Red Hat
Enterprise Linux

OpenSSL in RHEL: FIPS-140-3 certification

From FIPS-140-2 upstream to FIPS-140-3 downstream

Dmitry Belyavskiy
Senior Software Engineer

Red Hat

Who I am

Dmitry Belyavskiy
Red Hat Senior Software Engineer since 2020

OpenSSL committer since 2019
OpenSSL Technical Committee member since 2021

Beloved pet project: Russian GOST engine for OpenSSL
https://github.com/gost-engine/engine

Some necessary context

What is FIPS and FIPS certification

Red Hat FIPS certification

OpenSSL 3.0 architecture changes

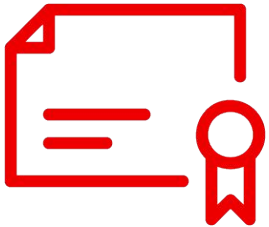
What is FIPS and FIPS certification

FIPS standards: code of laws
It is big, not all documents are public, permanently updated

FIPS certification process: technological process
Done by accredited labs. We provide code, they do tests

Required by US government
Current version: FIPS-140-3

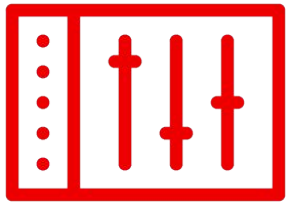
Red Hat FIPS certification



What do we certify
Kernel and crucial low level crypto libraries

Certification details: RHEL 8
How RHEL 8 is designed for FIPS 140-2 requirements

OpenSSL 3.0 architecture changes



Upstream approach
1.0 series: invasive runtime checks

RHEL 8: 1.1.1 series
Set of patches to libcrypto/libssl
Even more invasive run-time checks

OpenSSL 3.0
Provider model
Compile-time checks
Mass API deprecation

Our patches

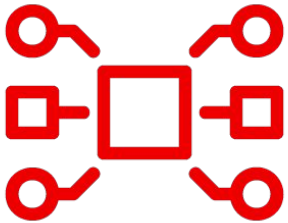
Loading and configuring the provider

Red Hat specific: indicators

Implementation details

Overall hardening

Loading and configuring the provider



Upstream approach
Loading via configuration file
Checksum as a part of configuration file

RHEL approach
Auto activation
Embedded checksum
FIPS-only algorithms

Concept of indicators

Why indicators?

Many algorithms, many combinations, many parameters, not all are approved.

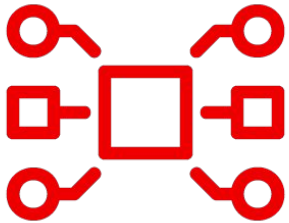
Implicit indicators

You try a crypto operation. If you failed, it is not approved. If it is successful, you are OK.

Explicit indicators

You try a crypto operation. If you failed, it is not approved. If it is successful, you check if it was approved.

Implementation details



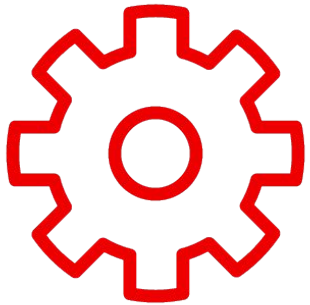
Not approved algorithms
No Edwards curves
No RSA PKCS#1 encryption
No 3DES

KAT tests
Deterministic tests for ECDSA signatures

Strict checks
KDF seed length
RNG algorithms limitation

Hardening
Checks and cleanup of public keys

Overall hardening



Crypto policies
Consistent list of algorithms for all libraries and applications

SHA1 is significantly limited
FIPS standards formally permit

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

Red Hat