PKI 技术及其在企业中的应用①

PKI Technology and Its Application in Enterprises

孙美青 王如龙 (湖南大学 软件学院 湖南 长沙 410082)

摘 要： 网络成为信息连通的动脉，网络信息安全成为人们关注的焦点之一。PKI 作为一种重要的网络安全基础设施，已经深入到电子商务、电子政务、网上银行等领域。企业作为网络环境中的一个重要主体，网络信息安全对于企业的正常运营起着保驾护航的作用。本文在深入分析 PKI 的概念、发展现状、核心服务和基本原理的基础上，探讨了企业 PKI 系统的构建，以及 PKI 技术在企业 OA 系统、移动办公、个人电脑等方面的应用。

关键词： PKI 技术 信息安全 企业应用

1 引言

网络技术迅速发展和普及，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生着重大影响。在开放的 Internet/Intranet 中，信息均以开放透明的方式在网络中传播[1]。由于缺乏有效的验证及约束机制，网络在为人们提供快捷与便利的同时，不可避免地存在信息安全隐患，如信息中断、窃听、篡改、伪造等，严重影响了网络信息的有效性、安全性。PKI 技术作为网络安全基础设施，为解决网络信息安全问题提供了有力保障和技术支持。在网络通信中，PKI 利用数字证书消除匿名带来的风险，利用加密技术消除开放网络带来的风险，以保证信息的保密性和完整性。

2 PKI概述

PKI是20世纪80年代由美国学者提出来的概念，是“Public Key Infrastructure”的缩写，意为“公钥基础设施”，是利用公钥理论和技术实施和提供信息安全服务的具有普适性的基础设施[1]。公钥体制是目前应用最广泛的一种加密体制，在这一体制在中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性，又能保证信息具有不可抵赖性。目前，公钥体制广泛应用于 CA 认证、数字签名和密钥交换领域。

在国外，PKI 应用已经有了长足的发展，很多厂家如 Baltimore Technologies，Entrust 和 Microsoft 等都推出了 PKI 产品；有些公司如 VeriSign 已经开始提供 PKI 服务；由美国 National Security Agency (NSA)推动的 DOD PKI 研究也正积极地进行，美国的许多大企业已经建立了自己的 PKI 系统；加拿大政府公开密钥基础设施 GOCPKI (Government Of Canada Public-Key Infrastructure)是世界上最早的大规模政府 PKI 计划，已在各行各业取得了成效。但总的来说，PKI 系统仅仅还处于示范工程阶段，新技术不断出现，PKI 的结构、对称及非对称密钥算法、密钥生命周期管理的方案等还在不断变化[1]。

在我国，上海、北京、深圳、重庆等城市已经建立了 CA 认证中心，以便为本地化通信网络提供安全服务[2]。CA 认证中心是 PKI 的重要组成部分。在国家直属部门，以中国人民银行为首的 12 家金融机构推出了“中国金融认证中心 CFCA”，中国电信也在开展 CA 机制的试验工作。另外，许多网络通信公司正在积极开发自己的基于 PKI 的安全产品。

① 基金项目:国家科技支撑计划(2006BAF01A13)
收稿时间:2008-11-14

3　PKI的核心服务

PKI 的核心是要解决信息网络空间中的信任问题，确定信息网络空间中身份的唯一性、真实性和合法性，保护信息网络空间中各种主体的安全利益[1]。PKI 是目前公认的保障网络社会安全的最佳体系[3]。PKI/CA 是基于网络信息加密应用的安全系统，PKI 解决了网络中的访问授权、数据加密、签名和身份认证等问题，适合应用于网络上的电子交流，包括电子商务、电子政务。它提供的核心服务主要包括：

(1) 认证。在通信过程中对双方进行认证，以保证互动双方身份的正确性。PKI 认证服务采用数字签名这一密码技术。

(2) 完整性。保证网络中所传输的信息不被中途篡改及通过重复发送进行虚拟交易。PKI 的完整性服务可以采用两种技术之一。一种是数字签名，另一种是消息认证码或 MAC。这项技术通常采用对称分组密码或密码杂奏函数。

