

Re: WS-Policy and WSE problems!

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet.webservices/2004-11/0050.htm>

From: Patrick (patl_at_reply.newsgroup.msn.com)

Date: 11/03/04

Date: Wed, 3 Nov 2004 16:38:04 -0000

Solved half of the problem-

WS-Policy not reading from reading config file because Config file tries to read from Local Machine certificate store and not the Current User certificate Store.

Can someone help with the app.config problem (i.e., ensure it reads from the app.config for the web service proxy client class library).

"Patrick" <patl@reply.newsgroup.msn.com> wrote in message news:OgJRR9ZwEHA.3288@TK2MSFTNGP14.phx.gbl...

> *Partially good news-*

> 1) *I got the WS-Policy WSE Drill down example working with my client certificate. It was not matching up the optional <wssp:TokenIssuer/> and <wssp:SubjectName/> attributes. I believe the CN, etc. are the wrong way around (i.e. DC=com ,DC=microsoft, CN=test and not CN=test, DC=microsoft, DC=com). Anyway, I commented out these two optional elements and I got the*

> *WSE client signing using my certificate.*

>

> 2) *However, if I took the same policy with my example code at*

>

> <http://www.geocities.com/drkestrel/3D6FE5CDC4D24FADA8371FD2B62D3C7E/367990ef058a0886240d2257f79f4>

> 2.1) *If I update the WSE properties of the test client and the Web Service*

> *Proxy client .NET class library, such that the corresponding app.config becomes:*

> `<microsoft.web.services2>`

> `<policy>`

> `<cache`

>

> `name="C:\dev\MsdnWse2SecuritySourceCode\SecurityPolicy\Client\PolicyX509.con`

> `fig" />`

> `</policy>`

> `</microsoft.web.services2>`

> 2.2) *I still get the original exception (I would expect the server not to*

> *accept the encryption because it's a WSE certificate, but it's failing even*

> *for the signing), from the trace I get:*

microsoft.public.dotnet.framework.aspnet.webservices: Re: WS-Policy and WSE problems!

```
> <wset:message action="http://twoten.press.net/webservices/PlaceOrder"
> messageId="uuid:e5e895c9-2667-4ffd-83a0-7faaf0f6a499" appDomain="test.exe"
> time="2004-11-03T12:10:29.1309685-00:00">
> <wset:compile qname="wsp:Policy" wsu:Id="#Sign-X.509-Encrypt-X.509"
> usage="Required" canEnforce="false">
> <wset:compile qname="wsp:MessagePredicate" usage="Required"
> canEnforce="true" />
> <wset:compile qname="wssp:Integrity" usage="Required"
> canEnforce="false">
>
>
<wset:annotation>ISecurityTokenManager.PermitsPolicyEnforcementTokenCaching
> is set to true in the token manager registered for this token type. A
token
> will be loaded from the token manager and cached for subsequent message
> enforcement.</wset:annotation>
> <wset:annotation>Invoking
> ISecurityTokenManager.LoadTokenFromSecurityTokenAssertion from the token
> manager registered for this token type.</wset:annotation>
> <wset:annotation>Could not find a security
token.</wset:annotation>
> <wset:annotation>Looking for a satisfactory token in the current
> message's token collection...</wset:annotation>
> <wset:annotation>Looking for a satisfactory token in policy
> enforcement token cache...</wset:annotation>
>
>
<wset:annotation>ISecurityTokenManager.PermitsPolicyEnforcementTokenCaching
> is set to true in the token manager registered for this token type.
> Attempting to use the previously cached token...</wset:annotation>
> <wset:annotation>Invoking
> ISecurityTokenManager.LoadTokenFromSecurityTokenAssertion from the token
> manager registered for this token type.</wset:annotation>
> <wset:annotation>Could not find a security
token.</wset:annotation>
> </wset:compile>
> </wset:compile>
> </wset:message>
>
> Also, if someone could shed some lights in terms of how/where .NET pick up
> which app.config, that would be excellent!!!!
>
> "Patrick" <patl@reply.newsgroup.msn.com> wrote in message
> news:%23Wq6ajZwEHA.908@TK2MSFTNGP11.phx.gbl...
> > I can confirm that with the WS-Policy example at
> >
> <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnws/html/wssecdrill.asp
> > 1) If I update the SecurityPolicyClient\PolicyX509.config to the
following
> > (to use the X.509 cert my Windows 2003 Test certificate authority
```

