

Ruby master - Bug #4421

[ext/openssl] Fix RSA public key encoding

02/22/2011 08:18 AM - MartinBosslet (Martin Bosslet)

Status:	Closed	
Priority:	Normal	
Assignee:	MartinBosslet (Martin Bosslet)	
Target version:	1.9.3	
ruby -v:	-	
Description		Backport:
<p>=begin</p> <p>When calling <code>RSA#to_der</code> and <code>RSA#to_pem</code> on RSA public keys, they currently get encoded using <code>i2d_RSAPublicKey</code> and <code>PEM_write_bio_RSAPublicKey</code>. This encoding was specified in PKCS#1 and is specific to RSA. It is also not the default encoding used by OpenSSL itself, which rather uses the generic format generated by <code>i2d_RSA_PUBKEY</code> and <code>PEM_write_bio_RSA_PUBKEY</code>. This format is the same that is used in a certificate's <code>SubjectPublicKeyInfo</code>, the advantage being that the format is generic and can be used to represent public keys of all kinds, including RSA, DSA and Elliptic Curve.</p> <p>The attached patch will make use of the generic format for encoding RSA keys. The change should not cause compatibility problems, since <code>RSA#initialize</code> uses several fallback scenarios that cover public keys of both formats.</p> <p>The fallbacks are also re-prioritized according to these changes.</p> <p>Regards, Martin =end</p>		

Associated revisions

Revision 1915a913 - 05/11/2011 09:51 PM - emboss

Thu May 12 07:27:31 2011 Martin Bosslet Martin.Bosslet@gmail.com

```
* ext/openssl/openssl_pkey_rsa.c: Use generic X.509 SubjectPublicKeyInfo
format for encoding RSA public keys.
[ruby-core:35327] [Bug #4421]
```

Previous revision: 31507

M ChangeLog
M ext/openssl/openssl_pkey_rsa.c

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@31520 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 31520 - 05/11/2011 09:51 PM - emboss

Thu May 12 07:27:31 2011 Martin Bosslet Martin.Bosslet@gmail.com

```
* ext/openssl/openssl_pkey_rsa.c: Use generic X.509 SubjectPublicKeyInfo
format for encoding RSA public keys.
[ruby-core:35327] [Bug #4421]
```

Previous revision: 31507

M ChangeLog
M ext/openssl/openssl_pkey_rsa.c

Revision 31520 - 05/11/2011 09:51 PM - emboss

Thu May 12 07:27:31 2011 Martin Bosslet Martin.Bosslet@gmail.com

```
* ext/openssl/openssl_pkey_rsa.c: Use generic X.509 SubjectPublicKeyInfo
format for encoding RSA public keys.
```

[ruby-core:35327] [Bug #4421]

Previous revision: 31507

M ChangeLog
M ext/openssl/ssl_pkey_rsa.c

Revision 31520 - 05/11/2011 09:51 PM - emboss

Thu May 12 07:27:31 2011 Martin Bosslet Martin.Bosslet@gmail.com

```
* ext/openssl/ssl_pkey_rsa.c: Use generic X.509 SubjectPublicKeyInfo
format for encoding RSA public keys.
[ruby-core:35327] [Bug #4421]
```

Previous revision: 31507

M ChangeLog
M ext/openssl/ssl_pkey_rsa.c

Revision 31520 - 05/11/2011 09:51 PM - emboss

Thu May 12 07:27:31 2011 Martin Bosslet Martin.Bosslet@gmail.com

```
* ext/openssl/ssl_pkey_rsa.c: Use generic X.509 SubjectPublicKeyInfo
format for encoding RSA public keys.
[ruby-core:35327] [Bug #4421]
```

Previous revision: 31507

M ChangeLog
M ext/openssl/ssl_pkey_rsa.c

Revision 31520 - 05/11/2011 09:51 PM - emboss

Thu May 12 07:27:31 2011 Martin Bosslet Martin.Bosslet@gmail.com

```
* ext/openssl/ssl_pkey_rsa.c: Use generic X.509 SubjectPublicKeyInfo
format for encoding RSA public keys.
[ruby-core:35327] [Bug #4421]
```

