

## Re: CryptAPI(encryption/decryption)

---

*Source:*

<http://www.tech-archive.net/Archive/PocketPC/microsoft.public.pocketpc.developer/2007-06/msg00403.html>

---

- *From:* "Dylan DSilva \ (MS\)" <[ddsilva@xxxxxxxxxxxxxx](mailto:ddsilva@xxxxxxxxxxxxxx)>
  - *Date:* Mon, 25 Jun 2007 14:53:12 -0700
- 

Glad to be of help. I understand that this caused you some grief, but I don't think that the Crypto API intended to support complete compatibility with OpenSSL. I believe your question about importing PEM keys was answered early in this thread :)

--  
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](mailto:SKumar@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:6CEB100D-F7CE-4D18-B1F1-A7B0A9EB552C@xxxxxxxxxxxxxxxxxxxx](mailto:news:6CEB100D-F7CE-4D18-B1F1-A7B0A9EB552C@xxxxxxxxxxxxxxxxxxxx)

Thanks DSilva,

Thanks a lot. It worked. The openssl encrypted data format is in bigendian according to block size. To import to MS CSP, I reversed the data byte array in a block and it worked. Thanks a lot for the intime help.

Why there is so many compatibility difference between MS Crypt and openssl?  
Is there any way I can import the PEM formated private key to the MS CSP and do operations on it?

Thanks,  
S.Kumar

"Dylan DSilva (MS)" wrote:

Sorry I misunderstood you the last time. The byte ordering of the

Re: CryptAPI(encryption/decryption)

encrypted  
data generated by openssl rsautl is the reverse of that which is accepted  
by  
the CryptDecrypt API. You will need to reverse the order of the encrypted  
bytes before passing them to CryptDecrypt. Also it seems that Step 4. is  
redundant since the Base64 encoding doesn't buy you anything.

--

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:A570F198-5EF0-402B-A287-76328E13B123@xxxxxxxxxxxxxxxxxxxx

Hi DSilva,

No, I'm decoding the base64 encoded data before trying to  
decrypt. My  
doubt  
is, Is there any format difference in the encrypted data  
between  
openssl  
and  
MS Crypto.  
I couldn't find any documents in the net stating these. Please  
help me.  
These are steps I did for creating the Key Pair and to encrypt  
the  
data.

1. openssl genrsa -out privkey.pem -f4 1024
2. openssl rsa -in privkey.pem -pubout -out pubkey.pem
3. openssl rsautl -pubin -inkey pubkey.pem -in string -out  
xcstring -encrypt  
(input file "string", output file "xcstring")
4. openssl base64 -e -in xcstring -out naptr1  
("naptr1" is the output file contains base64 encoded data)

I need to decrypt this data with the "privkey" in windows  
mobile. I  
could  
able to decode the base64 data to binary. can you tell me a  
suitable  
way  
to

Re: CryptAPI(encryption/decryption)

implement this. I'm digging the net for a suitable information, but still

I couldn't. Your feedback will be helpful.

Thanks,  
S.Kumar.

"Dylan DSilva (MS)" wrote:

It seems like you're missing the Base64 decode step when trying to decrypt the OpenSSL data.

--

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:736AA167-0632-44BB-B09F-B80CD8B3CD70@xxxxxxxxxxxxxxxxxxxx](mailto:news:736AA167-0632-44BB-B09F-B80CD8B3CD70@xxxxxxxxxxxxxxxxxxxx)

Hi DSilva,

Thanks for your replay. I misspelled the Private Key as Primary Key.

Thanks for taking pain to understand the issue. I'll narrate the whole issue here.

There are multiple users and for each there is a key pair (Private key/  
Public key). This is

Re: CryptAPI(encryption/decryption)

generated using openssl  
(genrsa ...). For  
example  
take  
two users user "A" and user  
"B". user "A" wants to send  
some message  
to  
user  
"B". so user "A" will get the  
user "B"'s Public Key and  
encrypt the  
data,  
base64 encode it and sends  
to user "B". user "B" will  
take this  
base64  
encoded Encrypted data,  
decode it to the encrypted  
string (base64  
decode)  
and  
decrypts it using B's private  
key. All this process is  
working fine  
in  
openssl.

I'm porting the client  
application for Windows  
Mobile and I need to  
decrypt  
the base64 encoded  
Encrypted string. I have the  
base64 encoded  
Encrypted  
data  
and the private key in PEM  
format. I could able to  
base64 decode.  
since  
PEM  
is not acceptable in  
Windows I made a .pfx out  
of this Private key  
and  
trying  
to Decrypt the data. my  
doubt is

Is it possible to import the

Re: CryptAPI(encryption/decryption)

keys made in openssl to  
Microsoft CSP?  
Is there any variation in the  
encryption format in openssl  
compared  
to  
CSP?

