Ruby master - Bug #4885

[ext/openssl] Use BIO_reset and ERR_get_error in conjuntion

06/14/2011 07:26 PM - MartinBosslet (Martin Bosslet)

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

Description

This is related to the bug in http://redmine.ruby-lang.org/issues/4879.

There are still some places in Ruby OpenSSL C code where just BIO_reset
is used but not ERR_get_error if a fallback from PEM to DER is tried or
the other way round. This might cause encoding errors to pile up and
mislead users or cause tests to fail that shouldn't.

I'd like to expose the conjunction of

BIO_reset(bio);
ERR_get_error();

as a publicly accesible macro (similar to what's in ossl_pkey.c) and
replace existing code by using it where appropriate.

Please let me know if you have any objections!

Regards,
Martin

Related issues:

Related to Ruby master - Bug #4879: test_new(OpenSSL::TestPKeyRSA) fails on W...	**Closed**	**06/14/2011**

Associated revisions

Revision 26cb830d - 06/22/2011 08:41 AM - emboss

- ext/openssl/ossl.h: Introduced OSSL_BIO_reset macro for PEM/DER fallback scenarios.
- ext/openssl/ossl_pkey_dsa.c
- ext/openssl/ossl_x509req.c
- ext/openssl/ossl_pkey_rsa.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_ssl_session.c
- ext/openssl/ossl_x509crl.c
- ext/openssl/ossl_pkey.c
- ext/openssl/ossl_pkey_dh.c
- ext/openssl/ossl_x509cert.c
- ext/openssl/ossl_pkcs7.c: Use OSSL_BIO_reset.
- ext/openssl/ossl_ssl.c
- ext/openssl/ossl_cipher.c

- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_pkcs12.c
- ext/openssl/ossl_ssl_session.c: Replace rb_raise occurences by ossl_raise. This automatically flushes OpenSSL's error queue.
- ext/openssl/ossl_pkcs7.c: Raise error if DER fallback for parsing fails.
- test/openssl/test_pkey_ec.rb
- test/openssl/test_pkey_dsa.rb
- test/openssl/test_pkey_rsa.rb: Add assertions that OpenSSL.errors is empty.
- test/openssl/test_pkey_rsa.rb: Remove initial OpenSSL.errors call in test_new.
  [Ruby 1.9 - Bug #4885] [ruby-core:37134]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@32199 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 32199 - 06/22/2011 08:41 AM - emboss

- ext/openssl/ossl.h: Introduced OSSL_BIO_reset macro for PEM/DER fallback scenarios.
- ext/openssl/ossl_pkey_dsa.c
- ext/openssl/ossl_x509req.c
- ext/openssl/ossl_pkey_rsa.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_ssl_session.c
- ext/openssl/ossl_x509crl.c
- ext/openssl/ossl_pkey.c
- ext/openssl/ossl_pkey_dh.c
- ext/openssl/ossl_x509cert.c
- ext/openssl/ossl_pkcs7.c: Use OSSL_BIO_reset.
- ext/openssl/ossl_ssl.c
- ext/openssl/ossl_cipher.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_pkcs12.c
- ext/openssl/ossl_ssl_session.c: Replace rb_raise occurences by ossl_raise. This automatically flushes OpenSSL's error queue.
- ext/openssl/ossl_pkcs7.c: Raise error if DER fallback for parsing fails.
- test/openssl/test_pkey_ec.rb
- test/openssl/test_pkey_dsa.rb
- test/openssl/test_pkey_rsa.rb: Add assertions that OpenSSL.errors is empty.
- test/openssl/test_pkey_rsa.rb: Remove initial OpenSSL.errors call in test_new.

