Windows2000公钥基础结构及在电子商务中应用 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/242/2021_2022_Windows200_c40_242490.htm １、概述 Windwos 2000为电子商务提供了一个理想的平台， 其安全性（包括证书管理、 CA服务、 公用密钥基本体系）， 保证了电子商务的开展。 结合Windows 2000的IIS 5.0服务， 可以快速创建一个网上电子商务的平台。 Windows 2000中有两种验证协议， 即Kerberos和公钥基础结构（Public Key Infrastructure， PKI）， 这两者的不同之处在于：Kerberos是对称密钥， 而PKI是非对称密钥。在Internet环境中， 需要使用非对称密钥加密。 即每个参与者都有一对密钥， 可以分别指定为公钥(PK)和私钥(SK)， 一个密钥加密的消息只有另一个密钥才能解密， 而从一个密钥推断不出另一个密钥。 公钥可以用来加密和验证签名；私钥可以用来解密和数字签名。 每个人都可以公开自己的公钥， 以供他人向自己传输信息时加密之用。 只有拥有私钥的本人才能解密， 保证了传输过程中的保密性。 关键是需要每个人保管好自己的私钥。同时， 为了保证信息的完整性， 还可以采用数字签名的方法。 接下来的问题是， 如何获得通讯对方的公钥并且相信此公钥是由某个身份确定的人拥有的， 这就要用到电子证书。 电子证书是由大家共同信任的第三方--认证中心（Certificate Authority， CA）颁发的， 证书包含某人的身份信息、 公钥和CA的数字签名。 任何一个信任CA的通讯一方， 都可以通过验证对方电子证书上的CA数字签名来建立起和对方的信任， 并且获得对方的公钥以备使用。 Windows 2000的PKI是基于X.509协议的，X.509标准用于在大型计算机网络

提供目录服务，X.509提供了一种用于认证X.509服务的PKI结构，两者都属于ISO和ITU提出的X系列国际标准，目前，有许多公司发展了基于X.509的产品，例如Visa、MasterCard、Netscape，而且基于该标准的Internet和Intranet产品越来越多。X.509是目前唯一的已经实施的PKI系统。X.509 V3是目前的最新版本，在原有版本的基础上扩充了许多功能，目前电子商务的安全电子交易（SET）协议也采用基于X.509 V3。 2、Windows 2000的公钥基础结构 如何在数字化通信中建立起信任关系， 是电子商务发展的重中之重。 因此， 建立认证中心(CA)是关键的一步。 Windows 2000可以作为建立CA的技术方案， 其内置了一整套颁发证书和管理证书的基础功能。 Windows 2000 Server中有一个部件是证书服务器（Certificate Server）， 是原来Windows NT 4.0的选项包中Certificate Server 1.0的升级产品。 通过认证服务器， 企业可以为用户颁发各种电子证书， 比如用于网上购物的安全通道协议(SSL)使用的证书， 用于加密本地文件(EFS)的证书等等。 认证服务器还管理证书的失效， 发布失效证书列表等。 每个用户或计算机都有自己的一个证书管理器， 其中既放置着自己从CA申请获得的证书， 也有自己所信任的CA的根证书。 Windows 2000中的电子证书都是基于X.509协议的， 保证了与其他系统的互操作性。 国际标准组织CCITT建议以X.509作为X.500目录检索的一个组成部分， 提供安全目录检索服务。 X.500是CCITT建议的， 用于分布网络中存储用户信息的数据库的目录检索服务的协议标准。 X.509是采用公钥基础结构实施的认证协议，对通信双方按所用密码体制规定了几种认证识别方法， 它发表于1988年， 经多次修改， 1993年又公布了新的版本。 X.509

对所用具体加密、 数字签名、 公用密钥以及Hash算法未作限制， 将会有广泛的应用，已纳入PEM(Privacy Enhanced Mail)系统中。 就网上购物的过程来说， 目前常用的是SSL（安全通道协议）的方式， 即设置IIS就某些特定的文件或文件目录需要访问者提供客户端证书；除非拥有电子证书及相应的私钥， 一个访问者的浏览器无法获得这些文件和文件目录。 SSL的方式体现在浏览器的访问栏上， 应该是Https而不是普通的Http。 通过网站验证后的访问者， 可以被映射为活动目录中的用户或者用户组， 实现合作伙伴之间外部网（Extranet）的应用。 为了安全地保管私钥和电子证书， 在Windows 2000中， 微软为用户还提供了一套智能卡的结构。 智能卡因其高安全性和轻便的可移动性， 势必将发展成为类似鼠标/键盘一般的计算机的标准外设。 微软还提供了一套基于32位Windows平台的Smart Card for Windows产品， 包括API和开发工具。 众多的智能卡厂家， 如Gemplus， 只要生产符合国际ISO工业标准的智能卡产品， 就可以在微软的Smart Card软件平台上操作。 当用户用Internet Explorer向一个认证中心申请电子证书时， 就会有一对公钥和私钥自动产生出来；私钥可以存储在智能卡中， 公钥和其他身份信息（比如姓名、电子邮件地址等）发给认证中心。 如果认证中心批准该申请，那么包含公钥的电子证书就会被返回来， 存储在智能卡中。 这种电子证书的申请过程也可以由管理员设定的批处理方法来进行， 用户还可以通过LDAP来查询CA中通讯对方的公钥， 因为Windows 2000的认证服务器是可以与活动目录相结合的， 所以这方面的查询很方便。 智能卡存储私钥和电子证书的做法， 给最终用户提供了对自己安全信息的最大的控制，

