浅谈 PKI 网格安全技术及应用

作者：浙江财经学院　陈迪锋

［摘要］伴随着网格计算研究的深入，依据网格计算原理构建的网格状网络也已经作为新一代的网络连接关键技术之一，逐步代替了旧有的网络连接方式。怎样保障网格状网络的安全通信。这就需要提供诸如机密性、认证、完整性这些基本的安全服务。

［关键词］PKI；　数字证书；　CA 中心

人类社会对信息网络的依赖程度越来越大，伴随着网格计算研究的深入，依据网格计算原理构建的网格状网络也已经作为新一代的网络连接关键技术之一，逐步代替了旧有的网络连接方式，那么随之而来的问题便是，怎样保障网格状网络的安全通信.这就需要提供诸如机密性、认证、完整性这些基本的安全服务。本文研究的正是基于当前最流行的安全基础设施(PKI)技术来保障网格安全的方法。

一、PKI 概述

公开密钥基础设施(PKI)是一个用非对称密码算法原理和技术实现并提供安全服务的具有通用性的安全基础设施。PKI 是一种遵循标准的利用公钥加密技术为电子商务、电子政务的开展提供一整套安全的基础设施。它是保障大型开放式网络环境下网络和信息安全的最可行、最有效的措施。它基于保密性应用要求，有一个真正可靠、稳定、高性能、安全、互操作性强、完全支持交叉认证的系统。PKI 的本质就是实现了大规模网络中的公钥分发问题，建立了大规模网络中的信任基础。概括地说，PKI 是创建、管理、存储、分发和撤消基于公钥加密的公钥证书所需要的一套硬件、软件、策略和过程的集合。

PKI 的概念是近几年才提出来的，尽管在概念提出之前许多公司并没有直接销售 PKI 终极解决产品，但是 PKI 的技术早已经被用于他们的产品当中，例如 Lotus Notes 从 1989 年就开始用 PKI 对用户进行认证，PGP 从 1991 年就开始对用户进行认证。目前，PKI 基础理论研究已经比较完备，各个厂商已将他们的产品广泛地应用于需要数字证书的认证中。目前，国际上能够开发 PKI 产品的公司有很多。美国、欧洲各国以及韩国、日本是世界上较早涉足信息安全技术及产业的国家，他们大多数对 PKI 及其相关技术、产业用法律予以固化。

1、PKI 组成

PKI 是一种新的安全技术，它由公开密钥密码技术、数字证书、证书发放机构(CA)和关于公开密钥的安全策略等基本成分共同组成的，包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等基础技术。从某种意义上讲，PKI 包含了安全认证系统，即安全认证系统 CA 系统是 PKI 不可缺的组成部分。PKI 公钥基础设施是提供公钥加密和数字签名服务的系统或平台，目的是为了管理密钥和证书。一个机构通过采用 PKI 框架管理密钥和证书可以建立一个安全的网络环境。一个典型、完整、有效的 PKI 应用系统至少应具有以下部分:（1）X.509 格式的证书(X.509v3)和证书废止列表 CRL(X509v2)；(2)公钥密码证书管理；(3)黑名单的发布和管理；(4)密钥的备份和恢复；(5)自动更新密钥；(6)自动管理历史密钥；(7)支持交叉认证。

2、PKI 相关标准

不同厂商的 PKI 实现可能是不同的，但是在网上进行交易活动中建立信任的关键是保证不同厂商的 PKI 环境的互操作性，因而这就对 PKI 提出了互操作性要求。要保证 PKI 的互操作性，PKI 必须建立在标准之上。与 PKI 有关的标准和建议有很多，几乎都是围绕着 x.509 证书标准定义 PKI 体系的。

