

Re: Active Directory User Object certificate store to personal certificate store

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-02/0447.html>

From: Rob McShinsky (*List_at_mcshinsky.com*)

Date: 02/28/05

Date: Mon, 28 Feb 2005 09:16:29 -0500

So let me get this right. The certificates that are published to AD under the "Published Certificates" tab in AD users and computers, are not able to be used by applications? These are the certificates that show up in the "Active Directory User Object cert store" within the Certificate MMC.

Rob

"S. Pidgorny <MVP>" <slavickp@yahoo.com> wrote in message news:OU1EgEHHFHA.2276@TK2MSFTNGP15.phx.gbl...

> Rob,

>

> *Password protects a private key, not the certificate.*

>

> *Active Directory doesn't store private keys. The main goal of certificate publishing in AD is to make public key available to all other AD clients – that facilitates S/MIME encryption without perr key exchange, for example.*

> *When you're trying to utilise AD for private key storage, you're looking in*

> *a wrong direction.*

>

> *However, the keys and certificates are stored in the user profile – you can have roaming profiles that will follow the users.*

>

> *I recommend you to look into smart cards instead of "soft" certificates for "High security".*

>

> --

> *Svyatoslav Pidgorny, MVP, MCSE*

> *-- FI is the key --*

>

> *"Rob McShinsky" <List@mcshinsky.com> wrote in message news:euu0La2GFHA.3196@TK2MSFTNGP15.phx.gbl...*

>> *Is there a way to move AD published certs to from the Active Directory User*

microsoft.public.windows.server.security: Re: Active Directory User Object certificate store to personal certificate store

>> *Object cert store to the Personal cert store so that these will follow a*
>> *user around from computer to computer so they can be utilized by*
>> *applications. At the current time we are not looking at autoenrolling*
>> *certificates because we want to have users create High Security*
> *certificates*
>> *that will require a password before the cert is used for client*
>> *authentication. I can see the certs in the AD User Object cert store for*
>> *the user logged in but they are not accessible from IE, at least with my*
>> *current knowledge. This is where our current PKI test application is.*
>> *Is*
>> *there a GPO setting that will make these accessible within the Personal*
>> *store? Is there a way to have an application directly reference the AD*
> *User*
>> *Object cert store? Is there another programatic/scripting way to utilize*
>> *these certs? Thanks for your guidance on this subject.*
>>
>> *Rob McShinsky*
>>
>>
>
>