The Legion of the Bouncy Castle

- entry
- wiki
- issue tracker
- Java home
- C# home
- Object Identifiers

english français

WELCOME

Welcome to the home of the **Legion of the Bouncy Castle**. A fun place to stay, if you've got some time to kill.

Here at the Bouncy Castle, we believe in encryption. That's something that's near and dear to our hearts. We believe so strongly in encryption, that we've gone to the effort to provide some for everybody, and we've now been doing it for over 10 years!

The **Bouncy Castle Crypto APIs** consist of the following:

- A lightweight cryptography API for Java and C#.
- A provider for the Java Cryptography Extension and the Java Cryptography Architecture.
- A clean room implementation of the JCE 1.2.1.
- A library for reading and writing encoded ASN.1 objects.
- Lightweight APIs for TLS (RFC 2246, RFC 4346) and DTLS (RFC 4347).
- Generators for Version 1 and Version 3 X.509 certificates, Version 2 CRLs, and PKCS12 files.

NEWS

This release adds support for server/client side TLS 1.1 and server/client side DTLS 1.0, the SipHash MAC algorithm, the 4 DRBGs specified in NIST SP 800-90A, and the GMAC algorithm (NIST SP 800-38D). In addition, it is now possible to store OCSP objects in CMS SignedData, parameter and key generation is now fully supported for the keys sizes specified in DSA 2, and support has been added for the SHA-512/t digest variants. A number of bugs and an encoding regression with T61 Strings have also been fixed.

For more details go to our latest releases page, to download the new version and see the release notes

You can also find the latest versions on one of our mirrors:

- polydistortion.net

C# Release 1.7 is now out!

Thursday 7th April 2011

This release adds client authentication to the TLS package, in addition to compression and ECC cipher suites. The library can now also be built for Silverlight (2.0 and above) and support classes have been added for the ASN.1 structures in CRMF (RFC 4211) and CMP (RFC 4210).

If you are interested you can find it at our C# pages.

The Bouncy Castle Wiki is now up.

Wednesday 1st November

We now have a wiki for providing additional documentation. You can find it at http://www.bouncycastle.org/wiki.

- Generators for Version 2 X.509 attribute certificates.
- Generators/Processors for S/MIME and CMS (PKCS7/RFC 3852).
- Generators/Processors for OCSP (RFC 2560).
- Generators/Processors for TSP (RFC 3161 & RFC 5544).
- Generators/Processors for CMP and CRMF (RFC 4210 & RFC 4211).
- Generators/Processors for OpenPGP (RFC 4880).
- Generators/Processors for Extended Access Control (EAC).
- Generators/Processors for Data Validation and Certification Server (DVCS) - RFC 3029.
- A signed jar version suitable for JDK 1.4-1.7 and the Sun JCE.

The lightweight API works with everything from the J2ME to the JDK 1.7 and there is also an API in C# providing equivalent functionality for most of the above.

For further details have a look in either our Java project pages or our C# project pages where you can find downloads, mailing lists, and other resources.

If you want to provide feedback, offers of jobs (or more importantly beer) directly to the members of **The Legion** then please use feedback-crypto@bouncycastle.org

- Site hosted by Tau Ceti Co-operative Ltd.
- Graphics provided by Geoff Hook.
- Layout and design by Travis Winters.
- Java and JCE are registered trademarks of Oracle ®.
- C# is a registered trademark of Microsoft ®.