

Re: UserName and Kerberos tokens at the same time

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2005-12/>

- *From:* "Henrik Skak Pedersen" <skak@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 2 Dec 2005 16:05:00 +0100
-

Hi Steven,

Thanks again.

I think that you are right because I would expect the standard examples to work. I have tried it on a Windows 2003 server as well and there I get the same error.

My client is a Windows application and I can see that the kerberos token is ok, so it is something on the server side. Maybe the IIS is validation against a wrong source or something like that.

Do I have to do something special on the server side (IIS, Win3K) ?

Thanks Henrik.

"Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxxx> wrote in message [news:dGWW\\$H09FHA.1236@xxxxxxxxxxxxxxxxxxxxx](mailto:news:dGWW$H09FHA.1236@xxxxxxxxxxxxxxxxxxxxx)

> Thanks for your response and further info.

>

> I think the problem is likely due to the ASP.NET environment. Is your
> client application(which call the webservice) is also an asp.net
> application? The kerberos Security token will try establish the security
> token through the current execution context's security credential which
> must
> be a domain user account that can be authenticated by KDC(normally just
> the
> DC). So for ASP.NET the process identity is probably not a proper account.
> I would suggest you tried the code in a winform client or console
> application, the console app since in console or winform app, the current
> security context is the logon user session(which is likely a domain user
> ...) ...

>

> Also, you can also check the following notes in wse documentation(if your
> webservice is on a machine other than win 2003 server):

> =====

Re: UserName and Kerberos tokens at the same time

> Kerberos tokens work on computers with Windows Server 2003 or Windows XP
> with Service Pack 1 installed. When Windows XP is used, the account
> ASP.NET
> runs under is ASPNET by default and must be granted the Act as part of the
> operating system privilege. By default, the ASPNET account does not have
> this privilege. It is suggested that you run your Kerberos-secured Web
> services on Windows Server 2003. On Windows Server 2003, the Act as part
> of
> the operating system privilege is not required. On Windows XP you can
> configure the ASPNET account to have the Act as part of the operating
> system privilege using the Local Security Policy management application,
> but you should be aware that this affects all ASP.NET applications and
> results in less security for ASP.NET applications. Windows 2000 is not a
> supported operating system for this feature.

>
> =====

>
> Thanks,
>
> Steven Cheng
> Microsoft Online Support

>
> Get Secure! www.microsoft.com/security
> (This posting is provided "AS IS", with no warranties, and confers no
> rights.)

>
>
>
> -----

> From: "Henrik Skak Pedersen" <skak@xxxxxxxxxxxxxxxxxx>
> References: <uDOvP8Q8FHA.620@xxxxxxxxxxxxxxxxxxxxxxxxxx>
> <eHap0QR8FHA.1000@xxxxxxxxxxxxxxxxxxxxxxxxxx>
> <dau3PrY8FHA.3764@xxxxxxxxxxxxxxxxxxxxxxxxxx>
> <OS79EfF9FHA.1484@xxxxxxxxxxxxxxxxxxxxxxxxxx>
> <7SHqboN9FHA.4000@xxxxxxxxxxxxxxxxxxxxxxxxxx>
> <eG42Y8R9FHA.3416@xxxxxxxxxxxxxxxxxxxxxxxxxx>
> <t5c47rn9FHA.4028@xxxxxxxxxxxxxxxxxxxxxxxxxx>
> <Osge9Tr9FHA.4036@xxxxxxxxxxxxxxxxxxxxxxxxxx>
> Subject: Re: UserName and Kerberos tokens at the same time
> Date: Fri, 2 Dec 2005 13:25:57 +0100
> Lines: 394
> X-Priority: 3
> X-MSMail-Priority: Normal
> X-Newsreader: Microsoft Outlook Express 6.00.2900.2180
> X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
> X-RFC2646: Format=Flowed; Response
> Message-ID: <#WX2Nuz9FHA.2708@xxxxxxxxxxxxxxxxxxxxxxxxxx>
> Newsgroups: microsoft.public.dotnet.framework.webservices.enhancements
> NNTP-Posting-Host: 80.63.142.94
> Path: TK2MSFTNGXA02.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP12.phx.gbl
> Xref: TK2MSFTNGXA02.phx.gbl