(3) 保密性。保证信息在公开网络的传输过程中，即使被盗取也无法查阅。PKI 通常采用对称密钥加密技术和非对称密钥加密技术结合的方式来实现保密性。

4　PKI技术原理

PKI 是一个提供强大开放的数据加密和支持加密服务的典型方法。PKI 基础设施采用证书管理公钥，通过第三方的可信任机构——认证中心(Certificate Authority)，把用户的公钥和用户的其他标识信息捆绑在一起，在 Internet 网上验证用户的身份。PKI 基础设施把公钥密码和对称密码结合起来，在 Internet 上实现密钥的自动管理，保证网上数据的保密性、完整性。

下面详细分析 PKI 技术是如何保证网上数据传输保密性和完整性的。对于这个问题可以从以下几个方面来分析。

(1) 对发送文件加密。

信息发送方采用成熟的对称加密算法，如 DES、3DES、RC5 等对发送的信息加密，保证文件安全快速的到达接受方。对称加密采用了对称密码编码技术，它的特点是对文件加密和解密使用相同的密钥[4]。即使黑客截获此文件，用同一算法也不可以解密此文件，因为加密和解密均需要两个组件：加密算法和对称密钥，加密算法需要用一个对称密钥来解密，而黑客并不知道此密钥。

(2) 加密对称密钥。

对称密钥可以通过电话告知或者通过 Internet 发送给信息接受方，但是，这些方式都不安全，很有可能被黑客截获，为此，需要对对称密钥进行加密传输。采用的方法是用非对称密钥算法加密对称密钥后进行传送，也就是“数字信封”技术[5]。与对称密钥算法不同，非对称密钥算法需要两个密钥：公开密钥(Public Key)和私有密钥(Private Key)。公开密钥和私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，只有用对应的公开密钥才能解密。信息收发双方各有一对公/私密钥，公钥可在 Internet 上传送，私钥自己保存。这样发送方就可以利用接收方的公钥加密对称加密算法中的对称密钥。即使黑客截获到此密钥，也会因为黑客不知道接收方的私钥，而无法得到对称密钥，因此也解不开密文，进而保证了文件的安全。数字信封技术将对称密钥和非对称密钥结合起来用于密钥交换和发布，解决了长期困扰密钥在传输中的安全问题。因为公钥加密算法速度慢，因此通过数字信封来封装对称密钥，然后用对称密钥对信息进行加密和解密，这比直接用公钥加密盒私钥解密的非对称密钥要快得多，由于通信过程中交换的数据量大，通信双方用同一对称密钥来加密和解密数据可以大大节省时间，提高效率，而公钥仅用来封装对称密钥。

(3) 身份验证与篡改识别。

为了防止黑客利用接收方的公钥加密一份假文件的对称密钥，并发送给接收方，使接收方能够清楚辨别收到的文件是不是由发送方所发送，必须采用数字签名以证明发送方的身份。数字签名是通过散列算法，如 MD5、SHA-1 等算法从大块的数据中提取一个摘要[6]。而从这个摘要中不能通过散列算法恢复任何一点原文，即得到的摘要不会透露出任何最初明文的信息，但如果原信息受到任何改动，得到的摘要则肯定会有所不同。因此发送方可以对文件进行散列算法得到摘要，并用自己的私钥加密，这样即使黑客截获也无用。因为黑客不会从摘要内获得任何信息，但接收方却不一样，他可以用发送方的公钥解密，如果用发送方的公钥能够解开此摘要，说明此摘要肯定是发送

方所发送的，因为只有发送方的公钥才能解开用其自身的私钥加密的信息，因而可以确定文件发送者的身份，起到身份验证的作用；对收到的摘要解密后，再对收到的文件(解密后的文件)也进行同样的散列算法，并通过比较摘要是否一样，就可得知此文件是否被篡改过，因为根据散列算法的特点，诺摘要相同，则肯定信息未被改动。这样不仅解决了证明发送人身份的问题，同时也解决了辨别文件是否被篡改的问题。

