Ruby - Bug #10497

OpenSSL Servers Do Not Support EC Certificates

11/11/2014 10:56 PM - bnagy (Ben Nagy)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.1.0p0 (2013-12-25 revision 44422) [x86_64-darwin12.0]	**Backport:**	2.0.0: UNKNOWN, 2.1: UNKNOWN

Description

Also see https://bugs.ruby-lang.org/issues/10257

Here's a gist https://gist.github.com/bnagy/7a81e5387beeeea866c1 which works fine with an RSA key and fails with an EC key. I tried with an externally verified cert, which I have tested using the openssl s_server/s_client tools, as well as with an EC key that I pass to the ruby issue_cert method. I see:

SSL_accept returned=1 errno=0 state=SSLv3 read client hello C: no shared cipher
/Users/ben/.rubies/ruby-2.1.0/lib/ruby/2.1.0/openssl/ssl.rb:194:in `accept'

MRI: ruby 2.1.0p0 (2013-12-25 revision 44422) [x86_64-darwin12.0]

and

SSL_accept returned=1 errno=0 state=SSLv3 read client hello C: no shared cipher
/Users/ben/.rubies/rubinius-2.2.1/runtime/gems/rubysl-openssl-2.0.4/lib/openssl/ssl.rb:184:in `accept'

rubinius 2.2.1 (2.1.0 3ed43137 2013-11-17 JI) [x86_64-darwin12.4.0]

Can't test with JRuby because it doesn't support the ECDH suites at all yet.

Unfortunately, I haven't got any further yet because that's where the call vanishes into openssl itself, but I suspect 'no shared cipher' is a red herring (I'm not specifying or restricting any cipher suites at either end)

Related issues:

Related to Ruby - Bug #11739: OpenSSL::SSL::SSLServer doesn't negotiate ECDHE...	**Rejected**
Related to Ruby - Feature #11356: Add ECDH support to OpenSSL wrapper	**Closed**

History

#1 - 09/13/2015 03:24 AM - zzak (zzak _)

- Assignee set to 7150

#2 - 07/02/2016 02:23 AM - rhenium (Kazuki Yamaguchi)

- Related to Bug #10257: Generate X.509 certificate/request/CRL with elliptic curve keys added

#3 - 07/02/2016 07:38 AM - rhenium (Kazuki Yamaguchi)

- Status changed from Open to Closed

ext/openssl didn't support ephemeral ECDH in server mode up until Ruby 2.3.

You can use OpenSSL::SSL::SSLSocket#tmp_ecdh_callback in Ruby 2.3, for now. In Ruby 2.4 (r55214), ephemeral ECDH will be enabled by default just like ephemeral DH.

#4 - 07/02/2016 07:38 AM - rhenium (Kazuki Yamaguchi)

- Related to deleted (Bug #10257: Generate X.509 certificate/request/CRL with elliptic curve keys)

#5 - 07/02/2016 07:38 AM - rhenium (Kazuki Yamaguchi)

- Related to Bug #11739: OpenSSL::SSL::SSLServer doesn't negotiate ECDHE- ciphersuites added*

#6 - 07/02/2016 07:40 AM - rhenium (Kazuki Yamaguchi)

- Related to Feature #11356: Add ECDH support to OpenSSL wrapper added