

RE: Propagating caller identity across applications from a bare ASMX Service method to a WSE3 Service method

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2007-01/>

- *From:* stcheng@xxxxxxxxxxxxxxxxxxxxxx (Steven Cheng[MSFT])
 - *Date:* Wed, 10 Jan 2007 07:07:53 GMT
-

{\rtf1\ansi\ansicpg936\deff0\deflang1033\deflangfe2052{\fonttbl{\f0\fnil\prq2\fcharset0 MS Sans Serif;}}
\viewkind4\uc1\pard\lang2052\f0\fs20 Hello Howard,
\par
\par Glad to see you again.
\par
\par Seems you're still struggling with the multi-tier webservice authentication issue. As you described here, your original architecture is
\par
\par client browser <---> web application <---> end webservice (windows authentication)
\par
\par and currently, due to some asp.net web application is using .NET 1.1(can not afford wse 3.0). You adjust the architecture as below:
\par
\par client browser <---> web application<-->proxy webservice<--->end webservice (windows authentication).
\par
\par I think forwarding the windows security identity from client browse to the end webservice(accross all the intermediate services) is quite difficult. To do this, all the computers (from client to end services and intermeidate server) should be in the same local domain or trusted domain. And they need to be configured so as to use kerberos delegation. Configuring kerberos delegation including configrue all the possible client accounts and all the server account and machines which will peform delegation. Just the same as configuring double hop scenario for ASP.NET application.
\par
\par #How to configure an ASP.NET application for a delegation scenario
\par <http://support.microsoft.com/kb/810572/en-us>
\par
\par Have all the application and services in your scenario been configured for kerberos delegation? For configuration specific problem, there is a document for troubleshooting kerberos delegation
\par
\par #Kerberos authentication and troubleshooting delegation issues
\par <http://support.microsoft.com/kb/907272/en-us>
\par
\par
\par And as you mentioned, currently you put all the services on the server machine, is this also the topology in production enviroment? If not, I suggest you make other serivces on a separate machine with the ASP.NET

RE: Propagating caller identity across applications from a bare ASMX Service method to a WSE3 Service method

web application. Because if they're on the same machine, the windows identity in ASP.NET web application can be forwarded to other services on the same machine without using kerberos delegation.

\par

\par In addition, I'm not sure whether using kerberos delegation and windows authentication across all the hops is a must-to-use approach for your scenario. For windows 2003 domain, there has provided a constrained delegation and S4U type token that can help the server generate a windows security token(the windowsIdentity class in .net framework) without password(only the user principal name is necessary). Thus, it opens a way for N-TIER application which need flow security identity/context across multi application/services. Here are some MSDN reference describing on this, I think this is also an option you can consider.

\par

\par #How To: Use Protocol Transition and Constrained Delegation in ASP.NET 2.0

\par <http://msdn2.microsoft.com/en-us/library/ms998355.aspx>

\par

\par #Exploring S4U Kerberos Extensions in Windows Server 2003

\par <http://msdn.microsoft.com/msdnmag/issues/03/04/SecurityBriefs/default.aspx>

\par

\par Hope this helps.

\par

\par Sincerely,

\par

\par Steven Cheng

\par

\par Microsoft MSDN Online Support Lead

\par

\par

\par

\par =====

\par

\par Get notification to my posts through email? Please refer to

<http://msdn.microsoft.com/subscriptions/managednewsgroups/default.aspx#notifications>.

\par

\par

\par

\par Note: The MSDN Managed Newsgroup support offering is for non-urgent issues where an initial response from the community or a Microsoft Support Engineer within 1 business day is acceptable. Please note that each follow up response may take approximately 2 business days as the support professional working with you may need further investigation to reach the most efficient resolution. The offering is not appropriate for situations that require urgent, real-time or phone-based interactions or complex project analysis and dump analysis issues. Issues of this nature are best handled working with a dedicated Microsoft Support Engineer by contacting Microsoft Customer Support Services (CSS) at <http://msdn.microsoft.com/subscriptions/support/default.aspx>.

\par

\par =====

\par

\par

\par

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

\par

\par

\par

RE: Propagating caller identity across applications from a bare ASMX Service method to a WSE3 Service method

RE: Propagating caller identity across applications from a bare ASMX Service method to a WSE3 Service method

\par
\par
\par
\par
\par
\par
\par
\par
\par
\par
\par }

RE: Propagating caller identity across applications from a bare ASMX Service method to a WSE3 Service method