Previous revision: 31507

M ChangeLog
M ext/openssl/ssl_pkey_rsa.c

Revision 31520 - 05/11/2011 09:51 PM - emboss

Thu May 12 07:27:31 2011 Martin Bosslet Martin.Bosslet@gmail.com

```
* ext/openssl/ssl_pkey_rsa.c: Use generic X.509 SubjectPublicKeyInfo
format for encoding RSA public keys.
[ruby-core:35327] [Bug #4421]
```

Previous revision: 31507

M ChangeLog
M ext/openssl/ssl_pkey_rsa.c

Revision cb57042b - 05/13/2011 07:25 PM - emboss

Sat May 14 04:19:06 2011 Martin Bosslet Martin.Bosslet@gmail.com

```
* NEWS: Describe altered behaviour for RSA and DSA public key
encoding. [Ruby 1.9 - Bug #4421, Bug #4422]
[ruby-core:35327, 35328]
```

Previous revision: 31553

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@31554 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 31554 - 05/13/2011 07:25 PM - emboss

Sat May 14 04:19:06 2011 Martin Bosslet Martin.Bosslet@gmail.com

* NEWS: Describe altered behaviour for RSA and DSA public key encoding. [Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]

Previous revision: 31553

Revision 31554 - 05/13/2011 07:25 PM - emboss

Sat May 14 04:19:06 2011 Martin Bosslet Martin.Bosslet@googlemail.com

* NEWS: Describe altered behaviour for RSA and DSA public key encoding. [Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]

Previous revision: 31553

Revision 31554 - 05/13/2011 07:25 PM - emboss

Sat May 14 04:19:06 2011 Martin Bosslet Martin.Bosslet@googlemail.com

* NEWS: Describe altered behaviour for RSA and DSA public key encoding. [Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]

Previous revision: 31553

Revision 31554 - 05/13/2011 07:25 PM - emboss

Sat May 14 04:19:06 2011 Martin Bosslet Martin.Bosslet@googlemail.com

* NEWS: Describe altered behaviour for RSA and DSA public key encoding. [Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]

Previous revision: 31553

Revision 31554 - 05/13/2011 07:25 PM - emboss

Sat May 14 04:19:06 2011 Martin Bosslet Martin.Bosslet@googlemail.com

* NEWS: Describe altered behaviour for RSA and DSA public key encoding. [Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]

Previous revision: 31553

Revision 31554 - 05/13/2011 07:25 PM - emboss

Sat May 14 04:19:06 2011 Martin Bosslet Martin.Bosslet@googlemail.com

* NEWS: Describe altered behaviour for RSA and DSA public key encoding. [Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]

Previous revision: 31553

Revision ad10cfcb - 05/14/2011 01:33 AM - emboss

Sat May 14 10:32:36 2011 Martin Bosslet Martin.Bosslet@googlemail.com

* test/openssl/test_pkey_rsa.rb: Add tests that ensure new public key encoding behavior and also ensure backward compatibility. [Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]

previous revision: 31559

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@31560 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 31560 - 05/14/2011 01:33 AM - emboss

Sat May 14 10:32:36 2011 Martin Bosslet Martin.Bosslet@googlemail.com

* test/openssl/test_pkey_rsa.rb: Add tests that ensure new public key encoding behavior and also ensure backward compatibility. [Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]

previous revision: 31559

Revision 31560 - 05/14/2011 01:33 AM - emboss

Sat May 14 10:32:36 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* test/openssl/test_pkey_rsa.rb: Add tests that ensure new public key
encoding behavior and also ensure backward compatibility.
[Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]
```

previous revision: 31559

Revision 31560 - 05/14/2011 01:33 AM - emboss

Sat May 14 10:32:36 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* test/openssl/test_pkey_rsa.rb: Add tests that ensure new public key
encoding behavior and also ensure backward compatibility.
[Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]
```

