Ruby trunk - Feature #11356

Add ECDH support to OpenSSL wrapper

07/15/2015 09:10 PM - tenderlovemaking (Aaron Patterson)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		

Description

FireFox wants to use ECDH on HTTP/2 connections, and there is no way to add it to the SSL context. This patch adds an ECDH callback (similar to the DH callback).

With this patch and #9390, I am able to get an HTTP/2 server running in Chrome and FireFox! :)

Related issues:

Related to Ruby trunk - Bug #10497: OpenSSL Servers Do Not Support EC Certifi...	**Closed**
Related to Ruby trunk - Bug #11739: OpenSSL::SSL::SSLServer doesn't negotiate...	**Rejected**

Associated revisions

Revision 5326593a - 07/22/2015 06:34 PM - tenderlove

- ext/openssl/ossl_ssl.c: add ECDH callback support. [Feature #11356]
- test/openssl/test_pair.rb: test for ECDH callback support

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@51348 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 51348 - 07/22/2015 06:34 PM - tenderlovemaking (Aaron Patterson)

- ext/openssl/ossl_ssl.c: add ECDH callback support. [Feature #11356]
- test/openssl/test_pair.rb: test for ECDH callback support

Revision 51348 - 07/22/2015 06:34 PM - tenderlove

- ext/openssl/ossl_ssl.c: add ECDH callback support. [Feature #11356]
- test/openssl/test_pair.rb: test for ECDH callback support

Revision 51348 - 07/22/2015 06:34 PM - tenderlove

- ext/openssl/ossl_ssl.c: add ECDH callback support. [Feature #11356]
- test/openssl/test_pair.rb: test for ECDH callback support

Revision 51348 - 07/22/2015 06:34 PM - tenderlove

- ext/openssl/ossl_ssl.c: add ECDH callback support. [Feature #11356]
- test/openssl/test_pair.rb: test for ECDH callback support

Revision 51348 - 07/22/2015 06:34 PM - tenderlove

- ext/openssl/ossl_ssl.c: add ECDH callback support. [Feature #11356]
- test/openssl/test_pair.rb: test for ECDH callback support

History

#1 - 07/16/2015 08:06 AM - nobu (Nobuyoshi Nakada)

```
static VALUE
ossl_call_tmp_ecdh_callback(VALUE *args)
```

I think this argument should be a VALUE and casted in the function.

```
    success = rb_protect((VALUE(*)_((VALUE)))ossl_call_tmp_ecdh_callback,
                         (VALUE)args, NULL);
```

Then we can remove the cast of the function and an indirect cast.

#2 - 07/17/2015 03:08 PM - tenderlovemaking (Aaron Patterson)

- File 0001-add-ecdh-support.patch added

nobu (Nobuyoshi Nakada),

Thanks for the feedback! I've attached a new patch that refactors those parts.

#3 - 07/22/2015 06:35 PM - Anonymous

- Status changed from Open to Closed

Applied in changeset r51348.

- ext/openssl/ossl_ssl.c: add ECDH callback support. [Feature #11356]
- test/openssl/test_pair.rb: test for ECDH callback support

#4 - 07/02/2016 07:40 AM - rhenium (Kazuki Yamaguchi)

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

#5 - 07/02/2016 07:40 AM - rhenium (Kazuki Yamaguchi)

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

Files

0001-add-ecdh-support.patch	6.81 KB	07/15/2015	tenderlovemaking (Aaron Patterson)
0001-add-ecdh-support.patch	6.78 KB	07/17/2015	tenderlovemaking (Aaron Patterson)