

Several questions on code signing / smartcards / Win CA

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-08/0272.html>

From: Martin (*MartinNae1_at_nospam.nospam*)

Date: 08/25/05

Date: Thu, 25 Aug 2005 04:24:03 -0700

I have a couple of questions around code signing with MS technology:

1. Is there a way to transfer the generated strong name signing private key directly to a smartcard (or generate it on the smart card), without the unsecure intermediate storage to the filesystem using `sn -k` and `sn -i`?
2. What is the format of the key files produced by `sn -k` and `sn -p`?
3. Is there a way to generate a PKCS#10 format certificate request from the `sn -p` public key for generation of a certificate with the Windows2003 server CA?
4. Is there any other way to generate a certificate with the Windows 2003 server CA from a `sn -p` public key?
5. How/what for can the certificate that is generated using Windows 2003 server CA and the Code Signing template be used? SN signing? Authenticode signing? DOTNET strong name signing? Sth else?
6. How do I write the certificate and private key that is generated using Windows 2003 server CA and the Code Signing template to a smart card (for this template the private key is marked non-exportable)?
7. How do I generate an authenticode SW publisher cert using the Windows 2003 server CA (without involving an external CA such as Verisign)?
8. For 7, how do I get that private key onto a smartcard?

After some additional experimentation, it seems that 6/7/8 could be solved if I was able to either

9. Create the new key pair for a Code Signing cert in the Windows CA directly into the smartcard using the smartcard CSP. Problem: I can in this user interface only select one of the three Windows CSPs, but not my smartcard CSP.

microsoft.public.windows.server.security: Several questions on code signing / smartcards / Win CA

or

10. Use for the generation of a Code Signing cert in the Windows CA a preexisting key pair in a container on my smartcard, which I generated either using `sn -k/sn -i`, or using `makecert` (diregarding the test cert). Again, this approach fails because I can not select the smartcard CSP as key source.

Thanks for any help/guidance!

Best regards,
Martin