previous revision: 31559

Revision 31560 - 05/14/2011 01:33 AM - emboss

Sat May 14 10:32:36 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* test/openssl/test_pkey_rsa.rb: Add tests that ensure new public key
encoding behavior and also ensure backward compatibility.
[Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]
```

previous revision: 31559

Revision 31560 - 05/14/2011 01:33 AM - emboss

Sat May 14 10:32:36 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* test/openssl/test_pkey_rsa.rb: Add tests that ensure new public key
encoding behavior and also ensure backward compatibility.
[Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]
```

previous revision: 31559

Revision 31560 - 05/14/2011 01:33 AM - emboss

Sat May 14 10:32:36 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* test/openssl/test_pkey_rsa.rb: Add tests that ensure new public key
encoding behavior and also ensure backward compatibility.
[Ruby 1.9 - Bug #4421, Bug #4422] [ruby-core:35327,35328]
```

previous revision: 31559

History

#1 - 02/22/2011 09:44 AM - naruse (Yui NARUSE)

- Status changed from Open to Assigned
- Assignee set to nahi (Hiroshi Nakamura)

=begin

=end

#2 - 04/22/2011 06:35 PM - naruse (Yui NARUSE)

=begin
Hi, Martin,

We don't have enough resource and knowledge about ext/openssl. So do you need a commit bit?

If you want, please express it; and after the approval of matz, you can commit to our repo.
(of course, before a commit you need to reach a consensus)

See also [DeveloperHowTo](#) and [CommitterHowTo](#).

=end

#3 - 04/23/2011 05:10 AM - MartinBosslet (Martin Bosslet)

=begin
Hi Yui,

Yes, I'd love to contribute and I would really appreciate it!
=end

#4 - 05/10/2011 07:37 AM - MartinBosslet (Martin Bosslet)

Hi all,

now that I have SVN access - would it be fine if I assigned the issues that I reported and that are still open to myself?
What about those already assigned?

Regards,
Martin

#5 - 05/10/2011 07:59 AM - naruse (Yui NARUSE)

Welcome to committers!
Yeah you can change the assignee and commit the patch.

#6 - 05/10/2011 09:01 AM - MartinBosslet (Martin Bosslet)

- Assignee changed from nahi (Hiroshi Nakamura) to MartinBosslet (Martin Bosslet)

Great :) Thanks for all the help so far!

#7 - 05/10/2011 09:29 AM - tenderlovmaking (Aaron Patterson)

- ruby -v changed from ruby 1.9.2p180 (2011-02-18 revision 30909) [i686-linux] to -

On Tue, May 10, 2011 at 07:37:13AM +0900, Martin Bosslet wrote:

Issue [#4421](#) has been updated by Martin Bosslet.

Hi all,

now that I have SVN access - would it be fine if I assigned the issues that I reported and that are still open to myself?

Yay! Congrats Martin!

--
Aaron Patterson
<http://tenderlovmaking.com/>

#8 - 05/12/2011 06:51 AM - Anonymous

- Status changed from Assigned to Closed
- % Done changed from 0 to 100

This issue was solved with changeset r31520.
Martin, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

Thu May 12 07:27:31 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* ext/openssl/openssl_pkey_rsa.c: Use generic X.509 SubjectPublicKeyInfo
format for encoding RSA public keys.
[ruby-core:35327] [Bug #4421]
```

Previous revision: 31507

M ChangeLog
M ext/openssl/openssl_pkey_rsa.c

#9 - 05/13/2011 01:32 PM - nahi (Hiroshi Nakamura)

Martin: Congrats! Go ahead.

Some comments;

- Please add a test for each commit to express the intent of the change. It must help us in the future.
- Please add some description about PKey format change to NEWS file. I think this change is OK (our older ruby should be able to read new format) but DSA might have some incompat behavior. DSA#p could be nil? Test it!

Regards,
// NaHi

#10 - 05/14/2011 06:23 AM - MartinBosslet (Martin Bosslet)

First of all thanks for the kind words!

Some comments;

Â * Please add a test for each commit to express the intent of the change. It must help us in the future.

