

Re: Smartcard CSP Problem

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2005-01/0063.html>

From: WinstonT (wyt168_at_earthlink.net)

Date: 01/10/05

Date: Mon, 10 Jan 2005 06:14:43 GMT

We are trying to do similar things too—except we do have a hardware USB flash drive with an embedded crypto processor to perform the encryption.

However, the crypto processor is not a smart card and it has its own crypto interface API for the application to access its crypto functions.

We are trying to write a custom CSP to allow apps to access the crypto processor via the CryptoAPI to perform things like two factor authentication. In a sense, we want the USB token to perform the exact function of a smart card.

Here's my questions:

1. Would a simple CSP DLL work in this case? My idea is to write the CSP DLL to access the native crypto processor's API and wrap them so as to expose these native API's as the CryptoSPI.

2. Is there a need to emulate a smart card? If the answer to Q1 is no, then I may have to write a driver to virtualize our USB token as a smart card. Do I have to emulated the complete PC/SC interface? i.e. do I have to emulate all the card tracking functions, the T=0, T=1 transactions, etc.?

3. From your comments below, it appears that MSGina actually monitor the card insertion/removal events to check for the physical presence of a smart card. Can we define a new custom class of devices such as USB tokens such that they can also be allowed for WinLogon or authentications?

Best regards,

Winston

"Eric Perlin [MS]" <ericperl@online.microsoft.com> wrote in message news:%23T0VpV%232EHA.1076@TK2MSFTNGP09.phx.gbl...

> *You don't need to emulate a smartcard CSP for it to work with S-MIME. A software CSP can be used in this case.*

> *But your "simulated" smartcard CSP is not going to work for Windows logon.*

> *Winlogon/msgina really look for physical smartcards.*

> *Without something that's exposed through the smartcard subsystem, you're*

> *not*

> *even going to get a PIN prompt.*

> --

> *Eric Perlin [MS]*

> *This posting is provided "AS IS" with no warranties, and confers no*

> *rights.*

> ---

>

> "Alf" <alf1982@hotmail.de> wrote in message
> news:eoy#CMg1EHA.2624@TK2MSFTNGP11.phx.gbl...
>> Hello, maybe somebody can help me out!
>>
>> I am to develop a SmartCard CSP, but with no actual SmartCard behind it,
> but
>> rather a Software System that simulates it.
>>
>> I so far developed a CSP which wrappes the MS Base CSP for the common
>> functionality and will use the System for the Rest.
>>
>> Now, I have a logical problem.
>>
>> The CSP should be used for Mail Signing and encrypting in Outlook, as
>> well
>> as for windows logon.
>>
>> If I understood the concept of the certificate handling in windows, you
> have
>> to enroll a certificate for a certain user who is present in the active
>> directory – let's call him Bob. When enrolling this certificate, you
> choose
>> the type (smartcard certificate) and the corresponding CSP (in this case,
> my
>> CSP).
>>
>> The result of the enrollement would be a new certificate stored on the
>> SmartCard and installed in windows.
>>
>> Question: Am I righth with the above?
>> Then – next Question: How does the enrollemnt process create and store
>> the
>> certificates on the SmartCard since the CryptoApi (CP*) functions do not
>> provide certification handling – Does the enrollement task itsself store
> the
>> certificate to the SmartCard? (And how, cia driver?)
>>
>> Are there any other usefull documentations on what a SmartCard CSP has to
>> implement?
>>
>> Thanks!
>>
>>
>>
>
>