

公钥基础设施 PKI 简介

中科院计算机网络信息中心 在读研究生 孔宁

摘要：本文简介了当前广泛用于解决电子商务中安全问题的 PKI 技术。PKI(Public Key Infrastructure)是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。PKI 的核心组成部分 CA(Certification Authority)，即认证中心，它是数字证书的签发机构。数字证书，有时被称为数字身份证，是一个符合一定格式的电子文件，用来识别电子证书持有者的真实身份。

关键词：公钥基础设施 PKI 认证中心 CA 数字证书

一 PKI 简介

随着 Internet 的普及，人们通过因特网进行沟通越来越多，相应的通过网络进行商务活动即电子商务也得到了广泛的发展。电子商务为我国企业开拓国际国内市场、利用好国内外各种资源提供了一个千载难逢的良机。电子商务对企业来说真正体现了平等、竞争、高效率、低成本、高质量的优势，能让企业在激烈的市场竞争中把握商机、脱颖而出。发达国家已经把电子商务作为 21 世纪国家经济的增长重点，我国的有关部门也正在大力推进我国企业发展电子商务。然而随着电子商务的飞速发展也相应的引发出一些 Internet 安全问题。概括起来，进行电子交易的互联网用户所面临的安全问题有：一，保密性：如何保证电子商务中涉及的大量保密信息在公开网络的传输过程中不被窃取；二，完整性：如何保证电子商务中所传输的交易信息不被中途篡改及通过重复发送进行虚假交易；三，身份认证与授权：在电子商务的交易过程中，如何对双方进行认证，以保证交易双方身份的正确性；四，抗抵赖：在电子商务的交易完成后，如何保证交易的任何一方无法否认已发生的交易。这些安全问题将在很大程度上限制电子商务的进一步发展，因此如何保证 Internet 网上信息传输的安全，已成为发展电子商务的重要环节。

为解决这些 Internet 的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被广泛采用的 PKI 技术(Public Key Infrastructure-公钥基础设施)，PKI (公钥基础设施) 技术采用证书管理公钥，通过第三方的可信任机构--认证中心 CA(Certificate Authority)，把用户的公钥和用户的其他标识信息（如名称、e-mail、身份证号等）捆绑在一起，在 Internet 网上验证用户的身份。目前，通用的办法是采用基于 PKI 结构结合数字证书，通过把要传输的数字信息进行加密，保证信息传输的保密性、完整性，签名保证身份的真实性和抗抵赖。

二 PKI 的基本定义与组成

PKI 的基本定义十分简单，所谓 PKI 就是一个用公钥概念和技术实施和提供安全服务的具有普适性的安全基础设施。

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。PKI 是利用公钥技术实现电子商务安全的一种体系，是一种基础设施，网络通讯、网上交易是利用它来保证安全的。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 (Public Key Infrastructure) 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。PKI 主要包括四个部分：X.509 格式的证书（X.509 V3）和证书废止列表 CRL（X.509 V2）；CA 操作协议；CA 管理协议；CA 政策制定。一个典型、完整、有效的 PKI 应用系统至少应具有以下五个部分；

- 1) **认证中心 CA** CA 是 PKI 的核心，CA 负责管理 PKI 结构下的所有用户（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，CA 还要负责用户证书的黑名单登记和黑名单发布，后面有 CA 的详细描述。
- 2) **X.500 目录服务器** X.500 目录服务器用于发布用户的证书和黑名单信息，用户可通过标准的 LDAP 协议查询自己或其他人的证书和下载黑名单信息。
- 3) **具有高强度密码算法(SSL)的安全 WWW 服务器** Secure socket layer(SSL)协议最初由 Netscape 企业发展，现已成为网络用来鉴别网站和网页浏览者身份，以及在浏览器使用者及网页服务器之间进行加密通讯的全球化标准。
- 4) **Web（安全通信平台）** Web 有 Web Client 端和 Web Server 端两部分，分别安装在客户端和服务端，通过具有高强度密码算法的 SSL 协议保证客户端和服务端数据的机密性、完整性、身份验证。
- 5) **自开发安全应用系统** 自开发安全应用系统是指各行业自开发的各种具体应用系统，例如银行、证券的应用系统等。

完整的 PKI 包括认证政策的制定（包括遵循的技术标准、各 CA 之间的上下级或同级关系、安全策略、安全程度、服务对象、管理原则和框架等）、认证规则、运作制度的制定、所涉及的各方法律关系内容以及技术的实现等。

