CRYPTO IN JAVA/KOTLIN + BOUNCYCASTLE

PETER SCHNEIDER

FEB 12, 2020

Created: 2021-02-12 Fr 10:20

1 JAVA CRYPTOGRAPHY ARCHITECTURE (JCA)

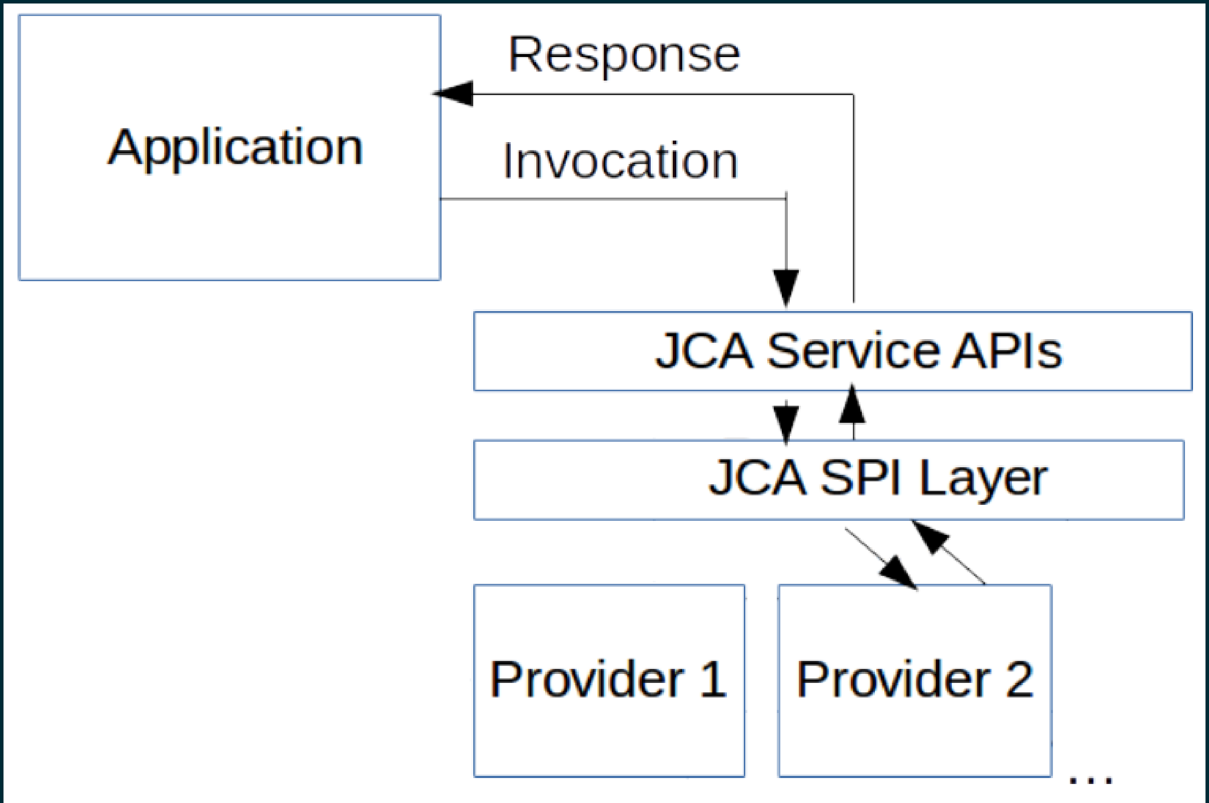

Figure 1: From “Java Cryptography: Tools and Techniques”, David Hook, Jon Eaves

2 ADDING PROVIDERS

```
Security.addProvider(BouncyCastleFIPSProvider())
for (i: Provider in Security.getProviders()) {
    println(i.name)
    println(i.info)
}
```

3 USING CIPHERS

```
val c = Cipher.getInstance("Blowfish")
val d = Cipher.getInstance("Blowfish/CBC/PKCS5Padding", "BC")
d.init(Cipher.ENCRYPT_MODE, key)
d.doFinal(msg)
```

4 BOUNCYCASTLE API ARCHITECTURE

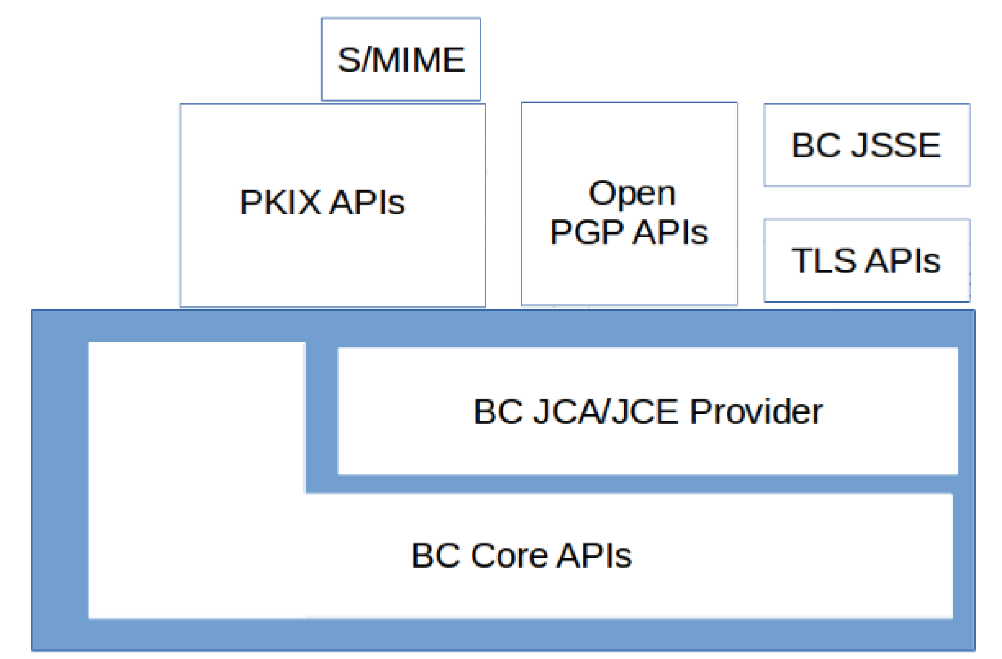

Figure 2: From “Java Cryptography: Tools and Techniques”, David Hook, Jon Eaves https://bouncycastle.org/docs/docs1.5on/index.html

5 GRADLE DEPENDENCY

check your dependencies in `app/build.gradle.kts`

```
dependencies {
    // Align versions of all Kotlin components
    implementation(platform("org.jetbrains.kotlin:kotlin-bom"))
    // User Cbor serialization
    implementation("org.jetbrains.kotlinx:kotlinx-serialization-cbor:1.0.1")
    // Use Bouncycastle FIPS version 1.0.2
    implementation("org.bouncycastle:bc-fips:1.0.2")
}
```