Ruby master - Bug #12162

OpenSSL::PKCS7 seems to create broken objects (nested asn.1 error)

03/09/2016 03:05 PM - wesoly_opos (Jarosław Górny)

Status: Third Party's Issue
Priority: Normal
Assignee: 
Target version:
Backport: 2.1: UNKNOWN, 2.2: UNKNOWN, 2.3: UNKNOWN

Description
When trying to read previously created OpenSSL::PKCS7 object, it fails with 'nested asn.1 error'. Seems like object is broken.

Steps to reproduce:
1. Generate x.509 certificate (either from CLI or in Ruby) and store it in OpenSSL::X509::Certificate object.
2. Create new OpenSSL::PKCS7 object, set the 'type' attribute to ':signed'
3. Add OpenSSL::X509::Certificate object to OpenSSL::PKCS7 object with #add_certificate() method
4. Try to read back the object created in step '3' with: OpenSSL::PKCS7.new(pkcs7_obj.to_s)

Result:
ArgumentError: Could not parse the PKCS7: nested asn1 error
from (pry):8:in `initialize'

Expected result:
OpenSSL::PKCS7.new() should be able to read from previously created PKCS7 object (casted to string with #to_s method)

The session is attached to this ticket. It can be also found online: https://gist.github.com/jnahorny/9ccbb186c9f7c20c9f3e

note 1: I was able to reproduce this problem with ruby 2.2.x and latest head (2.4.0). On Linux too.
note 2: This code used to work when ruby was linked to openssl v 0.9.8.

Related issues:
Has duplicate Ruby master - Bug #12794: Invalid ASN1 from OpenSSL::X509::Requests added

Rejected

History
#1 - 03/16/2016 09:12 AM - shyouhei (Shyouhei Urabe)
- Status changed from Open to Assigned
- Assignee set to 7150

#2 - 07/02/2016 07:47 AM - rhenium (Kazuki Yamaguchi)
- Status changed from Assigned to Third Party's Issue

The direct reason is that PKCS7#to_s returns a broken PEM. It looks like the behavior was changed in OpenSSL 1.0.1i:
https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d70c0be4c1e33985a79d691786db72661dfdf057

But since the PKCS7 object is actually incomplete at that time you call PKCS7#to_s, I'm not sure whether if this is a bug or not.

#3 - 09/28/2016 07:21 AM - rhenium (Kazuki Yamaguchi)
- Has duplicate Bug #12794: Invalid ASN1 from OpenSSL::X509::Requests added

Files
gistfile1.txt  4.35 KB  03/09/2016  wesoly_opos (Jarosław Górny)