

RE: Encryption and signing using Security context tokens using WS

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2005-03/>

From: Thomas S. Trias (ThomasSTrias_at_discussions.microsoft.com)

Date: 03/15/05

Date: Tue, 15 Mar 2005 09:05:06 -0800

Kiran,

If you are going to enforce requirements on both ends of the communication using policy, then you definitely need policy documents on both the caller and callee. Since it looks like you are setting up policy both for your SCT service and your main web service, the policy document should be specified in the web.config for each if they are in separate ASP.NET applications and in the common web.config otherwise.

```
> <mappings>
> <endpoint
> uri="http://server1/SecureConvCodeService/SecureConvService.asmx">
> <defaultOperation>
> <request policy="#Sign-SCT-Encrypt-SCT" />
> <response policy="" />
> <fault policy="" />
> </defaultOperation>
> <operation
> requestAction="http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT">
> <request policy="" />
> <response policy="" />
> <fault policy="" />
> </operation>
> </endpoint>
> </mappings>
```

This portion of the policy file indicates that you have a web service at "<http://server1/SecureConvCodeService/SecureConvService.asmx>"; the operations on this service will be mapped to the specified policies based upon the SoapAction header received. SCT requests (SoapAction = "<http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT>"), will have no policy applied to requests, responses or faults, and all other requests must be signed and encrypted by an SCT (although responses and faults will neither be signed nor encrypted).

The point of failure is that the "To:" portion of the WS-Addressing part of the Soap envelope in the request does not match "http://server1/SecureConvCodeService/SecureConvService.asmx", so WSE can't match the request to the policy. If you change the URI to "http://name-or-addr-of-the-load-balancer/SecureConvCodeService/SecureConvService.asmx", the policy will probably be found, but you will run into another error: the connection information from the HTTP request will not match the "To:" information, since the "To:" will contain the external URI, and the HTTP connection will actually be made to a particular internal server. Since the client cannot know which internal server they will get, the only solution is to add a SoapActor attribute to your web services; I recommend using the external URI as your SoapActor, so that you don't have to change any existing proxies / clients. If you choose some other URI as your SoapActor (make it the same for all internal servers), clients will have to specify that SoapActor as the "To:" (along with Via information referencing the external URI).

BTW, thanks for the information; you may have just pointed me towards a solution for my post about autoIssueSecurityContextToken and SoapActor.

Thomas S. Trias
Senior Developer
Afni Insurance Services
<http://www.afniinc.com/>