PKI/CA 体系简介

为解决 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 ,通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

一、单钥密码算法（加密）

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，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 网上实现密钥的自动管理，保证网上数据的安全传输。

从广义上讲 ,所有提供公钥加密和数字签名服务的系统 ,都可叫做 PKI 系统，PKI 的主要目的是通过自动管理密钥和证书，可以为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便的使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性 ,数据的机密性是指数据在传输过程中，不能被非授权者偷看；数据的完整性是指数据在传输过程中不能被非法篡改；数据的有效性是指数据不能被否认。一个有效的 PKI 系统必须是安全的和透明的，

用户在获得加密和数字签名服务时 ,不需要详细地了解 PKI 是怎样管理证书和密钥的，一个典型、完整、有效的 PKI 应用系统至少应具有以下部分：

- 公钥密码证书管理。
- 黑名单的发布和管理。
- 密钥的备份和恢复。
- 自动更新密钥。
- 自动管理历史密钥。
- 支持交叉认证。

由于 PKI 基础设施是目前比较成熟、完善的 Internet 网络安全解决方案，国外的一些大的网络安全公司纷纷推出一系列的基于 PKI 的网络安全产品 ,如美国的 Verisign, IBM ,加拿大的 Entrust、SUN 等安全产品供应商为用户提供了一系列的客户端和服务器端的安全产品，为电子商务的发展以及政府办公网、EDI 等提供了安全保证。简言之，PKI(Public Key Infrastructure)公钥基础设施就是提供公钥加密和数字签名服务的系统，目的是为了管理密钥和证书，保证网上数字信息传输的机密性、真实性、完整性和不可否认性。

1．单钥密码算法（加密）

单钥密码算法，又称对称密码算法：是指加密密钥和解密密钥为同一密钥的密码算法。因此，信息的发送者和信息的接收者在进行信息的传输与处理时，必须共同持有该密码（称为对称密码）。在对称密钥密码算法中,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。最典型的是 DES（Data Encryption Standard)算法。

DES（Data Encryption Standard，数据加密标准）算法，它是一个分组加密算法，它以 64 bit 位（8 byte）为分组对数据加密，其中有 8 bit 奇偶校验，有效密钥长度为 56 bit。64 位一组的明文从算法的一端输入，64 位的密文从另一端输出。DES 是一个对称算法，加密和解密用的是同一算法。DES 的安全性依赖于所用的密钥。

密钥的长度为 56 位。（密钥通常表示为 64 位的数，但每个第 8 位都用作奇偶校验，可以忽略。）密钥可以是任意的 56 位的数，且可以在任意的时候改变。其中极少量的数被认为是弱密钥，但能容易地避开它们。所有的保密性依赖于密钥。简单地说，算法只不过是加密的两个基本技术--混乱和扩散的组合。DES 基本组建分组是这些技术的一个组合（先代替后置换），它基于密钥作用于明文，这是众所周知的轮（round）。DES 有 16 轮，这意味着要在明文分组上 16 次实施相同的组合技术。此算法只使用了标准的算术和逻辑运算，而其作用的数也最多只有 64 位。

DES 对 64 位的明文分组进行操作，通过一个初始置换，将明文分组分成左半部分和右半部分，各 32 位长。然后进行 16 轮完全相同的运算，这些运算被称为函数 f，在运算过程中数据与密钥结合。经过 16 轮后，左、右半部分合在一起经过一个末置换（初始置换的逆置换），这样该算法就完成了。在每一轮中，密钥位移位，然后再从密钥的 56 位中选出 48 位。通过一个扩展置换将数据的右半部分扩展成 48 位，并通过一个异或操作与 48 位密钥结合，通过 8 个 s 盒

将这 48 位替代成新的 32 位数据，再将其置换一次。这四步运算构成了函数 f。然后，通过另一个异或运算，函数 f 输出与左半部分结合，其结果即成为新的右半部分，原来的右半部分成为新的左半部分。将该操作重复 16 次，便实现了 DES 的 16 轮运算。

2．双钥密码算法（加密、签名）

双钥密码算法，又称公钥密码算法：是指加密密钥和解密密钥为两个不同密钥的密码算法。公钥密码算法不同于单钥密码算法，它使用了一对密钥：一个用于加密信息，另一个则用于解密信息，通信双方无需事先交换密钥就可进行保密通信。其中加密密钥不同于解密密钥,加密密钥公之于众,谁都可以用；解密密钥只有解密人自己知道。这两个密钥之间存在着相互依存关系：即用其中任一个密钥加密的信息只能用另一个密钥进行解密。若以公钥作为加密密钥，以用户专用密钥(私钥)作为解密密钥，则可实现多个用户加密的信息只能由一个用户解读；反之，以用户私钥作为加密密钥而以公钥作为解密密钥，则可实现由一个用户加密的信息而多个用户解读。前者可用于数字加密，后者可用于数字签名。

