电子商务概论知识辅导：密钥管理 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/170/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_170716.htm 众所周知，公钥机制涉及到一对密钥，即公钥和私钥，如何实现密钥管理是PKI服务系统的关键问题。其中，私钥只能由证书持有者秘密掌握，无需在网上传输。而公钥是公开的，需要在网上传送，故公钥体制的密钥管理主要是公钥的管理问题。一、公钥的用途在公钥体制的实际应用中，公钥主要有两大类用途：1、用于验证数字签名信息接收者使用发送者的公钥对接收的信息的数字签名进行验证。2、用于加密信息信息发送者使用接收者的公钥来加密用于对称加密信息的常规密钥，从而进行加密密钥的传递。二、签名密钥和加密密钥由于公钥所具有的两种不同用途，在实际应用中，需要分别配置用于数字签名／验证的密钥对和用于数据加密／脱密的密钥对，这里分别称为签名密钥对和加密密钥对。这两对密钥由于用途不同，因此，对于密钥的管理也就有着不同的要求。1、签名密钥对的管理签名密钥对由签名私钥和验证公钥组成。签名私钥是发送方身份的证明，具有日常生活中公章、私章的效力。为保证其唯一性，签名私钥绝对不能够做备份和存档，丢失后只需重新生成新的密钥对。验证公钥需要存档，用于验证旧的数字签名。用做数字签名的这一对密钥一般可以有较长的生命期。2、加密密钥对的管理加密密钥对由加密公钥和脱密私钥组成。为防止密钥丢失时数据无法恢复，脱密私钥应该进行备份，同时还可能需要进行存档，以便能在任何时候脱密历史密文数据。加密公钥则无需备份和存档，加密公钥丢

失时，只需重新产生密钥对即可。这种密钥应该频繁更换，故加密密钥对的生命周期较短。不难看出，这两对密钥的密钥管理要求存在互相冲突的地方，因此，必须针对不同的用途使用不同的密钥对。尽管有的公钥体制算法(如RSA)，既可以用于加密，又可以用于签名，但由于这两对密钥在管理上截然不同的要求，在使用中仍然必须为用户配置两对密钥、其一用于数字签名，另一用于加密。而采用一对密钥，既用于加密，又用于签名，这种做法是不安全的。三、公钥的产生用户的公钥可有两种产生方式：1、用户生成在这种方式中，用户自己生成密钥对，然后将公钥以安全的方式传送给CA。2、CA生成这种方式是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，故对CA的可信性有更高的要求。如果是签名密钥，CA必须在事后销毁用户的私钥。四、公钥的获取用户在网上可通过两种方式获取通信对方的公钥，以用来传送加密数据，实现安全通信。1、由通信对方将自己的公钥随同发送的正文信息一起传送给用户。2、所有的证书集中存放于一个证书库中，用户在网上可从该地点取得通信对方的证书。五、密钥备份和恢复在PKI环境中，有时用户会丢失他们的私钥。这通常是由于以下原因：n 遗失或忘记口令。虽然用户的加密私钥在物理上是存在的，但实际上不可使用。n 介质的破坏。如硬盘和IC卡损坏。如果用户由于某种原因丢失了解密私钥，则被加密的数据因无法解开，而造成数据的丢失。例如，在某项业务中的重要文件被对称密钥加密，而对称密钥又被某个用户的公钥加密起来，假如该用户的解密私钥丢失了，这些

文件将无法恢复。为了避免这种情况的发生，PKI提供了密钥备份与解密密钥的恢复机制，这就是PKI的密钥备份与恢复系统。但值得强调的是，密钥备份与恢复只能针对解密密钥，而签名密钥不能做备份。密钥的备份与恢复形成了PKI定义的重要部分。1、密钥／证书的生命周期密钥／证书的生命周期主要分初始化一颁发一取消三个阶段。（1）初始化阶段初始化阶段是用户实体在使用PKI的支持服务之前，必须经过初始化进入PKI。初始化（注册）阶段由以下几部分组成：n 实体注册。n 密钥对产生。n 证书创建和密钥／证书分发。n 证书分发。n 密钥备份。（2）颁发阶段颁发阶段是私钥和公钥证书一旦被产生即可进入颁发阶段。主要包括：n 证书检索远程资料库的证书检索。n 证书验证确定一个证书的有效性。n 密钥恢复不能正常解读加密文件时，从CA中恢复。n 密钥更新当一个合法的密钥对将要过期时，新的公／私密钥自动产生并颁发。