

## Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

---

*Source:*

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2006-03/>

---

- *From:* "James Hancock" <~jamie@xxxxxxxxxxxxxxxxxxxxxx>
  - *Date:* Sun, 26 Mar 2006 23:54:22 -0500
- 

OK, so still trying to get this thing locked down...

I updated my policy cache file like so:

```
<policies xmlns="http://schemas.microsoft.com/wse/2005/06/policy>
```

```
<extensions>
```

```
<extension name="compressionAssertion"  
type="Evolution.Web.Services.CompressionAssertion, Evolution.Web.Services"/>
```

```
<extension name="usernameAssertion"  
type="Evolution.Web.Services.UsernameServiceAssertion,  
Evolution.Web.Services" />
```

```
<extension name="wse3Trace" type="WSETracingFilter.WSEFilterAssertion,  
WSETracingFilter, Version=3.0.0.0, Culture=neutral,  
PublicKeyToken=aa253a6b9020c4eb"/>
```

```
</extensions>
```

```
<policy name="RegistrationPolicy">
```

```
<authorization>
```

```
<allow role="Administrators"/>
```

```
<deny role="*" />
```

```
</authorization>
```

```
<protection>
```

```
<request signatureOptions="IncludeAddressing, IncludeTimestamp,
```

```
IncludeSoapBody" encryptBody="true" />
```

```
<response signatureOptions="IncludeAddressing, IncludeTimestamp,
```

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

```
<IncludeSoapBody encryptBody="true" />  
<fault signatureOptions="IncludeAddressing, IncludeTimestamp,  
IncludeSoapBody encryptBody="false" />  
</protection>  
<requireActionHeader />  
<compressionAssertion compressionMode="BZip2" compressionLevel="Maximum"  
threshold="128"/>  
<usernameAssertion />  
<wse3Trace/>  
</policy>  
</policies>
```

usernameAssertion is my own, it is not based on  
usernameForCertificateSecurity because I'm not using it. I am not using any  
certificates at all, all of the encryption stuff is done in my custom  
assertion. Even with all of that stuff added to the policy cache file, you  
can still go in and it will give you results from your browser window. What  
am I doing wrong?

Thanks.

James Hancock

"Pablo Cibraro" <pcibraro@xxxxxxxxxxxx> wrote in message  
news:%23ViEU4nTGHA.224@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi James,

1. In order to use authorization, you must add the authorizationAssertion  
to your policy. The sample below shows how to do that:

```
<policy name="usernameTokenSecurity">  
<authorization>  
<allow role="Administrators" />  
<deny role="*" />  
</authorization>  
<usernameForCertificateSecurity establishSecurityContext="true"  
renewExpiredSecurityContext="true" requireSignatureConfirmation="false"
```

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

```
messageProtectionOrder="SignBeforeEncryptAndEncryptSignature"  
requireDerivedKeys="true" ttlInSeconds="60">  
<serviceToken>  
<x509 storeLocation="LocalMachine" storeName="My"  
findValue="CN=WSE2QuickStartServer"  
findType="FindBySubjectDistinguishedName" />  
</serviceToken>  
<protection>  
<request signatureOptions="IncludeAddressing, IncludeTimestamp,  
IncludeSoapBody" encryptBody="true" />  
<response signatureOptions="IncludeAddressing, IncludeTimestamp,  
IncludeSoapBody" encryptBody="true" />  
<fault signatureOptions="IncludeAddressing, IncludeTimestamp,  
IncludeSoapBody" encryptBody="false" />  
</protection>  
</usernameForCertificateSecurity>  
<requireActionHeader />  
</policy>
```

2. If you want to support Secure Conversation in your custom assertion,  
then the Soap filters returned by your assertion must derive from the  
following classes:

- ClientInputFilter : SecureConversationClientReceiveSecurityFilter
- ClientOutputFilter : SecureConversationClientSendSecurityFilter
- ServiceInputFilter : SecureConversationServiceReceiveSecurityFilter
- ServiceOutputFilter : SecureConversationServiceSendSecurityFilter

Your assertion must derive from the class SecurityPolicyAssertion as well.