Re: WS-Policy and WSE problems!

```
> generate)
> > <wssp:Integrity wsp:Usage="wsp:Required">
> > <wssp:TokenInfo>
> > <!--The SecurityToken element within the TokenInfo element
> > describes which token type must be used for Signing.-->
> > <wssp:SecurityToken>
> >
> >
> >
<wssp:TokenType>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509
> > -token-profile-1.0#X509v3</wssp:TokenType>
> > <wssp:TokenIssuer>CN=TestServer, DC=test, DC=null,
> > DC=uk</wssp:TokenIssuer>
> > <wssp:Claims>
> > <!--By specifying the SubjectName claim, the policy system
> > can
> > look for a certificate with this subject name in the certificate store
> > indicated in the application's configuration, such as LocalMachine or
> > CurrentUser. The WSE X.509 Certificate Tool is useful for finding the
> > correct values for this field.-->
> > <wssp:SubjectName MatchType="wssp:Exact">C=GB, S=Test,
> > L=Location, O=TEST, OU=ICT, CN=DEVELOPMENT USE ONLY,
> > E=websupport@Test.null</wssp:SubjectName>
> > <wssp:X509Extension OID="2.5.29.14"
> > MatchType="wssp:Exact">W4p1d4CRBh3Kti95k2wbkkZBDxw=</wssp:X509Extension>
> > </wssp:Claims>
> > </wssp:SecurityToken>
> > </wssp:TokenInfo>
> > <wssp:MessageParts
> > Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">wsp:Body()
> > wsp:Header(wsa:Action) wsp:Header(wsa:FaultTo) wsp:Header(wsa:From)
> > wsp:Header(wsa:MessageID) wsp:Header(wsa:RelatesTo)
> > wsp:Header(wsa:ReplyTo)
> > wsp:Header(wsa:To) wse:Timestamp()</wssp:MessageParts>
> > </wssp:Integrity>
> > 2) I get an exception, as logged in the SendPolicy trace file:
> > <wset:message
> > action="http://blogs.dev4net.com/wse/samples/2004/08/AddEntry"
> > messageId="uuid:3b21997f-3b01-42a2-ae35-860fe4aff00a"
> > appDomain="WeblogClientSample.exe"
> > time="2004-11-03T11:21:38.8829013-00:00">
> > <wset:compile qname="wsp:Policy" wsu:Id="#Sign-X.509-Encrypt-X.509"
> > usage="Required" canEnforce="false">
> > <wset:compile qname="wsp:MessagePredicate" usage="Required"
> > canEnforce="true" />
> > <wset:compile qname="wssp:Integrity" usage="Required"
> > canEnforce="false">
> >
> >
> >
<wset:annotation>ISecurityTokenManager.PermitsPolicyEnforcementTokenCaching
```

microsoft.public.dotnet.framework.aspnet.webservices: Re: WS–Policy and WSE problems!

> > *is set to true in the token manager registered for this token type. A*
> *token*
> > *will be loaded from the token manager and cached for subsequent message*
> > *enforcement.</wset:annotation>*
> > *<wset:annotation>Invoking*
> > *ISecurityTokenManager.LoadTokenFromSecurityTokenAssertion from the token*
> > *manager registered for this token type.</wset:annotation>*
> > *<wset:annotation>Could not find a security*
> *token.</wset:annotation>*
> > *<wset:annotation>Looking for a satisfactory token in the current*
> > *message's token collection...</wset:annotation>*
> > *<wset:annotation>Looking for a satisfactory token in policy*
> > *enforcement token cache...</wset:annotation>*

