

microsoft.public.platformsdk.security: Re: [SmartCard CSP] How can I obtain a PIN to sign HASH ?

Re: [SmartCard CSP] How can I obtain a PIN to sign HASH ?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2003-10/0136.html>

From: Euphen Liu (euphen_liu_at_ncksoft.com)

Date: 10/10/03

Date: Fri, 10 Oct 2003 10:52:35 +0800

Do you kindly tell me what are the differences between CRYPT_IMPL_MIXED and CRYPT_IMPL_HARDWARE ? I think CRYPT_IMPL_MIXED means that I implemented something based the smartcard and others by call some base CSP such as "Microsoft Base Cryptographic Provider v1.0". But from you email, the "CRYPT_IMPL_MIXED" means not call other CSP. Am I correct?

Let me explain this issue more clearly:

1. There are two method when use EAP to authenticate user, one is "Use my smart card", another is "Use a certificate on this computer". When I select the first one to logon the wireless network, Windows show me a "Input SmartCard PIN" dialog box, but when I select the second way, such dialog box never appear.
2. When I select the second way, the CSP caller (here is the WinLogon.exe, I guess), always call CPACquireContext() whit CRYPT_SILENT, so I can not obtain the user's PIN by myself.
3. When CPSignHash() be called, because there are not login into my smart card, so what I can do is fail with set last error code to NTE_SILENT_CONTEXT.

And I had tried the CRYPT_IMPL_MIXED | CRYPT_IMPL_REMOVEABLE, it still does not show the PIN require dialog box.

"Eric Perlin [MS]" <ericperl@microsoft.com> wrote in message news:eapWUXrjDHA.2416@TK2MSFTNGP10.phx.gbl...
> *Have you actually tried with CRYPT_IMPL_MIXED | CRYPT_IMPL_REMOVEABLE?*
> *I doubt that you implemented everything on the smartcard (it would be very slow) so this is actually the correct value.*
> --

Re: [SmartCard CSP] How can I obtain a PIN to sign HASH ?

microsoft.public.platformsdk.security: Re: [SmartCard CSP] How can I obtain a PIN to sign HASH ?

> Eric Perlin [MS]
> This posting is provided "AS IS" with no warranties, and confers no
rights.
> ---
>
> "Euphen Liu" <euphen_liu@ncksoft.com> wrote in message
> news:#Q9uQHxjDHA.1284@TK2MSFTNGP09.phx.gbl...
>> Hi all, (sorry for my pool English.)
>>
>> We have created a RSA-FULL CSP based SmartCard. It works fine with
>> IE/OE, etc.
>>
>> Now we are using wireless network connection with EAP (Use SmartCard or
>> other certificates) on WindowsXP(with SPI installed), I selected the
"Use
> a
>> certificate on this computer", when the network connected, my CSP be
>> called as following:
>> ...
>> ...
>> CPAcquireContext(...) [called with the container name, ok]
>> CPGetProvParam(..., PP_IMPTYPE) [return CRYPT_IMPL_HARDWARE /
>> CRYPT_IMPL_REMOVEABLE, ok]
>> CPCreateHash(...) [ok]
>> CPSetHashParam(...) [ok]
>> CPSignHash(...) [can not work because not logon to the smartcard, so
>> can not use the private key to sign data.]
>> ...
>>
>> I don't know why the system does not show the "Input the PIN" dialog box
>> just like I select "Use my smart card". How can I make the system show
> such
>> dialog box to obtain the PIN from user input?
>>
>> BTW, I searched all these archives and can not find any idea about this
>> issue, some one discuss the smart card CSP should return
>> CRYPT_IMPL_MIXED | CRYPT_IMPL_REMOVEABLE, but for my instance, we
>> does not call other base CSP, we implemented all functions/algorithms.
>> Some of the algorithms implemented as software like hashdata, some by
>> hardware like RSA-compute.
>>
>> I had try more than 5 days but can not find the right way.
>>
>> Is any body can resolve my problem?
>>
>>
>
>

Re: [SmartCard CSP] How can I obtain a PIN to sign HASH ?