The real benefit of applying this patch and <http://redmine.ruby-lang.org/issues/4422> is that <http://redmine.ruby-lang.org/issues/4424> becomes possible. You can create a PKey without knowing what kind of key it actually is, much like what EVP_PKEY allows in OpenSSL itself. I have included tests in 4424 that would test the changes in this patch and 4422. If there is no objection, maybe I could commit 4424 to add the tests and make the intent more clear? I was reluctant about the naming in 4424, maybe you could help me out?

Â * Please add some description about PKey format change to NEWS file. I think this change is OK (our older ruby should be able to read new format) but DSA might have some incompat behavior. DSA#p could be nil? Test it!

I'll add explicit tests for DSA and RSA that will use the old format to "prove" backwards compatibility. Thanks for the hint with DSA. I'll add the tests and fix it should any incompatibility show up. I also added a few words to NEWS!

Regards,
Martin

#11 - 05/16/2011 12:23 PM - naruse (Yui NARUSE)

Hi,

thank you for your contributions!

I have another comment: nahi and emboss's commit message has extra header and indent like:

Mon May 16 05:13:20 2011 Martin Bosslet Martin.Bosslet@googlemail.com

```
* ext/openssl/openssl_asn1.c: Add documentation.
```

Previous revision: 31583

It should be

- ext/openssl/openssl_asn1.c: Add documentation.

--

NARUSE, Yui Â naruse@airemix.jp

#12 - 06/20/2011 02:23 PM - nahi (Hiroshi Nakamura)

On Mon, May 16, 2011 at 11:47, NARUSE, Yui naruse@airemix.jp wrote:

I have another comment: nahi and emboss's commit message has extra header and indent like:

Mon May 16 05:13:20 2011 Â Martin Bosslet Â Martin.Bosslet@googlemail.com

Â Â * ext/openssl/openssl_asn1.c: Add documentation.

Previous revision: 31583

It should be

- ext/openssl/openssl_asn1.c: Add documentation.

OK. I copied ChangeLog and left it. I changed my style.

Thanks for your suggestion!

Regards,
// NaHi

#13 - 03/13/2012 01:32 AM - ntalbott (Nathaniel Talbott)

FYI, this does seem to break compatibility if you're using a fingerprint of the key for something, since (I just learned) key fingerprints are dependent on the format the key is stored in (since the fingerprint is based on the MD5 of the der-encoded key). Not sure there's much that can be done, but figured I'd leave this note here for anyone else that comes along later and encounters breakage due to this.

Our solution is to do a temporary hack to continue to spit out the old fingerprint, and migrate to a fingerprint based on the new format. Tricky, but doable.

#14 - 03/13/2012 05:25 AM - MartinBosslet (Martin Bosslet)

Nathaniel Talbott wrote:

FYI, this does seem to break compatibility if you're using a fingerprint of the key for something, since (I just learned) key fingerprints are dependent on the format the key is stored in (since the fingerprint is based on the MD5 of the der-encoded key). Not sure there's much that can be done, but figured I'd leave this note here for anyone else that comes along later and encounters breakage due to this.

Our solution is to do a temporary hack to continue to spit out the old fingerprint, and migrate to a fingerprint based on the new format. Tricky, but doable.

Yes, unfortunately this broke things like fingerprints - someone approached me about a similar issue not that long ago. What might help in the process of migration is the fact that it is not too hard to port the pre-1.9.3 format to the newer X.509 public key format [1]. Similarly, you could also do the "downgrade" from the 1.9.3 format to the PKCS#1 format used by pre-1.9.3, allowing you to keep the old fingerprints.

If this would help you in your migration process and you need the latter instead of the former, let me know, I could also provide a code sample for that case.

-Martin

[1] <https://gist.github.com/1470287>

#15 - 03/20/2012 05:31 AM - wolfgangw (Wolfgang Woehl)

MartinBosslet (Martin Bosslet) wrote:

[...] and you need the latter instead of the former, let me know, I could also provide a code sample for that case.