三 PKI 的原理

公钥基础设施 PKI 的原理，顾名思义 PKI 是基于公钥密码技术的。要想深刻理解 PKI 的原理，就一定要对 PKI 涉及到的密码学知识有比较透彻的理解。下面简单介绍一下密码学知识。对于普通的对称密码学，加密运算与解密运算使用同样的密钥。通常，使用的加密算法比较简便高效，密钥简短，破译极其困难，由于系统的保密性主要取决于密钥的安全性，所以，在公开的计算机网络上安全地传送和保管密钥是一个严峻的问题。正是由于对称密码学中双方都使用相同的密钥，因此无法实现数据签名和不可否认性等功能。而与此不同的非对称密码学，具有两个密钥，一个是公钥一个是私钥，它们具有这种性质：用公

钥加密的文件只能用私钥解密，而私钥加密的文件只能用公钥解密。公钥顾名思义是公开的，所有的人都可以得到它；私钥也顾名思义是私有的，不应被其他人得到，具有唯一性。这样就可以满足电子商务中需要的一些安全要求。比如说要证明某个文件是特定人的，该人就可以用他的私钥对文件加密，别人如果能用他的公钥解密此文件，说明此文件就是这个人的，这就可以说是一种认证的实现。还有如果只想让某个人看到一个文件，就可以用此人的公钥加密文件然后传给他，这时只有他自己可以用私钥解密，这可以说是保密性的实现。基于这种原理还可以实现完整性。这就是 PKI 所依赖的核心思想，这部分对于深刻把握 PKI 是很重要的，而恰恰这部分是最有意思的。

比如在现实生活中，我们想给某个人在网上传送一个机密文件，该文件我们只想让那个人看到，我们设想了很多方法，首先我们想到了用对称密码将文件加密，而在我们把加密后的文件传给他后，我们又必须得让他知道解密用的密钥，这样就又出现了一个新的问题，就是我们如何保密的传输该密钥，此时我们发现传输对称密钥也不可靠。后来我们可以改用非对称密码的技术加密，此时发现问题逐渐解决了。然而又有了一个新的问题产生，那就是如何才能确定这个公钥就是某人的，假如我们得到了一个虚假的公钥，比如说我们想传给 A 一个文件，于是开始查找 A 的公钥，但是这时 B 从中捣乱，他把自己的公钥替换了 A 的公钥，让我们错误的认为 B 的公钥就是 A 的公钥，导致我们最终使用 B 的公钥加密文件，结果 A 无法打开文件，而 B 可以打开文件，这样 B 实现了对保密信息的窃取行为。因此就算是采用非对称密码技术，我们仍旧无法保证保密性的实现，那我们如何才能确切的得到我们想要的人的公钥呢？这时我们很自然的想到需要一个仲裁机构，或者说是一个权威的机构，它能为我准确无误的提供我们需要的人的公钥，这就是 CA。

这实际上也是应用公钥技术的关键，即如何确认某个人真正拥有公钥（及对应的私钥）。在 PKI 中，为了确保用户的身份及他所持有密钥的正确匹配，公开密钥系统需要一个值得信赖而且独立的第三方机构充当认证中心（Certification Authority, CA），来确认公钥拥有人的真正身份。就象公安局发放的身份证一样，认证中心发放一个叫“数字证书”的身份证明。这个数字证书包含了用户身份的部分信息及用户所持有的公钥。象公安局对身份证盖章一样，认证中心利用本身的私钥为数字证书加上数字签名。任何想发放自己公钥的用户，可以去认证中心申请自己的证书。认证中心在鉴定该人的真实身份后，颁发包含用户公钥的数字证书。其他用户只要能验证证书是真实的，并且信任颁发证书的认证中心，就可以确认用户的公钥。认证中心是公钥基础设施的核心，有了大家信任的认证中心，用户才能放心方便的使用公钥技术带来的安全服务。

四 PKI 的核心部分 CA

认证中心 CA 作为 PKI 的核心部分，CA 实现了 PKI 中一些很重要的功能，概括地说，认证中心（CA）的功能有：证书发放、证书更新、证书撤销和证书验证。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-证书的审批。
- (3) 向申请者颁发、拒绝颁发数字证书-证书的发放。
- (4) 接收、处理最终用户的数字证书更新请求-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（CRL）。
- (7) 数字证书的归档。

(8) 密钥归档。

(9) 历史数据归档。

认证中心 CA 为了实现其功能，主要由以下三部分组成：

注册服务器：通过 Web Server 建立的站点，可为客户提供 24 × 7 不间断的服务。客户在网上提出证书申请和填写相应的证书申请表。

证书申请受理和审核机构：负责证书的申请和审核。它的主要功能是接受客户证书申请并进行审核。

认证中心服务器：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、证书废止列表 (CRL) 的生成和处理等服务。

