Ruby trunk - Bug #13100

OpenSSL::PKey::EC#public_key Group

01/04/2017 09:36 AM - azuchi (Shigeyuki Azuchi)

Status:	Assigned		
Priority:	Normal		
Assignee:	openssl		
Target version:			
ruby -v:	ruby 2.4.0p0 (2016-12-24 revision 57164) [x86_64-linux]	**Backport:**	2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN

Description

OpenSSL::PKey::EC#public_key=
OpenSSL::PKey::EC::Point:compressed
OpenSSL::PKey::EC#public_key
:compressed:uncompressed

2.3.0:compressed2.4

OpenSSL::PKey::EC#public_key

```
require "test/unit"

class OpenSSL::TestEC < Test::Unit::TestCase

  def test_point_conversion_form
    pub_key = '03cdd34ec0a05d91c026fe8cb74434923075d3acc20f3f673fb855c8f2c04ca522' # compressed pu
bkey
    key = OpenSSL::PKey::EC.new("secp256k1")

    # success 2.4 and 2.3
    point = OpenSSL::PKey::EC::Point.new(key.group, OpenSSL::BN.new(pub_key, 16))
    point.group.point_conversion_form = :compressed
    assert_equal point.group.point_conversion_form, :compressed

    # success 2.3, but fail 2.4
    key.public_key = OpenSSL::PKey::EC::Point.new(key.group, OpenSSL::BN.new(pub_key, 16))
    key.public_key.group.point_conversion_form = :compressed
    assert_equal key.public_key.group.point_conversion_form, :compressed
  end

end
```

History

#1 - 01/08/2017 05:51 AM - znz (Kazuhiro NISHIYAMA)

- Assignee set to openssl

- Status changed from Open to Assigned