Re: UserName and Kerberos tokens at the same time

> microsoft.public.dotnet.framework.webservices.enhancements:7813
> X-Tomcat-NG: microsoft.public.dotnet.framework.webservices.enhancements
>
> Extra info:
>
> If I run the example Kerberos solution I get some a detailed error
> message:
>
> Microsoft.Web.Services3.Security.SecurityFault: An invalid security token
> was provided ---> System.Security.SecurityException: WSE594:
> AcceptSecurityContext call failed with the following error message: Logon
> failure: unknown user name or bad password. . at
> Microsoft.Web.Services3.Security.Tokens.Kerberos.KerberosServerContext.Accep
> tContext(Byte[]
> inToken) at
>
> Does that help you in any way?
>
> "Henrik Skak Pedersen" <skak@xxxxxxxxxxxxxxxxxxxx> wrote in message
> news:Osge9Tr9FHA.4036@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>> Hi again Steven,
>>
>> Again, thank you very much for looking into this problem for me.
>>
>> I just tried to run my test project on a colleagues machine and he gets
>> the same error. I guess that there is nothing special in our environment,
>> we have a normal DC. I used to run kerberos authentication in wse for
> NET
>> 1.1 and there it worked fine.
>>
>> I have tried to run the two Quickstart examples:
>> WSSecurityKerberosPolicyService and WSSecurityKerberosCodeService and
>> there I get the following exception (inner exception of a soap exception)
>>
>> "Security requirements are not satisfied because the security header is
>> not present in the incoming message."
>>
>> But when I run my test project which is using a custom policy I get the
>> following exception:
>>
>> WSE2005: Protection requirements in KerberosAssertion are not satisfied
>>
>> I guess that it basicly is the same problem I am having the the two
>> solutions.
>>
>> I can see that the Kerberos is beeing generated and assigned to the
>> proxy.
>>
>> I am BTW running the web service on the build in ASP . NET Development
>> Server if that has anything to do with the problem? Has it something to
> do

Re: UserName and Kerberos tokens at the same time

>> with impersonation?
>>
>> Any ideas??
>>
>> Thanks Henrik.
>>
>>
>> "Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxx> wrote in message
>> news:t5c47rn9FHA.4028@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>> Thanks for your followup Henrik,
>>>
>>> Then, it seems that the kerberos Token is not quite attached correctly
>>> at
>>> clientside... Have you ensure that the environment is qualified of using
>>> kerberos authentication, are you in a certain domain environment with a
>>> KDC(or DC....) ?
>>>
>>> Regards,
>>>
>>> Steven Cheng
>>> Microsoft Online Support
>>>
>>> Get Secure! www.microsoft.com/security
>>> (This posting is provided "AS IS", with no warranties, and confers no
>>> rights.)
>>>
>>> -----
>>> From: "Henrik Skak Pedersen" <skak@xxxxxxxxxxxxxxxx>
>>> References: <uD0vP8Q8FHA.620@xxxxxxxxxxxxxxxxxxxxxxxx>
>>> <eHap0QR8FHA.1000@xxxxxxxxxxxxxxxxxxxxxxxx>
>>> <dau3PrY8FHA.3764@xxxxxxxxxxxxxxxxxxxxxxxx>
>>> <OS79EfF9FHA.1484@xxxxxxxxxxxxxxxxxxxxxxxx>
>>> <7SHqboN9FHA.4000@xxxxxxxxxxxxxxxxxxxxxxxx>
>>> Subject: Re: UserName and Kerberos tokens at the same time
>>> Date: Tue, 29 Nov 2005 20:57:13 +0100
>>> Lines: 285
>>> X-Priority: 3
>>> X-MSMail-Priority: Normal
>>> X-Newsreader: Microsoft Outlook Express 6.00.2900.2180
>>> X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
>>> X-RFC2646: Format=Flowed; Original
>>> Message-ID: <eG42Y8R9FHA.3416@xxxxxxxxxxxxxxxxxxxxxxxx>
>>> Newsgroups: microsoft.public.dotnet.framework.webservices.enhancements
>>> NNTP-Posting-Host: 80.63.142.94
>>> Path: TK2MSFTNGXA02.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP15.phx.gbl
>>> Xref: TK2MSFTNGXA02.phx.gbl
>>> microsoft.public.dotnet.framework.webservices.enhancements:7770
>>> X-Tomcat-NG: microsoft.public.dotnet.framework.webservices.enhancements
>>>
>>> Hi Steven,
>>>

