# DidiSoft OpenPGP Library for Java version 2.5

## Table of contents

# Introduction

## Introduction

This documentations refers to DidiSoft OpenPGP Library for Java.
Intended audience: software engineers, software architects, system administrators.

## About the Library

DidiSoft OpenPGP Library for Java is a 100% Java library with no external dependencies.

The library provides functions for OpenPGP encryption, decryption, signing, verification of signed data, clear text signing, one pass signing and encryption, key pair generation, key signing, key revocation, etc.

The library uses internally the open source BouncyCastle Java library.

# Setup

The library consists of three JAR files located in the **Bin** folder of the library distribution ZIP file:

1) bcpg-jdk14-145.jar
2) bcprov-ext-jdk14-145.jar
3) pgplib-2.5.jar

They must be copied, referenced and distributes with your software in order the library to work.

Note: If you **already have** some of the **BouncyCastle** JAR files in your project (for example another library already depends on them), please refer to section BouncyCastle compatibility

## Unlimited JCE

Due to export control restrictions, by default the JDK is supplied with limited cipher key lengths.

In order to enable full cipher key length additionally should be downloaded:
**Java Cryptography Extension** (JCE) Unlimited Strength Jurisdiction Policy Files

In both cases you have to download a ZIP file and copy the content of the ZIP in
your JRE's jre/lib/security/ folder.

**Note:** This operation has to be done for every machine where this library will be distributed.

Bellow you will find links where you can download them for Oracle (*previously Sun*) and IBM JVM's (Java Virtual Machine) version 1.7 (Java 7), 1.6 (Java 6), 1.5 (Java 5) and 1.4.

### Java 1.7

Oracle JVM 1.7
http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html

IBM JVM 1.7
http://www.ibm.com/developerworks/java/jdk/security/70/
Scroll down to '*IBM SDK Policy files*'
(Login for the IBM web site is required)

### Java 1.6

Oracle JVM 1.6
http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html

IBM JVM 1.6
http://www.ibm.com/developerworks/java/jdk/security/60/
Scroll down to '*IBM SDK Policy files*'
(Login for the IBM web site is required)

### Java 1.5

Sun JVM 1.5
http://java.sun.com/javase/downloads/index_jdk5.jsp
Scroll down to "Other Downloads" - Java Cryptography Extension (JCE)
Unlimited Strength Jurisdiction Policy Files 5.0

IBM JVM 1.5
http://www.ibm.com/developerworks/java/jdk/security/50/

Scroll down to IBM SDK Policy files
(Login for the IBM web site is required)

### Java 1.4

Sun JVM 1.4
http://java.sun.com/j2se/1.4.2/download.html
Scroll down to Other Downloads > Java Cryptography Extension (JCE)
Unlimited Strength Jurisdiction Policy Files 1.4.2

IBM JVM 1.4
Visit:
https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

If you have trouble to set up the Unlimited JCE policy files, please do not hesitate to contact us.

## From Evaluation to Production

After a purchase you will receive **download** instructions for the **production copy** of the library.

Please **download** the **production copy** ZIP file and **replace** in your project the **evaluation** version JAR files with the once from the **/Bin** folder of the **production copy** ZIP archive.

The same process should be applied also for **upgrade to a newer version** of the library.

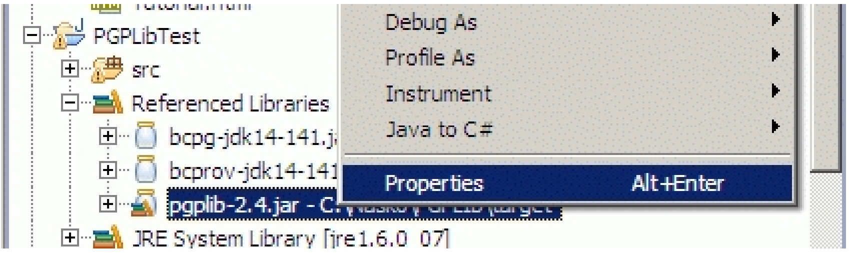
## Javadoc in Eclipse

This article is a short list of steps to perform in order to see more meaningful **tooltips** when programming with DidiSoft OpenPGP Library for Java. It assumes that you use Eclipse as your Java IDE.

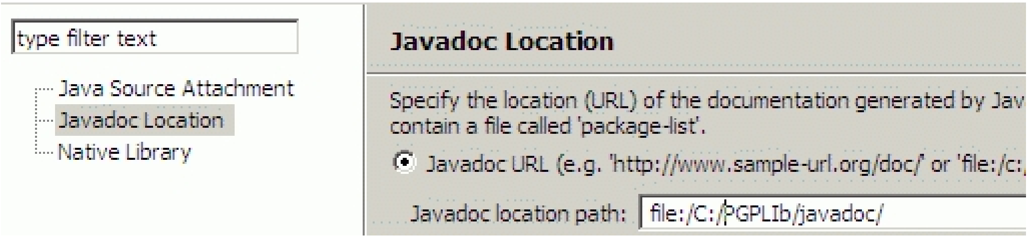
1. Download and unpack library ZIP.

2. Start a new **Eclipse project** and reference the three JARS located in the **Bin** folder in the location from step 1.

3. In your project **Referenced Libraries** section in the Eclipse **Package Explorer** tab right click pgplib-x.x.jar (x.x is your version in use), select **Properties**.