在具体实施时，CA 的必须做到以下几点：

- 1) 验证并标识证书申请者的身份。
- 2) 确保 CA 用于签名证书的非对称密钥的质量。
- 3) 确保整个签证过程的安全性，确保签名私钥的安全性。
- 4) 证书资料信息 (包括公钥证书序列号，CA 标识等) 的管理。
- 5) 确定并检查证书的有效期限。
- 6) 确保证书主体标识的唯一性，防止重名。
- 7) 发布并维护作废证书列表。
- 8) 对整个证书签发过程做日志记录。
- 9) 向申请人发出通知。

在这其中最重要的是 CA 自己的一对密钥的管理，它必须确保其高度的机密性，防止他方伪造证书。CA 的公钥在网上公开，因此整个网络系统必须保证完整性。CA 的数字签名保证了证书(实质是持有者的公钥)的合法性和权威性。用户的公钥有两种产生的方式：(1) 用户自己生成密钥对，然后将公钥以安全的方式传送给 CA，该过程必须保证用户公钥的验证性和完整性。(2) CA 替用户生成密钥对，然后将其以安全的方式传送给用户，该过程必须确保密钥对的机密性，完整性和可验证性。该方式下由于用户的私钥为 CA 所产生，所以对 CA 的可信性有更高的要求。CA 必须在事后销毁用户的私钥。

一般而言公钥有两大类用途，就像本文前面所述，一个是用于验证数字签名，一个是用于加密信息。相应的在 CA 系统中也需要配置用于数字签名/验证签名的密钥对和用于数据加密/脱密的密钥对，分别称为签名密钥对和加密密钥对。由于两种密钥对的功能不同，管理起来也不大相同，所以在 CA 中为一个用户配置两对密钥，两张证书。

CA 中比较重要的几个概念点有：证书库。证书库是 CA 颁发证书和撤销证书的集中存放地，它像网上的“白页”一样，是网上的一种公共信息库，供广大公众进行开放式查询。这是非常关键的一点，因为我们构建 CA 的最根本目的就是获得他人的公钥。目前通常的做法是将证书和证书撤销信息发布到一个数据库中，成为目录服务器，它采用 LDAP 目录访问协议，其标准格式采用 X.500 系列。随着该数据库的增大，可以采用分布式存放，即采用数据库镜像技术，将其中一部分与本组织有关的证书和证书撤销列表存放本地，以提高证书的查询效率。这一点是任何一个大规模的 PKI 系统成功实施的基本需求，也是创建一个有效的认证机构 CA 的关键技术之一。

另一个重要的概念是证书的撤销。由于现实生活中的一些原因，比如说私钥的泄漏，当事人的失踪死亡等情况的发生，应当对其证书进行撤销。这种撤销应该是及时的，因为如果撤销延迟的话，会使得不再有效的证书仍被使用，将造成一定的损失。在 CA 中，证书的撤销使用的手段是证书撤销列表或称为 CRL。即将作废的证书放入 CRL 中，并及时的公布于众，根据实际情况不同可以采取周期性发布机制和在线查询机制两种方式。

密钥的备份和恢复也是很重要的一个环节。如果用户由于某种原因丢失了解密数据的

密钥，那么被加密的密文将无法解开，这将造成数据丢失。为了避免这种情况的发生，PKI 提供了密钥备份于解密密钥的恢复机制。这一工作也是应该由可信的机构 CA 来完成的，而且，密钥的备份与恢复只能针对解密密钥，而签名密钥不能做备份，因为签名密钥用于不可否认性的证明的，如果存有备份的话，将会不利于保证不可否认性。

还有，一个证书的有效期是有限的，这样规定既有理论上的原因，又有实际操作的因素。在理论上诸如关于当前非对称算法和密钥长度的可破译性分析，同时在实际应用中，证明密钥必须有一定的更换频度，才能得到密钥使用的安全性。因此一个已颁发的证书需要有过期的措施，以便更换新的证书。为了解决密钥更新的复杂性和人工干预的麻烦，应由 PKI 本身自动完成密钥或证书的更新，完全不需要用户的干预。它的指导思想是：无论用户的证书用于何种目的，在认证时，都会在线自动检查有效期，当失效日期到来之前的某时间间隔内，自动启动更新程序，生成一个新的证书来替代旧证书。

结束语

个人感觉 PKI/CA 技术很有发展前途，只是在我国的应用才刚刚起步。另外 CA 作为电子商务的特殊实体，它必须具有权威性，这种权威性来自政府或公共组织的授予；它必须使公众所依赖的机构，它颁发的证书可信；它必须是公正的，不参与交易双方的。本文仅是停留在比较简单的理论介绍，希望此文能让更多人了解 PKI，投入到 PKI 的研究中来。

参考书目：

- [1] 《公钥基础设施(PKI)实现和管理电子安全》 [美] Andrew Nash 等著 清华大学出版社
- [2] 《公钥基础设施 PKI 与认证机构 CA》 关振胜 著 电子工业出版社出版