KEYFACTOR

DATASHEET

Bouncy Castle Support

Get support for Bouncy Castle APIs, right from the developers.

Bouncy Castle is trusted around the world as one of the most widely used FIPS-certified open-source Java/C# cryptographic APIs.

Bouncy Castle was originally founded in the year 2000 and now combines FIPS 140-3 certifications and an Open-Source license.

The APIs provide a cost-effective and efficient way to introduce certified cryptography to your applications and platforms.

Keyfactor support services will help your developers effectively use Bouncy Castle APIs by accelerating their problem-solving and dealing with any needed customization issues, allowing you and your team to focus on developing the optimal solution for the problem your application is trying to solve. Overcome any hurdles that arise when using the APIs with direct support from people with extensive Bouncy Castle projects knowledge and who are current committers to the project.

Support options

Keyfactor provides support services directly to you from the Bouncy Castle API maintainers. Our support comes in three different packages designed for the needs of small development teams and Enterprise organizations.

Entry

Entry-level support offers 24 hour response time and up to 20 hours of support directly from the developers behind Bouncy Castle APIs, so your team can get the help they need to implement, update and maintain Bouncy Castle. Includes early access to FIPS and LTS API releases.

Development

Ideal for development teams that require faster response times and more support hours, development support offers 12 hour response, up to 50 hours of support, as well as early access to FIPS and LTS API releases.

Enterprise

Enterprise support provides prioritized response, up to 100 hours of support from Bouncy Castle experts for unlimited contacts within the same domain, as well as early access to FIPS and LTS API releases.

Support services provide:

Long Term Support (LTS) Early Access and Customization Program

Support contract holders have early access to new LTS releases under development, and the ability to request extra features in situations that do not otherwise affect backwards compatibility. LTS releases will be maintained for 5 years, with the first 4 years allowing for the addition of extra features and security updates.

Help with Private Label Validation

Companies that need a FIPS certificate tailored to include the vendor's name and product name can do a "Private Label Validation". Support services provide FIPS testing tools in addition to the source of the module and editable drafts of some of the compliance documentation that will be required. Through an arrangement with the Bouncy Castle software Charity organization, Legion of the Bouncy Castle Inc., it is possible to rebrand the Bouncy Castle FIPS certificate for the module you are using for an additional fee, accelerating the time required to get your own certificate.

Help with Problem-Solving and API Usage

Access help from the long term developers of the Bouncy Castle project to get answers quickly. If a bug in the BC APIs is causing an issue, have it rapidly identified and permanently fixed upstream, rather than maintaining your own patches. Get help migrating from the general Bouncy Castle Library to the FIPS ones or other general releases.

Consulting Hours

All support contracts come with consulting hours to help deal with those situations where you need a custom addition made to the APIs or you need a member of our team to assist with code directly.

The FIPS Early Access Program

Access the development code base for the Bouncy Castle FIPS APIs, and other support libraries, such as for TLS, CMS, X.509 certificates and other IETF protocols. Including the latest Bouncy Castle FIPS modules going through the NIST submission process, enabling you to trial the release against your environment and applications in preparation for the module's final release.

Complete List of Bouncy Castle APIs Specifications and Interoperability ↗

https://www.bouncycastle.org/documentation/specification_interoperability/

Technical Specifications

The Bouncy Castle APIs include core cryptography support and a suite of APIs for using standard protocols to build applications. NIST standard algorithms are supported, including the new secure post-quantum algorithms.

- Lightweight Cryptography APIs for Java and C#
- FIPS 140-2 and FIPS 140-3 releases, LTS releases and non-FIPS releases
- Provider for the Java Cryptography Extension (JCE) and the Java Cryptography Architecture (JCA) for both FIPS and non-FIPS applications
- Provider for the Java Secure Socket Extension (JSSE) for both FIPS and non-FIPS applications

Additional protocol and service support:

- APIs for Cryptographic Message Syntax (CMS/ PKCS#7) and Secure MIME (S/MIME)
- APIs for OpenPGP, including the KeyBox format
- Extended API support for TLS and DTLS
- APIs for supporting certificate generation and certificate request generation using X.509, PKCS#10, CRMF, EST, and CMP.
- APIs for supporting certificate revocation using CRLs and OCSP
- APIs for key storage formats such as PKCS#12 and BCFKS
- APIs for supporting Time-Stamp Protocol (TSP) and Evidence Records (ERS)
- NIST standard secure post-quantum algorithms, including the round 4 candidates