

Is this Possible?

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2007-03/>

- *From:* bbq101@xxxxxxxxxx
 - *Date:* 20 Mar 2007 11:36:18 -0700
-

A little background. The company I work for has exposed web services to our clients and currently uses HTTPS as a mechanism to keep our services secure. We are looking to expand our offerings to other clients including new applications that as of yet do not have any web services available.

One of our concerns using HTTPS to secure our transactions is scalability. We realize that HTTPS slows down the whole process, especially if we are looking to do any farming. Because of this, we are looking into using WSE 2.0 to help secure our services without the need for HTTPS.

I have gotten the asymencrypt sample to work, and have even ported it over to work with one of our existing services. I additionally was able to encrypt a soap header we use for authorization. As many of you know, in the client code of the asymencrypt example, the client gets the public key of the server's certificate to encrypt the data sent to the server. The server then uses its private key to decrypt the message and do its work.

My question is, is it possible to switch this? We would like each of our clients to get their own x509 certificate and give us their public key. This way, they could use their private key to encrypt their messages, and our servers running the services would decrypt using their public key. This would help us further authenticate who is sending us the message since only the correct public key would be able to decrypt, and we would encrypt the response using their public key which only they would be able to decrypt. Is this scenario possible?

In looking at the examples, it is not clear to me how the server picks the certificate it uses to decrypt the message. All I see is in the config it is told to look in the localmachine store.

Any info would be greatly appreciated. Specific questions:

- 1) Is the above scenario possible?
- 2) What is the best practice for securing webservices? Is HTTPS really a concern?

Is this Possible?

3) Is it more common to have your clients encrypt their messages using your servers public key, but then sign part of the message using their own private key? The server then can get their public key from this sign, and encrypt the response using their public key (there is an sample of this in the quicksamples of wse 2.0 I beleive)?

Thanks!

BBQ

.