

Ruby master - Bug #4879

test_new(OpenSSL::TestPKeyRSA) fails on Win32

06/14/2011 02:11 AM - arton (Akio Tajima)

Status: Closed	
Priority: Normal	
Assignee: MartinBosslet (Martin Bosslet)	
Target version: 1.9.3	
ruby -v: -	Backport:

Description

#####

openssl\test_pkey_rsa.rb:48 fail##### Visual C++10 #####

1) Failure:

test_new(OpenSSL::TestPKeyRSA) [C:/Users/arton/Documents/ruby/trunk/test/openssl/test_pkey_rsa.rb:48]:

<[]> expected but was

<["error:0906D06C:PEM routines:PEM_read_bio:no start line"]>.

#####

Ruby#####

irb(main):001:0> require 'openssl'

=> true

irb(main):002:0> key = OpenSSL::PKey::RSA.new 512

=> -----BEGIN RSA PRIVATE KEY-----

MIIBOgIBAAJBAMuc7mPnOVmPweq1XMZrOZaOMVoTCX88fsU4460qF0me4S+yGL90

([])

-----END RSA PRIVATE KEY-----

irb(main):003:0> pem = key.public_key.to_pem

=> "-----BEGIN PUBLIC KEY-----\nMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMuc7mPnOVmPweq1

XMZrOZaOMVoTCX88nfsU4460qF0me4S+yGL902+yR5Gv2R6B4QvE5EnxGY5zD9t355+IKaQMCAwEAAQ

==\n-----END PUBLIC KEY-----\n"

irb(main):004:0> OpenSSL::PKey::RSA.new pem

=> -----BEGIN PUBLIC KEY-----

MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMuc7mPnOVmPweq1XMZrOZaOMVoTCX88

fsU4460qF0me4S+yGL902+yR5Gv2R6B4QvE5EnxGY5zD9t355+IKaQMCAwEAAQ==

-----END PUBLIC KEY-----

irb(main):005:0> OpenSSL.errors

=> []

#####test_new#####test_new#####

def test_new

\$stderr.puts OpenSSL.errors.inspect

\$stderr.flush

key = OpenSSL::PKey::RSA.new 512

pem = key.public_key.to_pem

OpenSSL::PKey::RSA.new pem

assert_equal([], OpenSSL.errors)

end

#####fail#####

.....["error:0D07803A:asn1 e

ncoding routines:ASN1_ITEM_EX_D2I:nested asn1 error"]...([])

OpenSSL 1.0.0a

irb(main):001:0> require 'openssl'

=> true

irb(main):002:0> OpenSSL::OPENSSL_VERSION

=> "OpenSSL 1.0.0a 1 Jun 2010"

Related issues:

Related to Ruby master - Bug #4885: [ext/openssl] Use BIO_reset and ERR_get_e...

Closed

06/14/2011

Associated revisions

Revision bfa6c6b4 - 06/14/2011 01:38 AM - naruse (Yui NARUSE)

Clear error messages before process and get errors. [ruby-dev:43791] [Bug #4879]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@32076 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 32076 - 06/14/2011 01:38 AM - naruse (Yui NARUSE)

Clear error messages before process and get errors. [ruby-dev:43791] [Bug #4879]

Revision 32076 - 06/14/2011 01:38 AM - naruse (Yui NARUSE)

Clear error messages before process and get errors. [ruby-dev:43791] [Bug #4879]

Revision 32076 - 06/14/2011 01:38 AM - naruse (Yui NARUSE)

Clear error messages before process and get errors. [ruby-dev:43791] [Bug #4879]

Revision 32076 - 06/14/2011 01:38 AM - naruse (Yui NARUSE)

Clear error messages before process and get errors. [ruby-dev:43791] [Bug #4879]

Revision 32076 - 06/14/2011 01:38 AM - naruse (Yui NARUSE)

Clear error messages before process and get errors. [ruby-dev:43791] [Bug #4879]

Revision 32076 - 06/14/2011 01:38 AM - naruse (Yui NARUSE)

Clear error messages before process and get errors. [ruby-dev:43791] [Bug #4879]

History

#1 - 06/14/2011 02:24 AM - jonforums (Jon Forums)

This failure also occurs when building trunk@32072 with MinGW GCC v4.5.2 (TDM) and OpenSSL 1.0.0d:

```
sh-3.1$ make test-all TESTS='openssl fiddle psych'
```

...

