Ruby trunk - Bug #8178

OpenSSL::PKCS7::SignerInfo

03/28/2013 07:04 AM - Jacob640 (Joseph Coyle)

Status:	Assigned		
Priority:	Normal		
Assignee:	openssl		
Target version:			
ruby -v:	ruby 2.1.0dev (2013-03-28 trunk 39971) [x86_64-darwin11.4.2]	**Backport:**	

Description

The instance method OpenSSL::PKCS7::SignerInfo.name does not return the signing certificate name but the X509 name of the signer's issuer. This is because SignerInfo.name is actually an alias of SignerInfo.issuer. This appears to be a mistake particularly because OpenSSL::PKCS7::RecepientInfo doesn't have a corresponding name method.

Perhaps OpenSSL::PKCS7::SignerInfo.name should be considered for removal since the method name is misleading.

History

#1 - 03/28/2013 09:08 AM - MartinBosslet (Martin Bosslet)

- Category set to ext

- Status changed from Open to Assigned

- Assignee set to MartinBosslet (Martin Bosslet)

- Target version set to 2.1.0

#2 - 03/28/2013 09:39 AM - Jacob640 (Joseph Coyle)

Because of this bug I have been looking at why it is so difficult to get useful identifying info for pkcs7 signers. I see that OpenSSL provides a utility function to extract a certificate from a pkcs7 message corresponding to a supplied signer info struct called PKCS7_cert_from_signer_info.

Unfortunately due to OpenSSL closely following the pkcs7 data structures SignerInfo structs do not appear to contain the certificate or name of the signing certificate. Because of this PKCS7_cert_from_signer_info requires both a pkcs7 message and a signerInfo struct to provide the signer certificates.

However if we wish to follow the design decisions of OpenSSL it is fairly easy to construct a utility method for OpenSSL::PKCS7 that takes a SignerInfo object and outputs the corresponding certificate. I have written a basic demonstration in this commit:
https://github.com/Jacob640/ruby/commit/10e5f0b74cd08ee23f2b6643a7f86a6dbec857c1

#3 - 07/06/2013 07:30 AM - MartinBosslet (Martin Bosslet)

I agree that SignerInfo#name is misleading. It should be easier to get the relevant information, I'll consider your proposal and will think about other ways to improve the API!

#4 - 01/30/2014 06:16 AM - hsbt (Hiroshi SHIBATA)

- Target version changed from 2.1.0 to 2.2.0

#5 - 09/13/2015 03:13 AM - zzak (Zachary Scott)

- Assignee changed from MartinBosslet (Martin Bosslet) to openssl