

Re: Question regarding Certificate Trust Lists

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-11/msg00075.html>

- *From:* "Brian Komar" <brian.komar@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 21 Nov 2007 09:27:44 -0600
-

Your whole idea is flawed.

Trusted root certificates outweigh CTLs.

Since both CAs chain to the *same* trusted root, all certificates are trusted by any client within the two domains.

Brian

"DLN" <dnadon_nospm@xxxxxxxxxxxx> wrote in message
news:OSte527KIHA.5764@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello all,

I have two Windows domains (domain "A" and domain "B", for the sake of simplicity) with web servers sitting in both domains. I would like to be able to secure all the sites in both domains using CTLs, but there is a single site in domain B that I need to prevent users in domain A from accessing. Anonymous access to this site needs to stay enabled (for various reasons, I can't enable Windows authentication on the site). I was hoping I could also use a CTL for this.

Both domains have enterprise subordinate CAs installed with the subordinate CA certificate for both being issued by the same stand-alone root CA. My thinking was that I could accomplish what I want by adding domain B's CA cert to the CTL and require client certificates, thereby blocking access to the site from domain A's users. The problem I'm running into is that in order to create a CTL, I can only add the root CA to the CTL. If I attempt to add the domain B's subordinate CA certificate to the CTL, I receive a "Only self-signed certificates are added to the CTL" from the IIS CTL wizard.

If I correctly understand the information I'm reading regarding CTLs, only root CAs are allowed, so the error message I'm getting from the IIS CTL wizard is valid, but it doesn't solve my problem. If I add the root CA to the CTL, it'll accept certificates issued from the CAs in either domain. Is there a way to create a CTL that includes a subordinate CA only, or am I going to have to find a different mechanism to accomplish what I need?

Thanks.