In that way, your assertion will automatically support Secure  
conversation.

The STS quickstart from the Pattern & Practices implements a Custom  
Assertion for SAML tokens that uses Secure Conversation.

<http://www.gotdotnet.com/codegallery/codegallery.aspx?id=8da852b9-2c0d-4eb7-a2de-77222a4075f6>

3. If you want to compress the messages, you can find a nice  
implementation of WS-Compression [here](http://weblogs.shockbyte.com.ar/rodolfof/archive/2006/02/07/4585.aspx)  
<http://weblogs.shockbyte.com.ar/rodolfof/archive/2006/02/07/4585.aspx>

Thanks

Pablo Cibraro

<http://weblogs.asp.net/cibrax>

"James Hancock" <~jamie@xxxxxxxxxxxxxxxxxxxxxx> wrote in message  
news:u\$JrmeTGHA.792@xxxxxxxxxxxxxxxxxxxxxxxxxx

BTW, I still think that there is a lot of benefit for Secure Conversation  
for what I'm doing (hundreds of requests back and forth).

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

Can you give me some suggestions on how to impliment it in my custom assertion or give me a direction to look to impliment my own custom version of whatever I need to do please?

Thanks!

James Hancock

"Pablo Cibraro" <pcibraro@xxxxxxxxxxxx> wrote in message news:uwKfoPbTGHA.2004@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi James.

First of all, the UsernameOverTransport turn-key assertion does not use message security and therefore it does not encrypt the message. You need to combine this assertion with a secure transport like SSL if you want to protect your messages. WSE does not provide a turn-key assertion to encrypt messages using a username token only, so you will have to develop a custom assertion in order to do that.

Secondly, you should add an authorization assertion to restrict the access to your webmethods.

Thirdly, secure conversation does not optimize the amount of data sent over the wire. This article in my weblog gives a description of this feature

<http://weblogs.asp.net/cibrax/archive/2006/02/21/438670.aspx>

All the turn-key assertions that use message security add the headers required by WS-Security to the message, and it is difficult to optimize that part. You should use an assertion for transport security instead.

This security guide from the Pattern & Practices team also provides really good information about this topic

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/WSSP.asp>

I hope this can help you.

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

Regards,  
Pablo Cibraro  
<http://weblogs.asp.net/cibrax>

"James Hancock" <~jamie@xxxxxxxxxxxxxxxxxxxxxx>  
wrote in message  
news:%23jGmjmwTGH.736@xxxxxxxxxxxxxxxxxxxxxxxxxx

OK, thanks to Julia's help and a bunch of  
stuff in the newsgroups I've  
got  
some of this working but not all...

Basically I need to be able to encrypt both  
sides of the communication  
between client and server using a  
UserNameToken that passes the  
UserName but  
not the password but is a shared secret. I  
cannot use X.509 or anything  
like  
that because the number of client computers  
is unknown and could easily  
be  
thousands, and the server may not  
necessarily have an SSL key and I  
don't  
want to leave it up to my clients to  
optionally get an SSL key, because  
most  
of them won't because they're lazy or cheap  
or some other "really good  
reason" that will jeopardize their data.  
<aside>Hence Shared secret,  
which I  
used in WSE 2.0 with great effect because  
the shared secret password  
was  
unique per client computer, and it was a 512  
bit hash which is really  
hard  
to break, and after every operation the hash  
would change (sent in the  
encrypted message body by the server to the  
client and then stored in a  
different encryption in the local database).  
(Yes, I know, if you break  
one  
message, you break 'em all, but you can't use  
two messages to compare

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

between the two... I was working on an algorithm that the server and client would use to calculate the new hash without one sending it to the other, but since this works, and is very secure the way it is, it wasn't high on the list of priorities...</aside>

I was able to do this stuff in WSE 2.0 before using the now depreciated Context.Security... stuff. No go in WSE 3.0 because it's depreciated.

If I use the depreciated functions, it works fine... I think... can't tell because it doesn't use the policy stuff of course.

