

Re: UsernameOverTransportSecurity+SSL Confusion, please help

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2006-09/>

- *From:* "mike" <michal.tesar@xxxxxxxxxx>
 - *Date:* 21 Sep 2006 00:21:03 -0700
-

Hi Pablo,

thank you again for the response.

I tried to put this under System.Web section in the Web.config file in the root of my web service:

```
<webServices>
<soapServerProtocolFactory
type="Microsoft.Web.Services3.WseProtocolFactory,
Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35" />
<soapExtensionImporterTypes>
<add
type="Microsoft.Web.Services3.Description.WseExtensionImporter,
Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35" />
</soapExtensionImporterTypes>

<protocols>
<remove name="HttpPost" />
<remove name="HttpGet" />
</protocols>
</webServices>
```

But when I go to my web service:

<https://localhost/UsernameTokenWithDatabaseService/Service.asmx>

I still see the methods and can execute them. What am I doing wrong?

Thank you,
Mike

Pablo Cibraro [MVP] wrote:

How come the authentication is not working there? What settings should I have under IIS settings for my WebService?

Re: UsernameOverTransportSecurity+SSL Confusion, please help

1. You have to add the following section to the configuration file,

```
<webservices>
<protocols>
<remove name="HttpPost" />
<remove name="HttpGet" />
</protocols>
</webservices>
```

One more question. In order to use SSL, I will have to purchase the Certificate, right?

2. It depends, you can buy a certificate in one of the well-know certificate authorities, such as Verisign or RSA, or you can create your own certificate using Microsoft Certificate Server.

I will have a private key on the server, and I will give the private key to my client? They will need to install it on their server, correct? And I don't have to do anything in the config files regarding this, correct?

3. If you use SSL, you only need to configure the certificate with the private key on the IIS server.

The client will automatically get the public key and negotiate a key to secure the channel. There is a predefined handshake between the client and the service, you do not have to do anything regarding this or distribute anything on the client machines.

Regards,
Pablo Cibraro.

"mike" <michal.tesar@xxxxxxxxxx> wrote in message
news:1158737105.416645.99320@xx

Hi Pablo,

thank you for your response.

I am still confused little bit.

I generated the wsdl file suing https://. From my client app if I supply invalid credentials, I get an exception, so the authentication seems to be working there. However, if I paste the url of my webservice on my local machine, either in IE or Firefox, I can see the methods and execute them.

ie <https://localhost/myservice>

How come the authentication is not working there? What settings should I have under IIS settings for my WebService?

Re: UsernameOverTransportSecurity+SSL Confusion, please help

One more question. In order to use SSL, I will have to purchase the Certificate, right? I will have a private key on the server, and I will give the private key to my client? They will need to install it on their server, correct? And I don't have to do anything in the config files regarding this, correct?

Thanks a million!!

Mike

Pablo Cibraro [MVP] wrote:

Hi Mike,

If you are using transport security, the following section is not necessary
(It is only used by message security),

<security>

```
<x509 verifyTrust="true"
allowTestRoot="true"
revocationMode="Offline"
verificationMode="TrustedPeopleOrChain"/>
<binarySecurityTokenManager>
<add
type="Microsoft.Web.Services3.Security.Tokens.X509SecurityTokenManager,
Microsoft.Web.Services3, Version=3.0.0.0,
Culture=neutral,
PublicKeyToken=31BF3856AD364E35"
valueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token
<keyAlgorithm name="RSA15" />
</add>
</binarySecurityTokenManager>
</security>
```

I am not sure to understand what your problem is. Have you configured the service to use SSL in the IIS ?
If the service is running with https, it is automatically signed and encrypted by the transport, you do not need to worry about that.
The code for the client application looks fine.

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

Re: UsernameOverTransportSecurity+SSL Confusion, please help

"mike" <michal.tesar@xxxxxxxx> wrote in message
news:1158594278.807718.65720@xx

Hi,

I am confused. I have a web service, and a client. Both are connected over VPN. I want to use direct authentication from WSE 3.0. To secure the transport of the messages, I just want to use SSL.

I have this set up working, but I am confused. I installed a test certificate on my web server, so I need to access my web service over SSL. However, in my policy config file on the client I have:

```
<policy name="usernameTokenSecurity">  
<usernameOverTransportSecurity />  
<requireActionHeader />  
</policy>
```

in app.config on the client I have:

```
<microsoft.web.services3>  
<diagnostics>  
<trace enabled="false"  
input="InputTrace.webinfo"  
output="OutputTrace.webinfo" />  
<detailedErrors enabled="false" />  
</diagnostics>  
<policy  
fileName="Configuration\wse3policyCache.config"  
/>  
<security>  
<x509 verifyTrust="true"  
allowTestRoot="true"  
revocationMode="Offline"  
verificationMode="TrustedPeopleOrChain"/>  
<binarySecurityTokenManager>  
<add  
type="Microsoft.Web.Services3.Security.Tokens.X509SecurityTokenManager,  
Microsoft.Web.Services3, Version=3.0.0.0,  
Culture=neutral,  
PublicKeyToken=31BF3856AD364E35"  
valueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token  
<keyAlgorithm name="RSA15" />  
</add>  
</binarySecurityTokenManager>  
</security>
```

Re: UsernameOverTransportSecurity+SSL Confusion, please help

Re: UsernameOverTransportSecurity+SSL Confusion, please help

</microsoft.web.services3>

in my client winform I have:

Service1.ServiceWse proxy = new
Service1.ServiceWse();

UsernameToken token;

token =

GetUsernameToken(txtUsername.Text,
txtPassword.Text,
PasswordOption.SendPlainText);

proxy.SetClientCredential(token);
proxy.SetPolicy("usernameTokenSecurity");

Service1.Product product =

proxy.GetProductInformationWithSendPlainText(txtProduct.Text);

lblResults.Text =

String.Format(CultureInfo.InvariantCulture,
"Product: {0}, Quantity {1}, Unit price
{2}";

product.Name, product.Quantity,
product.UnitPrice);

lblResults.Text += proxy.ValidateLogin();

I am just confused if this is what I want this
to be? Is my app.config
file correct? The direct authentication works.
My concern is if the SSL
is set up ok. Where do I sign the message
with the public key?

Please help!!!

Thanks,

Mike