

Re: Data Recovery Agent expired in Windows 2003 AD

enterprise CA for the domain. It's an old CA running windows 2000. It's a member of the domain, but that's about all I know about it.

To be honest I'm playing with the thought, to remove from AD and install a new windows 2003 Enterprise CA and design it correct (If I can figure out how to do that *Grins*)

I've just ordered "Microsoft® Windows ServerT 2003 PKI and Certificate Security " by Brian Komar, since my understanding of PKI is only basic and I need a bit more.

That's also the reason why I'm in a doubt, with the present situation. But I would very much like a real EFS design with recovery agents etc.

So if you have a link to some good guides I would very much appreciate it.

Yours Sincerely,
Benjamin

"Steven L Umbach" wrote:

Is your CA an enterprise CA?? If it is you should be able to logon to a known secure domain computer as a domain administrator and request a new Recovery Agent Certificate via the mmc snapin for certificates for user and then going to the personal/certificates folder, right click, select all tasks – request certificate. If that works you can export the RA certificate [not including private key] to a .cer file and then import that into your Group Policy PKI setting for EFS. Also you would then want to export the RA certificate and private key to a password protected .pfx file in offline media and store in a couple very secure places and you may want to delete it from the computer you generated it on. --- Steve

"Bendji" <Bendji@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:DF31AAE2-B91C-40DB-B867-D16E0D771EEB@xxxxxxxxxxxxxxxxxxxx

Greetings all,

Thanks for a great forum with a lot of knowledge. Hope I one day have the time to search it through and read all the interesting articles

But back to the topic. I've recently got the task to figure out a

Re: Data Recovery Agent expired in Windows 2003 AD

way
to
encrypt the companys data on laptops. My first thought was
to wait on
Vista
with BitLocker, but thats to far away in the horisont.

So I desided to use the build in EFS in windows.
I tried to rightclick on a folde and select advance and then
encrypt
but
did
receive the following error:

An error...Recovery policy configured for this system
contains invalid
recovery certificate.

I did enter the rsop.msc on the client and looked under
"Computer
configuration"-->"Windows settings"-->"Public Key
Policies"-->"Encrypting
File System", and here I find an old default certificat, which
is no
longer
valid. It's issue to "Administrator" and byt the
"administrator", so
its
proberly the default one from when the AD was created.

If I enter Active Directory Users and Computers and enter
the "default
domain policy" and looks under the above "road" I can see
thats it's
here
the
certificate gets distributed.

Now my problem is that I want people to be able to encrypt
files again
using
EFS, but I also want us "the company/administrators" to be
able to
decrypt
the files if an emplyee leaves. Any suggestoins on how I
create/renew
the
setup?

The network consists of 3 AD servers running windows
2003. We also have

Re: Data Recovery Agent expired in Windows 2003 AD

an
old CA running windows 2000 which is a member of the
domain (but no
real
PKI
atm).

Is there an easy way to make 2 recovery agents and
distribute them in
AD,
so the users can encrypt files? And that the administrators
can recover
encrypted files if a profile is lost etc.

Thanks in advance for any replies or links to places where I
can find
any
knowledge about this topic.

I've looked a bit on the following, which explains a bit about
it,
except
the
default administrator certificate which is expired in a
domain.

<http://www.atlguide2000.com/windowsxp/index.php?act=view&aid=114>

Btw any suggestions on a good Windows Certificate book,
would be
appreciated. One there tell the basis and then how to make a
full use
in
an
Windows 2003 environment with Exchange 2003 and ISA
2004. Always nice
to
have something to read in the sparetime

Yours Sincerely,
Benjamin