Martin, I'd appreciate an example for the latter, yes, thanks in advance. In my code I need to reach public key digests which correspond to info embedded in X.509v3 certs' CNs (generated elsewhere, not with some ruby/openssl) and 1.9.3(-p125) breaks this.

Also I'm wondering: With 1.8.7-p352 and 1.9.2-p290 I can reproduce values computed by openssl 0.9.8k. With 1.9.3-p125 I cannot. So did openssl's default encoding change?

Here's what I'm doing:

```
$ openssl x509 -pubkey -noout -in x509v3.pem | openssl base64 -d | dd bs=1 skip=24 2> /dev/null | openssl sha1 -binary | openssl base64  
NPq2kOXj9wUCE/Q/L+YSWm8Es9k=
```

```
$ irb
```

```
RUBY_VERSION  
=> "1.9.2"
```

```
cert = OpenSSL::X509::Certificate.new( open 'x509v3.pem' )
```

```
=> #
```

```
puts cert.public_key.to_pem  
-----BEGIN RSA PUBLIC KEY-----  
MIIBCgKCAQEA7YZMQoS91QPXD1IMbyJQIK7jPidOMZ2hCsuq6UaJQslyqDuu3RkJ  
3Byl2xayvFmt7NSAwUEQvaCC0hoUPASB9GJJ9G/nAk4kPP1vbSmnyEjeWe+deb+m
```

```
6BB9/4GvRnacoHYw2MoOXScqrLVBj2JoNvSXcPjqxZ266bb8b0mznuDubGACOH8L
luATgTdomeBmh80hl+Kpb4mfFKoyNGoIQPSybwoFDzTxgDo1YHD/rUgCF8Djim9W
c+/Rllz5q+FhxsZ9VgxY0E2yV6vdUML+n4fqK9QmM9Z0e9X5TOz5Ntj6lZFCjmE
Hot18W+HNhncghiPkfEMDwyldP+/797ruwIDAQAB
-----END RSA PUBLIC KEY-----
=> nil
```

```
asn1 = Base64.decode64( cert.public_key.to_pem.split( "\n" )[ 1 .. -2 ].join )
=>
"0x82x01xn02x82x01x01x00xEDx86LBx84xBDxD5x03xD7x0FYLo"Px94xAExE3>'N1x9DxA1nxCBxA1xE9FxB9BxC22xA
8;xAExDDx19ftxDCx1Cx0A5xDBx16xB2xBCYxADxECD4x80xC1A1x10xBDxA0x82xD2x1A1x14<x04x81xF4b\F4oxE7x02
N$<xFDom)xA7xC8HxDEYxEFxB9DyxBFxA6xE8x10}xFFx81xAFFv\x9CxA0v0xD8xCAx0EJ]*ACxB5A'bh6xF4x97p\F8xEAx
C5x9DxBAxE9xB6\FCoLxB3x9E\xE0\xEE\x028x7Fv\x96\xE0x13x817h\x99\xE0fx87xCD!\x97xE2xA9o\x89\x9F\x14xAA24j\b@x
F4xB2o\n\x05x0F4\F1x80:5p\xFF\xADH\x02x17xC0xE3x8AoS\xEFxD1x96\F9\xABxE1axC6xCC\FDV\fecA6xC9
\xAFuCl\xFA--\x1FxA8\xAFP\x98\xCFYxD1\xEFWxE53xB3xE4xDBc\xEAVE\n9x84\x1E\x8Bu\F1o\x876x19xDCx82x18x8F\x91\xF1f\x0Ff\xA5t\xFF\xBF\xEF\xDE\xEB\xBB\x02\x03\x01\x00\x01"

dnq_calc = Base64.encode64( OpenSSL::Digest.new( 'sha1', asn1 ).digest ).chomp
=> "NPq2kOXj9wUCE/Q/L+YSWm8Es9k="
exit
```

```
$ rbenv global 1.9.3-p125
$ irb
```

```
RUBY_VERSION
=> "1.9.3"
cert = OpenSSL::X509::Certificate.new( open 'x509v3.pem' )
```

```
=> #
```

```
