Ruby - Bug #6939

Uninformative exception in FIPS mode

08/28/2012 12:36 AM - vo.x (Vit Ondruch)

Status:	Third Party's Issue		
Priority:	Normal		
Assignee:	MartinBosslet (Martin Bosslet)		
Target version:			
ruby -v:	trunk	**Backport:**	

Description

cat /proc/sys/crypto/fips_enabled

1
]# irb
irb(main):001:0> require 'openssl'
=> true
irb(main):002:0> OpenSSL::PKey::DH.new(1024)
=> -----BEGIN DH PARAMETERS-----
MIGHAoGBAMjWrD9U8wfqxMEMPBaBnihhTJb6CGgy7Auy1Aark27nFER3RuYY4ZXC
2lZ11/mDhyymW/LPNr8cupYgs5AsZttguT/zhpr6j2sobnjkcvj8T6FkQ42TC4Dw
PS+O+Mdvz1BP8ZUWXV8QBxyxCKCanPVWvPGI8tC5amj9QM66VyUTAgEC
-----END DH PARAMETERS-----

irb(main):003:0> OpenSSL::PKey::DH.new(128)
OpenSSL::PKey::DHError: BN lib
from (irb):3:in initialize' from (irb):3:in new'
from (irb):3
from /bin/irb:12:in `'
irb(main):004:0>

Could you please provide better exception message? While it is fine that DH.new fails with short key, it is not obvious from the message what is the reason. Thank you.

History

#1 - 08/28/2012 01:02 AM - vo.x (Vit Ondruch)

- Assignee changed from duerst (Martin Dürst) to MartinBosslet (Martin Bosslet)

#2 - 08/28/2012 02:01 AM - MartinBosslet (Martin Bosslet)

I'm not sure whether this is possible at all - the message being generated is what OpenSSL itself generates at this point. I'd have to check if there is a reliable way to detect whether we are in FIPS mode or not. Still, I'd prefer if OpenSSL itself provided a better exception message.

#3 - 08/29/2012 04:20 AM - MartinBosslet (Martin Bosslet)

- Status changed from Open to Assigned

#4 - 12/20/2012 10:22 AM - MartinBosslet (Martin Bosslet)

- Status changed from Assigned to Third Party's Issue

This is indeed a third party issue. The exception message (or better, the lack thereof) is generated by OpenSSL. They're fine for RSA, DSA and EC ("key too short"), but miserable for DH, agreed.

I really wouldn't want to start to improve OpenSSL error messages in the Ruby extension, that's not where this belongs IMHO. We could try to open an issue on the OpenSSL tracker, though.

Closing as TPI for now, please feel free to reopen if your opinions differ from mine.

#5 - 12/20/2012 04:11 PM - vo.x (Vit Ondruch)

MartinBosslet (Martin Bosslet) wrote:

> We could try to open an issue on the OpenSSL tracker, though.

Would be cool if you can do this.