Ruby master - Bug #11739

OpenSSL::SSL::SSLServer doesn't negotiate ECDHE-* ciphersuites

11/25/2015 06:39 AM - weeks (Branodn Weeks)

Status:	Rejected		
Priority:	Normal		
Assignee:	openssl		
Target version:			
ruby -v:		**Backport:**	2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN

Description

I'm trying to configure an instance of OpenSSL::SSL::SSLServer that supports Elliptic curve Diffie–Hellman. No matter what combination of Ruby and OpenSSL versions I try the negotiation with the client fails.

Proof of concept:
https://gist.github.com/brandonweeks/e26414cc1e9eea9453a8

Then run:

```
openssl s_client -connect localhost:8443
```

Also attaching a pcap file of the failed handshake.

Related issues:

Related to Ruby master - Bug #10497: OpenSSL Servers Do Not Support EC Certif...	**Closed**
Related to Ruby master - Feature #11356: Add ECDH support to OpenSSL wrapper	**Closed**

History

#1 - 12/07/2015 07:33 AM - ko1 (Koichi Sasada)

- Assignee set to openssl

#2 - 07/02/2016 07:38 AM - rhenium (Kazuki Yamaguchi)

- Related to Bug #10497: OpenSSL Servers Do Not Support EC Certificates added

#3 - 07/02/2016 07:40 AM - rhenium (Kazuki Yamaguchi)

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

#4 - 07/02/2016 07:41 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 (Feature #11356).

#5 - 08/04/2016 07:25 AM - usa (Usaku NAKAMURA)

- Status changed from Closed to Rejected

Files

tls_handshake.pcap	4.93 KB	11/25/2015	weeks (Branodn Weeks)