在通过网络传输信息时，公钥密码算法体现出了单密钥加密算法不可替代的优越性。对于参加电子交易的商户来说，希望通过公开网络与成千上万的客户进行交易。若使用对称密码，则每个客户都需要由商户直接分配一个密码，并且密码的传输必须通过一个单独的安全通道。相反，在公钥密码算法中，同一个商户只需自己产生一对密钥，并且将公开钥对外公开。客户只需用商户的公开钥加密信息，就可以保证将信息安全地传送给商户。

公钥密码算法中的密钥依据性质划分，可分为公钥和私钥两种。用户产生一

对密钥，将其中的一个向外界公开，称为公钥；另一个则自己保留，称为私钥。凡是获悉用户公钥的任何人若想向用户传送信息，只需用用户的公钥对信息加密，将信息密文传送给用户便可。因为公钥与私钥之间存在的依存关系，在用户安全保存私钥的前提下，只有用户本身才能解密该信息，任何未受用户授权的人包括信息的发送者都无法将此信息解密。

RSA 公钥密码算法是一种公认十分安全的公钥密码算法。它的命名取自三个创始人：Rivest、Shamir 和 Adelman。RSA 公钥密码算法是目前网络上进行保密通信和数字签名的最有效的安全算法。RSA 算法的安全性基于数论中大素数分解的困难性，所以，RSA 需采用足够大的整数。因子分解越困难，密码就越难以破译，加密强度就越高。

RSA 既能用于加密又能用于数字签名，在已提出的公开密钥算法中，RSA 最容易理解和实现的，这个算法也是最流行的。RSA 的安全基于大素数分解的难度。其公开密钥和私人密钥是一对大素数（100 到 200 个十进制数或更大）的函数。从一个公开密钥和密文中恢复出明文的难度等价于分解两个大素数之积。

3．公开密钥数字签名算法（签名）

DSA（Digital Signature Algorithm，数字签名算法，用作数字签名标准的一部分），它是另一种公开密钥算法，它不能用作加密，只用作数字签名。DSA 使用公开密钥，为接受者验证数据的完整性和数据发送者的身份。它也可用于由第三方去确定签名和所签数据的真实性。DSA 算法的安全性基于解离散

对数的困难性，这类签字标准具有较大的兼容性和适用性，成为网络安全体系的基本构件之一。

4．数字签名与数字信封

公钥密码体制在实际应用中包含数字签名和数字信封两种方式。

数字签名是指用户用自己的私钥对原始数据的哈希摘要进行加密所得的数据。信息接收者使用信息发送者的公钥对附在原始信息后的数字签名进行解密后获得哈希摘要，并通过与自己用收到的原始数据产生的哈希哈希摘要对照，便可确信原始信息是否被篡改。这样就保证了数据传输的不可否认性。

哈希算法是一类符合特殊要求的散列函数(Hash)函数，这些特殊要求是:

（1）接受的输入报文数据没有长度限制;

（2）对任何输入报文数据生成固定长度的摘要("数字指纹")输出;

（3）由报文能方便地算出摘要;

（4）难以对指定的摘要生成一个报文,由该报文可以得出指定的摘要;

（5）难以生成两个不同的报文具有相同的摘要。

数字信封的功能类似于普通信封。普通信封在法律的约束下保证只有收信人才能阅读信的内容 ;数字信封则采用密码技术保证了只有规定的接收人才能阅读信息的内容。

数字信封中采用了单钥密码体制和公钥密码体制。信息发送者首先利用随机产生的对称密码加密信息，再利用接收方的公钥加密对称密码，被公钥加密后的对称密码被称之为数字信封。在传递信息时，信息接收方要解密信息时，必须先

用自己的私钥解密数字信封，得到对称密码，才能利用对称密码解密所得到的信息。这样就保证了数据传输的真实性和完整性。

5．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。证书是一个经证书认证中心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。

从证书的用途来看，数字证书可分为签名证书和加密证书。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；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。

简单的说，数字证书是一段包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。身份验证机构的数字签名可以确保证书信息的真实性。证书格式及证书内容遵循 X.509 标准。

6．数字证书的应用

现有持证人甲向持证人乙传送数字信息，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） 甲准备好要传送的数字信息（明文）。

（2） 甲对数字信息进行哈希（hash）运算，得到一个信息摘要。

（3） 甲用自己的私钥（SK）对信息摘要进行加密得到甲的数字签名，并将其附在数字信息上。

（4） 甲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。

（5） 甲用乙的公钥（PK）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乙。

（6）乙收到甲传送过来的密文和加过密的 DES 密钥 ,先用自己的私钥(SK) 对加密的 DES 密钥进行解密，得到 DES 密钥。

（7） 乙然后用 DES 密钥对收到的密文进行解密，得到明文的数字信息，然后将 DES 密钥抛弃（即 DES 密钥作废）。

（8） 乙用甲的公钥（PK）对甲的数字签名进行解密，得到信息摘要。

（9） 乙用相同的 hash 算法对收到的明文再进行一次 hash 运算，得到一个新的信息摘要。

（10） 乙将收到的信息摘要和新产生的信息摘要进行比较，如果一致，说明收到的信息没有被修改过。

二、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。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/RA 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/RA 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 出口到中国的 WWW 服务器，如微软的 IIS 5.0，受出口限制，其 RSA 算法的模长最高为 512 位，对称算法为 40 位，不能满足对安全性要求很高的场合，为解决这一问题，采用了山东大学网络信息安全研究所开发的具有自主版权的 SSL 安全模块，在 SSL 安全模块中使用了自主开发的 SJY 系列密码设备，并且把 SSL 模块集成在 Apache WWW 服务器中，Apache WWW 服务器在 WWW 服务器市场中占有百分之 50 以上的份额，其可移植性和稳定性很高。

