Does .pem file contain both private and public keys?

Asked 13 years, 2 months ago Modified 1 year, 3 months ago

Viewed 117k times

88

I am wondering if PEM-files contain both private and public keys? What does "PEM" stand for?

security ssl ssh openssl

Share

Improve this question

Follow

edited May 6, 2020 at 10:26

Spontifixus

6,660 ● 9 ● 47 ● 64

asked Sep 24, 2011 at 14:28

user705414

21.1k ● 42 ● 118 ● 162

1 related: Convert pem key to ssh-rsa format – ryenus Sep 4, 2019 at 6:31

2 Answers

Sorted by: Highest score (default)

A PEM file may contain just about anything including a public key, a private key, or both, because a PEM file is not a standard. In effect PEM just means the file contains

118

a base64-encoded bit of data. It is called a PEM file by allusion to the old **P**rivacy-**E**nhanced **M**ail standards which preceded S/MIME as a mail security standard. These standards specified the format of various keys and messages in a particular base64 format. See RFC 1421 for example.

Typically a PEM file contains a base64 encoded key or certificate with header and footer lines of the form `-----BEGIN <whatever>-----` and `-----END <whatever>----`. Over time there have evolved many possibilities for `<whatever>`, including private keys, public keys, X509 certificates, PKCS7 data, files containing multiple certificates, files containing both the private key and the X509 certificate, PKCS#10 certificate signing requests, ...

RFC 7468 has been written to document this de facto format.

Share Improve this answer Follow

edited Aug 30, 2023 at 20:31

answered Sep 24, 2011 at 14:31

President James K. Polk

41.9k ● 26 ● 107 ● 142

7 Thanks for explaining what the abbreviation stands for – hek2mgl Nov 29, 2013 at 14:50

@hek2mgl The abbreviation was originally for *PEM Encapsulation Mechanism*, according to the explanation in mentioned RFC 7468. – not2savvy Jan 9 at 13:51

@not2savvy: RFC 7469 does not say *PEM* is an abbreviation for *PEM Encapsulation Mechanism*.
– President James K. Polk Jan 9 at 14:16

@PresidentJamesK.Polk Quoting from RFC 4768, Introduction, page 3: *The tradition within the RFC series can be traced back to Privacy- Enhanced Mail (PEM) [RFC1421], based on a proposal by Marshall Rose in Message Encapsulation [RFC934]. Originally called "PEM encapsulation mechanism", [...]* – not2savvy Jan 9 at 15:08

1 @not2savvy: Yes, that's the encapsulation mechanism, but it doesn't say PEM is an abbreviation for PEM encapsulation mechanism. It's not a recursive acronym like GNU.
– President James K. Polk Jan 9 at 19:43

36

You can decode your PEM formatted x509 certificate with the following command:

```
openssl x509 -in cert.pem -text -noout
```

PEM certificate contains public key only **or** private key only **or** both.

For the following example:

```
-----BEGIN CERTIFICATE-----
MIICLDCCAdKgAwIBAgIBADAKBggqhkjOPQQDAjB9MQswCQYDVQQG
A1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2VydGlmaWNh
aXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdudVRMUyBj
ZSBhdXRob3JpdHkwHhcNMTEwNTIzMjAzODIxWhcNMTIxMjIyMDc0
CQYDVQQGEwJCRTEPMA0GA1UEChMGR251VExTMSUwIwYDVQQLExxH
dGlmaWNhdGUgYXV0aG9yaXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAj
dVRMUyBjZXJ0aWZpY2F0ZSBhdXRob3JpdHkwWTATBgcqhkjOPQIB
```

```
BwNCAARS2I0jiuNn14Y2sSALCX3IybqiIJUvxUpj+oNfzngvj/Ni
uQ4RTEiywK87WRcWMGgJB5kX/t2no0MwQTAPBgNVHRMBAf8EBTAD
DwEB/wQFAwMHBgAwHQYDVR0OBBYEFPC0gf6YEr+1KLlkQAPLzB9m
SM49BAMCA0gAMEUCIDGuwD1KPyG+hRf88MeyMQcqOFZD0TbVleF+
l4wOuDwKQa+upc8GftXE2C//4mKANBC6It01gUaTIpo=
-----END CERTIFICATE-----
```

you will get:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = BE, O = GnuTLS, OU = GnuTLS
certificate authority, ST = Leuven, CN = GnuTLS
certificate authority
        Validity
            Not Before: May 23 20:38:21 2011
GMT
            Not After : Dec 22 07:41:51 2012
GMT
        Subject: C = BE, O = GnuTLS, OU =
GnuTLS certificate authority, ST = Leuven, CN =
GnuTLS certificate authority
        Subject Public Key Info:
            Public Key Algorithm: id-
ecPublicKey
                Public-Key: (256 bit)
                pub:

04:52:d8:8d:23:8a:e3:67:d7:86:36:b1:20:0b:09:

7d:c8:c9:ba:a2:20:95:2f:c5:4a:63:fa:83:5f:ce:

78:2f:8f:f3:62:ca:fd:b7:f7:80:56:9d:6e:17:b9:

0e:11:4c:48:b2:c0:af:3b:59:17:16:30:68:09:07:
                    99:17:fe:dd:a7
                ASN1 OID: prime256v1
                NIST CURVE: P-256
```

```
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
```

To understand difference between `Public Key Algorithm` and `Signature Algorithm` sections read this (both are public).

Share Improve this answer Follow

edited Aug 1, 2017 at 14:55

answered Jul 30, 2017 at 9:19

patryk.beza
5,086 ● 5 ● 39 ● 57