Java FIPS Road Map

Current FIPS Overview

The BC FIPS Java Description contains a broad overview of the motivations and design of the BC FIPS Java module.

As of BC Java 1.54 from a JCA/JCE point of view the module is largely a drop in replacement and can be used with the other BC APIs for certificate generation, CMS, TSP, S/MIME, OpenPGP and other protocols. Owing to the requirements of FIPS, particularly in respect to boundary issues the lightweight API is quite different, however the ASN.1 packages and the EC math package are the same.

Release

Name: bc-fips-1.0.0.jar

Status: Released 11 November, 2016.

The module is currently tested against the JRE 1.7 and the JRE 1.8. The module is source and byte code compatible back to JDK 1.5.

Planned Releases

1. bc-fips-1.0.1.jar
   patch release of bc-fips-1.0.0 (bug fixes, some improvements)
   - CAVP Lab Testing completed 8th June 2017
   - Lab Code Review completed 7th June 2017

2. bc-fips-1.1.0.jar

Planned Retests

We expect to do a retest of BC FIPS Java 1.0.1 against JDK 1.9 when it is finalised.

Scheduled Additions for BC FIPS 1.1.0:

Support for PKIXRevocationChecker in the CertPath implementation.

Option for SOFT_FAIL style revocation checking flagfor the extended PKIXParameters class.

Approved Mode Algorithms

SHA-3 HMAC

SHA-3 Signature Algorithms: PKCS#1.5, RSA PSS, ECDSA, DSA

SP 800-38G: Methods for format preserving encryption

Additional KAS modes for ephemeral keys.

Non-approved Mode Algorithms

NewHope

SPHINCS-256

ChaCha20

Poly1305

GOST R 34.11-2012

Possible Additions for BC FIPS 1.1.0:

CSHAKE

KMAC