公钥基础结构及其关键技术
Public Key Infrastructure and Its Key Techniques

宋 玲　吕立坚　赵 明　蒋 华
Song Ling　Lü Lijian　Zhao Ming　Jiang Hua

（广西大学计算机与信息工程学院　南宁　530004）
(College of Comp. & Info. Eng., Guangxi Univ., Nanning, 530004)

摘要　介绍公钥基础结构体系的数据加密和创建数字认证的两大功能，对 PKI 所涉及的信息完整性验证、数字签名技术和信息加密等关键技术进了探讨，表明公钥基础结构安全标准是网络通信安全赖以存在的基础结构。

关键词　公钥基础结构　网络安全　认证权威机构　数字证书
中图法分类号　TP393.08

Abstract　The main functions of the public key infrastructure including management of registration, certificates and secret keys, as well as certificate authority are described. Some critical techniques involving message completeness check, digital signatures and message encryption are discussed.

Key words　public key infrastructure, network security, certificate authority, digital certificate

随着计算机和 Internet 技术的飞速发展，网络技术已应用到社会的各个领域，以惊人的速度改变着人们的工作效率和生活方式。然而，开放性和匿名性也决定了互联网不可避免地存在信息安全隐患。特别是电子商务的出现和蓬勃发展，给网络安全提出了更高的要求，用户身份验证及信息传输的加密处理成为保障网络安全的有效途径。以往使用简单的用户名和口令机制来进行身份验证的方法，以及传统的对称体制的加密处理方法，已不能满足日趋严峻的网络安全的要求。这就促使我们重新考虑网络安全通信平台的构建问题，以提供更加安全可靠的通信安全保障。

基于密码学和认证权威机构 (Certificate Authority 简称 CA) 的公钥基础结构 (Public Key Infrastructure 简称 PKI) 体系的出现，使我们可以利用 CA 颁发的数字证书进行通信双方的身份认证、通信信息加密和解密，以达到加强网络通信安全的目的。PKI 成为保证数据的完整性、真实性、保密性、不可否认性的基石。

1　PKI 体系及其主要功能

PKI 是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名

2001-07-02 收稿。

等密码服务及所必需的密钥和证书管理体系。区别于原有的对称密钥加密技术，PKI 采用非对称的加密算法，即由明文加密成密文的密钥不同于由密文解密为明文的密钥，以避免第三方获取密钥后将密文解密。

一个 PKI 有众多部件组成，PKI 系统的核心如图 1 所示。服务器（即后端）由 CA 数据库、X.500 目录数据库及相应的管理子系统组成，用于管理数字认证、公钥及私钥（分别用于数据加密和解密）。PKI 系统中的客户机是运行 S/MIME、SSL 及 VPN（IP Sec）等的客户，它们在认证过程中需针对每一认证及相关的公钥对 X.500 树型目录进行查询。

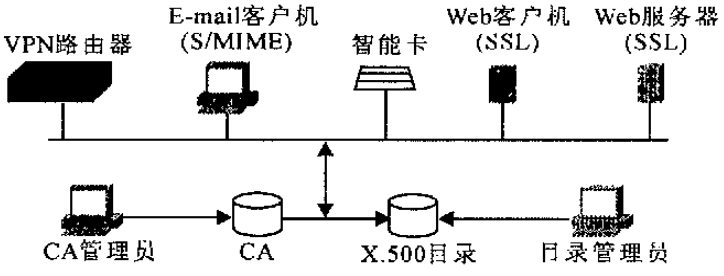

图 1 PKI 系统的核心

PKI 的功能很多，归结为两个，即数据加密和创建数字认证。这两大功能细化为以下的一些主要方面。

1.1 注册管理

注册管理主要完成审查用户的申请资格，决定是否同意 CA 给其签发数字证书。PKI 推荐由一个独立的注册机构（RA）来完成注册管理的任务，这样可以减少整个应用系统的安全风险。RA 接受用户的注册申请，因此，RA 可以设置在直接面对客户的业务部门，如银行的营业部、公司的人力资源部等，并非一定要放在科技部门。

对于一个规模较小的 PKI 应用系统来说，可把注册管理的职能由认证中心 CA 来完成，而不设立独立运行的 RA。

1.2 CA 系统

CA 是 PKI 的核心，是整个 PKI 体系中各方都承认的一个值得信赖的公正的第三方机构。众所周知，构建密码服务系统的核心内容是如何实现密钥管理。目前较好的解决方案是数字证书机制。

数字证书的格式遵循 ITU-T X.509 国际标准，包含以下内容：证书的版本信息、证书唯一的序列号、证书所使用的签名算法、证书的发行机构名称（X.500 格式）、证书的有效期（采用 UTC 时间格式，计时范围为 1950-2049）、证书所有人的名称（X.500 格式）、证书所有人的公开密钥、证书发行者对证书的签名。