Re: UserName and Kerberos tokens at the same time

Re: UserName and Kerberos tokens at the same time

```
>>> Thank you for your reply.
>>>
>>> Yes I works well with the UsernameToken.
>>>
>>> I get the same exception without the choiceAssertion. I have changed the
>>> policy to this:
>>> <policies xmlns="http://schemas.microsoft.com/wse/2005/06/policy>
>>>
>>> <extensions>
>>>
>>> <extension name="kerberosSecurity"
>>> type="Microsoft.Web.Services3.Design.KerberosAssertion,
>>> Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,
>>> PublicKeyToken=31bf3856ad364e35" />
>>>
>>> <extension name="requireActionHeader"
>>> type="Microsoft.Web.Services3.Design.RequireActionHeaderAssertion,
>>> Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,
>>> PublicKeyToken=31bf3856ad364e35" />
>>>
>>> </extensions>
>>>
>>> <policy name="ServicePolicy">
>>>
>>> <kerberosSecurity establishSecurityContext="false"
>>> renewExpiredSecurityContext="true" requireSignatureConfirmation="false"
>>> messageProtectionOrder="SignBeforeEncrypt" requireDerivedKeys="true"
>>> ttlInSeconds="300">
>>>
>>> <protection>
>>>
>>> <request signatureOptions="IncludeAddressing, IncludeTimestamp,
>>> IncludeSoapBody" encryptBody="true" />
>>>
>>> <response signatureOptions="IncludeAddressing, IncludeTimestamp,
>>> IncludeSoapBody" encryptBody="true" />
>>>
>>> <fault signatureOptions="IncludeAddressing, IncludeTimestamp,
>>> IncludeSoapBody" encryptBody="false" />
>>>
>>> </protection>
>>>
>>> </kerberosSecurity>
>>>
>>> <requireActionHeader />
>>>
>>> </policy>
>>>
>>> </policies>
>>>
>>> Do I need some signing or encryption? I guess that I don't need it
```

Re: UserName and Kerberos tokens at the same time

>>> because

>>> I

>>> am running over SSL, but maybe the KerberosAssertion requires it?

>>>

>>> Regards

>>>

>>> Henrik.

>>>

>>> "Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxx> wrote in message

>>> news:7SHqboN9FHA.4000@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

>>>> Hi Henrik.

>>>>

>>>> From the error message, request message's security header doesn't meet

>>>> the

>>>> server policy assertion's requirement. Also this occurs when you using

>>>> the

>>>> Kerberos token at clientside, but works well when you using

>>>> UsernameToken.

>>>> yes? Have you ever tried only using Kerberos token from clientside

>>>> (without using choiceAssertion) to see whether you can get kerberos

>>>> token

>>>> work correctly?

>>>>

>>>> Thanks.

>>>>

>>>> Steven Cheng

>>>> Microsoft Online Support

>>>>

>>>> Get Secure! www.microsoft.com/security

>>>> (This posting is provided "AS IS", with no warranties, and confers no

>>>> rights.)

