

## Re: WSE 2.0 SP2: UsernameTokens must be encrypted to request SCT?

**Source:**

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2005-02/>

---

**From:** William Stacey [MVP] ([staceywREMOVE\\_at\\_mvps.org](mailto:staceywREMOVE_at_mvps.org))

**Date:** 02/11/05

Date: Fri, 11 Feb 2005 02:08:31 -0500

aah. Ok, that makes more sense. Thanks.

--

William Stacey, MVP

<http://mvp.support.microsoft.com>

"Softwremaker" <[msdn@removethis.softwaremaker.net](mailto:msdn@removethis.softwaremaker.net)> wrote in message  
news:OUvvQZAEFHA.1292@TK2MSFTNGP10.phx.gbl...

> William,

>

> > I am not sure what they are talking about with that either. I have SP2

> and

> > can send UT and sign the message with them with SendPlain and SendHashed

> > using just the default UTM and it works. So not sure what they are

> talking

> > about. Anyone?

>

> [WilliamT] I am not sure if you are using the UT in the context of the  
> SecurityTokenServiceClient. I think the statement above by Keith is wrt to  
> the SecurityTokenServiceClient. I quote:

> The SecurityTokenServiceClient class will now automatically encrypt any  
> Username tokens included in a request. Similarly, the SecurityTokenService  
> class will automatically encrypt any username tokens included in a  
response.

> Unless I am missing something as well, I dont think it forces a UNT  
> encryption if you are sending plain UNT as authentication credentials

>

> The following methods have been added to the token issuing framework:

> protected virtual void

> SecurityTokenServiceClient.EnforceRequestUsernameTokenEncryption().

> Called from EnforceRequestPolicy(), this method enforces the requirement

> that any Username tokens in an RST message must be encrypted. The

> issuerToken is used as the encrypting token. This method will throw an

> exception if it cannot encrypt the UsernameTokens in an RST message.

> Override this method to suppress this behavior.

>

> protected virtual void

> SecurityTokenService.VerifyRequestUsernameTokenEncryption().

> Called from VerifyRequestPolicy(), this method verifies that tokens in an

> RST message are encrypted. This method will throw an exception if it

> encounters an unencrypted UsernameToken in an RST message.

> Override this method to suppress this test.

>

> protected virtual void

```
> SecurityTokenService.EnforceResponseUsernameTokenEncryption().
> Called from EnforceResponsePolicy(), this method enforces the requirement
> that any Username tokens in an RSTR message must be encrypted. The
> ResponseEncryptingToken is used as the encrypting token. This method will
> throw an exception if it cannot encrypt the UsernameTokens in an RSTR
> message.
> Override this method to suppress this behavior.
>
> protected virtual void
> SecurityTokenServiceClient.VerifyResponseUsernameTokenEncryption().
> Called from VerifyResponsePolicy(), this method verifies that tokens in an
> RSTR message are encrypted. This method will throw an exception if it
> encounters an unencrypted UsernameToken in an RSTR message.
> Override this method to suppress this test.
>
>
>
> --
> Thank you.
>
> Regards,
> William T (Softwaremaker)
> http://www.softwaremaker.net/blog
> =====
>
> "William Stacey [MVP]" <staceywREMOVE@mvps.org> wrote in message
> news:#sj5$m$DFHA.2180@TK2MSFTNGP10.phx.gbl...
> > "The Web Services Enhancements (WSE) team is so concerned about the
> > misuse
> > of Username tokens that as of SP2, the WSE 2.0 token-issuing framework
> > will
> > reject any request that contains an unencrypted Username token (one
> > acceptable form of encryption is simply to use SSL). And there will be
> > no
> > configuration option to change this behavior. If you really want to
> > relax
> > this restriction, you'll need to write code to do it."
> >
> > I am not sure what they are talking about with that either. I have SP2
> > and
> > can send UT and sign the message with them with SendPlain and SendHashed
> > using just the default UTM and it works. So not sure what they are
> > talking
> > about. Anyone?
> >
> >
> > > I understand the issues involved with the use of UsernameTokens to
> > sign
> > and
> > to encrypt. However, for my application, it's not feasible to give
> > certificates to users, nor will they be on the same domain (so, no
> > Kerberos
> > either). Also, the business case just isn't valuable enough for anyone
> > to
> > > really try hard to mess with the data.
> >
> > If it does not matter, then don't even require a password or security.
> > Just
> > keep it open. If it does require security, then don't use UTs unless
> > you
> > are using SSL or have a SCT and can encrypt them. If you can't use
> > certs
```

```
> to
> > get a SCT, have a look at my post on using just the public rsa key to
get
> a
> > SCT at
> >
>
<u>http://spaces.msn.com/members/staceyw/Blog/cns!1pnsZpX0fPvDxLKC6rAAhLs0!303.entryhttp://mvp.support.microsoft.com
> >
> > "SA" <informatica@freemail.nl> wrote in message
> > news:OhgIhP9DFHA.4072@TK2MSFTNGP10.phx.gbl...
> > > Hi all,
> > >
> > > In Keith Brown's article [1], I read
> > >
> > > "The Web Services Enhancements (WSE) team is so concerned about the
> > misuse
> > > of Username tokens that as of SP2, the WSE 2.0 token-issuing framework
> > will
> > > reject any request that contains an unencrypted Username token (one
> > > acceptable form of encryption is simply to use SSL). And there will be
> > no
> > > configuration option to change this behavior. If you really want to
> > relax
> > > this restriction, you'll need to write code to do it."
> > >
> > > Is this actually the case? I am still running SP 1 of WSE 2.0 and will
> > need
> > > to change a lot of code.
> > >
> > > I understand the issues involved with the use of UsernameTokens to
sign
> > and
> > > to encrypt. However, for my application, it's not feasible to give
> > > certificates to users, nor will they be on the same domain (so, no
> > Kerberos
> > > either). Also, the business case just isn't valuable enough for anyone
> > to
> > > really try hard to mess with the data.
> > >
> > > Is there a workaround available?
> > >
> > > [1]
> > >
> > >
> > >
<u>http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnwse/html/secusernameto
> > > --
> > >
> > >
> > > Sven.
> > >
> > >
> > >
> > >
> > >
> > >
```