数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私钥，用它进行解密和签名；同时设定一把公钥，并由本人公开，为一组用户所共享，用于加密和验证签名。

为合法的申请者签发数字证书，可以说是 CA 甚至是整个 PKI 的核心功能。由于数字证书中存在 CA 对证书的数字签名，因此对证书中任何内容的改动都可以被发现，证书的安全也就有了坚实的保证，它可以公开发布。

用户在接受通信对方的证书时，必须校验对方证书的有效性，包括 CA 的签名是否正确，证书是否被作废处理等。CA 通过维护 1 个证书作废表（CRL）来告知用户有关的证书废除信息。

1.3 证书管理

证书管理包括的内容十分广泛，大致可分为证书的存取、证书链校验，以及交叉认证等

方面。

1.3.1 证书的存取

PKI中使用证书存取库（Repository）来发布和存放所有用户的数字证书和证书作废表等信息，并提供目录服务。轻量目录访问协议（LDAP）被认为是访问证书存储库的最佳方式，它已成为访问PKI目录服务的标准协议。

1.3.2 证书链校验

在PKI体系中，CA是有层次结构的，如图2所示。在信任体系的最高层是根认证中心（Root CA），一般它只有一个，并且自己给自己签发证书。Root CA的下级是策略认证中心（Policy CA），它可以有多个，其证书由根认证中心签发。策略认证中心的下级是用户认证中心（User CA），它负责为最终用户签发数字证书，而它本身的证书则由策略认证中心签发。从证书的层次上看，它们构成了一条证书链。

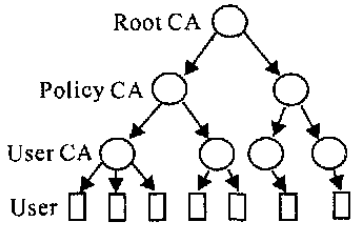

图2 CA的树型结构

1.3.3 交叉认证

利用交叉认证技术可以扩展CA的信任范围，它允许不同信任体系中的认证中心建立起可信任的相互依赖关系，从而使各自签发的证书可以相互认证和校验。交叉认证包括两方面的内容：首先，两个CA建立起信任关系。这就要求双方安全地交换用于校验签名的公开密钥，并利用自己的私有密钥为对方签发数字证书，从而双方都拥有了交叉证书。其次，利用CA的交叉证书校验最终用户的证书。这对用户来说，就是利用本方CA的公钥来校验对方CA的交叉证书，从而决定对方CA是否可信；再利用对方CA的公钥来校验对方用户的证书，从而决定对方用户是否可信。

1.4 密钥管理

在PKI体系中，密钥的生命期主要包括密钥生成、密钥更新、密钥备份和恢复、密钥销毁和归档处理等。

1.4.1 密钥产生

用于加密/解密的密钥对，可以在客户端产生，也可以在一个可信的第三方机构产生。用于签名/校验的密钥对必须在客户端产生。但用于校验签名的公钥可以在网络中传输，还可以随处发布。

1.4.2 密钥备份和恢复

当用户丢失密钥，或存储用户密钥的设备损坏时，可以由可信的第三方机构，可以备份的密钥是用于加密/解密的密钥对，而用于签名/校验的密钥对则不可备份，必须重新产生。

1.4.3 密钥更新

当密钥到期时，PKI应用系统应该可以自动为用户进行密钥更新。当密钥作废时，也需要为用户更新密钥。

1.4.4 密钥归档

当用于加密/解密的密钥对成功更新后，原来使用的密钥对必须进行归档处理，以保证原来的加密信息可以正确地解密。但用于签名/校验的密钥对成功更新后，原来密钥对中用于签名的私钥必须安全地销毁；而原来密钥对中用于校验签名的公开密钥则可以进行归档管理，以便将来对原来的签名信息进行校验。

2 PKI涉及的关键技术

PKI技术中最主要的安全技术包括两个方面：公钥加密技术、数字签名技术。公钥加密技术可以提供信息的保密性和访问控制的有效手段，它保证了利用公钥加密后的数据。而数字签名技术则为我们提供了在网络通信之前相互认证的有效方法、在通信过程中保证信息完整性的可靠手段、以及在通信结束之后防止双方相互抵赖的有效机制。

2.1 信息完整性验证

常用的信息完整性验证方法有两种：一种是采用信息认证码（Message Authentication Code）简记为MAC；另一种是窜改检测码（Message Detection Code），简记为MDC。

