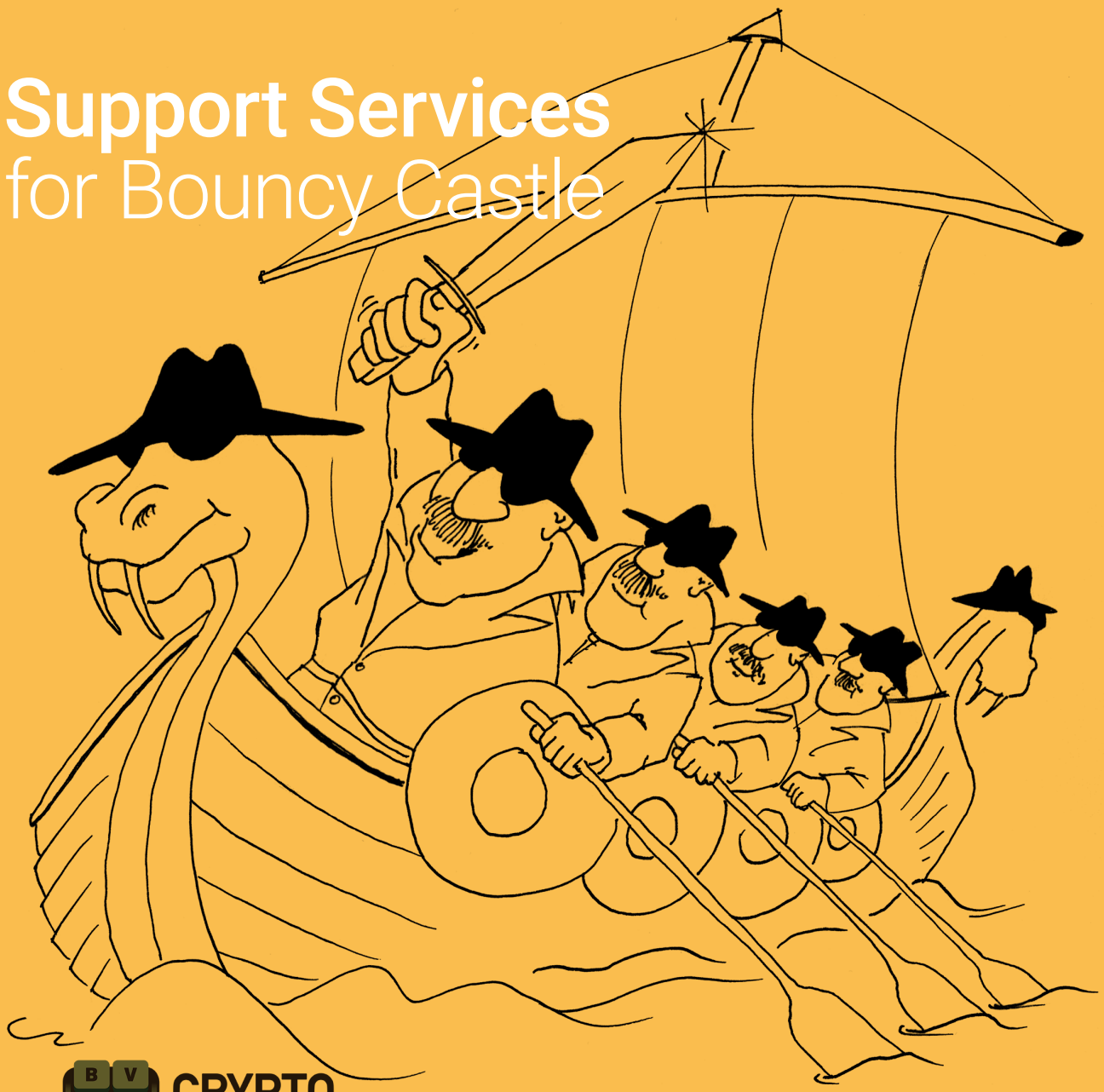
Support Services for Bouncy Castle



CRYPTO WORKSHOP

Support and FIPS Early Access

Bouncy Castle is one of the most widely used FIPS-certified crypto APIs for Java and C#. With PrimeKey Support Services, you will overcome any obstacles that arise when using the APIs with direct support from the people who understand Bouncy Castle Projects.

PrimeKey®

Bouncy Castle Support and FIPS Early Access

PrimeKey support services give you the ability to make more effective use of the Bouncy Castle APIs by accelerating problem solving and dealing with customization issues, allowing you and your team to concentrate on developing your optimal solution.

