

## Re: Issues with SSL on Win CE 5.0

---

*Source:*

<http://www.tech-archive.net/Archive/WindowsCE/microsoft.public.windowsce.embedded/2007-06/msg00011.html>

---

- *From:* Tom <[kuhnto@xxxxxxxxxx](mailto:kuhnto@xxxxxxxxxx)>
  - *Date:* Fri, 01 Jun 2007 19:48:16 -0000
- 

On Jun 1, 3:33 pm, Tom <[kuh...@xxxxxxxxxx](mailto:kuh...@xxxxxxxxxx)> wrote:

On Jun 1, 3:10 pm, Tom <[kuh...@xxxxxxxxxx](mailto:kuh...@xxxxxxxxxx)> wrote:

On Jun 1, 2:56 pm, Tom <[kuh...@xxxxxxxxxx](mailto:kuh...@xxxxxxxxxx)> wrote:

On May 29, 7:46 pm, "Dylan DSilva \ (MS)"  
<[ddsi...@xxxxxxxxxxxxxxxx](mailto:ddsi...@xxxxxxxxxxxxxxxx)>  
wrote:

The CRYPT\_MACHINE\_KEYSET flag will cause the PFX blob to be imported into the HKLM certificate store whereas the web server looks for certificates in the HKCU certificate store. Removing the CRYPT\_MACHINE\_KEYSET import flag should fix your problem.

--  
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.

Re: Issues with SSL on Win CE 5.0

"Tom" <kuh...@xxxxxxxx> wrote in message

[news:1180446907.183805.33990@xx](mailto:news:1180446907.183805.33990@xx)

On May 26, 9:29 am, Tom  
<kuh...@xxxxxxxx>  
wrote:

Sorry about  
the cross  
post...

We are  
switching to  
a new CE  
hardware  
platform  
and in the  
process of  
transferring  
over our C#  
code that  
runs on it.  
The  
platform  
has a web  
server that  
uses SSL.  
We used to  
add a .cer  
and .pvk to  
the MY  
store  
and tell the  
web server  
to use it.  
Everything  
worked  
great. We  
then  
switched to  
only being

## Re: Issues with SSL on Win CE 5.0

allowed to  
use .PFX  
and .P12  
certs. Below  
is  
the code we  
are using. It  
is based on  
many  
examples  
on the  
groups and  
elsewhere.  
For some  
reason on  
out NEW  
platform,  
with new  
image, SSL  
no longer  
works with  
the server.  
The import  
code below  
still seems  
to work  
when I step  
through it,  
and the cert  
gets  
imported  
(Looking in  
Control  
Panel). But  
starting the  
HTTPD,  
will get the  
authentication  
error – "The  
web server  
cannot  
initialize  
SSL, no  
SSL actions  
will be  
performed.  
Error code  
=  
0x8009030d".  
This  
worked on

Re: Issues with SSL on Win CE 5.0

the previous  
hardware  
platform,  
but not this  
for some  
reason.

I can  
manually  
enter a CER  
and PVK  
through the  
control  
panel, and  
change the  
HTTPD\SSL  
key to  
reflect it,  
restart the  
web server,  
and it  
will work  
fine again.

I ensured  
that the  
PKCS #12  
component  
was added  
to the  
platform.

When  
importing  
the PFX the  
import flags  
are set for  
CRYPT\_MACHINE\_KEYSET  
|  
CRYPT\_EXPORTABLE.

Anyone  
know what  
could be  
causing  
this? Am I  
missing a  
flag  
somewhere?

I have been  
looking into  
this some

Re: Issues with SSL on Win CE 5.0

more. I  
have loaded  
the OS and  
our  
program  
onto  
another of  
the same  
platforms. I  
loaded the  
PFX  
through  
software  
and it did  
not work.  
But in  
checking  
the log for  
the HTTPD  
service, it  
did not have  
any errors.  
But I am  
getting  
weary of  
this  
log, as the  
dates do not  
seem to be  
matching  
anything. I  
then loaded  
the CER  
and PVK  
through the  
control  
panel and  
everything  
worked.  
BUT,  
when I  
reboot, The  
old cert was  
in. I guess I  
did not  
flush the  
registry. I  
readded and  
flushed, but  
on reboot it  
still does

Re: Issues with SSL on Win CE 5.0

not  
work. If I  
delete it and  
reinstall it,  
it will work.  
I did a  
comparison  
of the  
HKEY\_Local\_machine,  
at boot, and  
after  
reinstalling  
the  
certificate.  
Only one  
thing  
changed,  
but since I  
am  
not at the  
office right  
now, I can  
not  
remember  
the value,  
but it was  
under  
HTTPD  
somewhere.  
I will find  
out  
Tuesday.

```
FileInfo  
fileInfo =  
new  
FileInfo(sFileLocation);  
BinaryReader  
br = new  
BinaryReader(fileInfo.OpenRead());  
byte[] Bytes  
= new  
byte[fileInfo.Length];  
br.Read(Bytes,  
0,  
(int)fileInfo.Length);  
br.Close();
```