puts cert.public_key.to_pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE7YZMQoS91QPXD1IMbyJQ
IK7jPidOMZ2hCsuq6UaJQslyqDuu3Rk3Byl2xayvFmt7NSAwUEQvaCC0hoUPASB
9GJJ9G/nAk4kPP1vbSmnyEjeWe+deb+m6BB9/4GvRnacoHYw2MoOXScqrLVBj2Jo
NvSXcPjqxZ266bb8b0mznuDubGACOH8LluATgTdomeBmh80hl+Kpb4mfFKoyNGoI
QPSybwoFDzTxgDo1YHD/rUgCF8Djim9Wc+/Rllz5q+FhxsZ9VgxY0E2yV6vdUML
+n4fqK9QmM9Z0e9X5TOz5Ntj6lZFCjmEHot18W+HNhncghiPkfEMDwyldP+/797r
uwIDAQAB
-----END PUBLIC KEY-----
=> nil
```

```
asn1 = Base64.decode64( cert.public_key.to_pem.split( "\n" )[ 1 .. -2 ].join )
=>
"0x82x01"0rx06t*x86Hx86xF7rx01x01x05x00x03x82x01x0F0x000x82x01xn02x82x01x01x00xEDx86LBx84xBDxD5\
x03xD7x0FYLo"Px94xAExE3>'N1x9DxA1nxCBxA1xE9FxB9BxC22xA8;xAExDDx19ftxDCx1Cx0A5xDBx16xB2xBCYxADxE
CxD4x80xC1A1x10xBDxA0x82xD2x1A1x14<x04x81xF4b\F4oxE7x02N$<xFDom)xA7xC8HxDEYxEFxB9DyxBFxA6xE8x10}\x
FFx81xAFFv\x9CxA0v0xD8xCAx0EJ]*ACxB5A'bh6xF4x97p\F8xEAxC5x9DxBAxE9xB6\FCoLxB3x9E\xE0\xEE\x028x7Fv\x9
6xE0x13x817h\x99\xE0fx87xCD!\x97xE2xA9o\x89\x9F\x14xAA24j\b@x\F4xB2o\n\x05x0F4\F1x80:5p\xFF\xADH\x02x17xC0xE3\
x8AoS\xEFxD1x96\F9\xABxE1axC6xCC\FDV\fecA6xC9
\xAFuCl\xFA--\x1FxA8\xAFP\x98\xCFYxD1\xEFWxE53xB3xE4xDBc\xEAVE\n9x84\x1E\x8Bu\F1o\x876x19xDCx82x18x8F\x91\xF1f\x0Ff\xA5t\xFF\xBF\xEF\xDE\xEB\xBB\x02\x03\x01\x00\x01"

dnq_calc = Base64.encode64( OpenSSL::Digest.new( 'sha1', asn1 ).digest ).chomp
=> "7pxBugGtDPy/CAbE8IDHuj4LUY4="
```

#16 - 06/10/2012 06:50 AM - MartinBosslet (Martin Bosslet)

Sorry Wolfgang, I just saw your request. Better late than never, here's the example for what you asked for: <https://gist.github.com/2902696>

To reproduce the same digests as you got in pre-1.9.3, you need to create the format as in the gist, then compute the hash on that value. The default format has indeed changed with 1.9.3 (note the "BEGIN RSA PUBLIC KEY" vs. "BEGIN PUBLIC KEY"). We now use the more generic X.509 encoding of public keys instead of the RSA-specific PKCS#1 encoding.

#17 - 12/09/2013 10:32 PM - davidw (David Welton)

Hi,

It certainly would have been useful to have the code available in gist <https://gist.github.com/2902696> available in some form, because this patch broke backwards compatibility for a system I was working on.

Files

fix_rsa_pub_encoding.diff	1.65 KB	02/22/2011	MartinBosslet (Martin Bosslet)
noname	500 Bytes	05/10/2011	tenderlovemaking (Aaron Patterson)