

Re: ADFS and SSL Certificates

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg00451

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 6 Sep 2006 18:44:31 -0500
-

Yes, we are using certificates issued by our in house CA. It trusts an RSA CA cert which chains up to the valicert public root.

We actually had no problem at all with the SSL/IIS part of the configuration. With the ADFS token signing part, I absolutely could NOT get ADFS to verify our trust chain. There seems to be an issue with CRL checking that I could not configure my way out of. The problem was either that our CA cert's CRL could not be reached due to proxy issues or the RSA CA cert doesn't publish a CRL (which is normal for root CAs, but I guess not a normal for CAs signed by something else, based on what I was able to find out).

In order to get around that problem, I had to disable CRL checking in the trust policy file. This setting is not exposed in the UI, but can be changed manually with a text editor or can be changed with the vbscript that they include with ADFS for command line trust policy mods. I can't remember the exact setting, but I'm pretty sure we set it to "None".

The SSL problems with IIS are usually just an issue of not having the cert installed in the right store, not having the trust chain set up right with the intermediate CAs in the intermediate store and trusted root in the trusted root CA store, or you don't have the private key installed correctly or the current process identity doesn't have rights to read it (this happens a lot!).

I hope that gives you some more hints. If it is just SSL, you can try connecting to a normal html page in the same site but not under the ADFS virtual directory to see if you can get that working. That will get ADFS out of the picture.

Also, this stuff comes up in the regular IIS newsgroups all the time outside of the realm of ADFS, so make sure you do some searches in other newsgroups.

Best of luck again!

Joe K.

Re: ADFS and SSL Certificates

Joe Kaplan—MS MVP Directory Services Programming
Co—author of "The .NET Developer's Guide to Directory Services Programming"
<http://www.directoryprogramming.net>

--

"Susieber" <Susieber@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:B409B60B-B149-4205-8442-73059B0E1A83@xxxxxxxxxxxxxxxxxxxx>

Well, that event turned out not to help. We don't get any errors trying to access the web app from the client now. Nothing happens on the client (although he can access the default "under construction" page on the Web server). And no messages show up on the server. Did you ever get this working with a CA yourself?

"Susieber" wrote: