

Leveraging OpenSSL

Building Compliance Confidence

Jaroslav Reznik

Products Security Compliance

What we'll discuss today

- ▶ How Red Hat leverage OpenSSL in compliance activities.
- ▶ How you could leverage OpenSSL in your compliance activities.
- ▶ A proposal!
- ▶ To be revealed :)



How Red Hat leverage OpenSSL in compliance activities.



OpenSSL in Red Hat's compliance activities

- ▶ Red Hat's own FIPS 140-2 and 140-3 validations.
 - RHEL 9 and newer all modules FIPS 140-3, OpenSSL uses the upstream FIPS provider, minor changes to the upstream.
 - FIPS 140 is a requirement for FedRAMP.
- ▶ Current status
 - RHEL 8: FIPS 140-2 for openssl-1.1.1k-12.el8_9 as #4642
 - RHEL 9 and 10: FIPS 140-3 for openssl-fips-provider-3.0.7-6.el9 as #4857 (RHEL 10 pending OE update)

Source:

<https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/4642>

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4857>



Where OpenSSL is used?

- ▶ Golang in OpenShift through OpenSSL C bindings (replacing BoringSSL).
 - This will change with upstream's Golang Crypto FIPS validation.
- ▶ RHEL & Common Criteria (OSPP)
 - A lot of functionality depends on OpenSSL.



How you could leverage
OpenSSL in your
compliance activities.



Module rebranding

1733 7.1.8 Rebrand (RBND)

1734 This scenario applies if there are no modifications to a module and the new module is a re-
1735 branding of an already validated Original Equipment Manufacturer (OEM) module. The CSTL
1736 **shall:**

- 1737 1. determine that the re-branded module is identical to the OEM module (n.b. this
1738 requirement applies equally to open source and non-open-source modules).
- 1739 2. include the OEM's written approval for re-branding in the submission package which
1740 **shall** note the terms of permission (e.g., subsequent addition of OEs, possible re-use of
1741 CAVP certificates, entropy, non-security relevant changes, remediation of CVE, whether
1742 a rebrand of a rebrand is acceptable, etc.) including who owns/controls the codebase and
1743 is responsible for updates to it post validation. E.g., if these terms do not explicitly allow
1744 a vendor to further rebrand the OEM module, then a rebrand of that rebranded module is
1745 not permitted unless written permission is granted by the OEM.
- 1746 3. (for modules containing any open-source licensed code) ensure the open-source licensing
1747 requirements are met (e.g., any required notices are contained in the Security Policy).



Do I have to rebrand?

**NO, YOU DON'T
HAVE TO!**



Do I have to rebrand?



Module rebranding

- ▶ It is perfectly ok to use distribution/upstream modules as posted on the CMVP website on the list of validated modules – if hardware platform matches.
- ▶ Do your own FIPS 140-3 validation.

HOWEVER

Rebranding with Red Hat will give you



Module rebranding

Fast track to regulated markets

- Own FIPS 140-3 validation may take years.
- Own FIPS 140-3 validation is expensive.
 - SMEs costs.
 - Lab costs.



Module rebranding

- ▶ If you use RHEL or any Red Hat's layered products, talk to me!
 - Red Hat offers rebranding of the OpenSSL module free of charge as long as OE is Red Hat's product.
 - Lab fees not included.
- ▶ If you use other Linux distribution, talk to your distribution! Some do rebrandings.
- ▶ If you use upstream OpenSSL, talk to OpenSSL Corporation.



Module rebranding – limitations

- ▶ Interim certificates are NOT eligible for rebranding.
- ▶ FIPS 140-2 to sunset in September 2026 but rebrandings may not be possible even before.
- ▶ Vendor affirmation vs full validation on your hardware platform.
- ▶ Vendor affirmation can be leveraged instead of rebranding.



A proposal.



Where is the problem?

- ▶ Compliance is usually an expensive and slow moving process.
- ▶ There's a proliferation of different standards, certifications and regulations across the globe.
- ▶ No competition until certificates are issued.



Where is the problem?

- ▶ Compliance is usually an expensive and slow moving process.
- ▶ There's a proliferation of different standards, certifications and regulations across the globe.
- ▶ No competition until certificates are issued.



Where is the problem?

