java认证辅导:J2ME软件签名证书和获取Java认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/585/2021_2022_java_E8_AE_A4_E8_AF_81_c104_585029.htm 内容简述 背景 一个好的J2ME应用程序，最后就是在程序读取系统资源的时候（网络，sms，pim，file等）无需弹出烦人的提示。本文的目的就是探讨这方面的知识。 内容介绍 J2ME 的证书可以解决上面提出的问题，本文主要是对网络上的一些解决方案跟经验做次总结 预期读者跟建议 需要对J2ME程序签证的开发者，假设开发者已经熟悉了J2ME。 由于本人水平有限，存在一些错误的地方，希望大家多多交流。 MIDlets 签证 什么是Java 数字证书 原文链接 http://www.blogjava.net/zpuser/archive/2006/07/22/59528.html 也许您对"数字证书"这一概念还很陌生，其实，数字证书就是标志网络用户身份信息的一系列数据，用来在网络通讯中识别通讯各方的身份，即要在 Internet上解决"我是谁"的问题，就如同现实中我们每一个人都要拥有一张证明个人身份的身份证或驾驶执照一样，以表明我们的身份或某种资格。 数字证书是由权威公正的第三方机构即CA中心签发的，以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性，签名信息的不可否认性，从而保障网络应用的安全性。 数字证书采用公钥密码体制，即利用一对互相匹配的密钥进行加密、解密。每个用户拥有一把仅为本人所掌握的私有密钥（私钥），用它进行解密和签名；同时拥有一把公共密钥（公钥）并可以对外公开，

用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样，信息就可以安全无误地到达目的地了，即使被第三方截获，由于没有相应的私钥，也无法进行解密。通过数字的手段保证加密过程是一个不可逆过程，即只有用 私有密钥才能解密。在公开密钥密码体制中，常用的一种是RSA体制。 用户也可以采用自己的私钥对信息加以处理，由于密钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名。采用数字签名，能够确认以下两点：（1）保证信息是由签名者自己签名发送的，签名者不能否认或难以否认；（2）保证信息自签发后到收到为止未曾作过任何修改，签发的文件是真实文件。 数字证书可用于：发送安全电子邮件、访问安全站点、网上证券、网上招标采购、网上签约、网上办公、网上缴费、网上税务等网上安全电子事务处理和安全电子交易活动。 字证书的格式一般采用X.509国际标准。目前，数字证书认证中心主要签发安全电子邮件证书、个人和企业身份证书、服务器证书以及代码签名证书等几种类型证书。 数字证书的格式遵循ITUTX.509国际标准。一个标准的X.509数字证书包含以下一些内容： 证书的版本信息；证书的序列号，每个证书都有一个唯一的证书序列号；证书所使用的签名算法，如RSA算法；证书的发行机构（CA中心）的名称，命名规则一般采用X.500格式；证书的有效期，现在通用的证书一般采用UTC时间格式，它的计时范围为1950年-2049年；证书拥有者的名称，命名规则一般采用X.500格式；证书拥有者的公开密钥；证书发行机构（CA中心）对证书的数字签名。 更多优质资料尽在百考试题论坛 百考试题