

Re: WS Security issues

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2005-06/>

- *From:* Dilip Krishnan <"dilip.krishnan AT apdiya DOT com">
 - *Date:* Wed, 01 Jun 2005 14:48:58 -0500
-

+1,

If you're looking to sign and encrypt using user name token, keep in mind the service will not be interoperable with java or other technologies.

I guess your best option is to use username token for authentication and authorization. And use X509 certs for signing and encrypting. This is a little slower than ssl but from a purist standpoint you are now transport independent!

Henrik Skak Pedersen wrote:

Hi Yedu,

Thank you very much for your reply.

Would you use UsernameTokens for signing, encrypting and authentication?
How can I send the current UsernameToken?
How are you deploying "SSL settings"?

Regards

Henrik

"Yedu" <Yedu@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:C7E4560D-F7DF-43A1-9799-97BF2A2E48FC@xxxxxxxxxxxxxxxxxxxxxxxx

We have a similar setup that you described.
We are sending the Username/password in the
userName token, the Webservice
server machine needs to be in the same domain as of

Re: WS Security issues

the AD, if an invalid username/password is sent and it cannot be authenticated it will throw a SoapFault. The username/password is sent as plaintext in the usernameToken.

We are using SSL for making sure that the channel is secure.

If you plan to implement the X.509 for encryption my guess is that it will be drag on the performance.

"Henrik Skak Pedersen" wrote:

Hello,

I am working on a product when we are shipping a web service and a windows client to several end-customers. The web service should be able to run either on the inside or on the outside of their firewall. The same CD are being sent to all customers, so it is not possible to modify anything from customer to customer. The software should run directly after installation, without obtaining certificates or anything else. The clients are running on Windows 2000 server and client, Windows XP and Windows Server 2003.

I have two demands:

- 1) All WS requests from the client needs to be authorized by AD. It should be possible to log in using the current credentials or by specifying an user name/password pair.

- 2) All WS requests from the client needs to be encrypted and signed

I have looked into X509SecurityToken, KerberosToken and UsernameToken. But I

Re: WS Security issues

just can't see how I solve this the the
best way.

If I use X.509 for signing and encryption, then I guess that I have to
distribute the same certificate to all customers, which I guess not i a
smart idea.

I have read that the KerberosToken does not work for Windows 2000.

Any recommendations?

Regards

Henrik Skak Pedersen

--

HTH

Regards,

Dilip Krishnan

MCAD, MCS.D.net

dilip.krishnan AT apdiya DOT com

.