1) Failure:

```
test_new(OpenSSL::TestPKeyRSA) [c:/Users/Jon/Documents/RubyDev/ruby-git/test/openssl/test_pkey_rsa.rb:48]:
```

```
<[]> expected but was
```

```
<["error:0906D06C:PEM routines:PEM_read_bio:no start line"]>.
```

```
sh-3.1$ ruby --version
```

```
ruby 1.9.3dev (2011-06-14 trunk 32072) [i386-mingw32]
```

```
sh-3.1$ ruby -ropenssl -e 'puts OpenSSL::OPENSSL_VERSION'
```

```
OpenSSL 1.0.0d 8 Feb 2011
```

#2 - 06/14/2011 02:56 AM - MartinBosslet (Martin Bosslet)

- *Category set to ext*

- *Status changed from Open to Assigned*

- *Assignee set to MartinBosslet (Martin Bosslet)*

Thanks for reporting this! I might have an idea, I'll see what I can find out.

Regards,

Martin

#3 - 06/14/2011 10:38 AM - naruse (Yui NARUSE)

- *Status changed from Assigned to Closed*

- *% Done changed from 0 to 100*

This issue was solved with changeset r32076.

Akio, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

Clear error messages before process and get errors. [ruby-dev:43791] [Bug #4879]

#4 - 06/14/2011 07:27 PM - MartinBosslet (Martin Bosslet)

Thanks, Yui, for the fix!

My guess was that some uncleared error caused this when several tests are run in sequence.

I briefly checked and there are still fallback scenarios in Ruby OpenSSL code where something is first interpreted as PEM and then as DER or the other way round. This way such an error as described is put into OpenSSL's own error queue. Most C code now uses

```
BIO_reset(bio);  
ERR_get_error();
```

in conjunction now. For the those places and the remaining code that does not yet I'd propose to expose this functionality as a public macro and I would use it where appropriate. This would prevent test failures as described here in the future.

What do you think?

Regards,
Martin

PS: I opened a new issue for this (<http://redmine.ruby-lang.org/issues/4885>) so that the others are also aware and can intervene should they have any doubts or objections.

#5 - 06/14/2011 11:57 PM - naruse (Yui NARUSE)

Martin Bosslet wrote:

My guess was that some uncleared error caused this when several tests are run in sequence.

I briefly checked and there are still fallback scenarios in Ruby OpenSSL code where something is first interpreted as PEM and then as DER or the other way round. This way such an error as described is put into OpenSSL's own error queue. Most C code now uses

```
BIO_reset(bio);  
ERR_get_error();
```

in conjunction now. For the those places and the remaining code that does not yet I'd propose to expose this functionality as a public macro and I would use it where appropriate. This would prevent test failures as described here in the future.

What do you think?

I agree with it, such way is suitable than my hack.

#6 - 06/15/2011 01:23 AM - MartinBosslet (Martin Bosslet)

- ruby -v changed from ruby 1.9.3dev (2011-06-13) [i386-mswin32_100] to -

What do you think?

I agree with it, such way is suitable than my hack.

OK, great! I'll implement this then soon.

Thanks,
Martin

#7 - 06/15/2011 01:23 AM - MartinBosslet (Martin Bosslet)

What do you think?

I agree with it, such way is suitable than my hack.

OK, great! I'll implement this then soon.

Thanks,
Martin

#8 - 06/22/2011 05:46 PM - MartinBosslet (Martin Bosslet)

- Status changed from Closed to Feedback

I just committed the fix for <http://redmine.ruby-lang.org/issues/4885>
in revision 32199.

This should solve the issue that was discovered here, and I was also
able to run the tests without Yui's fix.

Could you please confirm that it works for you, too?

Regards,
Martin

#9 - 07/22/2011 09:23 AM - MartinBosslet (Martin Bosslet)

- Status changed from Feedback to Closed

I close this since there have been no further complaints.