

Re: Trying to determine best strategy for web service security

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2004-10/>

From: Ben Bloom (*bbloom_at_macg.s.p.a.m.regor.com*)

Date: 10/14/04

Date: Thu, 14 Oct 2004 15:03:46 -0400

Hi Mac,

I would check out the Hands On Labs for WSE 2.0. Specifically, look at the SecureCommunication example. While I haven't implemented it specifically, it sounds like it will solve your problem of authenticating a user and then passing a token around (instead of authenticating every web service call.)

Good luck!

-Ben

M. Ferguson wrote:

> *Hi all,*

>

> *I am new to WSE 2.0 and a little overwhelmed by the breadth of what's*

> *included, and I have a specific security situation for which I'm*

> *trying to determine the best strategy. Basically I know it's going to*

> *involve using WSE but I would appreciate comments and suggestions from*

> *people who know the framework better than I do.*

>

> *I have a group of web services which provide a facade for a COM+*

> *application, and I need to implement role-based authorization at the*

> *method level. The only clients of the web services will be ASP.NET*

> *apps calling them over SSL (or possibly even a trusted network), so I*

> *am not terribly worried about the integrity of the conversation.*

>

> *What I would like to have is an authentication web service that would*

> *be called with a UsernameToken based on a forms login at the ASP.NET*

> *app and on successful authentication would return something*

> *representing the authenticated principal including its roles. This*

> *structure would then be stored in the user's ASP.NET session and used*

> *to create a token which could be sent back to the web services with*

> *each call so that the services could then authorize the roles in the*

> *token against a policy for the method being called.*

>

> *I don't want to send a UsernameToken with every call to the facade*
> *because to authenticate against a database or directory and retrieve*
> *credentials with every call to the facade would add a lot of*
> *unnecessary overhead.*
>
> *Has anyone else implemented anything like this? I am pretty certain*
> *that I can figure out how to configure WS-Policy to allow/restrict*
> *roles, but I would appreciate any suggestions on how I should return*
> *my credentials from the authentication service and what kind of token*
> *I should use to pass them with the facade calls. Pointers, examples,*
> *suggested starting points for reading, or just being told that I can't*
> *get there from here, Bob would all be warmly received.*
>
> *thanks muchly,*
>
> *Mac Ferguson*

--
to reply, remove .s.p.a.m. from email