(4) 确定公钥和公钥所属人。

通过对称加密算法加密其文件，在通过非对称算法加密其对称密钥，有通过散列算法证明发送者身份和其信息的正确性，但这样仍然还存在问题，即接收方并不能肯定他所用的所谓公钥一定是发送方的。对此，解决办法是用数字证书来帮助确定公钥和公钥所属人。

数字证书是一种数字标识，提供用户在互联网上的身份认证，它是一个经证书授权中心数字签名的包含公开密钥拥有者信息和公开密钥的文件[6]。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名[7]。在一般情况下，证书中还包含的密钥的有效时间、发证机关(证书授权中心)名称、该证书的序列号等信息。它是由一个权威机构——CA 机构，又称为证书授权中心发放。CA 机构作为网络信息交流中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。CA 中心为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA 机构的数字签名使得攻击者不能伪造和篡改证书，它是 PKI 的核心，负责管理 PKI 结构下所有用户(包括各种应用程序)的证书，把用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份。

5　企业PKI系统

5.1 企业 PKI 系统逻辑结构

完整的 PKI 系统必须具有权威认证机构(CA)、数字证书库、密钥备份及恢复系统、证书撤销系统、应用接口(API)等基本构成部分[8]。根据企业的实际需求，对于企业 PKI 系统的构建，设计了统一认证 SSO (Single Sign On)平台，通过此平台可以实现所需要的安全服务，包括数字证书的申请、注册，对于应用系统的安全访问和数据的安全存储等。其逻辑结构如图 1 所示。

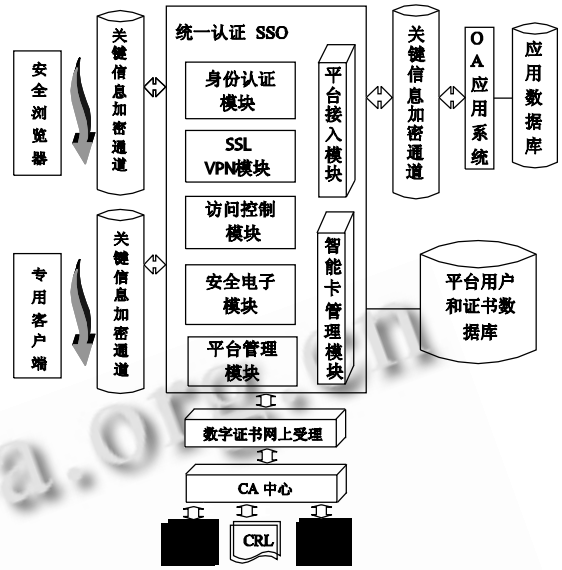

图 1　企业 PKI 系统逻辑结构图

5.2 企业 PKI 系统网络结构

企业 PKI 系统网络结构如图 3 所示，由平台 WEB/应用服务器、认证/接入服务器、CA 及证书受理服务器、数据库服务器、Secure VPN 服务器组成。

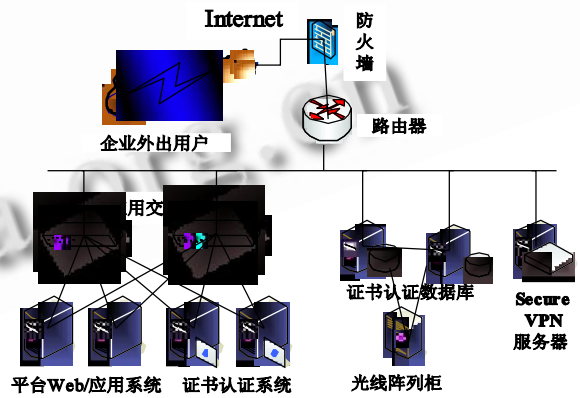

图 2　企业 PKI 系统网络结构

WEB/应用服务器提供平台管理；认证/接入服务器负责用户身份认证和业务系统接入；CA 及证书受理服务器负责用户证书的签发；数据库服务器提供平台用户信息、证书信息等数据的存储；Secure VPN 服务器负责为用户通过 Internet 访问内部网应用提供安全认证和接入。

