Ruby master - Bug #11774

OpenSSL::PKey.read produces ArgumentError on invalid passphrases

12/05/2015 04:54 PM - temikus (Artem Yakimenko)

Status:	Third Party's Issue		
Priority:	Normal		
Assignee:	openssl		
Target version:			
ruby -v:	ruby 2.2.3p173 (2015-08-18 revision 51636) [x86_64-darwin15]	**Backport:**	2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN

Description

If we try to read out an RSA encrypted key with an invalid passphrase like so:

```
require 'openssl'
OpenSSL::PKey.read(File.read("#{ENV['HOME']}/.ssh/id_rsa"), 'invalid')
```

We get an argument error:

```
ArgumentError: Could not parse PKey: no start line
from (pry):6:in `read'
```

However, if I understand the situation correctly, it should produce a decode error: OpenSSL::PKey::RSAError, as per the doc:

> OpenSSL::PKey::RSAError
> Generic exception that is raised if an operation on an RSA PKey fails unexpectedly or in case an instantiation of an instance of RSA fails due to non-conformant input data.

Reproduction:

1. Create a password protected ssh key (if none exists):

   ```
   ssh-keygen -t rsa -b 4096
   ```

2. Run the following snippet (assuming ~/.ssh/id_rsa is the key location)

   ```
   require 'openssl'

   OpenSSL::PKey.read(File.read("#{ENV['HOME']}/.ssh/id_rsa"), 'invalid_passphrase')
   ```

Tested on:
MacOSX 10.11.1
OpenSSL 1.0.2d 9 Jul 2015
Ruby 2.1.7
Ruby 2.2.3

History

#1 - 12/06/2015 06:10 AM - nobu (Nobuyoshi Nakada)

- Description updated

Seems that OpenSSL doesn't tell what kind failure happened.

#2 - 12/07/2015 06:54 AM - ko1 (Koichi Sasada)

- Assignee set to openssl

#3 - 07/03/2016 03:41 AM - rhenium (Kazuki Yamaguchi)

- Status changed from Open to Feedback

OpenSSL does not give the information what type of key is contained in the PEM when an error occurs. So it's impossible to raise PKey::RSAError here.

But for consistency with PKey::{DH,DSA,RSA,EC}.new, it may be better to raise PKey::PKeyError (is the super class of PKey::RSAError) rather than ArgumentError.

https://github.com/ruby/openssl/pull/55

#4 - 11/10/2017 04:33 AM - rhenium (Kazuki Yamaguchi)

- Status changed from Feedback to Third Party's Issue