**SkyDRM Server SDK User guide**

In order to use the SkyDRM Server SDK, you must configure your Java Runtime Environment (on the machine running RMJavaSDK) to support 256-bit keys. Due to import limits on cryptographic algorithms in some countries, the Oracle implementation of the JDK/JRE provides a default cryptographic jurisdiction policy file that limits the strength of cryptographic algorithms to a 128-bit key size, as detailed on the Oracle website on [this web link](http://docs.oracle.com/javase/7/docs/technotes/guides/security/SunProviders.html).

*Note:* As the SDK consumer, it is your responsibility to verify that you are permitted to use a 256-bit key in accordance with local regulations. Install the [Java Cryptography Extensions (JCE) Unlimited Strength JurisdictionPolicy Files](http://www.oracle.com/technetwork/java/javase/downloads/index.html) corresponding to the version of JDK/JRE you have for your machine running RMJavaSDK.

The minimum sourceCompatibility for the consumer project is Java 1.7. It can be deployed on that and later versions of Java.

If you are deploying on Java 7, there is a bug about Diffie-Hellman prime length restriction <http://bugs.java.com/bugdatabase/view_bug.do?bug_id=6521495> (Skip this if you are using Java 8). Please follow the instructions in this answer to solve the problem: <https://stackoverflow.com/questions/6851461/java-why-does-ssl-handshake-give-could-not-generate-dh-keypair-exception/29176597#29176597> (but use the version of the 2 bouncy castle jars from lib folder instead of jars in the link)

**Steps for using RMJavaSDK**:

1. Obtain API user credentials.

API user credentials are used to authenticate the user of the Server SDK. The credentials consist of an appId and appKey. These credentials are provided by the SkyDRM super-admin. The consumers of the Server SDK need to use these two parameters in code while using some of the SDK functions. These credentials authenticate the caller with the SkyDRM server.

1. Write your program to consume RMJavaSDK.

In your program, you need to use appId and appKey (obtained from step 1) together with routerURL to construct a RightsManager object. With this RightsManager object, you’ll be able to encrypt/decrypt files.

1. Encrypt/decrypt files.

With the encrypt and decrypt methods of RightsManager, you can enrypt/decrypt files. Refer to the sample codes we provided. Note that the tenantName parameter is optional, if tenantName is null, the default public tenant will be used internally.

1. Run your code.

All the libraries required to run the RMJavaSDK are located in the lib folder. Assuming your program (Runner.java for example) is in the same directory with the lib folder, then you can compile and run the program with following steps:

* 1. javac –cp ;lib\\* Runner.java
  2. java –cp ;lib\\* Runner

1. Javadocs and references.

Refer to sample code classes in the zipped file to see how to use the SDK. The SDK has thorough Javadocs also. It is highly recommended to read the Javadocs if there is any uncertainty about usage of the SDK.

**Token Caching:**

The SDK also has the ability to cache the token if a system property was set in the JVM. Currently this is used only during decryptPartial operations but in the future can be made available to whole file decrypt operations, and potentially also during encryption (as it’s the same token).

sdk.cache.token=true (this will enable the token caching feature)

sdk.cache.config="/file/path/to/file/sdk.properties" (to specify custom expiry in minutes and maxSize, otherwise it defaults to 10 minutes and 10,000 keys)

The contents of sdk.properties (the name of the file specified above) have format:

sdk.cache.config.maximumsize=500

sdk.cache.config.expiry=5

Sample run of standalone (from console):

C:\Users\pkumar\Desktop\runner>  
C:\Users\pkumar\Desktop\runner>"%JAVA\_HOME%\bin\javac.exe" -cp ;lib\* launcher\PartialDecryptPartialInputStream.java  
C:\Users\pkumar\Desktop\runner>"%JAVA\_HOME%\bin\java.exe" -agentlib:jdwp=transport=dt\_socket,address=8003,server=y,suspend=n -Dsdk.cache.token=true -Dsdk.cache.config="C:\Users\SDKUser\Desktop\runner\sdk.properties" -cp ;lib\* launcher.PartialDecryptPartialInputStream

Listening for transport dt\_socket at address: 8003  
16:33:26.758 [main] INFO RightsManager - Initialized RMJavaSDK v9.1.001 with token caching true  
16:33:27.572 [main] INFO RightsManager - Encrypted file test.txt successfully  
16:33:27.600 [main] DEBUG TokenCache - TokenCache initialized with maximumSize = 500, expiry (minutes) = 5  
16:33:27.682 [main] DEBUG RightsManager - Prefetched token into cache for duid 15C456806213C5FCAD6BD0AD70F74B59  
16:33:27.682 [main] DEBUG RightsManager - Prefetching token took time (ms) 105  
16:33:27.684 [main] DEBUG RightsManager - Decrypt took time (ms) 1  
Partial Decryption Completed