[Ruby 1.9 - Bug #4885] [ruby-core:37134]

Revision 32199 - 06/22/2011 08:41 AM - emboss

- ext/openssl/ossl.h: Introduced OSSL_BIO_reset macro for PEM/DER fallback scenarios.
- ext/openssl/ossl_pkey_dsa.c
- ext/openssl/ossl_x509req.c
- ext/openssl/ossl_pkey_rsa.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_ssl_session.c
- ext/openssl/ossl_x509crl.c
- ext/openssl/ossl_pkey.c
- ext/openssl/ossl_pkey_dh.c
- ext/openssl/ossl_x509cert.c
- ext/openssl/ossl_pkcs7.c: Use OSSL_BIO_reset.
- ext/openssl/ossl_ssl.c
- ext/openssl/ossl_cipher.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_pkcs12.c
- ext/openssl/ossl_ssl_session.c: Replace rb_raise occurences by ossl_raise. This automatically flushes OpenSSL's error queue.
- ext/openssl/ossl_pkcs7.c: Raise error if DER fallback for parsing fails.
- test/openssl/test_pkey_ec.rb
- test/openssl/test_pkey_dsa.rb
- test/openssl/test_pkey_rsa.rb: Add assertions that OpenSSL.errors is empty.
- test/openssl/test_pkey_rsa.rb: Remove initial OpenSSL.errors call in test_new.
  [Ruby 1.9 - Bug #4885] [ruby-core:37134]

Revision 32199 - 06/22/2011 08:41 AM - emboss

- ext/openssl/ossl.h: Introduced OSSL_BIO_reset macro for PEM/DER fallback scenarios.
- ext/openssl/ossl_pkey_dsa.c
- ext/openssl/ossl_x509req.c
- ext/openssl/ossl_pkey_rsa.c
- ext/openssl/ossl_pkey_ec.c

- ext/openssl/ossl_ssl_session.c
- ext/openssl/ossl_x509crl.c
- ext/openssl/ossl_pkey.c
- ext/openssl/ossl_pkey_dh.c
- ext/openssl/ossl_x509cert.c
- ext/openssl/ossl_pkcs7.c: Use OSSL_BIO_reset.
- ext/openssl/ossl_ssl.c
- ext/openssl/ossl_cipher.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_pkcs12.c
- ext/openssl/ossl_ssl_session.c: Replace rb_raise occurences by ossl_raise. This automatically flushes OpenSSL's error queue.
- ext/openssl/ossl_pkcs7.c: Raise error if DER fallback for parsing fails.
- test/openssl/test_pkey_ec.rb
- test/openssl/test_pkey_dsa.rb
- test/openssl/test_pkey_rsa.rb: Add assertions that OpenSSL.errors is empty.
- test/openssl/test_pkey_rsa.rb: Remove initial OpenSSL.errors call in test_new.
  [Ruby 1.9 - Bug #4885] [ruby-core:37134]

Revision 32199 - 06/22/2011 08:41 AM - emboss

- ext/openssl/ossl.h: Introduced OSSL_BIO_reset macro for PEM/DER fallback scenarios.
- ext/openssl/ossl_pkey_dsa.c
- ext/openssl/ossl_x509req.c
- ext/openssl/ossl_pkey_rsa.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_ssl_session.c
- ext/openssl/ossl_x509crl.c
- ext/openssl/ossl_pkey.c
- ext/openssl/ossl_pkey_dh.c
- ext/openssl/ossl_x509cert.c
- ext/openssl/ossl_pkcs7.c: Use OSSL_BIO_reset.
- ext/openssl/ossl_ssl.c
- ext/openssl/ossl_cipher.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_pkcs12.c

- ext/openssl/ossl_ssl_session.c: Replace rb_raise occurences by ossl_raise. This automatically flushes OpenSSL's error queue.
- ext/openssl/ossl_pkcs7.c: Raise error if DER fallback for parsing fails.
- test/openssl/test_pkey_ec.rb
- test/openssl/test_pkey_dsa.rb
- test/openssl/test_pkey_rsa.rb: Add assertions that OpenSSL.errors is empty.
- test/openssl/test_pkey_rsa.rb: Remove initial OpenSSL.errors call in test_new.
  [Ruby 1.9 - Bug #4885] [ruby-core:37134]

