Java处理PFX格式证书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_ti2020/644/2021_2022_Java_E5_A4_84_E7_90_86_c104_644970.htm 在Security编程中，有几种典型的密码交换信息文件格式: DER-encoded certificate: .cer, .crt PEM-encoded message: .pem PKCS#12 Personal Information Exchange: .pfx, .p12 PKCS#10 Certification Request: .p10 PKCS#7 cert request response: .p7r PKCS#7 binary message: .p7b .cer/.crt是用于存放证书，它是2进制形式存放的，不含私钥。 .pem跟crt/cer的区别是它以Ascii来表示。 pfx/p12用于存放个人证书/私钥，他通常包含保护密码，2进制方式 p10是证书请求 p7r是CA对证书请求的回复，只用于导入 p7b以树状展示证书链(certificate chain)，同时也支持单个证书，不含私钥。 其中，我介绍如何从p12/pfx文件中提取密钥对及其长度: 1，首先，读取pfx/p12文件（需要提供保护密码） 2，通过别名(Alias, 注意，所有证书中的信息项都是通过Alias来提取的)提取你想要分析的证书链 3，再将其转换为一个以X509证书结构体 4，提取里面的项，如果那你的证书项放在第一位（单一证书），直接读取 x509Certs[0]（见下面的代码）这个X509Certificate对象 5，X509Certificate对象有很多方法，tain198127网友希望读取RSA密钥（公私钥）及其长度（见http://www.matrix.org.cn/thread.shtml?topicId=43786 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