Ruby - Misc #19608

Being a co-maintainer of the ruby/openssl for the OpenSSL FIPS mode

04/18/2023 01:07 PM - jaruga (Jun Aruga)

Status:	Closed	
Priority:	Normal	
Assignee:	matz (Yukihiro Matsumoto)	

Description

Motivation and context

Recently I have been working for the ruby/openssl to support OpenSSL 3 FIPS mode such as sending pull-requests and reporting issues to the OpenSSL project. The related issue ticket is here.

Currently a challenge of the ruby/openssl is that it doesn't work well on the OpenSSL FIPS mode, and I want ruby/openssl to work on it by adding the OpenSSL 3 FIPS mode case to the CI, and by adding more FIPS related unit tests and features. To solve this challenge, I would like to be a co-maintainer of the ruby/openssl for the FIPS mode related things. What do you think?

What is FIPS mode?

For someone who is interested in knowing the FIPS mode. Let me share the related documents below. In my understanding, FIPS mode is a security policy developed by US government. In some cases, the shipped Linux OS systems need to follow this policy. And OpenSSL has a feature to enable the FIPS mode. The README is here. And there can be FIPS specific issues in the ruby/openssl with the OpenSSL FIPS mode enabled.

FIPS related documents:

- FIPS Wikipedia
- Red Hat Enterprise Linux (RHEL)
- Amazon Linux
- SUSE Linux
- Ubuntu

Past FIPS related issue tickets

As a reference, I just found some old issue tickets below. It is about OpenSSL 1.0 and 1.1 FIPS mode.

- https://bugs.ruby-lang.org/issues/6946
- https://bugs.ruby-lang.org/issues/19073

History

#1 - 04/18/2023 01:53 PM - jaruga (Jun Aruga)

- Description updated

#2 - 04/19/2023 02:06 AM - hsbt (Hiroshi SHIBATA)

- Status changed from Open to Assigned

- Assignee set to matz (Yukihiro Matsumoto)

+1

I'll support @jaruga (Jun Aruga) if you need extra permissions of our resources.

#3 - 04/21/2023 12:50 PM - jaruga (Jun Aruga)

@hsbt (Hiroshi SHIBATA) thanks for your help!

Everyone, any other comments?

#4 - 04/24/2023 03:20 PM - jaruga (Jun Aruga)

- Description updated

#5 - 05/09/2023 09:01 AM - jaruga (Jun Aruga)

For someone who is interested in how to debug the ruby/openssl with OpenSSL 3 FIPS mode, I created a document about the topic below.

https://hackmd.io/@jaruga/ryDnksRm2

#6 - 05/10/2023 12:00 PM - hsbt (Hiroshi SHIBATA)

In Dev Meeting 5/10 at Matsumoto, no one objects this proposal.

#7 - 05/15/2023 12:47 PM - jaruga (Jun Aruga)

Thank you for discussing the topic in the meeting.
I started to work as a co-maintainer of the ruby/openssl for the FIPS mode.

#8 - 05/16/2023 08:42 AM - hsbt (Hiroshi SHIBATA)

- Status changed from Assigned to Closed

Thank you. If you have any issue, please notify me.