

Service Oriented Architecture: In the Security Perspective

As electricity, if used tactfully then many useful things can be done but a little carelessness can make a big loss. As the same way Information, if accessed by the authorized person, produces effective output but unauthorized access to the same may create unpredictable nuisance. Many e-Governance applications are being developed with Service Oriented Architecture (SOA), so that to provide interoperability with other applications and also application security has been taken care. But the interlinking point between two different applications i.e. the Web Services found still unprotected, which are going to become the biggest interest of the Hackers community. This scenario is like, two plastic covered & secured electric wires connected with each other but the interlinking point is still naked and exposed to the outer environment. It is the time to address this kind of dangerous interoperability. So, in this article our focus is to provide a simple but effective way for making Private Web Services more secure.



Niladri Bihari Mohanty
District Informatics Officer
niladri.mohanty@nic.in



Ravindra Kumar Jaiswal
Scientific Officer/Eng-SB
ravindra.jaiswal@nic.in

e-Governance is suffering from out of date data, improper integration between applications, redundant implementation of projects, non consumption and cyber security failures. After the Govt of India has initiated National e-Governance Plan (NeGP) in the year 2006, many ICT based projects have been implemented. Among those one of the most ambitious project initiated by the Department of IT, GOI is, rolling out of Citizen Service Centers (CSC) across the country whose success entirely depends on the quality of Interoperability between different e-Gov applications. Web services are being developed for the interoperability issue and depending on the nature of interoperability; this can be divided in to two categories.

Public Web Services: This can be accessed by any external applications for Information and process interoperability.

Ex: Weather forecasting Services, Railway enquiry Services, Global Time Setting etc

Private Web Services: This can be accessed by only a group of authenticated external applications. This kind of web services check the authentication of incoming request and only then send the response to the consumer.

Ex: Payment gateway system of Banking, Inter Banking ATMs, Integration of CSCs with Back end e-Gov Application etc.

Many initiatives have been taken up to scratch the ground

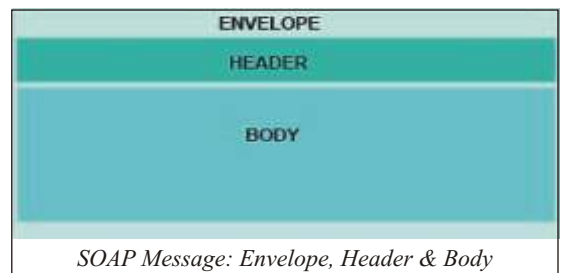
of SOA. Developments as well as the migration to SOA based applications have already been started. Protecting the private or restricted Web Services is still the head ach for many developers. So, in this article our focus is to provide a simple but effective way for making Private web services more secure.

Providing Security to the Web Services and to validate the client request can be done in two major ways. One is by passing authentication credentials through the Simple

Object Access Protocol (SOAP) Header and other is through the feature-rich Application Programming Interface (API) of Web Services Enhancement (WSE) Ver-3.0. We have tried to focus the simple way to check the authentication of the secured Web Services by passing security credentials through the SOAP header without any third party Software as well as a brief introduction about the advance tool i.e WSE-Security has also been introduced.

Authentication through SOAP Header:

Headers are the one of the three elements that a SOAP message can contain i.e The Envelope, the Header and the Body.

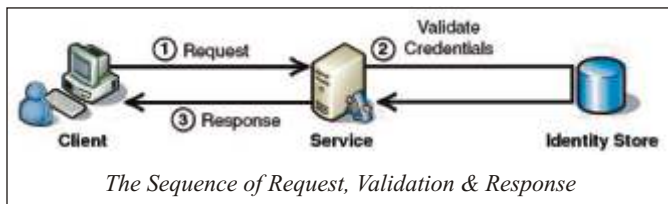


Envelope: This is the highest level & contains both Header & the body.

Header: The header element is an optional and contains metadata but can be effectively used to pass the authentication credential in the request.

Body: This is the main portion of the message where all the real data is located.

The Service provider validates the credential received through the header element against the identity store and sends the response to the client.



This type of authentication can only possible when the client and the service provider share the trusted relationship and exchange the password to be used in each transaction. Basic steps to implement this authentication are:

1. Create the Web Service

2. Create the custom Header Class

```
Public Class header Inherits system. Web.
Services. Protocols. Soap Header
```

3. Add the authentication method to the Class

```
Public uid As String
Public pwd As String
Public Function validate() As Boolean
If uid = #(db(uid)) And pwd =#(db(pwd)) Then
Return 1
Else
Return 0
End If
End Function
-----
```

Note:#db(uid/pwd):Hash value of the user name/password fetched from the identity database

4. Add the Header object to the Web Service

```
Public Class Service Inherits System. Web
Services. WebService
'' Create the object of the header class
Public obj As header
''Assign the object to the header class to the
web method
```

```
<WebMethod(), SoapHeader("obj", Direction:=SoapHeaderDirection.InOut)>
```

5. Verify the credential supplied by the client by calling authentication method through the object of the header class.

Authentication through WSE-Security:

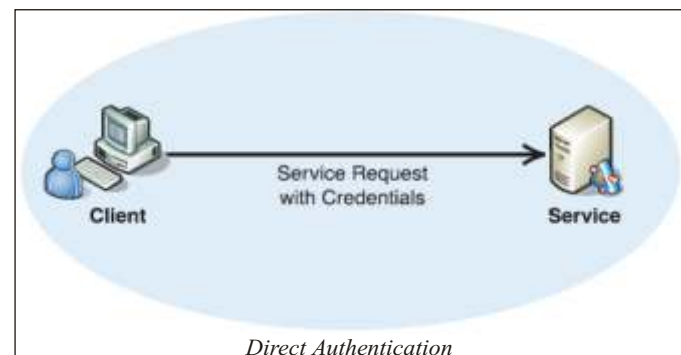
WSE provides advanced functionalities that are not readily available otherwise. Security is one of the major benefits of using WSE. And by using it; developers have access to feature-rich and easy to use API for providing enhanced Security to SOAP message. WSE 3.0 applies the security at a higher level using a set of security assertions. It enables Web Service to be secured imperatively in code and declaratively using security policy. The concept of WSE works on “security zone” methodology. Suppose one security agency has been assigned to provide security to an international cricket team during movement in their entire tour. Then the agency is having two options. The first one is to provide dedicated guards to each individuals and the second one is, without giving security to individuals, secure the zone (Rout) of their movement as well as their source (Hotel) & destination (Field) for the entire team. Definitely in the first look the choice is the second one. In the WSE-3.0 also the concept is similar and it provides the end to end security at client & server side as well as transport security to provide a completely secured zone.

Authentication type in WSE-Security:

Depending on the relationship between client & service provider, two different type of authentication can be implemented to secure the Web Services.

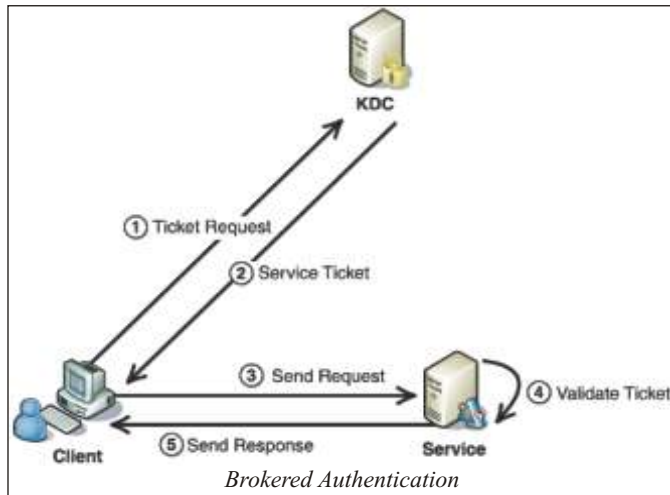
• Direct Authentication

If the Web Service provider and the consumer share the security credentials and participate in the trusted relationship then Direct Authentication is useful, in which the credentials like password can be shared between the parties.



• Brokered Authentication

If the Web Service provider and the consumer don't participate in direct trusted relationship then the Web Service consumer need to get a security ticket from Key Distribution Centre,




whose responsibility is to verify the client and issue security ticket. The Web Service provider provides the service after verifying the ticket but not necessarily verifying the Client. Brokered Authentication can be implemented by 3 types.

- 2.1 Security Token Service
- 2.2 X.509 Public Key Infrastructure
- 2.3 Kerberos Token

WSE Security provides an efficient way of message layer security, which is having some advantages over as usual transport layer security (Specifically SSL) that includes:

- It is not affected by standard Firewall but SSL need the 443 port to be opened in Firewall
- Parts of the message (Intermediaries need to view so as to determine the destination), can be signed or encrypted instead of the entire message, where as in SSL entire message need to be encrypted.
- Using message layer security, messages can be sent over many different protocols such as SMTP, FTP, and TCP without having to rely on the protocol for security.

Cyber Security and Cyber Crime are complementary of each other. So no security can be said as full proof as the increasing rate of cyber crimes. Different kind of hybrid security system can also be developed with the help of powerful WSE-Security tool. 

For Further Information contact
Niladri Bihari Mohanty
 NIC, Peren District Unit, Nagaland
niladri.mohanty@nic.in

Upcoming ICT Events

12th International Conference on Computer and Information Technology

Dhaka, Bangladesh
 December 21st-23rd, 2009
<http://www.iccitbd.net/>

International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2009

Trivandrum, Kerala, India
 December 28th-29th, 2009
<http://www.icacett.com/>

International Conference on eGovernment and eGovernance

Ankara, Turkey
 March 11th-12th, 2010
<http://www.icegeg.info/>

International Conference on Information Management and Evaluation

University of Cape Town, South Africa
 March 25th -26th, 2010
<http://academic-conferences.org/icime/icime2010/icime10-home.htm>

17th International Conference on Telecommunications

Doha, Qatar
 April 4th-7th, 2010
<http://www.qu.edu.qa/ict2010/>

12th International Conference on Computer System Design and Operation in the Railway and other Transit Systems

Beijing, China
 August 31st September 2nd, 2010
<http://www.wessex.ac.uk/10-conferences/comprail-2010.html>

5th Ministerial eGovernment Meeting and Conference

November 18th 20th, 2010
 Malmo, Sweden
<http://www.egov2009.se/>

Incase you know of any such conferences, please write to us at:
editor.info@nic.in