

Re: CryptAPI(encryption/decryption)

Source:

<http://www.tech-archive.net/Archive/PocketPC/microsoft.public.pocketpc.developer/2007-06/msg00122.html>

- *From:* "Dylan DSilva \ (MS\)" <ddsilva@xxxxxxxxxxxxxx>
 - *Date:* Thu, 7 Jun 2007 12:07:56 -0700
-

<Common reply to both posts>

The PFX format encrypts the private key with the user supplied password so exchanging private keys using this format is as safe as using the PEM format. I would highly recommend using it since you've been having a lot of trouble with the conversion. This can be done by combining the .cer and .pem files into a PFX with OpenSSL on the server (with the command line `pkcs12 -export -in <CER file> -inkey <PEM file> -out <PFX file>`) transferring the PFX file over to the device and then importing it and getting a handle to the key.

—
Dylan DSilva
Software Development Engineer
Microsoft Corporation

This posting is provided "AS IS" with no warranties, and confers no rights. You assume all risk for your use. © Microsoft Corporation. All rights reserved.

"S.Kumar" <SKumar@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:A493FBFB-14D9-4240-AF44-71D7D2EECF24@xxxxxxxxxxxxxxxxxxxxx

Hi DSilva

Thanks for the valid information. I tried with a sample .pfx file and its getting the handle of the private key. But actually I need to import the pem format private key into the CSP. The private key is available in the server and I have to use this private key to decrypt the encrypted data that is encrypted using its Public key. I got a tool named "pvktool" which saying it will convert to PRIVATEKEYBLOB but while importing its saying bad data. Is there any alternative way to do this or its compulsory that we have to use .pfx(pkcs#12) formats for windows mobile. Hope its not a good practice to keep the private keys in server as .pfx format. so we are trying to use .pem format.

Re: CryptAPI(encryption/decryption)

Thanks again
S.Kumar

"Dylan DSilva (MS)" wrote:

To answer your question – Yes, a PFX file will allow you to import both the certificate and the associated private key.

To get a handle to the private key after importing the PFX file you will need to locate the certificate in the store using the CertFindCertificateInStore API and then get access to the private key by calling the CryptAcquireCertificatePrivateKey API followed by the CryptGetUserKey API.

—
Dylan DSilva
Software Development Engineer
Microsoft Corporation

This posting is provided "AS IS" with no warranties, and confers no rights.
You assume all risk for your use. © Microsoft Corporation. All rights reserved.

"S.Kumar" <SKumar@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:426E69EC-624C-4DF7-941E-4E2C6850301C@xxxxxxxxxxxxxxxxxxxx

Hi Dsilva,
Thanks again. Thanks for your valid information.
I got one tool but its in JAVA. I don't have any idea about it.
I'm trying to understand the basics of these public key and Certificate.
I tried using the openssl library, tried to import the .pvk file after convertin with pvktool but noting is working for me. I'm in total mess.
I understood your reply to make the blob in the format given.
I'm in the R&D of how to make it.

One another doubt. If I use a PFX file instead of PEM can I import the private key?
I can import the PFX file using PFXImportCertStore(). Now I don't know how

Re: CryptAPI(encryption/decryption)

to proceed. Can you give some suggestion

Thanks
S.Kumar

"Dylan DSilva (MS)" wrote:

Yes, the PEM format is Base64 encoded and may additionally be encrypted with a symmetric cipher (AES, 3DES etc.). In addition to decoding it to unencrypted binary, you would need to create the PRIVATEKEYBLOB structure with the fields described in <http://msdn2.microsoft.com:80/en-us/library/ms884374.aspx>. Only a PRIVATEKEYBLOB can be imported into a Microsoft CSP. As I mentioned in my earlier post, you should be able to find tools that support this conversion.

--

Dylan DSilva
Software Development Engineer
Microsoft Corporation

This posting is provided "AS IS" with no warranties, and confers no rights.
You assume all risk for your use. ©
Microsoft Corporation. All rights reserved.

"S.Kumar"
<SKumar@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message
<news:B8B841E0-5299-4D5F-B619-EE6F7FF02B2D@xxxxxxxxxxxxxxxxxxxx>

Thanks DSilva,
I like to get little more details.
Is the PEM format is in base64 coded? If I convert the PEM to

Re: CryptAPI(encryption/decryption)

binary,
can
I
load it into Microsoft
CSP's?

Thanks in advance

S.Kumar.

"Dylan DSilva (MS)" wrote:

Unfortunately
the
Microsoft
CSPs do not
support
importing
keys in
pem
format. You
would need
to convert
your key to
the blob
format
described
in
<http://msdn2.microsoft.com/en-us/library/ms884374.aspx>
(I believe
there
are
tools out on
the internet
that let you
do this) or
use a
custom CSP
that
supports
keys in pem
format.

--

Dylan
DSilva
Software
Development
Engineer
Microsoft

Re: CryptAPI(encryption/decryption)

Corporation

This posting
is provided
"AS IS"
with no
warranties,
and confers
no
rights.
You assume
all risk for
your use. ©
Microsoft
Corporation.
All
rights
reserved.

"S.Kumar"

<SKumar@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in
message

news:D1B60822-0411-4666-8263-B58B2ECAF340@xxxxxxxxxxxx

Hi
All,

I'm
facing
a
problem
in
encryption
decryption.

I
have
the
privatekey
in
pem
format.

How
can

I
import
this
into
CSP
and
decrypt

Re: CryptAPI(encryption/decryption)

the
data
which
is
encrypted
using
public
key.

I
tried
using
CryptImportKey
(
but
no
success.

Thanks