Re: Issues with SSL on Win CE 5.0

```
//We need
to marshal
the byte
array Bytes
into a
pointer
IntPtr buffer
=
Marshal.AllocHGlobal(Bytes.Length);
Marshal.Copy(Bytes,
0, buffer,
Bytes.Length);
```

```
//Create the
PFX Blob
CRYPT_DATA_BLOB
cryptBlob =
new
CRYPT_DATA_BLOB();
cryptBlob.cbData
=
(int)fileInfo.Length;
cryptBlob.pbData
= buffer;
```

```
//Check to
make sure
that the
BLOB is
valid
if
(PFXIsPFXBlob(ref
cryptBlob))
{
//Check the
password
if
(PFXVerifyPassword(ref
cryptBlob,
sCertPassword,
0))
{
uint
hTempCertStore
= 0;
uint
hContext =
```

Re: Issues with SSL on Win CE 5.0

```
0;
uint
dwImportFlags
=
CRYPT_MACHINE_KEYSET
|
CRYPT_EXPORTABLE;

//Import the
cert to temp
storage
hTempCertStore
=
PFXImportCertStore(ref
cryptBlob,
sCertPassword,
dwImportFlags);

//Make sure
tha thte
pointer is
not 0
if
(hTempCertStore
!= 0)
{
while
((hContext
=
CertEnumCertificatesInStore(hTempCertStore,
hContext))
!= 0)
{
//Get the
name and
issuer
char[]
cSubjectNameString
= new
char[256];
char[]
cIssuerNameString
= new
char[256];
```

Re: Issues with SSL on Win CE 5.0

```
int
nSubjectLength
=
CertGetNameString(hContext,
CERT_NAME_SIMPLE_DISPLAY_TYPE,
0,
IntPtr.Zero,
cSubjectNameString,
255);
int
nIssuerLength
=
CertGetNameString(hContext,
CERT_NAME_SIMPLE_DISPLAY_TYPE,
CERT_NAME_ISSUER_FLAG,
IntPtr.Zero,
cIssuerNameString,
255);
```

```
try
{
string
sSubject =
new
string(cSubjectNameString);
string
sIssuer =
new
string(cIssuerNameString);
```

```
sSubject =
sSubject.Substring(0,
nSubjectLength
- 1);
sIssuer =
sIssuer.Substring(0,
nIssuerLength
- 1);
```

```
//If the web
server
certificate is
being
updated,
you must
```

Re: Issues with SSL on Win CE 5.0

```
set the cert  
subject in  
the  
registry  
if  
(sCertStore.ToUpper()  
==  
"MY")  
{  
//Update the  
registry  
with  
the web  
server  
subject
```

```
JCIDUtils.RegistryHelper.SetRegistryKeyValue("Comm\\HTTPD\\S  
"CertificateSubject",  
sSubject);  
}
```

```
//Compare  
the subject  
to the  
issuer to see  
if the root  
cert is  
included  
if  
(sSubject.Equals(sIssuer))  
{  
//Open the  
JCID stores  
MY , CA  
and Root  
IntPtr  
hRootStore  
=  
IntPtr.Zero;  
//Add to  
root  
hRootStore  
=  
CertOpenStoreStringPara(CERT_STORE_PROV_SYSTEM_W,  
0,  
hRootStore,  
CERT_STORE_NO_CRYPT_RELEASE_FLAG
```

Re: Issues with SSL on Win CE 5.0

```
|  
CERT_SYSTEM_STORE_CURRENT_USER,  
"ROOT");
```

```
CertAddCertificateContextToStore((uint)hRootStore,  
hContext,  
CERT_STORE_ADD_REPLACE_EXISTING,  
0);
```

```
CertCloseStore((uint)hRootStore,  
0);  
}  
else  
{  
//Open the  
stores MY ,  
CA  
and Root  
IntPtr  
hStore =  
IntPtr.Zero;  
hStore =  
CertOpenStoreStringPara(CERT_STORE_PROV_SYSTEM_W,  
0, hStore,  
CERT_STORE_NO_CRYPT_RELEASE_FLAG  
|  
CERT_SYSTEM_STORE_CURRENT_USER,  
sCertStore);
```

```
CertAddCertificateContextToStore((uint)hStore,  
hContext,  
CERT_STORE_ADD_REPLACE_EXISTING,  
0);
```

```
CertCloseStore((uint)hStore,  
0);  
}  
}  
catch  
(Exception  
ex)  
{  
Logger.logException("Exception
```

Re: Issues with SSL on Win CE 5.0

```
in
ImportPFXCertificate(),
adding cert
to store",
ex);
}
}
```

```
Marshal.FreeHGlobal(cryptBlob.pbData);
```

```
//Close the
temp cert
storage
memory
CertCloseStore(hTempCertStore,
0);
bReturn =
true;
}
}
```

The only registry change was \comm\HTTPD and was the SystemChangeNumber. After rebooting, the number keeps incrementing, so I doubt that this is the problem.

I am still having problems with this. It is really driving me crazy.  
I removed the CRYPT\_MACHINE\_KEYSET, and the same thing still happens.  
I hate to

...

[read more »](#)

What is strange is that I can not view the ROOT cert I added in Remote

Re: Issues with SSL on Win CE 5.0

registry viewer. It keeps crashing on that particular value. Could it be corrupt in some strange way.