Why I can't read openssl generated RSA pub key with PEM_read_RSAPublicKey?

Ask Question

Asked 9 years, 1 month ago Active 6 months ago Viewed 16k times

I'm trying to read a RSA public key generated with openssl like this:

```
Private Key:
    openssl genrsa -out mykey.pem 1024

Public Key afterwards:
    openssl rsa -in mykey.pem -pubout > somewhere.pub
```

Then I try to read:

```
FILE *keyfile = fopen("somewhere.pub", "r");
RSA *rsa_pub = PEM_read_RSAPublicKey(keyfile, NULL, NULL, NULL);
//rsa_pub == NULL!
```

When I'm reading the private key it works

```
FILE *keyfile = fopen("mykey.pem", "r");
RSA *rsa_pri = PEM_read_RSAPrivateKey(keyfile, NULL, NULL, NULL);
//all good
```

Any ideas?

I've read that openssl generate a X509 key of the RSA public key. But I could not manage to load even a X509 pub key.

Thanks

c encryption openssl rsa

share improve this question follow

edited Oct 19 '11 at 21:32 Book Of Zeus 47.9k 15 169 166

asked Oct 19 '11 at 7:48 Jonas Schnelli 9,777 3 43 57

add a comment

3 Answers

Active Oldest Votes

26

You might try `PEM_read_RSA_PUBKEY()` instead of `PEM_read_RSAPublicKey()`.

This is all about formats.

The default public key file format generated by openssl is the PEM format.

`PEM_read_RSA_PUBKEY()` reads the PEM format. `PEM_read_RSAPublicKey()` reads the PKCS#1 format.

So if you want to stick to `PEM_read_RSAPublicKey()` you could generate the public key file using the PKCS#1 format by specifying the `-outform DER` option when generating the public key.

share improve this answer follow

edited Oct 19 '11 at 17:05

answered Oct 19 '11 at 16:58 alk 65.7k 9 81 209

2 Have my upvote for writing an explanation far less cryptic than the one mentioned in the OpenSSL docs. – Imron Dec 26 '12 at 4:46

I generated public key with `-outform DER` but it still gives segmentation fault. – mustafa.yavuz Mar 17 '14 at 11:53

I want to read public key from memory not from file. I have used `PEM_read_bio_RSA_PUBKEY` but did not work. – mustafa.yavuz Mar 17 '14 at 12:15

@mustafa.yavuz: As these issues do not seem to be related tio this particular question, please pose your issue as a new question. – alk Mar 17 '14 at 13:27

18 This answer is incorrect and misleading. Both `PEM_read_RSA_PUBKEY` and `PEM_read_RSAPublicKey` read PEM format, but the former expects a SubjectPublicKeyInfo structure, while the latter expects a RSAPublicKey structure. The former, generated by the openssl command line tool, starts with BEGIN PUBLIC KEY, the latter starts with BEGIN RSA PUBLIC KEY. – Nikolai Apr 11 '14 at 8:31

show 2 more comments

3

it seems there are two format of rsa public key, with different encoding.

A. RSA_PUBKEY

```
RSA* rsaPubKey = PEM_read_bio_RSA_PUBKEY( bio, NULL, 0, pass ) ;
```

read `PUBKEY` with this format

```
-----BEGIN PUBLIC KEY-----
...
-----END PUBLIC KEY-----
```

generated by

```
$ openssl rsa -in key.pri -pubout -out key.pub1
```

B. RSAPublicKey

```
RSA* rsaPubKey = PEM_read_bio_RSAPublicKey( bio, NULL, 0, pass ) ;
```

read `PublicKey` with this format

```
-----BEGIN RSA PUBLIC KEY-----
...
-----END RSA PUBLIC KEY-----
```

generated by

```
$ openssl rsa -in key.pri -RSAPublicKey_out -out key.pub2
```

convert

A to B format

```
$ openssl rsa -in key.pub1 -pubin -RSAPublicKey_out -out key.pub2_
```

B to A format

```
$ openssl rsa -in key.pub2 -RSAPublicKey_in -pubout -out key.pub1_
```

share improve this answer follow

edited May 20 at 11:11

answered Jan 24 '19 at 21:56 yurenchen 825 10 11

add a comment

1

> The openssl rsa utility saves the public key using the function PEM_write_bio_RSA_PUBKEY and not PEM_write_bio_RSAPubicKey. So, if you want your program to be compatible with its output, then you should use PEM_write_bio_RSA_PUBKEY and PEM_read_bio_RSA_PUBKEY for saving/loading public key files.

http://openssl.6102.n7.nabble.com/RSA-public-private-keys-only-work-when-created-programatically-td12532.html

share improve this answer follow

answered Sep 8 '17 at 3:19 徐谷苦 11 1

add a comment

Your Answer

Sign up or log in

Sign up using Google

Sign up using Facebook

Sign up using Email and Password

Post as a guest

Name

Email

Required, but never shown

Post Your Answer

By clicking "Post Your Answer", you agree to our terms of service, privacy policy and cookie policy

Not the answer you're looking for? Browse other questions tagged c encryption openssl rsa or ask your own question.