限管理子功能。用户身份认证功能一方面能够辨别签署者身份的真伪,另一方面能够确保签署者身份的不可抵赖性,即一旦签名而且身份认证通过,则签名者将无法否认此签名。用户权限管理功能对用户的权限(包括签章使用权限和公文使用权限)进行分配和控制。

(2) 签章管理模块。它包括签章类型管理、签章文件管理和签章授权管理。①签章类型管理:通过安全方式对数据库进行操作,对签章的类型(公章、私章、签名等)进行管理。②签章文件管理:管理电子签章对应实际签章的图形文件,其通过安全方式存储在数据库中。③签章授权管理:将签章和持有者进行绑定,用户登录系统后可以获得其有权使用的签章列表。

(3) 签章使用模块。它包括文档签署和撤销签章功能。①文档签署:在浏览器中嵌入中文办公套件,调用中文办公套件的 API 完成对文档加盖图章或签名,而后台则透明地进行相应的数字签名操作。这里无缝集成加盖签章的前台与后台操

作, 实现用户盖章的透明性。②撤销签章: 在进行撤销签章动作之前, 首先对执行此动作的人的身份进行认证, 判断与签署者是否是同一个人, 从而保证只有签署者才能够撤销自己的签章。

(4) 签章认证模块。它包括签章验证和公文验证功能。①公文验证: 对发送电子公文的单位进行验证, 以及对电子公文的完整性进行验证。如果签署后的文档发生了变更, 验证时则会提示文档验证未通过。②签章验证: 对公文中的每个签章进行验证, 判断电子公文中的签章是否为声明者所签署。

3.3　电子签章中间件的实现

中间件的实现需要考虑到安全服务的具体实现, 以及中间件自身的通用性、易集成性和可扩展性。在中间件的具体实现中, 作了如下考虑:

(1) 采用 E-key 技术鉴别用户身份。E-key 又称电子钥匙, 是一种专用硬件存储介质, 存放有个人信息、证书信息以及私钥信息等。E-key 使用 PIN 码进行保护, 以保证私钥的安全。登录系统时, 需要使用者插入 E-key, 并输入相应的 PIN 码, 防止未经授权的访问。另外, 对文档进行签署以及撤销签署时, 要求签署者提供 E-key, 从而保证数字签名的安全性。

(2) 采取公文和签章分级管理的机制, 用一个公文认证类 DocumentAuth 对应于公文的认证管理, 该类对应于整个公文的认证信息; 而对于公文中的每一个签章, 用一个签章认证类 SealAuth, 记录该签章的认证信息。公文认证对象和签章认证对象是一对多的包含关系, 将公文和签章分开管理, 分别进行签名和加密, 这样就可以在单个文章中加盖多个签章, 且可以分别对这多个签章以及整个公文进行验证, 从而实现了单文档多签章机制。

(3) 将电子签章中间件设计为 EJB, 可以方便地将其部署在电子政务体系中, 实现与中文办公套件的无缝集成。电子签章中间件在电子政务系统中的位置如图 4 所示。

图 4

4　结论

公开密钥基础设施(PKI) 作为一种重要的安全机制, 通过具体的构建、应用、策略等组合来为网络应用提供认证、访问控制、机密性、完整性和不可抵赖性服务。基于 PKI 的电子签章中间件保证电子公文的完整性、机密性、电子签章的真实性和不可否认性, 对电子签章的使用者进行授权, 实现对电子签章的查看和使用权限管理。

在西部电子政务示范工程的实施过程中, 分析了电子政务系统总体应用环境, 设计和实现了电子签章中间件。作为整个电子政务系统中的功能部件, 电子签章中间件具有通用性、易集成性和可扩展性, 具有广泛的应用前景。

参考文献:

[1] 冯登国. 计算机通信网安全[M]. 北京: 清华大学出版社, 2001.

[2] Carlisle Adams Steve Loyd. 公开密钥基础设施 —— 概念、标准和实施[M]. 冯登国, 等. 北京: 人民邮电出版社, 2001.

[3] Bruce Schneier. 应用密码学 —— 协议、算法与 C 源程序[M]. 吴世忠, 祝世雄, 张文政, 等. 北京: 机械工业出版社, 2001.

[4] Nick Galbreath. Internet 和数据库加密[M]. 曾振宇 白克壮, 尹喆, 等. 北京: 电子工业出版社, 2003.

[5] Houseley R, Polk T. Planning for PKI [M]. Wiley Computer Publishing, 2000.

[6] Andreas Eberhart, Stefan Fischer. Java Tools [M]. Wiley Computer Publishing, 2002.

作者简介:

丁惠春(1980-), 男, 硕士研究生, 主要研究方向为网络与分布计算、信息安全; 谷建华(1965-), 男, 教授, 主要研究方向为分布对象计算技术、面向电子政务的 Internet 技术; 张凡(1979-), 男, 博士生, 主要研究方向为信息安全; 刘刚(1979-), 男, 博士生, 主要研究方向为网络与分布计算。

(上接第 134 页) TC, 返回给用户。若安全级为 c 的用户执行更新操作时, 则基于 TCB 模型, 将安全级为 c 的用户对多级数据视图的更新操作, 分别对应到单级关系 D_c ($c \geq c$) 中。

4　结束语

本多级安全数据库安全子系统为系统主体管理员、系统安全管理员分别提供了角色定义、用户定义和客体安全级定义的通用界面, 系统管理员通过动态选择数据库管理系统中的数据库、表以及表中的属性列可进行相应安全级的定义, 实现单级数据库与多级数据库之间的转换。在开发具体应用系统时, 负责各功能模块具体设计的程序员, 可以相应的形式调用此多级安全子系统, 来控制具体应用中对数据库进行操作的工作流的权限验证, 过滤返回相应的结果, 从而实现数据库数据项的强制访问控制, 实现系统的多级安全性。

参考文献:

[1] F Lunt, D E Denning. The SeaView Security Model[J]. IEEE Transacations on Software Engineering, 1990, 16(6): 593-607.

[2] F Cuppens, K Yazdanian. A Natural Decomposition of Multilevel Relations[J]. IEEE Symposium on Security and Privacy, 1992, (5): 273-284.

[3] 刘刀桂, 孟繁晶. Visual C++ 实践与提高(数据库篇)[M]. 北京: 中国铁道出版社, 2001.

作者简介:

卢贤玲(1975-), 女, 讲师, 主要从事网络和数据库技术的开发工作; 韦大伟(1962-), 男, 副教授, 主要从事系统工程和信息系统领域的研究; 徐斌(1971-), 男, 工程师, 主要从事信息管理系统和实际工程应用的开发工作。