

## Ruby - Bug #6938

### [PATCH] Increase DH key size to fix test suite in FIPS mode

08/28/2012 12:29 AM - vo.x (Vit Ondruch)

<b>Status:</b>	Closed	
<b>Priority:</b>	Normal	
<b>Assignee:</b>	MartinBosslet (Martin Bosslet)	
<b>Target version:</b>		
<b>ruby -v:</b>	ruby 2.0.0dev	<b>Backport:</b>
<b>Description</b> In FIPS mode, DH refuses to generate or use keys with modulus smaller than 1024 bits. This patch increases the key size to make the test suite pass.		
<b>Related issues:</b> Related to Ruby - Feature #6946: FIPS support? <span style="float: right;">Open</span>		

#### Associated revisions

**Revision 9871dd5783963ad3d341ddb58f6bfe7ca7ceb444 - 08/28/2012 08:03 PM - MartinBosslet (Martin Bosslet)**

- test/openssl/utis.rb  
test/openssl/test\_pair.rb  
test/openssl/test\_pkey\_dh.rb: Use 1024 bit DH parameters to satisfy OpenSSL FIPS requirements. Patch by Vit Ondruch.  
[Bug #6938] [ruby-core:47326]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@36843 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

**Revision 9871dd57 - 08/28/2012 08:03 PM - MartinBosslet (Martin Bosslet)**

- test/openssl/utis.rb  
test/openssl/test\_pair.rb  
test/openssl/test\_pkey\_dh.rb: Use 1024 bit DH parameters to satisfy OpenSSL FIPS requirements. Patch by Vit Ondruch.  
[Bug #6938] [ruby-core:47326]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@36843 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

#### History

**#1 - 08/28/2012 12:37 AM - naruse (Yui NARUSE)**

- Status changed from Open to Assigned
- Assignee changed from duerst (Martin Dürst) to MartinBosslet (Martin Bosslet)

Generating 1024bit key takes much more time then 256bit, so it should reuse the key instead of simply replacing like s/256/1024/.

**#2 - 08/28/2012 01:15 AM - vo.x (Vit Ondruch)**

- File 0001-Use-higher-DH-key-moudlus-to-pass-test-with-FIPS-ena.patch added

Hm, actually, it seems that the test\_pair one can be entirely dropped. Not sure about the test\_pkey\_dh.rb, since they are testing directly the DH algorithm.

**#3 - 08/28/2012 01:16 AM - vo.x (Vit Ondruch)**

- File deleted (0001-Use-higher-DH-key-moudlus-to-pass-test-with-FIPS-ena.patch)

**#4 - 08/28/2012 01:23 AM - vo.x (Vit Ondruch)**

- File 0001-Use-higher-DH-key-moudlus-to-pass-test-with-FIPS-ena.patch added

I'm using now the cached key. I hope I did not degraded the quality of TS too much.

**#5 - 08/28/2012 01:23 AM - vo.x (Vit Ondruch)**

- File deleted (0001-Use-higher-DH-key-moudlus-to-pass-test-with-FIPS-ena.patch)

**#6 - 08/28/2012 01:58 AM - MartinBosslet (Martin Bosslet)**

Yes, better with the cached key. Thanks for the patch!

**#7 - 08/29/2012 05:03 AM - Anonymous**

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r36843.

Vit, thank you for reporting this issue.

Your contribution to Ruby is greatly appreciated.

May Ruby be with you.

- 
- test/openssl/utls.rb  
test/openssl/test\_pair.rb  
test/openssl/test\_pkey\_dh.rb: Use 1024 bit DH parameters to satisfy  
OpenSSL FIPS requirements. Patch by Vit Ondruch.  
[Bug [#6938](#)] [[ruby-core:47326](#)]

**#8 - 09/02/2012 05:24 AM - naruse (Yui NARUSE)**

Why TEST\_KEY\_DH1024 in test/openssl/utls.rb doesn't use cache?

**#9 - 09/02/2012 08:51 PM - MartinBosslet (Martin Bosslet)**

Why TEST\_KEY\_DH1024 in test/openssl/utls.rb doesn't use cache?

Unfortunately DH doesn't allow serialization of the private exponent out of the box like the other PKeys do. But 1024 bits generation is eating up a lot of time, way too much for tests IMO. And what's worse, I saw that the "test-all" target for one run on rubyci timed out. I'm currently looking for a way to still be able to serialize DH keys including the private exponent to solve this.

**#10 - 09/02/2012 09:58 PM - MartinBosslet (Martin Bosslet)**

OK, I found a way to use a cached key (r36881). This still leaves us with the problem that "test\_new" in test\_pkey\_dh.rb consumes a lot of time. But I think I found a way how to handle this cleanly (cf. [#6946](#)).

**#11 - 09/02/2012 10:03 PM - naruse (Yui NARUSE)**

MartinBosslet (Martin Bosslet) wrote:

OK, I found a way to use a cached key (r36881). This still leaves us with the problem that "test\_new" in test\_pkey\_dh.rb consumes a lot of time. But I think I found a way how to handle this cleanly (cf. [#6946](#)).

Great!

I thought test\_new is unavoidable.

**Files**

---

0001-Use-higher-DH-key-moudlus-to-pass-test-with-FIPS-ena.patch	2.64 KB	08/28/2012	vo.x (Vit Ondruch)
---	---------	------------	--------------------