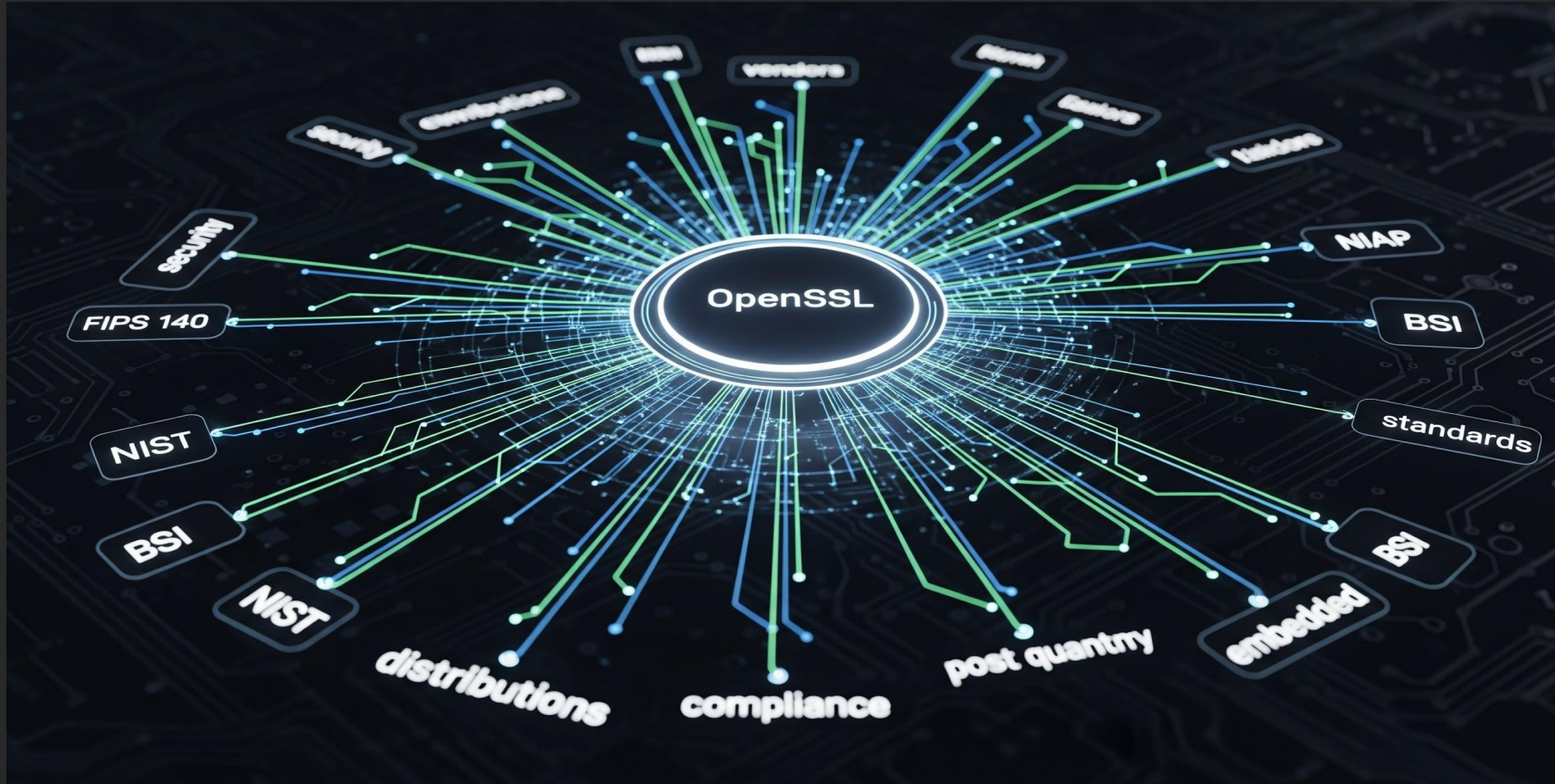


Why OpenSSL?

- ▶ OpenSSL is (very often) in the centre of every compliance activity.
- ▶ Do you want to see a proof?
 - Wednesday, October 8 - **The Use of OpenSSL in Common Criteria and FIPS 140 Certifications** by Martin Ukrop, Vladimir Penaz



Why OpenSSL?



FIPS 140

- ▶ FIPS provider!!!
- ▶ Automation
 - Algorithm validations (for example Stephan Mueller's ACVP Parser)
 - Module validations in the future?
- ▶ Mutual agreement between vendors and labs, no more conflicting understandings of requirements.
- ▶ Kryoptic module

Source:

<https://github.com/smuellerDD/acvpparser>

<https://github.com/latchset/kryoptic>



Common Criteria

- ▶ Used for cryptography (and algorithm certificates required by NIAP)
- ▶ Usef for TLS
 - And for example TLS FP 2.1 (NIAP)
- ▶ Vulnerabilities
 - Aka the famous 0 known CVEs rule
- ▶ Lab's test environments



Cyber Resilience Act (CRA)

- ▶ CRA will have impact on **every** so-called “product with digital elements” in the EU
- ▶ Open source communities stepped up and made open source possible under CRA
- ▶ Open source stewards? How OpenSSL will handle stewardship?
- ▶ An open source communities presence is still needed, we need OpenSSL Foundation/Corporation to step in
 - Harmonized vertical (ETSI) and horizontal (CEN/CENELEC) standards are just being drafted



What can we do as a community?

- ▶ Work together! And we have to coordinate.
- ▶ Do we need a Compliance (sub)community?
 - It should be vertical across Distribution, Small businesses and Large businesses communities (with impact on Academia and Committers).
- ▶ Share certification artifacts, configuration etc.



What can we do as a community?

- ▶ Participate in coordinated open source compliance/security efforts
 - OpenSSF under Linux Foundation,
 - Open Regulatory Compliance (ORC) Working Group under Eclipse Foundation.
 - CRA standardization
 - CEN/CENELEC, ETSI.
 - Talk to your MEPs about open source security and compliance!



Everyone wins!

- ▶ OpenSSL project
 - OpenSSL will foster its dominance among libraries.
- ▶ Vendors
 - Fast to the market, no more “stamp” blockers.
- ▶ Labs
 - More validations coming from more vendors.
- ▶ Regulators
 - Real security, no outdated OpenSSL with a stamp!





Talk to me!

jreznik@redhat.com



Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHat