

CACertFileName: Chicken or Egg?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-01/0293.html>

From: Dave W (DaveW_at_discussions.microsoft.com)

Date: 01/24/05

Date: Mon, 24 Jan 2005 11:39:13 -0800

I'd like to remove all DNS references from CA certificates, such that the AIA CRT publication path is "DNS free". As far as I can tell, including the DNS name in the CRT name is a bit of a security poser as it reveals a CA server's DNS name to all and sundry.

I can easily modify the AIA paths in a post CA installation setreg command, the problem is that the CA certificate always contains the server's DNS name, e.g. srv001_Company-ClientAuthCA.crt.

There is a registry value called CACertFileName that I can change to %%3%%4.crt which in theory doesn't include the DNS name, however, I cannot make this registry change before the CA server is installed and by then the CA server's certificate has already been published (including the DNS reference). I could manually change the CRT filename before publishing it to the AIA path, but this is not desired and I'm concerned that certificate renewal will be a problem.

This is not a showstopper, but I think it would be best practice to take any DNS server references out of a certificate's AIA path. I particularly like the idea that I can document CA server installation through various lifecycle environments, e.g. poc, dev, livelike, etc. without making any explicit DNS references.

Anyone got any ideas?

Dave