>>>>

>>>>

>>>> -----

>>>> From: "Henrik Skak Pedersen" <skak@xxxxxxxxxxxxxxxx>

>>>> References: <uDOvP8Q8FHA.620@xxxxxxxxxxxxxxxx>

>>>> <eHap0QR8FHA.1000@xxxxxxxx>

>>>> <dau3PrY8FHA.3764@xxxxxxxx>

>>>> Subject: Re: UserName and Kerberos tokens at the same time

>>>> Date: Mon, 28 Nov 2005 21:10:22 +0100

>>>> Lines: 176

>>>> X-Priority: 3

>>>> X-MSMail-Priority: Normal

>>>> X-Newsreader: Microsoft Outlook Express 6.00.2900.2180

>>>> X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

>>>> X-RFC2646: Format=Flowed; Original

>>>> Message-ID: <OS79EfF9FHA.1484@xxxxxxxx>

>>>> Newsgroups: microsoft.public.dotnet.framework.webservices.enhancements

>>>> NNTP-Posting-Host: 80.63.142.94

>>>> Path: TK2MSFTNGXA02.phx.gbl!TK2MSFTNGP08.phx.gbl!tk2msftngp13.phx.gbl

>>>> Xref: TK2MSFTNGXA02.phx.gbl

Re: UserName and Kerberos tokens at the same time

Re: UserName and Kerberos tokens at the same time

>>>> [microsoft.public.dotnet.framework.webservices.enhancements:7756](#)
>>>> [X-Tomcat-NG: microsoft.public.dotnet.framework.webservices.enhancements](#)
>>>>
>>>> [Hi Steven.](#)
>>>>
>>>> [Again thank you very much for your reply. I tried to implement the](#)
>>>> [PolicyChoiceAssertion from the example but now I get an exception when](#)
>>>> [I](#)
>>>> [run](#)
>>>> [with the KerberosAssertion. The code throws the exception when I call](#)
>>>> [HelloWorld in the example below. The PolicyChoiceAssertion is the same](#)
>>>> [as](#)
>>>> [the one from the example.](#)
>>>>
>>>> [Exception:](#)
>>>> [{"WSE2005: Protection requirements in KerberosAssertion are not](#)
>>>> [satisfied."}](#)
>>>>
>>>> [It works fine when I run with the UserNameAssertion. My policy looks](#)
>>>> [like](#)
>>>> [this:](#)
>>>>
>>>> [<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, Culture=neutral,](#)
>>>> [PublicKeyToken=31bf3856ad364e35" />](#)
>>>>
>>>> [<extension name="kerberosSecurity"](#)
>>>> [type="Microsoft.Web.Services3.Design.KerberosAssertion,](#)
>>>> [Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,](#)
>>>> [PublicKeyToken=31bf3856ad364e35" />](#)
>>>>
>>>> [<extension name="requireActionHeader"](#)
>>>> [type="Microsoft.Web.Services3.Design.RequireActionHeaderAssertion,](#)
>>>> [Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,](#)
>>>> [PublicKeyToken=31bf3856ad364e35" />](#)
>>>>
>>>> [<extension name="policyChoice"](#)
>>>> [type="MindKey.License.Assertion.PolicyChoiceAssertion, Service](#)
>>>> [Assertion](#)
>>>> [Library"/>](#)
>>>>
>>>> [</extensions>](#)
>>>>
>>>> [<policy name="ServicePolicy">](#)
>>>>
>>>> [<policyChoice>](#)

Re: UserName and Kerberos tokens at the same time

Re: UserName and Kerberos tokens at the same time

```
>>>>
>>>> <usernameOverTransportSecurity />
>>>>
>>>> <kerberosSecurity establishSecurityContext="false"
>>>> renewExpiredSecurityContext="true" requireSignatureConfirmation="false"
>>>> messageProtectionOrder="SignBeforeEncrypt" requireDerivedKeys="true"
>>>> ttlInSeconds="300">
>>>>
>>>> <protection>
>>>>
>>>> <request signatureOptions="IncludeAddressing, IncludeTimestamp,
>>>> IncludeSoapBody" encryptBody="true" />
>>>>
>>>> <response signatureOptions="IncludeAddressing, IncludeTimestamp,
>>>> IncludeSoapBody" encryptBody="true" />
>>>>
>>>> <fault signatureOptions="IncludeAddressing, IncludeTimestamp,
>>>> IncludeSoapBody" encryptBody="false" />
>>>>
>>>> </protection>
>>>>
>>>> </kerberosSecurity>
>>>>
>>>> </policyChoice>
>>>>
>>>> <requireActionHeader />
>>>>
>>>> </policy>
>>>>
>>>> </policies>
>>>>
>>>> and the code calling using the KerberosAssertion looke like this:
>>>> TestWS testWS = new TestWS();
>>>>
>>>> KerberosAssertion assertion = new KerberosAssertion();
>>>>
>>>> assertion.KerberosTokenProvider = new KerberosTokenProvider("host/" +
>>>> System.Net.Dns.GetHostName(), ImpersonationLevel.Identification);
>>>>
>>>> Policy policy = new Policy();
>>>>
>>>> policy.Assertions.Add(assertion);
>>>>
>>>> testWS.SetPolicy(policy);
>>>>
>>>> MessageBox.Show(testWS.HelloWorld());
>>>>
>>>>
>>>> I hope you can helpe me!
>>>>
>>>> Thanks Henrik.
```

Re: UserName and Kerberos tokens at the same time

Re: UserName and Kerberos tokens at the same time

>>>>

>>>> "Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxx> wrote in message

>>>> news:dau3PrY8FHA.3764@xxxxxxxxxxxxxxxxxxxxxxxx

>>>>> Hi Henrik,

>>>>>

>>>>> As for attaching different kind of Security Tokens in client request

>>>>> and

>>>>> let the serverside policy access and perform authenticate on all of

>>>>> them

>>>>> (or

>>>>> some of them...), that's certainly possible. However, currently the

>>>>> buildin

>>>>> WSE 3.0 PolicyAssertions (UsernameOverTransport,

>>>>> KerberosSecurity...

>>>>> .)