MAC利用Hash函数和密钥k将要发送的明文x或密文y变换成r位消息认证码Hash(k, x)或称为认证符附加在x或y之后送出，以$x+As$或$y+As$表示，其中"+"符号表示序列的链接。Hash函数又称为单向散列函数（one-way hash function），其作用是对整个消息进行变换，产生一个长度固定但较短的数据序列，这一过程可看作是一种压缩编码(compressed encoding)。MDC利用一个函数将要发送的明文数据变换成r位的窜改检测码Ds附加在明文之后，再一起加密实现保密认证。

接受者收到发送的信息序列后，按照发送端同样的方法对接收的数据或解密后的数据的前面部分进行计算，得到相应的r位数字Ar或Dr，而后与接收恢复后的As'或Ds'逐位进行比较，若全部相同，就可认为收到的信息是合法的，否则检出消息有错或被窜改过。当主动攻击者在不知道密钥的情况下，随机选择r位碰运气，其成功伪造消息的概率为2^{-r}。

2.2 数字签名技术

基于用户私钥的专有性，数字签名可以实现对数据发送者的身份进行确认。数字签名的方式有两种：一种是经过密码变换的被签信息整体，另一种是附加在被签名信息之后或某一特定位置上的一段签名序列。常见的数字签名机制有非对称密钥体制的数字签名和对称密钥体制的数字签名，前者比后者可提供更可靠的安全保证。

2.3 信息加密

加密一般可分为对称式加密体制和非对称式加密体制两种。对称式加密由于它的简便性，所以应用较为广泛，但是很容易造成安全漏洞，因为对称式加密体制使用同一个密钥进行加密和解密处理，一旦密钥被非法获得后，信息就有可能造成泄露。为了解决这种问题，在PKI体系中使用了非对称式加密体制的加密方式，即在使用证书的情况下，发送者使用接收方的公钥对需要传输的信息进行加密处理，接收方则利用其私有的密钥进行解密以将密文恢复成可识别的明文信息。而在未使用证书的情况下，利用Diffie—Hellman算法对信息进行加密处理[4]。

3 PKI的应用展望

国际电信联盟ITU X.509协议，是PKI技术体系中应用最为广泛、也是最为基础的一个国际标准。它的主要目的在于定义一个规范的数字证书的格式，以便为基于X.500协议的目录服务提供一种较强的认证手段。目前世界上已经出现了许多依赖于PKI的安全标准，如安全电子交易协议（SET）、安全套接层协议（SSL）、传输层安全协议（TLS）、安全多用途互

（下转第240页）

3 结语

综上所述，IP SEC 作为新一代的计算机网络安全协议，在协议这个层次上对 TCP/IP 协议进行了较为完善的补充，并且还可以为下一代的 IP V6 所采用。由于协议的开放性，在具体开发时，用户可以方便地嵌入特定的加密算法，具有很强的灵活性。特别是作为协议核心的 SA，较好地解决了协议层安全结构的构成问题。

参考文献

1 William R, Cheswick, Steven M. Firewalls and Internet Security: Repelling the Wily Hacker, 1994.
2 Security Architecture for the Internet Protocol (RFC 2401).
3 Martin W, Murhammer et al.. A guide to Virtual Private Network, 1998.
4 Steven Brown. Implementing Virtual private Networks, 2000.
5 胡昌振，李贵涛等. 面向 21 世纪网络安全与防护. 北京：希望电子出版社，1999. 10.

（责任编辑：黎贞崇）

（上接第 236 页）

连网邮件扩展协议（S/MIME）、用于开发新一代的 VPN 的 IP 安全协议（IP SEC）等。

PKI 标准也在进一步完善，X.509 的数字认证结构一直处于不断的演变之中，其新版本不断增加新的功能。如 X.509 第 2 版添加了发布者和受检者标识功能；第 3 版增加了一个认证授权方式字段——类型/临界状态/值，可记录密钥、加密策略、用户和 CA 属性以及认证路径约束等信息。一些软件（如 Windows 2000）中已良好地集成了 PKI 组件，可实现证书的申请、颁发、管理等操作，构建 PKI 平台。

随着电子商务、企业虚拟专用网络（VPN）等的蓬勃发展，保障网络通信的安全迫在眉睫。PKI 对数据加密、数据签名、反否认、数据完整性及甄别所需的密钥和认证实施了统一的集中化管理，它必将得到广泛推广和采用，成为所有安全应用赖以存在的基础结构。

参考文献

1 颜逸品. Windows 2000 Server 企业网络建构实务. 北京：中国铁道出版社，2001.
2 ITU-T, Recommendation X.509. The Directory: Authentication Framework, 1997.
3 Merike Kaeo. 网络安全性设计. 潇湘工作室译. 北京：人民邮电出版社，2000.
4 张 琳等. 网络组建、管理与安全. 北京：人民邮电出版社，2000.

（责任编辑：黎贞崇）