I've got the signing stuff done and working by using a Custom UserNameTokenManager on the server and then creating the right entries in my web.config file. Which works and is called and validates the whole deal.. assuming the client request adds a proper UserNameToken...

It still lets clients that don't use anything query my WebMethods however.

So I looked in the newsgroups here and decided I needed a policy file because the way I was doing it before was to query the Context.Security stuff looking for the entries... which is depreciated.

So I added the following on the server:

<policies  
xmlns="http://schemas.microsoft.com/wse/2005/06/policy">

<extensions>

<extension

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

```
name="usernameOverTransportSecurity"  
type="Microsoft.Web.Services3.Design.UsernameOverTransportAssertion,  
Microsoft.Web.Services3, Version=3.0.0.0,  
Culture=neutral,  
PublicKeyToken=31bf3856ad364e35" />
```

```
<extension name="wse3Trace"  
type="WSETracingFilter.WSEFilterAssertion,  
WSETracingFilter, Version=3.0.0.0,  
Culture=neutral,  
PublicKeyToken=aa253a6b9020c4eb"/>
```

```
</extensions>
```

```
<policy name="RegistrationPolicy">
```

```
<usernameOverTransportSecurity />
```

```
<requireActionHeader />
```

```
<wse3Trace/>
```

```
</policy>
```

```
</policies>
```

Then on the Service itself:

```
[WebServiceBinding(ConformsTo =  
WsiProfiles.BasicProfile1_1)]
```

```
[Policy("RegistrationPolicy")]
```

```
public class Registration :  
System.Web.Services.WebService {
```

```
...
```

and the following on the client:

```
<policies  
xmlns="http://schemas.microsoft.com/wse/2005/06/policy">
```

```
<extensions>
```

```
<extension  
name="usernameOverTransportSecurity"  
type="Microsoft.Web.Services3.Design.UsernameOverTransportAssertion,  
Microsoft.Web.Services3, Version=3.0.0.0,
```

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

```
Culture=neutral.  
PublicKeyToken=31bf3856ad364e35" />  
  
<extension name="wse3Trace"  
type="WSETracingFilter.WSEFilterAssertion.  
WSETracingFilter, Version=3.0.0.0.  
Culture=neutral.  
PublicKeyToken=aa253a6b9020c4eb"/>  
  
</extensions>  
  
<policy name="UserNamePolicy">  
  
<usernameOverTransportSecurity />  
  
</policy>  
  
</policies>
```

and in the client request:

```
Microsoft.Web.Services3.Security.Tokens.UsernameToken  
tok = new  
Microsoft.Web.Services3.Security.Tokens.UsernameToken(UserName,  
Password,  
Microsoft.Web.Services3.Security.Tokens.PasswordOption.SendNone):  
  
r.SetPolicy("UserNamePolicy");  
  
r.SetClientCredential(tok);
```

Note that I'm using Mike's tool to monitor  
the requests.... hence the  
added  
Extension...I tried removing it and users can  
still just request the  
WebMethod and it works.

Sorry if this is a dupe everyone. It didn't  
seem to go through the  
first time...

All is good in that Mike's tool tells me that  
the username token is  
added  
etc. However!

1. The contents of the message are not  
encrypted. They absolutely have  
to be  
encrypted.... But the docs say that

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

UsernameoverTransport doesn't support it, but when I query the UserNametoken it says that it does support encryption... Help please!

2. You can still request the WebMethods without any of this stuff and it works.

Also...

I would like to make sure that the minimum amount of data is sent over the wire (there could be dialup users using this!) so any suggestions on how to get this whole system to send stuff only once on the first request etc. would be greatly appreciated. (i.e. how do I enable SecureConversation??? Is that even the right way to go about it?)

I wish MS would just accept that this is a scenario that they need to support and put it in instead of making it harder and harder every time they do this, cause people are just going to get around it (like me) and thus likely are not going to get it right and think they have encrypted secure communications when they don't... better to have MS do it and do it right instead of letting people hack something together...

Thanks for any help you might be able to provide!

James Hancock

Re: WSE 3.0 + UserNameToken without X.509 Cert/Kerberos + Signing + Encryption How?

±