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器端，通过具有高强度密码算法的 SSL 协议保证客户端和服务器端数据的机密性、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。

三、认证中心（CA）简介

为保证网上数字信息的传输安全，除了在通信传输中采用更强的加密算法等措施之外，必须建立一种信任及信任验证机制，即参加电子商务的各方必须有一个可以被验证的标识，这就是数字证书。数字证书是各实体(持卡人/个人、商户/企业、网关/银行等)在网上信息交流及商务交易活动中的身份证明。该数字证书具有唯一性。它将实体的公开密钥同实体本身联系在一起，为实现这一目的，必须使数字证书符合 X.509 国际标准，同时数字证书的来源必须是可靠的。这就意味着应有一个网上各方都信任的机构，专门负责数字证书的发放和管理，确保网上信息的安全，这个机构就是 CA 认证机构。各级 CA 认证机构的存在组成了整个电子商务的信任链。如果 CA 机构不安全或发放的数字证书不具有权威性、公正性和可信赖性，电子商务就根本无从谈起。

数字证书认证中心（Certficate Authority,CA）是整个网上电子交易安全的关键环节。它主要负责产生、分配并管理所有参与网上交易的实体所需的身份认证数字证书。每一份数字证书都与上一级的数字签名证书相关联，最终通过安全链追溯到一个已知的并被广泛认为是安全、权威、足以信赖的机构-根认证中心（根 CA）。

电子交易的各方都必须拥有合法的身份，即由数字证书认证中心机构（CA）签发的数字证书，在交易的各个环节，交易的各方都需检验对方数字证书的有效性，从而解决了用户信任问题。CA 涉及到电子交易中各交易方的身份信息、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。

数字证书认证解决了网上交易和结算中的安全问题，其中包括建立电子商务各主体之间的信任关系，即建立安全认证体系（CA）；选择安全标准（如 SET、SSL）；采用高强度的加、解密技术。其中安全认证体系的建立是关键，它决定了网上交易和结算能否安全进行，因此，数字证书认证中心机构的建立对电子商务的开展具有非常重要的意义。

认证中心（CA），是电子商务体系中的核心环节，是电子交易中信赖的基础。它通过自身的注册审核体系，检查核实进行证书申请的用户身份和各项相关信息，使网上交易的用户属性客观真实性与证书的真实性一致。认证中心作为权威的、可信赖的、公正的第三方机构，专门负责发放并管理所有参与网上交易的实体所需的数字证书。

四、CA/RA 体系功能简介

开放网络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：Certification Authority）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（Certification Authority --认证中心）以及配套的 RA（Registration Authority --注册审批机构）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。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，证书认证中心（CA）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，在证书废止列表(CRL)中添加新项并周期性地发布这一数字签名的 CRL。

RA（Registration Authority），数字证书注册审批机构。RA 系统是 CA 的证书发放、管理的延伸。它负责证书申请者的信息录入、审核以及证书发放等工作；同时，对发放的证书完成相应的管理功能。发放的数字证书可以存放于 IC 卡、硬盘或软盘等介质中。RA 系统是整个 CA 中心得以正常运营不可缺少的一部分。

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，免去了排队等候等烦恼。

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。

从技术角度上说，PMI(Privilege Management Infrastructure，授权管理基础设施)与 PKI/CA 的结合是发展的趋势。X.509 公钥证书的原始含义很简单，目标就是提供不可更改的证据。但是现在人们发现，在许多应用领域，需要的信息远不止是身份信息，证书持有者的权限或者属性信息比身份信息更重要。为了使附加信息能够保存在证书中，X.509 v4.0 中引入了公钥证书扩展项，这种证书扩展项可以保存任何类型的附加数据，以满足应用的需求。

证书应用的普及也带动了证书便携性的需要，目前只有智能卡能提供证书

和其对应私钥的移动性要求。该技术将公钥和对应的私钥存放在智能卡中，但这种方法存在着易丢失、易损坏的缺陷，并且依赖读卡器。最新的方法是使用漫游证书，它通过第三方软件实现。它的原理是将用户的证书和私钥放在一个安全的服务器上，当用户登录到一个本地系统时，从服务器安全地检索出公钥和私钥，并将其放在本地系统的内存中，当用户注销后，该软件自动删除存放在本地系统中的用户证书和私钥。此外，随着无线通信技术的广泛应用，WPKI 技术的研究与应用正处于探索之中，这也是未来 PKI 发展的一个趋势。