Revision 32199 - 06/22/2011 08:41 AM - emboss

- ext/openssl/ossl.h: Introduced OSSL_BIO_reset macro for PEM/DER fallback scenarios.
- ext/openssl/ossl_pkey_dsa.c
- ext/openssl/ossl_x509req.c
- ext/openssl/ossl_pkey_rsa.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_ssl_session.c
- ext/openssl/ossl_x509crl.c
- ext/openssl/ossl_pkey.c
- ext/openssl/ossl_pkey_dh.c
- ext/openssl/ossl_x509cert.c
- ext/openssl/ossl_pkcs7.c: Use OSSL_BIO_reset.
- ext/openssl/ossl_ssl.c
- ext/openssl/ossl_cipher.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_pkcs12.c
- ext/openssl/ossl_ssl_session.c: Replace rb_raise occurences by ossl_raise. This automatically flushes OpenSSL's error queue.
- ext/openssl/ossl_pkcs7.c: Raise error if DER fallback for parsing fails.
- test/openssl/test_pkey_ec.rb
- test/openssl/test_pkey_dsa.rb
- test/openssl/test_pkey_rsa.rb: Add assertions that OpenSSL.errors is empty.
- test/openssl/test_pkey_rsa.rb: Remove initial OpenSSL.errors call in test_new.
  [Ruby 1.9 - Bug #4885] [ruby-core:37134]

Revision 32199 - 06/22/2011 08:41 AM - emboss

- ext/openssl/ossl.h: Introduced OSSL_BIO_reset macro for PEM/DER fallback scenarios.
- ext/openssl/ossl_pkey_dsa.c
- ext/openssl/ossl_x509req.c
- ext/openssl/ossl_pkey_rsa.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_ssl_session.c
- ext/openssl/ossl_x509crl.c
- ext/openssl/ossl_pkey.c
- ext/openssl/ossl_pkey_dh.c
- ext/openssl/ossl_x509cert.c
- ext/openssl/ossl_pkcs7.c: Use OSSL_BIO_reset.
- ext/openssl/ossl_ssl.c
- ext/openssl/ossl_cipher.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_pkcs12.c
- ext/openssl/ossl_ssl_session.c: Replace rb_raise occurences by ossl_raise. This automatically flushes OpenSSL's error queue.
- ext/openssl/ossl_pkcs7.c: Raise error if DER fallback for parsing fails.
- test/openssl/test_pkey_ec.rb
- test/openssl/test_pkey_dsa.rb
- test/openssl/test_pkey_rsa.rb: Add assertions that OpenSSL.errors is empty.
- test/openssl/test_pkey_rsa.rb: Remove initial OpenSSL.errors call in test_new.
  [Ruby 1.9 - Bug #4885] [ruby-core:37134]

History

#1 - 06/22/2011 05:41 PM - Anonymous

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r32199.
Martin, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/openssl/ossl.h: Introduced OSSL_BIO_reset macro for PEM/DER fallback scenarios.
- ext/openssl/ossl_pkey_dsa.c
- ext/openssl/ossl_x509req.c

- ext/openssl/ossl_pkey_rsa.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_ssl_session.c
- ext/openssl/ossl_x509crl.c
- ext/openssl/ossl_pkey.c
- ext/openssl/ossl_pkey_dh.c
- ext/openssl/ossl_x509cert.c
- ext/openssl/ossl_pkcs7.c: Use OSSL_BIO_reset.
- ext/openssl/ossl_ssl.c
- ext/openssl/ossl_cipher.c
- ext/openssl/ossl_pkey_ec.c
- ext/openssl/ossl_pkcs12.c
- ext/openssl/ossl_ssl_session.c: Replace rb_raise occurences by ossl_raise. This automatically flushes OpenSSL's error queue.
- ext/openssl/ossl_pkcs7.c: Raise error if DER fallback for parsing fails.
- test/openssl/test_pkey_ec.rb
- test/openssl/test_pkey_dsa.rb
- test/openssl/test_pkey_rsa.rb: Add assertions that OpenSSL.errors is empty.
- test/openssl/test_pkey_rsa.rb: Remove initial OpenSSL.errors call in test_new.
  [Ruby 1.9 - Bug #4885] [ruby-core:37134]