Bouncy Castle
As one of the most widely used FIPS-certified Java/C# libraries, Bouncy Castle is trusted around the globe. It is used in diverse cases, including being the basis for Java Cryptography in Android and in applications such as the Australian Government's AUSKey project. Bouncy Castle was founded in 2000 and now combines FIPS and an Open Source license. The APIs provide a cost-effective and efficient way to introduce certified cryptography to your applications and platforms.

PrimeKey Support Services for Bouncy Castle
PrimeKey offers two levels of support: Basic and Enterprise. The support is provided directly from the principal maintainers of the Bouncy Castle APIs to you. Our support will enable your developers to clear any road blocks in the use of the APIs by allowing them to deal directly with the people who understand Bouncy Castle Projects.

FIPS Early Access Program
In addition, both Basic and Enterprise support levels offer a FIPS early access program. The program includes developer support and access to the ongoing development code base for the Bouncy Castle FIPS APIs, including those for support libraries such as for TLS, CMS, X.509 certificates and other IETF protocols Bouncy Castle supports. It includes the latest BC FIPS module currently going through the NIST submission process, prior to its final release, as well as testing tools for validating the module and drafts of some of the compliance documentation required to do validations for yourself.

Crypto Workshop was acquired by PrimeKey in 2020

Crypto Workshop was established as the commercial wing of the Bouncy Castle project when the Australian software charity, Legion of the Bouncy Castle Inc., was officially incorporated in 2012. The company is responsible for managing on-going development and certification of the Bouncy Castle APIs. In 2020, PrimeKey acquired Crypto Workshop. The two organizations share common commitments to Open Source, open standards, and their shared community. PrimeKey has been a user of the Bouncy Castle APIs since the earliest days of EJBCA and it was the desire to fully secure our supply chain, as well as that of our customers, that led us to propose acquisition of Crypto Workshop.

David Hook, Crypto Workshop Founder, presenting at PrimeKey Tech Days 2019

Comprehensive Support

Two options for your choosing
Find a support solution that best reflects the way your organization uses the Bouncy Castle APIs. Choose between two support solutions: Basic and Enterprise.

Basic support is good for a single development team and limited to 2 named contacts in an organization and a single access point to the FIPS early access program.

Enterprise support is designed to support multiple teams and developers across an organization and allows domain based contacts to enter support requests and their issues dealt with. Enterprise support also includes 10 access points to the FIPS early access program and offers priority over Basic support and a faster response time.

In addition to access to the pre-certified FIPS modules, the FIPS early access program includes test harnesses as well as drafts for some of the compliance documentation required for certification.

Technical specifications

The Bouncy Castle APIs include both core cryptography support and a suite of APIs for using standard protocols to help build applications. The NIST standard algorithms are supported and there is additional support for a range of other international standards as well.

Core Cryptography Support:
- Lightweight cryptography APIs for Java and C# for FIPS and non-FIPS applications
- 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, CMP, CMS, and S/MIME
- APIs for supporting certificate revocation using CRLs and OCSP
- APIs for key storage formats such as PKCS#12
- APIs for supporting Time Stamp Protocol (TSP)
- APIs for supporting Extended Access Control (EAC), Data Validation and Certification Server (DVCS), and DNS-based Authentication of Named Entities (DANE)

About PrimeKey

PrimeKey is one of the world's leading companies for PKI solutions and has developed successful solutions, such as EJBCA Enterprise, SignServer Enterprise, PKI Appliance and PrimeKey SEE. As a pioneer in open source security software, PrimeKey provides businesses and organizations around the world with the ability to implement security solutions, such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation. Our products are Common Criteria and FIPS certified. We have numerous Webtrust/ETSI and eIDAS audited installations, and our internal processes are ISO 9001, 14001, and 27001 certified.

PrimeKey has offices in Stockholm, Sweden; Aachen, Germany; San Mateo, USA; and Melbourne, Australia. Together with our global network of technology and reselling partners, we are proud to count many of the industry leading companies and institutions within IT, Telecom, Banking, Industrial, Public CAs, and different branches of government as our long-time customers.

Contact
sales@primekey.com
www.primekey.com
Europe: +46 85 221-1660
USA: +1 (855) 583-7971

PrimeKey Headquarters
Sundbybergsvägen 1
SE-171 73 Solna
Sweden

PrimeKey Labs
Krantzstr. 7
52070 Aachen
Germany

C2 – A PrimeKey company
951 Mariners Island Blvd
San Mateo, CA 94404
USA

Crypto Workshop – A PrimeKey company
520 Bourke Street, Level 2
Melbourne, VIC 3000
Australia

PrimeKey®