

Re: PKI Certificate Server Install in AD Empty Root Domain

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-07/0293.html>

From: FastEddie (fasteddie_at_therockwells.net.no.spam)

Date: 07/21/05

Date: Thu, 21 Jul 2005 15:11:28 -0500

Questions inline:

"Brian Komar" <MVPbkomar@nospam.identit.ca> wrote in message
news:MPG.1d49905ceafd6bb39896c3@msnews.microsoft.com...

> *Answers inline:*

>

>

>

> *In article <eVKgergjFHA.1232@TK2MSFTNGP15.phx.gbl>,*

> *fasteddie@therockwells.net.no.spam says...*

>> *Platform: Windows 2003 AD with an empty root*

>>

>> *We are installing an Enterprise CA in our Active Directory 2003 Forest.*

>> *All*

>> *our resources, users, and computers and effective GP settings are in a*

>> *domain under the empty forest root domain.*

>>

>> *My questions:*

>>

>> *If I install the CA in the forest root, will the certificates and auto*

>> *issuing of certificates work correctly in the other domains within the*

>> *forest or should I install the Enterprise CA in the domain that houses*

>> *all*

>> *the resources, machines and users?*

>

> *It really does not matter which domain you install the certificates in.*

> *Whichever domain you choose, you will have to do some additional work to*

> *issue certificates to other domains in the forest.*

> *1) Certificate templates. The default permissions will only include*

> *groups in the forest root domain. You must modify permissions for other*

> *domains to assign Read and Enroll perms (possibly autoenroll).*

> *2) Publication to AD to the userCertificate attribute. An enterprise CA*

> *by default can only publish certificates to user objects in the same*

> *domain. Follow the instructions in Q281271 "Windows 2000 CA Config. to*

> *Publish Certs in AD of Trusted Domain" to assign the correct perms to*

> *the Cert Publishers group to the other domains in the forest.*

microsoft.public.windows.server.security: Re: PKI Certificate Server Install in AD Empty Root Domain

>
>>
>> *Also, can I use this CA to issue certs in another Forest?*
>
> *No. A CA can only issue certs to users in the same forest. You can in
> some cases, if the subject is provided in the request, but what you may
> want to look at is a root that is not specific to either forest, and
> then subordinate CAs in each forest.*

So you are saying I could have a Ent CA in my forest root (forest A, Domain A) and a subordinate in my member domain (Forest A, Domain B) to auto issue certs for machines and accounts?

Then also have a Subordinate CA in Forest B but not in the root domain, in a sub domain Forest B...?

Both subordinates can auto issue certs for machines and accounts?

>>
>> *thanks,*
>>
>> *Fast Eddie*
>>
>>
>>
>
> --
> ==
> *Brian Komar*
> *MVP – Windows – Security*
> <http://www.identit.ca/blogs/brian>