For me, following your  
suggestion, I could able to  
get the handle of  
the  
AT\_KEYEXCHANGE key  
and is possible to  
encrypt/decrypt the data.  
But  
when I  
tried to decrypt the data  
which is encrypted using  
openssl, I'm  
getting  
error  
as BAD\_DATA.  
I don't understand what is  
the issue or is my  
understanding is wrong  
about  
the Crypto. Please help.

Thanks,  
S.Kumar.

"Dylan DSilva (MS)" wrote:

I'm not  
entirely  
clear what  
you mean  
by "primary  
key". It  
seems  
that  
in  
your  
scenario B  
isn't using  
this primary  
key for  
decryption.  
Also make

Re: CryptAPI(encryption/decryption)

sure  
that  
the same  
options are  
used for  
encryption  
and  
decryption.

A common  
method  
used to send  
encrypted  
data is  
described  
here

<http://msdn2.microsoft.com/en-us/library/ms884369.aspx>.

In short A  
(sender)  
generates a  
symmetric  
session key  
(e.g. AES,  
DES key)  
which is  
used  
to  
encrypt the  
data. A  
encrypts  
this session  
key with B's  
public key  
and  
sends  
it along  
with the  
encrypted  
data. B uses  
his private  
key to  
decrypt  
the  
session key  
and then  
uses this  
session key  
to decrypt the  
data. This  
method  
is preferred

Re: CryptAPI(encryption/decryption)

over using  
the  
public/private  
key pair on  
the data  
directly  
since  
symmetric  
encryption  
is faster  
than public  
key  
encryption.

--

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:CCBCA988-E696-47DB-9899-5255F8780C9E@xxxxxxxxxxx](mailto:news:CCBCA988-E696-47DB-9899-5255F8780C9E@xxxxxxxxxxx)

Hi  
DSilva.

Thanks

Re: CryptAPI(encryption/decryption)

for  
your  
valid  
feedback  
on  
my  
doubts.

As  
per  
your  
reply  
I  
could  
get  
the  
handle  
of  
the  
private  
key.  
But  
while  
decrypting  
the  
data  
its  
saying  
BAD\_DATA.

what  
can  
be  
the  
reason?

Since  
I  
am  
a  
newbie  
I'm  
trying  
to  
understand  
the  
concepts.  
person  
A  
encrypted  
some

Re: CryptAPI(encryption/decryption)

Re: CryptAPI(encryption/decryption)

data  
using  
his  
primary  
key  
and  
B's  
Public  
key.  
Is  
it  
possible  
for  
B  
to  
decrypt  
the  
data  
using  
his  
Private  
Key.  
I  
have  
the  
encrypted  
data  
and  
the  
.pfx  
file  
containing  
the  
B's  
private  
key.

Regards,  
S.  
Kumar.

"Dylan  
DSilva  
(MS)"  
wrote:

<Common  
reply  
to

Re: CryptAPI(encryption/decryption)

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

Re: CryptAPI(encryption/decryption)

Re: CryptAPI(encryption/decryption)

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

Re: CryptAPI(encryption/decryption)

Re: CryptAPI(encryption/decryption)

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:A493FBFB-14D9-4240-AF44-71D7D2EECF](mailto:news:A493FBFB-14D9-4240-AF44-71D7D2EECF)

Hi  
DSilva

Thanks  
for  
the  
valid  
information.  
I  
tried

Re: CryptAPI(encryption/decryption)

Re: CryptAPI(encryption/decryption)

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

Re: CryptAPI(encryption/decryption)

Re: CryptAPI(encryption/decryption)

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  
compulsary  
that  
we  
have  
to  
use  
.pfx(pkcs#12)  
formats  
for  
windows  
mobile.  
Hope  
its  
not  
a  
good

Re: CryptAPI(encryption/decryption)

Re: CryptAPI(encryption/decryption)

practice  
to  
keep  
the  
private  
keys  
in  
server  
as  
.pfx  
format.  
so  
we  
are  
trying  
to  
use  
.pem  
format.

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

Re: CryptAPI(encryption/decryption)

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

Re: CryptAPI(encryption/decryption)

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:426E69EC-624C-4DF7-941E](mailto:news:426E69EC-624C-4DF7-941E)

Hi  
Dsilva,  
Thanks  
again.  
Thanks  
for  
your  
valid  
information.  
I  
got  
one

Re: CryptAPI(encryption/decryption)

Re: CryptAPI(encryption/decryption)

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  
converitn  
with  
pvktool  
but  
noting  
is  
working  
for  
me.  
I'm  
in  
total  
mess.  
I

Re: CryptAPI(encryption/decryption)

Re: CryptAPI(encryption/decryption)

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?