5.3 企业 PKI 系统证书认证数据库

平台数据库主要由用户数据、证书数据、业务系

统配置数据、访问控制(ACL)数据、日志等数据组成。证书认证数据库主要用来存储这些数据信息。

5.4 证书认证体系

系统对用户的身份认证主要依靠数字证书和USB-KEY 来完成，首先必须解决数字证书的来源和USB-KEY 的制作问题。CA 是数字证书签发和密钥管理的关键，负责为同一身份认证平台用户提供数字证书申请、作废和 USB-KEY 制作等服务，它由 CA 服务器、证书受理服务器、平台数据库、证书管理系统组成。

CA 服务器，接受证书申请请求，产生密钥对，签发用户证书；接受证书作废申请，作废用户证书，定期签发 CRL；

证书受理服务器，定时提取平台数据库中需要申请证书的用户信息，打包提交到 CA 服务；接受返回的证书并存入数据库。定时提取待作废证书的信息并提交作废请求至 CA 服务器。

证书管理系统，集成在平台的管理界面中，提供基于 web 的证书状态查询、证书下载、USB-KEY 制作、证书作废。

统一认证平台，平台构建统一的认证门户，用户需要使用 USB-KEY 登录认证成功后才能进入，主要作为各应用系统的统一访问入口和平台管理的入口。该门户可以进一步扩展为企业内部信息的发布平台，实现内部信息的共享。

6 PKI在企业中的实际应用

在构建企业 PKI 系统的基础上，本文实现了企业 OA 系统中秘密文件的加密存储和加密传输、企业电子邮件的签名和加密传输、本地文件使用个人证书进行加密保存和读取、使用证书通过 VPN 从互联网接入企业内网的移动办公。将 PKI 技术充分的应用到企业信息安全的需求之中，为企业的信息安全发挥全面的保护作用。

6.1 OA 公文的安全保密

在 OA 系统中，用户均采用浏览器登录和访问应用系统，在统一认证门户登录认证成功后，再访问 OA 系统。企业应用系统接入平台的架构如图 3 所示。用户通过统一认证平台访问 B/S 应用系统。通过统一认证平台，完成对于 OA 系统访问的具体过程如下：

(1) 用户登录统一认证平台，认证服务器完成身份认证，获取用户证书序列号信息；

(2) 平台应用服务器将加密签名的认证信息附加在业务系统认证 URL 上，并经由客户端跳转至 OA 应用服务器；

(3) OA 应用服务器调用接口，将加密签名的认证信息转至应用认证前置；

(4) 应用认证前置通过安全通道将加密签名的认证信息提交到平台认证服务器；

(5) 平台认证服务器解密验证得到业务系统认证所学的明文帐户信息，并经由加密通道安全的传回应用认证前置，并由其返回给 OA 系统；

(6) OA 系统按传回的帐户信息验证通过，建立访问会话；

(7) OA 系统与用户通过信息加密进行通讯，保证了信息的安全。

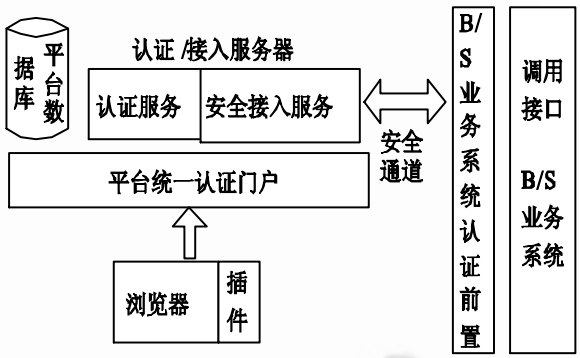

图 3　接入平台架构

6.2 移动安全办公

Secure VPN 提供了一项基于 PKI 的解决方案，支持企业将安全远程访问扩展到任何连接到互联网的用户——员工、客户和合作伙伴[9]。移动办公用户通过标准 Web 浏览器即可进行电子邮件、OA 应用和台式机远程控制的应用访问，保障信息的安全传输。

