

Ruby - Bug #12381

ext/openssl classes' dup/clone don't work well

05/14/2016 11:14 AM - rhenium (Kazuki Yamaguchi)

Status:	Closed	Backport: 2.1: WONTFIX, 2.2: REQUIRED, 2.3: REQUIRED
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:		
Description		
They don't copy the underlying C level structures.		
<pre>ssl_ctx = OpenSSL::SSL::SSLContext.new ssl_ctx.ciphers = "aNULL" p ssl_ctx.ciphers # => [["ADH-AES256-GCM-SHA384", "TLSv1.2", 256, 256], .. aNULL cipher suites ..] new_ctx = ssl_ctx.dup p new_ctx.ciphers # => [["ECDHE-ECDSA-AES256-GCM-SHA384", "TLSv1.2", 256, 256], .. the default cipher suites ..]</pre>		

Associated revisions

Revision be1baf4a9a62aade5a411eab3ebb704f3afd2cc8 - 06/19/2016 09:29 AM - rhenium (Kazuki Yamaguchi)

openssl: implement initialize_copy method for PKey classes

- ext/openssl/openssl_pkey_dh.c, ext/openssl/openssl_pkey_dsa.c, ext/openssl/openssl_pkey_ec.c, ext/openssl/openssl_pkey_rsa.c: Implement initialize_copy method for OpenSSL::PKey::*. [ruby-core:75504] [Bug #12381]
- test/openssl/test_pkey_dh.rb, test/openssl/test_pkey_dsa.rb, test/openssl/test_pkey_ec.rb, test/openssl/test_pkey_rsa.rb: Test they actually copy the OpenSSL objects, and modifications to cloned object don't affect the original object.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@55454 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision be1baf4a - 06/19/2016 09:29 AM - rhenium (Kazuki Yamaguchi)

openssl: implement initialize_copy method for PKey classes

- ext/openssl/openssl_pkey_dh.c, ext/openssl/openssl_pkey_dsa.c, ext/openssl/openssl_pkey_ec.c, ext/openssl/openssl_pkey_rsa.c: Implement initialize_copy method for OpenSSL::PKey::*. [ruby-core:75504] [Bug #12381]
- test/openssl/test_pkey_dh.rb, test/openssl/test_pkey_dsa.rb, test/openssl/test_pkey_ec.rb, test/openssl/test_pkey_rsa.rb: Test they actually copy the OpenSSL objects, and modifications to cloned object don't affect the original object.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@55454 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f31f1f1adf4b6c573d2620ee2bf72f3bc1fb854c - 06/19/2016 09:42 AM - rhenium (Kazuki Yamaguchi)

openssl: implement initialize_copy for OpenSSL::OCSP::*

- ext/openssl/openssl_ocsp.c: Implement OCSP::{CertificateId,Request, BasicResponse,Response}#initialize_copy. [ruby-core:75504] [Bug #12381]
- test/openssl/test_ocsp.rb: Test them.

Revision f31f1f1a - 06/19/2016 09:42 AM - rhenium (Kazuki Yamaguchi)

openssl: implement initialize_copy for OpenSSL::OCSP::*

- ext/openssl/openssl_ocsp.c: Implement OCSP::{CertificateId,Request, BasicResponse,Response}#initialize_copy.
[ruby-core:75504] [Bug #12381]
- test/openssl/test_ocsp.rb: Test them.

History

#1 - 06/19/2016 09:30 AM - Anonymous

- Status changed from Open to Closed

Applied in changeset r55454.

openssl: implement initialize_copy method for PKey classes

- ext/openssl/openssl_pkey_dh.c, ext/openssl/openssl_pkey_dsa.c, ext/openssl/openssl_pkey_ec.c, ext/openssl/openssl_pkey_rsa.c: Implement initialize_copy method for OpenSSL::PKey::*.
[\[ruby-core:75504\]](#) [Bug [#12381](#)]
- test/openssl/test_pkey_dh.rb, test/openssl/test_pkey_dsa.rb, test/openssl/test_pkey_ec.rb, test/openssl/test_pkey_rsa.rb: Test they actually copy the OpenSSL objects, and modifications to cloned object don't affect the original object.

#2 - 08/04/2016 07:13 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.1: UNKNOWN, 2.2: UNKNOWN, 2.3: UNKNOWN to 2.1: WONTFIX, 2.2: REQUIRED, 2.3: REQUIRED

#3 - 08/04/2016 07:58 AM - Tietew (Toru Iwase)

SSLContext#dup is not fixed yet?

```
$ RBENV_VERSION=2.4.0-dev ruby -v -ropenssl -e 'c = OpenSSL::SSL::SSLContext.new; c.ciphers = "aNULL"; p c.ciphers == c.dup.ciphers'
ruby 2.4.0dev (2016-08-03 trunk 55810) [x86_64-linux]
false
```

#4 - 08/04/2016 02:01 PM - rhenium (Kazuki Yamaguchi)

- File 0001-Implement-missing-initialize_copy.patch added

Thanks for reminding me.

I've just fixed the remaining at ruby/openssl (GitHub):

<https://github.com/ruby/openssl/commit/6dc9b914cae52c8af6e1b4d1156613bcd914eaf5>

Attached is the patch against 2.3 branch.

Files

0001-Implement-missing-initialize_copy.patch	16.2 KB	08/04/2016	rhenium (Kazuki Yamaguchi)
--	---------	------------	----------------------------