> >
> >
>
<wset:annotation>ISecurityTokenManager.PermitsPolicyEnforcementTokenCaching
> > *is set to true in the token manager registered for this token type.*
> > *Attempting to use the previously cached token...</wset:annotation>*
> > *<wset:annotation>Invoking*
> > *ISecurityTokenManager.LoadTokenFromSecurityTokenAssertion from the token*
> > *manager registered for this token type.</wset:annotation>*
> > *<wset:annotation>Could not find a security*
> *token.</wset:annotation>*
> > *</wset:compile>*
> > *</wset:compile>*
> > *</wset:message>*

> >
> > ****Also, question in regards to where to put the config file (as I asked*
> *in*
> > *my original post):*
> > *1) With my code (containing the web–service proxy client class library*
> *and*
> *a*
> > *windows forms test harness) at*
> >
>

<http://www.geocities.com/drkestrel/3D6FE5CDC4D24FADA8371FD2B62D3C7E/367990ef058a0886240d2257f79f4>

> > *1.1) How could I get WSE to pickup the Security Policy from the*
> *web–service*
> > *proxy client (rather than having to set a policy file from the test*
> *harness)*
> > *?*
> > *1.2) Asking 1.1, because the intended use is invoking the Web service*
> *proxy*
> > *client class library via .NET interop from ASP (so there will be no*
> *where*
> *to*
> > *put any app.config!). I am a bit rusty in terms of how/where .NET*
> *pickup*
> > *the app.config? Am I right thinking that it would always pickup the one*

Re: WS–Policy and WSE problems!

microsoft.public.dotnet.framework.aspnet.webservices: Re: WS–Policy and WSE problems!

> > *from the current application domain, whicch*
> > *1.2.1) If I am invoking my .net win forms test harness, would be my*
> > *test.exe win form app*
> > *1.2.2) If invoked from .NET interop from ASP, it would be picking up*
> > *app.config from the .NET class library itself??*
> >
> >
> > *"Patrick" <patl@reply.newsgroup.msn.com> wrote in message*
> > *news:OW464LZwEHA.908@TK2MSFTNGP11.phx.gbl...*
> > > *I don't have the server–side code, I'm afraid (I am consuming a*
> > > *WS–Security*
> > > *based public web service, which I need to "subscribe" to). I got a*
big
> > > *suspicion, however, that it is something wrong with the*
Security.config
> > > *itself (as quite clearly, if the signing/encrypting by code is working*
> > > *as*
> > > *in*
> > > *Order.cs, there isn't anything wrong with the server), also the policy*
> > > *trace*
> > > *file indicates there is something wrong!*
> > >
> > > *One point worth pointing out though– when I was trying out the*
WS–Policy
> > > *sample within the WSE Sample, I *Thought* I got the example working*
with
> > > *the*
> > > *WSE certificate but if I use mine, the policy trace is saying it*
didn't
> > > *find*
> > > *a matching rule, or something along that line....*
> > >
> > > *I wonder could it be do with the following??*
> > > *1) WSE Sample cert's TokenIssuer's CN name is very simple, mine has 1*
CN
> > > *attribute an 3 DC attributes (for my client cert), (are they in the*
> > > *right*
> > > *spacing, etc. format??)*
> > > *2) Similarly, my "real" certificates's subject name are more complex*
(It
> > > *has*
> > > *got C, S, L, O, OU, CN and E attributes)*
> > > *3) My client cert has been generated by an internal enterprise Test*
> > > *Certificate authority running Windows Server 2003*
> > >
> > > *"[MSFT]" <lukezhan@online.microsoft.com> wrote in message*
> > > *news:a8c1JWVwEHA.3436@cpmsftngxa10.phx.gbl...*
> > > > *Hello Patrick,*
> > > >
> > > > *Can you provide the server side code for me test and reproduce the*
> > > > *problem?*

Re: WS–Policy and WSE problems!

microsoft.public.dotnet.framework.aspnet.webservices: Re: WS-Policy and WSE problems!

> > > > *Cuurently, I successfully compile your client code but failed to*
> > *reproduce*
> > > > *the issue. (I replaced the certificate with the one in WSE sample.)*
> > > >
> > > > *Thanks,*
> > > >
> > > > *Luke*
> > > >
> > >
> > >
> >
> >
> >
>
>