PKI 是一个庞大复杂的理论体系，它以公钥理论为基础，并在 X.509 标准的基础上建立起来的，它的发展是一个长期的过程。公开密钥加密的概念最早是由两位美国科学家 Difie 和 Hellman 于 1976 年提出的，1978 年，MIT 的一个研究小组中的 Riveat，Shamir，Adleman 三人提出了一个实用的公开密钥加密算法 RSA。此后 RSA 算法得到了广泛的接受和实现，并经受了多年的考验而被证明是安全可靠的，成为公开密钥算法的事实上的工业标准。之后虽然有一些新的算法被陆续提出，但都还有待时间的考验。X.509 标准是最基本、获得最广泛支持的 PKI 的标准之一，它的最主要目的是定义一个标准的数字证书格式，被用于规范认证服务，以实施 X.500 目录服务。PKI 的一系列相关标准是以 X.509v3 为基础的。可互操作的 PKI 标准(PKIX)是由 Internet 工程任务组中(IETF)的 PKI 作组制订的一系列 RFC 文档组成，称为 PKIX 规范 。

二、CA 简介

在 Internet 上的电子商务，要求为信息安全提供有效的、可靠的保护机制。这些机制必须提供机密性、身份验证特性(使交易的每一方都可以确认其它各方的身份)、不可否认性(交易的各方不可否认它们的参与)。这就需要依靠一个可靠的第三方机构验证，而认证中心 CA 专门提供这种服务。证书机制是目前被广泛采用的一种安全机制。使用证书机制的前提是建立 CA 以及配套的 RA 系统。

CA 中心，又称为数字证书认证中心，作为电子商务交易中受信任的第三方，专门解决公钥体系中公钥的合法性问题。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名称与证书中列出的公开密钥相对应。以 CA 中心的数字签名使得攻击者不能伪造和篡改数字证书。在数字证书认证的过程中，以作为权威的、公正的、可信赖的第三方，其作用是至关重要的。认证中心就是一个负责发放和管理数字证书的权威机构。同样 CA 允许管理员撤销发放的数字证书，在证书撤销列表(CRL)中添加新项并周期性地发布这一数字签名的 CRL。数字证书认证中心机构的建立对电子商务等网上交易具有很重要的意义。CA 涉及电子交易中各方的身份信息、严格的加密技术和认证程序。基于其牢固的安全机制，CA 应用可扩大到一切有安全要求的网上数据传输服务。

1、CA 的组成

CA 为实现其功能，主要由如下部分组成:(1)注册服务器。通过 Webserver 建立的站点，可为客户提供每日 24 小时的服务。因此客户可在自己方便的时候在网上提出证书申请和填写相应的证书申请表，免去了排队等候的麻烦。(2) 证书申请受理和审核机构。它的主要功能是负责接受客户证书的申请并进行审核 。(3)认证中心服务器。它是数字证书生成、发放的运行实体，同时提供发放证书的管理、证书撤销列表(CRL)的生成和处理等服务。

2、CA 的功能

概括而言，CA 的功能主要有:(1)证书发放；(2)证书更新；(3)证书撤销；(4)证书验证。

CA 的核心功能就是发放和管理数字证书，具体描述如下:(1)接收验证最终用户数字证书的申请；(2)确定是否接受最终用户数字证书的申请，即证书的审批；(3)向申请者颁发、拒绝颁发数字证书，即证书的发放；(4)接收、处理最终用户的数字证书更新请求，即证书的更新；(5)接收最终用户数字证书的查询、撤销；(6) 产生和发布证书废止列表；(7)数字证书的归档；(8)密钥归档；(9)历史数据归档。

三、数字证书

数字证书是各类实体(持卡人/个人、商户/企业、网关/银行等)在网上进行信息交流及商务活动的身份证明。在电子交易的各个环节，交易的各方都需验证对方证书的有效性，从而解决相互间的信任问题。数字证书是一个经证书认证中心 CA 数字签名的包含公开密钥拥有者信息以及公开密钥的文件。数字证书的格式及内容遵循 x.509 标准。

