Bouncy Castle FIPS Migration Hints – BC-FJA 1.0.2.* to 2.0.0

Release Date: 16 July 2024

For the most part BC-FJA 2.0.0 represents an expansion of the BC-FJA 1.0.2 series. Providing an application is written using the JCA layer, it is unlikely any changes will be required due to API changes. Where changes may need to be made is in relation to FIPS transitions that are now expired as well as some additional changes in behaviour which can be adjusted using new system/security properties, or are due to changes in the JVM itself.

User Guide:

The User Guide for BC-FJA 2.0.0 is available at:

https://downloads.bouncycastle.org/fips-java/docs/BC-FJA-UserGuide-2.0.0.pdf

Code changes:

As with the latest versions of Bouncy Castle Java, **BC-FJA 2.0.0 introduces a bcutil-fips jar**. This jar includes dependencies for bcpkix, bcpg, and the other auxiliary jars which do not need to be in the actual FIPS jar. The reason behind this change is that by moving the classes out of the FIPS boundary into the bcutil jar, it's now much easier, cheaper, and faster to make any needed enhancements or bug fixes.

FipsAES and FipsTripleDES now has a new sub-class FipsAES.ParametersWithIV and the getIV() method has been removed from the FipsAES.Parameters class. The addition of the class has been made to provide cleaner support of Format Preserving Encryption which is one of the new additions in BC-FJA 2.0.0.

BC-FJA 2.0.0 removes the support for the internal Oracle defined KDFs required to support the Oracle JSSE provider. These classes are no longer easily accessible as of Java 17 and the experimental FIPS mode for the Oracle JSSE provider was also removed in Java 9. As a result, even if not requiring FIPS compliance, we now recommend use of the BCJSSE provider available in the bctls jar. The current user guide for the BC TLS APIs can be found at:

https://downloads.bouncycastle.org/fips-java/docs/BC-FJA-(D)TLSUserGuide-1.0.19.pdf

Behaviour Changes:

The MD5 digest is now disabled by default in approved-only mode. It can be re-enabled where required for use with TLS by setting:

org.bouncycastle.jsse.enable_md5=true

The provider will now block the use of DES-EDE encryption in approved mode. This is in-line with the transition period for DES-EDE that ended at the end of 2023. Applications looking to be FIPS compliant will need to move to AES. DES-EDE decryption is still available at the current time.

The provider will now block the use of RSA PKCS#1.5 encryption in approved mode. This is in-line with the transition period for RSA PKCS#1.5 that ended at the end of 2023. Applications looking to be FIPS compliant will need to move to OAEP if they still wish to use RSA keys. RSA PKCS#1.5 decryption is still available at the current time.

The provider will now bock the use of SHA-1 for signature generation in approved mode. This has been disallowed since the last release of NIST SP 800-131A revision 2 (so strictly speaking should not be getting used anywhere) but is now required to be enforced.