java 讀取使用keytool生產的keystore文件

windows 環境下，使用keytool 生產keystore文件

keytool -genkeypair -keyalg RSA -keysize 1024 -sigalg SHA1withRSA -validity 36000 -alias www.kunlunsoft.com -storepass abcdefg -keystore zlex.keystore -dname "CN=localhost, OU=zlex,O=zlex, L=BJ, ST=BJ, C=CN"

說明：-keyalg ：指定key的加密算法；

-sigalg：指定簽名算法；

-storepass：指定key的密碼

注意：keystore 密碼和主密碼必須相同

操作結果如下：

上述命令會生產一個文件zlex.keystore

keystore文件中既包含公鑰，也包含私鑰。

使用java 讀取zlex.keystore 文件：

用於保存私鑰和公鑰的bean：

Java代碼

```
1.  package com.common.bean;
2.  import java.io.Serializable;
3.  import java.security.PrivateKey;
4.  import java.security.PublicKey;
5.  public class PrivPubKeyBean implements Serializable {
6.      private static final long serialVersionUID = 1888415926054715509L;
7.      private PrivateKey privKey;
8.      private PublicKey publKey;
9.      private String sigAlgName;
10.     public PrivateKey getPrivKey() {
11.         return privKey;
12.     }
13.     public void setPrivKey(PrivateKey privKey) {
```

```
14.         this.privKey = privKey;
15.     }
16.     public PublicKey getPublKey() {
17.         return publKey;
18.     }
19.     public void setPublKey(PublicKey publKey) {
20.         this.publKey = publKey;
21.     }
22.     public String getSigAlgName() {
23.         return sigAlgName;
24.     }
25.     public void setSigAlgName(String sigAlgName) {
26.         this.sigAlgName = sigAlgName;
27.     }
28. }
```

讀取keystore文件獲取私鑰和公鑰：

Java代碼

```
1.     public static PrivPubKeyBean getPrivPubKeyBean(String keyStorePath,String password,String alias) throws Exception{
2.         PrivPubKeyBean privPubKeyBean=new PrivPubKeyBean();
3.         KeyStore ks =SystemUtil. getKeyStore(keyStorePath, password);
4.         PrivateKey privateKey = (PrivateKey) ks.getKey(alias, password.toCharArray());
5.         privPubKeyBean.setPrivKey(privateKey);
6.         X509Certificate x509Certificate = (X509Certificate) ks.getCertificate(alias);
7.         PublicKey pubKey=x509Certificate.getPublicKey();
8.         privPubKeyBean.setPublKey(pubKey);
9.         privPubKeyBean.setSigAlgName(x509Certificate.getSigAlgName());
10.         return privPubKeyBean;
11.     }
```

測試：

Java代碼

```
@Test
    public void test_03() {
        try {
            String message = "whuang";
            String keyStorePath = "d:\\Temp\\a\\a\\ca\\zlex.keystore";
            String password = "abcdefg";
            String alias = "www.kunlunsoft.com";
            PrivPubKeyBean privPubKeyBean = SystemUtil.getPrivPubKeyBean(
                    keyStorePath, password, alias);
            byte[] result = SystemUtil.encrypt(message,
                    privPubKeyBean.getPublKey());
            byte[] deResult = SystemUtil.decrypt(result,
                    privPubKeyBean.getPrivKey());
            System.out.println(new String(deResult));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
```

運行結果：whuang

Java代碼

1. SystemUtil 見附件，路徑：src\main\java\com\common\util\SystemUtil.java