可以方便地从一台机器携带到另一台机器使用；可以在任何一个地点使用。一般来说，智能卡还会用一个个人密码(PIN)保护起来，在要求高安全性的场合，PIN可以是一些生物信息，比如指纹等。智能卡中存储的信息是加密的，即使破坏了智能卡也得不到里面的内容。智能卡的阅读器也越来越普遍，有USB型的，也有PC卡型的，甚至Windows终端上也会有智能卡插槽。智能卡正在逐渐走向大众化。如果企业实施了基于Windows 2000的智能卡体制，由企业保安机构给每个员工颁发一个智能卡。员工就可以用这个卡完成很多的工作，比如打开公司的大门，打开自己的抽屉，登录到计算机和网络；加密自己的邮件和文件，这样即使管理员有完全控制的权限，管理员也不能获知其中的内容；员工还可以上网购物，比如购买一张机票，然后直接到飞机舱前划卡即可上飞机；还可以作为电话卡、信用卡使用；作为市政交费卡使用，支付水、电、煤气等费用；作为电子钱包式的储值卡来使用，支付小额的午餐费、出租车费等等。可以说智能卡的应用在Windows 2000推出之后，会有一个长足的进步。"公用密钥基本体系"通常简称为PKI（Public Key Infrastructure），是一个数字认证、证书授权和其他注册授权系统。使用公用密钥密码检验及检证电子商务中所涉及的每个机构的有效性。公用密钥基本体系的标准仍处于发展阶段，尽管它们作为电子商务的一个必要组成部分已得到广泛使用。图1是Windows 2000 的公钥基础结构，其核心是加密服务、证书管理服务，为应用程序的开发提供了加密API接口（CryptoAPI）。Windows 2000 的公钥基础结构具有以下特点：（１）牢靠的安全性。Windows 2000的公钥基础结构包

括采用智能卡的牢靠验证， 保持公用网的保密性， 以及确保传输数据的完整性。 此外， 管理员可使用 Windows 2000 安全权限指派用户证书的使用。 （２） 简易管理。 Windows 2000的公用密钥与活动目录和组策略的集成， 可以对管理企业内部的委托关系进行调整， 还提供将证书直接或经 Internet Information Services 映射到活动目录中用户帐户的能力。 （３） 新机遇。 可以安全地交换诸如Internet等公用网上的文件和数据， 具有实现安全 E_mail(S/MIME)的能力。此外， 作为电子商务的一个重要组成部分， 可以利用电子签名建立发送者的无法否认机制。 3、Windows 2000 公钥基础结构的证书服务 证书基本上是一个由权威发布的电子声明， 其作用在于担保证书持有者的身份。 证书将公用密码与持有相应私有密钥的个人、 机器或服务的身份绑定在一起。 证书由各种公用密钥安全服务和应用程序提供， 为非安全网（如 Internet ）提供数据验证、 数据完整性和安全通讯。 Windows 2000 基于证书的过程所使用的标准证书格式是 X.509 V3， X.509证书包括有关证书拥有的个人或实体的信息及证书颁发机构的可选信息。 实体信息包括实体名称、 公用密钥、 公用密钥运算法和可选的唯一主体 ID。 版本 3 证书的标准制定了以下规定：密钥标识符、 密钥用法、 证书策略、 替换名称和属性、 证书路径约束以及对证书撤消原因和列表分区。 Windows 2000 Server 证书服务是 Windows 2000 中的组件， 证书服务用于创建和管理证书颁发机构(CA)。 证书颁发机构负责建立和担保证书持有者的身份。 证书颁发机构还会在证书失效时， 将其撤消并发布证书撤消列表， 供证书检验机构使用。 最简单的公用密钥基本体系只有一个证书颁发机构。 事实上， 大

多数配置公用密钥基本体系的组织使用多个证书颁发机构，并将其有组织地形成证书分层结构。 Windows 2000的证书服务按证书颁发机构类型分为：（1）企业根CA,是企业中最受信任的证书颁发机构，应该在网络上的其它证书颁发机构之前安装，需要 Active Directory. (2) 企业从属CA，是标准证书颁发机构可以给企业中的任何用户或机器颁发证书，必须从企业中的另一个证书颁发机构获取证书颁发机构证书，需要 Active Directory. (3) 独立根CA，是证书颁发机构体系中最受信任的证书颁发机构，不需要 Active Directory. (4)独立从属CA，是标准的证书颁发机构可以给任何用户或机器颁发证书；必须从另一个证书颁发机构获取证书颁发机构证书，不需要 Active Directory。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com