PKI 安全服务

PKI 的应用非常广泛，其为网上金融、网上银行、网上证券、电子商务、电子政务等网络中的数据交换提供了完备的安全服务功能。PKI 作为安全基础设施，能够提供身份认证、数据完整性、数据保密性、数据公正性、不可抵赖性和时间戳六种安全服务。

身份认证

由于网络具有开放性和匿名性等特点，非法用户通过一些技术手段假冒他人身份进行网上欺诈的门槛越来越低，从而对合法用户和系统造成极大的危害。身份认证的实质就是证实被认证对象是否真实和是否有效的过程，被认为是当今网上交易的基础。在 PKI 体系中，认证中心(Certification Authority，CA)为系统内每个合法用户办一个网上身份认证，即身份证。

数据完整性

数据的完整性就是防止非法篡改信息，如修改、复制、插入、删除等。在交易过程中，要确保交易双方接收到的数据与原数据完全一致，否则交易将存在安全问题。如果依靠观察的方式来判断数据是否发生过改变，在大多数情况下是不现实的。在网络安全中，一般使用散列函数的方法(Hash 函数，也称密码杂凑函数)来保证通信时数据的完整性。通过 Hash 算法我们将任意长度的数据通过变换为长度固定的数字摘要(消息认证码，MAC)，并且原始数据中任何一位的改变都将会在相同的计算条件下产生截然不同的数字摘要。

这一特性使得人们很容易判断原始数据是否发生非法篡改，从而很好地保证了数据的完整性和准确性。目前，PKI 系统主要采用的散列算法有 SHA — 1 和 MD — 5。 [2]

数据保密性

数据的保密性就是对需要保护的数据进行加密，从而保证信息在传输和存储过程中不被未授权人获取。在 PKI 系统中，所有的保密性都是通过密码技术实现的。密钥对分为两种，一种称作加密密钥对，用作加解密；另一种称作签名密钥对，用作签名。一般情况下，用来加解密的密钥对并不对实际的大量数据进行加解密，只是用于协商会话密钥，而真正用于大量数据加解密的是会话密钥。 [2]

在实际的数据通信中，首先发送方产生一个用于实际数据加密的对称算法密钥，此密钥被称为会话密钥，用此密钥对所需处理的数据进行加密。然后，发送方使用接收方加密密钥对应的公钥对会话密钥进行加密，连同经过加密处理的数据一起传送给接收方。接收方收到这些信息后，首先用自己加密密钥对中的私钥解密会话密钥，然后用会话密钥对实际数据进行解密。

数据公正性

PKI 中支持的公正性是指数据认证。也就是说，公证人要证明的是数据的正确性，这种公汪取决于数据验证的方式，与公正服务和一般社会公证人提供的服务是有所不同的。在 PKI 中，被验证的数据是基于对原数据 Hash 后数字摘要的数字签名、公钥在数学上的正确性和私钥的合法性。

不可抵赖性

不可抵赖性保证参与双方不能否认自己曾经做过的事情。在 PKI 系统中，不可抵赖性来源于数字签名。由于用户进行数字签名的时候 . 签名私钥只能被签名者自己掌握，系统中的其他实体不能做出这样的签名，因此，在私钥安全的假设下签名者就不能否认自己做出的签名。保护签名私钥的安全性是不可抵赖问题的基础。

时间戳服务

时间戳也叫安全时间戳，是一个可信的时间权威，使用一段可以认证的数据来表示。

PKl 中权威时间源提供的时间并不需要正确 ,仅仅需要用户作为一个参照“时间” ，以便完成基于 PKI 的事务处理，如时间 A 发生在时间 B 的前面等。一般的 PKI 系统中都设置一个时钟统一 PKI 时间。当然也可以使用时间官方事件源所提供的时间，其实现方法是从网中这个时钟位置获得安全时间，要求实体在需要的时候向这些权威请求在数据上盖上时间戳。一份文档上的时间戳涉及对时间和文档内容的哈希值的签名，权威的签名提供了数据的真实性和完整性。一个 PKI 系统中是否需要实现时间戳服务，完全依照应用的需求来决定

数字签名

由于单一的、独一无二的私钥创建了签名，所以在被签名数据与私钥对应的实体之间可以建立一种联系，这种联系通过使用实体公钥验证签名来实现。如果签名验证正确 ,并且从诸如可信实体签名的公钥证书中知道了用于验证签名的公

钥对应的实体，那么就可以用数字签名来证明被数字签名数据确实来自证书中标识的实体。

因此，PK 的数字签名服务分为两部分：签名生成服务和签名验证服务。签名生成服务要求能够访问签名者的私钥，由于该私钥代表了签名者，所以是敏感信息，必须加以保护。如果被盗，别人就可以冒充签名者用该密钥签名。因此，签名服务通常是安全应用程序中能够安全访问签名私钥的那一部分。相反，签名验证服务要开放一些，公钥一旦被可信签名者签名，通常就被认为是公共信息。验证服务接收签名数据、签名、公钥或公钥证书，然后检查签名对所提供的数据是否有效。它返回验证成功与否的标识。