(1) Secure VPN 总体结构，如图 4 所示。

(2) 远程接入业务流程

· 用户打开浏览器，访问企业 Secure VPN 首页；

· 用户出示登录凭据——数字证书；

· Secure VPN 服务器根据用户的身份认证方式和登录凭据到认证源验证用户身份；

· 如果身份认证通过，根据用户身份信息和访问规则，引导用户进入 Secure VPN 工作平台；该工作平台罗列出用户能够访问的资源连接；

· 用户点击资源链接请求访问企业内部资源，根

据访问规则决定用户是否可以访问该资源；

• 根据资源类型，启动相应资源访问通道，为用户提供资源访问。

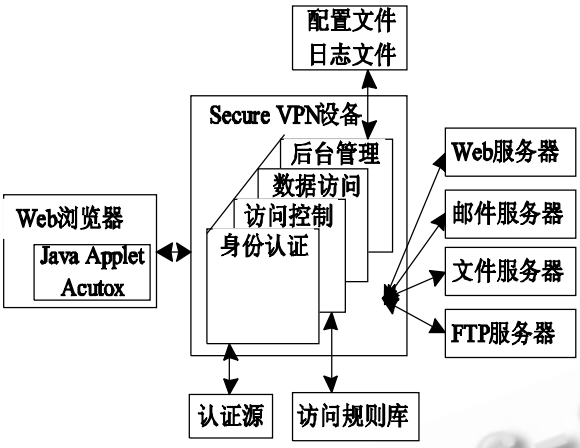

图 4 Secure VPN 总体结构图

6.3 个人信息加密与存储

在企业的个人电脑中存储了大量的电子文件，部分更有企业内部敏感或机密数据。大部分企业对这些文件的操作都只依靠操作系统的权限控制，这只能提供最基础的访问控制，在网络应用高度发达的今天是不够的。文件在没有足够保护的情况下，可导致可以下的情况：

(1) 泄露机密资料；

(1) 数据被非法更改。

通过 PKI 技术，采用公开密钥加密体系及加密算法(RSA 1024 位)，即个人数字证书，来对个人电脑中的文件惊醒加密存储和提取。即使硬盘被盗取，个人文件数据也不会被破解读取，为企业和个人的机密文件提供了更好的保护。

7 总结

PKI 是一项非常成功的技术，无论是 Internet 上的电子商务、电子政务应用，还是企业内部的 Web 应用，都越来越离不开 PKI 技术的支持。以 PKI 为基础的企业安全基本架构已经成为企业的网络安全应用的基础设施，将在企业内部的 OA 办公、电子邮件、数据库加密等信息保密方面得到越来越全面的应用。

参考文献

1 史创明,王立新.数字签名及 PKI 技术原理与应用.微计算机信息, 2005,21(8):122－124.

2 冯登国.PKI 技术及其发展现状.计算机安全, 2001,(1):46－51.

3 邓晓军.PKI 技术及其应用.湖南冶金职业技术学院学报, 2004,4(4):40－42,57.

4 张仕斌,何大可,代群. PKI 安全认证体系的研究.计算机应用研究, 2005,(7):127－130.

5 陆垂伟,成俊,郑实. PKI 技术分析及应用.计算机与数字工程, 2006,34 (9):56－58.

6 缑延军,赵恒,王宁宁.PKI 及其在电子邮件系统中的应用.网络与信息安全, 2006,(6):50－51,57.

7 尹晓晖.PKI 技术在应用系统中的应用.信息安全与通信保密,2008,(3):64－65.

8 王伟.PKI 技术及其在企业办公中的应用.海南通信学会学术年会论文集,2005:120－127.

9 代向东,陈性元,杜学绘.基于 PKI 的 VPN 安全管理系统的设计与实现.微计算机信息, 2006,22(9-3):94－96.

10 袁树雄.公钥基础设施与企业网络应用安全方案.重庆科技学院学报, 2005,7(2):91－94.