

How to get my CA to be trusted by external clients?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2004-03/0744.html>

From: 620 (no_at_no.no)

Date: 03/29/04

Date: Mon, 29 Mar 2004 09:34:47 -0800

I have an IIS box (.net 2003 iis 6) that issued it's own cert for the purposes of SSL on a website it serves. The IIS box is dual-nic'd and acts as a router/NAT for a private network. For the sake of discussion, all clients use IE 6.

External clients from the internet, when visiting the website, receive a security alert regarding the issuing CA – while the certificate for the site is valid, it is not from a trusted issuing/root CA. Understandable, as my CA is not on IE's default list of trusted CA's. However, within the dialog available in the alert message (when you hit details, or advanced, or... whatever that button is) the ability to traverse up the cert issuing hierarchy isn't there – only the site's certificate is available to install, and so there's no way for the client to install my CA as a trusted CA.

Internal clients from the intranet, when visiting the website, receive the same message – but when they go into the dialog of the alert message, they can see and install my CA as a trusted CA – which in turn solves the alert message and they don't see it anymore, because my CA is now trusted. I'd like my external internet clients to have this option, just as the intranet clients do – that way I can instruct them on installing my CA as trusted to resolve the alert message. At this point I assume this is some sort of name resolution / scope issue of some kind, but I'm not sure how to solve it.

The issuing CA of the certificate is www.mydomain.com. CN=www CN=mydomain CN=com. Why is it that the external internet clients can resolve and visit www.mydomain.com yet can't install this as a trusted CA? The windows name of the IIS box is 'www' and it is part of the windows domain mydomain.com, so it's fully qualified name is www.mydomain.dom. I did that naming on purpose in an attempt to make the root CA visible externally, but it didn't work. Is this just a naming logistics issue, or am I way off base here?