The TOP 10 Reasons
You Should Choose SafeLogic
Instead of Open Source Encryption

1

You are instantly FIPS compliant with SafeLogic.

Getting open source encryption to pass FIPS 140-2 testing is notoriously difficult. If you use SafeLogic, the already-validated CryptoComply library is at the core of the installation, even if you use open source components or upstream architecture. As a result, you can immediately reference SafeLogic's certificate, if you're in a pinch.

2

SafeLogic includes strong integration and technical support.

We use a familiar, easy-to-use support ticketing system for your ease of use and peace of mind. Good luck getting any questions answered by email, phone or carrier pigeon from the skeleton crew working on the open source projects (often just volunteers).

3

You get RapidCert, a full FIPS 140-2 validation in your name in approximately 8 weeks.

Nobody else can provide that! Open source options, like the other proprietary modules available, are just software alone and still take over a year to shepherd through the validation process, with the help of expensive consultants.

4

SafeLogic yields major cost savings on the FIPS 140-2 validation effort.

First you add up the cost of the consulting services, lab testing and the NIST fees for certification. Next, you must quantify the hours spent by your engineering team on the FIPS-compliant builds, the documentation effort, and the technical support for the algorithm and module testing, plus the time spent interfacing with the lab and consultants. Those hours were subtracted from your engineers' core activities, slowing down product development and hindering support activities, which incurs costs in other ways as well. Finally, you must calculate the opportunity cost of waiting 12-14 months for your FIPS 140-2 validation. How many more sales would have been made if you had your certificate in hand at 8 weeks?

5

Your team won't have to complete any more stressful module rebuilds.

SafeLogic takes care of the updates each time an upstream patch is released (for OpenSSL, for example). We recompile as needed, test it, confirm that compliance has been maintained, and push it out to you automatically.

© 2016 SafeLogic Inc.

6
You will receive immediate, dynamic, effortless updates to certified platforms.

New version of iOS coming out, for example? No problem. SafeLogic handles the testing so that your module always works and your validation always reflects the updated operating environment as soon as possible. You'll always be validated, unlike your competitors who have to start from scratch with their consultant each time, or wait and hope that someone will do a communal open source certification. Either way, their validation will be practically obsolete before it is even complete while yours is dynamic with no extra effort from your team.

7
You won't be stuck with proprietary lock-in when you choose SafeLogic.

Open source compatibility goes both directions! If you are unsatisfied with CryptoComply for any reason, you can remove the library and revert to a standard open source library within an hour. Other modules hold you hostage by requiring a full stack rebuild in order to uninstall.

8
Your FIPS 140-2 validation will show your company's name and specific details.

If you point to a communal open source certificate, there is no verification process. SafeLogic's RapidCert eliminates the ambiguity and you won't have to ask customers to 'just trust you' that the libraries are being used correctly, in compliance, and on validated platforms.

9
SafeLogic offers flexibility and accommodates various architectures.

SafeLogic's technical team is experienced in troubleshooting a variety of integration complications that open source teams simply ignore. CryptoComply is available with connectors to suit the customer's needs, alternative delivery formats, such as RPM, as requested, and SafeLogic has the flexibility and agility to deliver new solutions quickly.

10
You will avoid the stigma of open source encryption.

The stark reality is that open source encryption doesn't have the best reputation, thanks to a multitude of recent vulnerabilities. You don't have to admit that you're still using open source - just tell your customers that it's CryptoComply by SafeLogic. The perceived value of the upgrade is huge.

SafeLogic was established in 2012, is privately held, and is headquartered in Palo Alto, California. Contact us immediately for more information!

530 Lytton Ave, Suite 200
Palo Alto, CA 94301
(844) 4-ENCRYPTION
@SafeLogic
info@SafeLogic.com
www.SafeLogic.com

OpenSSL ➡ CryptoComply

Bouncy Castle ➡ CryptoComply for Java

SafeLogic Is Focused on Crypto

SafeLogic provides strong encryption products for solutions in mobile, server, Cloud, appliance, wearable, and IoT environments that are pursuing compliance to strict regulatory requirements. Our flagship product, CryptoComply, offers:

- Full FIPS 140-2 validation
- Drop-in compatibility options for OpenSSL & Bouncy Castle
- Suite B algorithms
- Various connectors to accommodate unique product architectures
- Instant compliance for federal deployments
- FIPS 140-2 validation in customer's name with:
    - Accelerated timeline
    - No additional engineering effort
    - Zero interaction with testing labs
    - Fixed cost

TESTED PLATFORMS
CryptoComply offers FIPS 140-2 encryption for:

- Apple iOS
- Apple Mac OS X
- Android
- Microsoft Windows
- Linux
- Others by Request

SafeLogic customers include some of the largest and most innovative technology companies in the world.

SUPPORTED STANDARDS

- FIPS 140-2
- FIPS 180-4
- FIPS 186-2
- FIPS 186-4
- FIPS 197
- FIPS 198
- PKCS#1
- RSASSA-PSS
- SP 800-38
- SP 800-67
- SP 800-90

ROBUST ALGORITHM SUPPORT
CryptoComply offers a variety of Suite B and FIPS-approved algorithms:

- AES 128, 192, 256 (ECB, CBC, CFB1, CFB8, OFB, CTR, CCM, CMAC, GCM, GMAC, XTS)
- TDES (ECB, CBC, CFB1, CFB8, CFB64, OFB, CMAC)
- SHA1, SHA-224, SHA-256, SHA-384, SHA-512
- HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512
- DH, ECDH, DSA, DSA2, RSA, ECDSA, ECDSA2
- RNG: SP 800-90 DRBG

SafeLogic was established in 2012, is privately held, and is headquartered in Palo Alto.

SafeLogic