>>>>> only target a single type of security token. So if you need to have

>>>>> your

>>>>> service utilize a policy which will authenticate multiple client

>>>>> security

>>>>> tokens (of different types), we should create our own PolicyAssertion

>>>>> classes. For creating WSE 3.0 custom Policy Assertion, you can refer

>>>>> to

>>>>> the

>>>>>

>>>>> "Custom Policy Assertions "

>>>>>

>>>>> section in the WSE 3.0 Document. And the QuickStart samples also

>>>>> including

>>>>> Custom Policy example. Also, the important things is that we need to

>>>>> define

>>>>> the proper InputFilters and OutputFilters for our custom

>>>>> PolicyAssertion.

>>>>> And for security Policy Assertion, we should make our inputFilter and

>>>>> outputFilter derived from "ReceiveSecurityFilter" and

>>>>> "SendSecurityFilter"

>>>>> class.

>>>>>

>>>>> After we define the custom PolicyAssertion, we can use it

>>>>> programmatically

>>>>> in code or define in Policy file statically.

>>>>>

>>>>> Hope helps. Thanks,

>>>>>

>>>>> Steven Cheng

>>>>> Microsoft Online Support

>>>>>

>>>>> Get Secure! www.microsoft.com/security

>>>>> (This posting is provided "AS IS", with no warranties, and confers no

>>>>> rights.)

>>>>>

>>>>>

Re: UserName and Kerberos tokens at the same time

Re: UserName and Kerberos tokens at the same time

>>>>

>>>> -----

>>>> From: "Henrik Skak Pedersen" <skak@xxxxxxxxxxxxxxxxxxxx>

>>>> References: <uDOvP8Q8FHA.620@xxxxxxxxxxxxxxxxxxxxxxxx>

>>>> Subject: Re: UserName and Kerberos tokens at the same time

>>>> Date: Thu, 24 Nov 2005 17:29:10 +0100

>>>> Lines: 19

>>>> X-Priority: 3

>>>> X-MSMail-Priority: Normal

>>>> X-Newsreader: Microsoft Outlook Express 6.00.2900.2180

>>>> X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

>>>> X-RFC2646: Format=Flowed; Response

>>>> Message-ID: <eHap0QR8FHA.1000@xxxxxxxxxxxxxxxxxxxxxxxx>

>>>> Newsgroups: microsoft.public.dotnet.framework.webservices.enhancements

>>>> NNTP-Posting-Host: 80.63.142.94

>>>> Path: TK2MSFTNGXA02.phx.gbl!TK2MSFTNGP08.phx.gbl!tk2msftngp13.phx.gbl

>>>> Xref: TK2MSFTNGXA02.phx.gbl

>>>> microsoft.public.dotnet.framework.webservices.enhancements:7731

>>>> X-Tomcat-NG:

>>>> microsoft.public.dotnet.framework.webservices.enhancements

>>>>

>>>> Extra comment:

>>>>

>>>> It should also be a policy.

>>>>

>>>> "Henrik Skak Pedersen" <skak@xxxxxxxxxxxxxxxxxxxx> wrote in message

>>>> news:uDOvP8Q8FHA.620@xxxxxxxxxxxxxxxxxxxxxxxx

>>>>> Hi,

>>>>>

>>>>> I would like to authorize the user using a Kerberos, a UserName or at

>>>>> custom token depending on what I receive from the user.

>>>>>

>>>>> Is that possible?

>>>>>

>>>>> Thanks

>>>>>

>>>>> Henrik

>>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>>>>

>

.

-
- **Follow-Ups:**
 - ◆ **Re: UserName and Kerberos tokens at the same time**
 - ◇ From: Steven Cheng[MSFT]
 - **References:**
 - ◆ **Re: UserName and Kerberos tokens at the same time**
 - ◇ From: Steven Cheng[MSFT]
 - ◆ **Re: UserName and Kerberos tokens at the same time**
 - ◇ From: Henrik Skak Pedersen
 - ◆ **Re: UserName and Kerberos tokens at the same time**
 - ◇ From: Henrik Skak Pedersen
 - ◆ **Re: UserName and Kerberos tokens at the same time**
 - ◇ From: Steven Cheng[MSFT]
 - Prev by Date: **Re: Signature Block in the signed message..**
 - Next by Date: **RE: WSE 3.0; Kerberos Token; An invalid security token was provided.**
 - Previous by thread: **Re: UserName and Kerberos tokens at the same time**
 - Next by thread: **Re: UserName and Kerberos tokens at the same time**
 - **Index(es):**
 - ◆ **Date**
 - ◆ **Thread**