1、数字证书分类

数字证书按性质可分为签名证书和加密证书两类:(1) 签名证书，主要用于对用户信息进行签名，以保证信息的不可否认性。(2)加密证书，主要用于对用户传送信息进行加密，以保证信息的真实性和完整性 。按用途可分为个人证书和服务器证书两类: 第　　一、个人证书:用户使用个人证书不仅可以访问安全的 Web 站点，而且能够收发安全电子邮件。数字证书中的加密特性可以阻止没有被授权的用户浏览邮件内容， 同时可以保证邮件的收发双方无法否认自己曾经发送或接收过电子邮件。第二、服务器证书:服务器证书用于服务器身份识别，使得连接到服务器的用户确定服务器的真实身份。Web 服务器与客户通过 SSL 的方式建立安全信道，对传输的数据进行加密和解密。服务器证书向用户提供真实身份的第三方证明。

假设持证人 A 向持证人 B 传送数字信息，为了保证信息传送的真实性、完整性和不可否认性，需要对要传送的信息进行数字加密和数字签名，其传送过程如下:(1)A 准备好要传送的数字信息，并对其进行 Hash 运算，得到一个消息摘要。(2) A 用自己的私有密钥 KR 对消息摘要进行加密得到 A 的数字签名，并将其附在数字信息上。(3) A 随机产生一个加密密钥(DES 密钥)，并用此密钥对要发送的信息进行加密，形成密文。(4) A 用 B 的公开密钥 KU 对刚才随机产生的加密密钥进行加密，将加密后的 DES 密钥连同密文一起传送给 B。(5) B 收到 A 传送过来的密文和加过密的 DES 密钥，先用自己的私有密钥 KR 对加密的 DES 密钥进行解密，得到 DES 密钥。然后用 DES 密钥对收到的密文进行解密，得到明文的数字信息。(6)B 用 A 的公开密钥 KU 对 A 的数字签名进行解密，得到消息摘要。并用相同的 Hash 算法对收到的明文再进行一次 Hash 运算，得到一个新的消息摘要。B 将收到的消息摘要和新产生的消息摘要进行比较，如果一致，说明收到的信息没有被修改过。

2、数字证书内容及格式

数字证书是一个经认证中心数字签名的包含数字证书拥有者信息和其公开密钥的文件。最简单的证书包含持有者的公开密钥、用户名称以及认证中心的数字签名。一般情况下证书还包括密钥的有效时间，发证机关的名称，该证书的序列号等信息，证书的格式遵循 ITUX.509 国际标准。

数字证书必须包含的信息如下:(1)证书版本号:版本号指明 X.509 证书的格式版本。目前已有版本三种。(2)证书序列号:序列号指定由 CA 分配给每一个证书的唯一的数字型标识符，当证书被取消时，实际是将此证书的序列号放入由 CA 签发的 CRL 中。(3)签名算法标识符，签名算法标识符用来指定由 CA 签发证书时所使用的签名算法 。算法标识符用来指定 CA 签发证书时所使用的公开密钥算法和 Hash 算法 。算法标识符须向国际知名组织注册。(4)签发机构名:此域用来标识签发证书的 CA 的 X.50 名字。包括国家、省市、地区、组织机构、单位部门和通用名。(5)有效期:指定证书的有效期，包括证书开始生效的日期和时间以及失效的日期和时间。证书在所指定的这两个时间之内有效。(6)证书用户名:指定证书持有者的 x.500 唯一名字。包括国家、省市、地区、组织 机构、单位部门和通用名，还包含 E-mail 地址等个人信息。(7)签名值:证书签发机构对证书上述内容的签名值。以确保这个证书在发放之后没有被篡改过。

[参考文献]

[1]谢冬青. 《PKI 原理与技术》.北京:清华大学出版社，2004.2
[2]严蔚敏，吴伟民.《数据结构》(C 语言版). 北京:清化大学出版社，1996.2
[3]卿思汉.《公钥基础设施(PKI)实现和管理电子安全》.北京:清华大学出版社，2002
[4l 王鸿谷.《经典密码学与现代密码学》第一版.北京:清华大学出版社，2005
[5]洪琳，李展. 《数字签名数字信封和数字证书》.计算机应用，2000