4. In the Javadoc Location dialog enter the location of the **JavaDoc** folder where the library was extracted in step 1.



Specify the location (URL) of the documentation generated by Jav
contain a file called 'package-list'.

● Javadoc URL (e.g. 'http://www.sample-url.org/doc/' or 'file:/c:

Javadoc location path: file:/C:/PGPLIb/javadoc/

5. Now the JavaDoc should appear when you type methods or properties of the objects from the library, or simply press **F2** when you are over an already typed method.

## WAR and EAR

If your project is running in an Application server (WAR or EAR project) you may encounter **strange exceptions** after **application start/stop**.
You can skip this section if you do not plan to stop/start the application that uses the library.

**The reason** for these exceptions is that the library JAR files are bundled with the web application. Hence after an application stop/start, they are loaded in another class loader, while the BouncyCastle security provider was already registered with class loader that is unavailable (*has been destroyed after the web application has stopped*)

**The solution** to this situation is to ship the application without the library JAR files.
They must be placed in a folder **shared** for all applications running on the Application server.

Below are listed the **shared folders** for some application servers.

**Glassfish**
<glassfish folder>/domains/domain1/lib/

**Tomcat** 5.x
<tomcat folder>/shared/lib/

**Tomcat** 6.x
$CATALINA_BASE/lib/

**Web Sphere (WAS)**
<was folder>/lib

**WebLogic**
<weblogic folder>/common/lib

*Note: If you application server is not mentioned here, please refer to your application server documentation in order to located the shared jar's folder.*

## BouncyCastle compatibility

If another **third party JAR** file already **depends** on the **BouncyCastle** JAR files and they are **different version** from the one distributed with *DidiSoft OpenPGP Library for Java*, you can copy only the **pgplib-x.x.jar** file and use your **existing** BouncyCastle JAR files from **bcprov-xxx-1.41** up to the newest one.

You can use any version targeting from **JDK** 1.4 up to 1.6.

Only for BouncyCastle bcprov **version 138** we provide a separate build!

# Migration guide

## From version 2.6.1 to 2.6.2

In version 2.6.2 additional code for Elliptic Curve cryptography was added to the bcpg-jdk14-145.jar file. In order to avoid using the old file the file has been renamed to:

**bcpg-jdk14-145-ecc.jar**

**Migration guide:**

1) Replace **bcpg-jdk14-145.jar** with **bcpg-jdk14-145-ecc.jar**

## From version 2.5.x to 2.6.0

As of version 2.6.0 the plain encrypt methods (**PGPLib.encrypt**...) throw **java.io.IOException** in addition to com.didisoft.pgp.PGPException.

In order to migrate from version 2.5 you will also have to catch **java.io.IOException** into an additional catch clause.

**Methods affected:**
PGPLib.encryptStream
PGPLib.encryptFile
PGPLib.encryptStreamPBE
PGPLib.encryptFilePBE

# Examples

## Example files

In the library distribution ZIP package you will find a folder named **Examples.**

Create a new Java project with your favorite IDE of choice and add the files from the **Examples\src** folder.

The other files in the Examples folder are used as data for some of the examples.

## Examples Online

All the examples below are available online at our web site:
http://www.didisoft.com/java-openpgp/examples/

Quick introduction to OpenPGP
Getting Started with the library
Setup instructions
Exception handling guidelines

### Most common functions

Encrypt
Decrypt
Decrypting with a password
Sign
Verify
Sign and Encrypt
Decrypt and Verify
Clear text sign

### KeyStore and key generation.

Properties of a Key
KeyStore introduction
Generate RSA keys
Generate DH/DSS keys
Import keys
Export keys
Deleting keys
Changing private key password

### Key revocation

Introduction to OpenPGP key revocation
Revoke key directly
Revocation certificate
Designated revoker

### Advanced Topics

Set preferred cypher (symmetric key algorithm)
Set preferred compression
Set preferred hashing

## Miscellaneous

Inspecting OpenPGP archives
Logging

# Appendix

## Common Exceptions

Some common exceptions that may occur when working with the library are:

org.bouncycastle.openpgp.PGPException: Exception creating cipher

org.bouncycastle.openpgp.PGPException: exception constructing public key

org.bouncycastle.openpgp.PGPException: exception encrypting session key

java.lang.SecurityException: Unsupported keysize or algorithm parameters

### Resolution:

Try to download the files listed in JCE Unlimited Strength Policy files and try again.

If the problem appears after that, please contact us.

## Exporting keys from a GnuPG keystore

List keys contained in the GnuPG keystore:

```
gpg --list-keys
```

Export Public key

```
gpg --export my_key -o my_public_key.gpg
```

Export Private key

```
gpg --export-secret-key my_key -o my_secret_key.gpg
```

# Support

## Technical support

To receive general information or **technical support**, please contact us at support@didisoft.com.

## Sales

For questions related to sales, volume licensing, or OEM licensing, please contact us at sales@didisoft.com.

## Product Updates

If you have purchased the library you can access our Customers' Portal where you can download new versions.

## Newsletter

To receive product update news, you can subscribe to our Newsletter

For further information, visit us at www.didisoft.com
If you have any ideas, wishes, questions or criticism, don't hesitate to contact us. We will be glad to hear from you.