Ruby master - Feature #4423

[ext/openssl] Allow encryption for PEM-encoding Elliptic Curve private keys

02/22/2011 08:36 AM - MartinBosslet (Martin Bosslet)

Status:	Closed	
Priority:	Normal	
Assignee:	MartinBosslet (Martin Bosslet)	
Target version:	1.9.3	

Description

=begin
There has already been some #if 0-excluded code that would actually take care of this, but it has not been implemented yet. The attached patch allows to encrypt PEM-encoded private keys, Cipher and password are ignored in the case of public keys (rather than raising an error).

The motivation for this patch is that it would provide uniform behavior of all three public key systems supported in Ruby, RSA, DSA (who already support PEM encryption) and now also Elliptic Curve. RDoc has been supplemented.

Regards,
Martin
=end

Associated revisions

Revision f14d97e1 - 05/11/2011 11:05 PM - emboss

Thu May 12 08:01:14 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
    * ext/openssl/ossl_pkey_ec.c: Allow encryption when PEM-encoding
      Elliptic Curve private keys.
      [ruby-core:35329] [Bug #4423]
```

Previous revision: 31525

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@31526 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 31526 - 05/11/2011 11:05 PM - emboss

Thu May 12 08:01:14 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* ext/openssl/ossl_pkey_ec.c: Allow encryption when PEM-encoding
  Elliptic Curve private keys.
  [ruby-core:35329] [Bug #4423]
```

Previous revision: 31525

Revision 31526 - 05/11/2011 11:05 PM - emboss

Thu May 12 08:01:14 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* ext/openssl/ossl_pkey_ec.c: Allow encryption when PEM-encoding
  Elliptic Curve private keys.
  [ruby-core:35329] [Bug #4423]
```

Previous revision: 31525

Revision 31526 - 05/11/2011 11:05 PM - emboss

Thu May 12 08:01:14 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* ext/openssl/ossl_pkey_ec.c: Allow encryption when PEM-encoding
  Elliptic Curve private keys.
  [ruby-core:35329] [Bug #4423]
```

Previous revision: 31525

Revision 31526 - 05/11/2011 11:05 PM - emboss

Thu May 12 08:01:14 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* ext/openssl/ossl_pkey_ec.c: Allow encryption when PEM-encoding
  Elliptic Curve private keys.
  [ruby-core:35329] [Bug #4423]
```

Previous revision: 31525

Revision 31526 - 05/11/2011 11:05 PM - emboss

Thu May 12 08:01:14 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* ext/openssl/ossl_pkey_ec.c: Allow encryption when PEM-encoding
  Elliptic Curve private keys.
  [ruby-core:35329] [Bug #4423]
```

Previous revision: 31525

Revision 31526 - 05/11/2011 11:05 PM - emboss

Thu May 12 08:01:14 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* ext/openssl/ossl_pkey_ec.c: Allow encryption when PEM-encoding
  Elliptic Curve private keys.
  [ruby-core:35329] [Bug #4423]
```

Previous revision: 31525

History

#1 - 02/22/2011 09:45 AM - naruse (Yui NARUSE)

- Status changed from Open to Assigned

- Assignee set to nahi (Hiroshi Nakamura)

=begin

=end

#2 - 03/01/2011 07:56 AM - MartinBosslet (Martin Bosslet)

- File ec_pem_pwd2.diff added

=begin
Added support for PEM decryption in EC#initialize,
to be consistent with DSA and RSA.

Regards,
Martin
=end

#3 - 05/12/2011 07:40 AM - MartinBosslet (Martin Bosslet)

- Assignee changed from nahi (Hiroshi Nakamura) to MartinBosslet (Martin Bosslet)

#4 - 05/12/2011 08:05 AM - Anonymous

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r31526.
Martin, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

Thu May 12 08:01:14 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* ext/openssl/ossl_pkey_ec.c: Allow encryption when PEM-encoding
  Elliptic Curve private keys.
  [ruby-core:35329] [Bug #4423]
```

Previous revision: 31525

Files

ec_pem_pwd.diff	3.37 KB	02/22/2011	MartinBosslet (Martin Bosslet)
ec_pem_pwd2.diff	4.44 KB	03/01/2011	MartinBosslet (Martin Bosslet)