

Re: Need for encryption in WSE 3.0 if using SS-avoid man-in-middle

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2006-10/msg00118.html>

- *From:* John K <KTJ@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 19 Oct 2006 10:14:01 -0700
-

SSL only validates you are talking to a SSL certified server; not necessarily the "right" SSL certified server. We allow the client user to change what URL the software uses for accessing web services. This is our customer wants to host the server components of the system we are selling on their server(s) instead of ours. Thus, we do not need to send a special version of the software to the customer. They can simply edit the URL the client program access.

Thus, I am wondering what is a secure way of verifying the client program is talking to a "valid" server (the one with the actual web services that need to be accessed) BEFORE it sends the user's ID and password. I believe this can be done by using a X.509 certificate on both ends, but I thought the adds message level security which is overkill since we are using SSL. What do you recommend for testing if the client program is talking to the "right" server before it freely gives the user ID and password for authentication. Since we allow the user to change the URL in the client program; a malicious user could temporarily change the URL and then an unsuspecting user would attempt to log in and when the S/W tries to do that; it would give the "malicious" server it's password.

--

Thank you.

"Dominick Baier" wrote:

SSL, thus message level security adds unnecessary overhead. Is there a good way to do mutual authentication at first connection to the web service so there is no significant overhead for message based security?

thats exactly what SSL is doing.

for client certificate authentication, simply require SSL client certificates in IIS (directory security tab).

Re: Need for encryption in WSE 3.0 if using SS–avoid man–in–middle

Finally, if I do need a client certificate to do the mutual authentication; how do I generate a client certificate? Can I

You can use a public CA or Windows Certificate Services or makercert.exe

Dominick Baier, DevelopMentor
<http://www.leastprivilege.com>

Dominick said I don't need message level security since I am using SSL, thus message level security adds unnecessary overhead. Is there a good way to do mutual authentication at first connection to the web service so there is no significant overhead for message based security? Is there any "how to" or examples on how to implement mutual authentication, ideally, without requiring message based security? Finally, if I do need a client certificate to do the mutual authentication; how do I generate a client certificate? Can I generate a client certificate from a server SSL certificate (which my server has) OR do I need another type of certificate on my server.

I know there are several questions here, but please answer each one.

"Steven Cheng[MSFT]" wrote:

Hello John,

If you use WSE message layer security, the "mutualCertificate10" and "mutualCertificate11" will both support mutual authentication against both server and client.

As for transport layer security through SSL/HTTPS, as I mentioned in the last reply, you can add code logic in your webservice client and hook the Server Certificate validation process to determine whether the https/SSL server is a valid and expected server.

Sincerely,

Steven Cheng

Microsoft MSDN Online Support Lead

Re: Need for encryption in WSE 3.0 if using SS—avoid man—in—middle

This posting is provided "AS IS" with no warranties, and
confers no
rights.