

## Re: CA's Key on Smart Card Problem

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-01/0277.html>

---

**From:** S. Pidgorny (*slavickp\_at\_yahoo.com*)

**Date:** 01/23/05

Date: Sun, 23 Jan 2005 21:38:09 +1100

Steve,

As far as I know Microsoft is using HSMs for storing the root CA keys. At a very high level, HSM is the same thing as the smart cards: private key is protected and never leaves the device, Windows interacts with it using a CSP.

So some guideleines would be really appreciated.

Denis: I would try to use another card/CSP – to see if I'll have the same problem. I think that "not implemented" is kinda self-explanatory and some advanced CSP may indeed be required.

--

Svyatoslav Pidgorny, MVP, MCSE

= F1 is the key =-

"Steve Riley [MSFT]" <steriley@microsoft.com> wrote in message  
news:54751632419367852042832@news.microsoft.com...

> This really isn't something we test. Specifically, the problem you're  
seeing

> is because the CA runs as LocalSystem. But when you're getting the prompt  
> to enter the PIN, that's running in your user context.

>

> More importantly, though, remember that the CA needs to access its own  
private

> key every time it issues a certificate, so you'd need to leave the  
smartcard

> in the reader all the time, which pretty much negates the reason for using  
> a smartcard.

>

> Steve Riley

> steriley@microsoft.com

>

>

>

> > Hi.

> > To improve the security of an offline root CA I want to

> > store the CA's private Key on a Smart Card. During the

> > installation process of the certificate services I

> > selected a Smart Card CSP (Gemplus) and activated the

> > checkbox "Allow this CSP to interact with the desktop".

> > When the setup process generates the cryptographic key I

> > have to enter the PIN of the Smart Card and then I got an

> > error message box "An error occurred when setting the

microsoft.public.windows.server.security: Re: CA's Key on Smart Card Problem

> > security access on the private key "Name of the CA", or  
> > the CSP selected does not support setting security access  
> > on private keys. Please make sure the CSP is installed  
> > correctly or select another CSP. Not implemented  
> > 0x80004001 (-2147467263)". After this the installation of  
> > the certificate services fails. I've already tried tested  
> > this with different Smart Cards and different Computers,  
> > but always got the same error.  
> > Can anyone help me with the error, or has anyone already  
> > installed the CA's Key on a Smart Card, which Smart Card  
> > and CSP should I use?  
> > Thanks in advance,  
> >  
> > Denis  
> >  
>  
>