**Authentication using WCF Message Security - 1**

**Rameshkartik. RS**

**Table of Contents**

[Introduction 3](#_Toc394297020)

[Deciding Authentication Schema 4](#_Toc394297021)

[Windows Authentication over the message security 4](#_Toc394297022)

[Custom username- and password –Based Mutual authentication What is Mutual authentication? 7](#_Toc394297023)

[Implementation in WCF 8](#_Toc394297025)

[Refer the code attached for the further details 10](#_Toc394297028)

[Summary 10](#_Toc394297029)

# Introduction

Before coming into this article I recommend you to take my last article “Basics on WCF Security” if you are not good at the basics on WCF Security. In this article we will see how the authentication can be achieved using Windows authentication over message security ,custom username and password authentication over the message security, and finally the Mutual X509 authentication over the message security.

# Deciding Authentication Schema

Authentication Schema

“*It Determines the type of credentials expected for authenticating the client*”

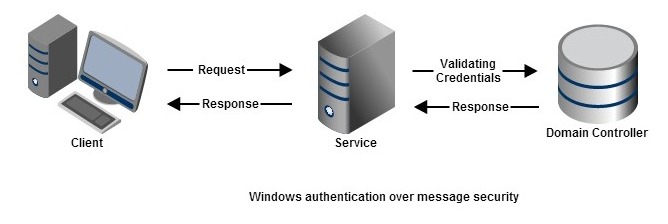
The available type of credentials is None, Windows, Username, Certificate and Token. Yes, Few services will expect only the windows credentials to get it authorized, few will expect only the certificate to authorize the client. Depending upon the project requirement, the service can set the authentication schema to attain the message security. Also the mutual authentication can also be achieved using, the type of credentials listed below

|  |  |
| --- | --- |
| **None** | Clients are not authenticated by the service |
| **Windows** | Clients are authenticated by the service using the windows authentication |
| **Username** | Clients are authenticated by the service using the username and password |
| **Certificate** | Clients are authenticated by the service using the information provided in an X509 certificate |
| **Token** | Clients are authenticated by the service with the token issued by a third party |

Authentication schema determines the complete authentication mechanism in a service. Let’s discuss these options in detail.

# Windows Authentication over the message security

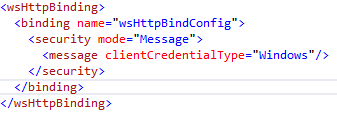
Just try to give a blind guess by seeing the below image



Hope you got it, I believe, Yes the windows credentials which were presented to the service will be sent to the domain controller which will validate the credentials and confirm the authentication, The authentication process will be done using the Kerberos or NTLM protocol. Let's see the steps what you need to do in WCF to get this authentication facility

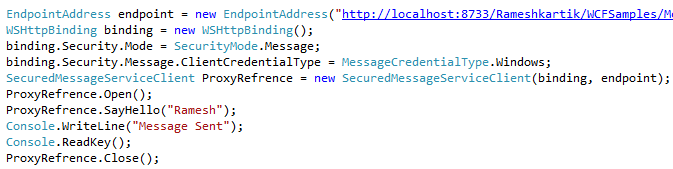
**Step 1:**

Once you have defined your ABC i.e Address, Binding and Contract in the Service, you need to create the security mode and client credential type in the Host or Service project.



With this step, we have defined that clients are authenticated by the service using the windows credentials what client is supplying.

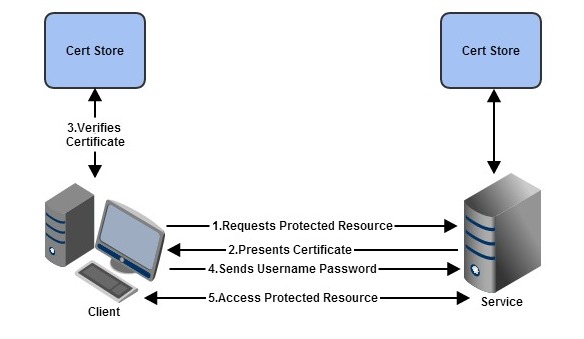
**Step 2:**

As a next step you need to create the same mode ,clientcredentialtype in the client side as like below snapshot

That’s it, Nothing complex here, just refer the attached source code and run it, your service will validate the client requests based on windows credentials.

# Custom username- and password –Based Mutual authentication What is Mutual authentication?

# Client and server authenticate each other before doing any operation. The client must prove its identity to the server,and the server must prove its identity to the client, Because before making any security operations, it is not only important to authorize the client, but it is very important to authorize the server, because the client should provide his secure information like credit card credentials only to the right server.



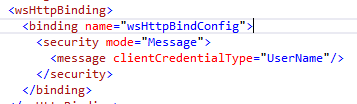
Let us see how the client and server authenticate themselves before doing any operation. The client makes a request to the service for a protected resource, The service then presents his certificate to the client,Client verifies the certificate and send his username and password which will be protected using X509 Certificate provided by the service.Server then verifies the client credentials and grants access to the protected resource to the client when the verification is done.

# Implementation in WCF

Let's think about how the same discussed concept can be implemented using WCF,

# Step 1:

Once you have defined your ABC i.e Address, Binding and Contract in the Service, you need to create the security mode and client credential type in the Host or Service project.



With this step, we have defined that clients are authenticated by the service using the custom username and password what client is supplying.

**Step 2:**

The Next step is that, we need to create the service credentials which are validated by the clients to identify his server, In our example, the service credential will be an X509 certificate, which is a digital certificate having the public key infrastructure(PKI) standard to verify that a public key belongs to the user,computer. The following are the syntax to define the service certificate.

certificate.png

The above tag will comes under the service behavior, findValue attribute holds the name of the certificate which is available on the localmachine, Local machine certificate store is local to the computer and is global to all users on the computer. This certificate store is located in the registry under the HKEY\_LOCAL\_MACHINE root, X509FindType identifies the type of value provided in the *findValue* parameter. Kindly refer the attachment to find the tool for creating certificates on your computer.

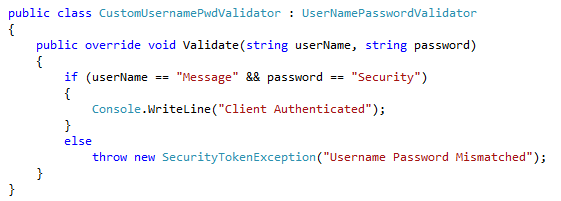
**Step 3:**

As a next step you need to write code for verifying the client credentials in the service side, Since the client credentials, we have been supplying should be verified in the server side to secure the exchange we should have a validation mechanism ,Following is the syntax to enable the validation part

validation.png

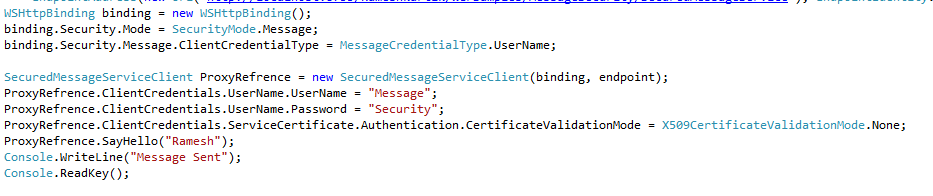
# This portion of the code has to be written in the service credentials , We need to put username validation mode as custom since we are supplying here is custom user name passwords, in the customusername password validator type just mention the namespace and assembly name of class where you have written your username,password validation.

The mechanism or authenticating the user credentials against an identity store is implemented through the abstract class System.IdentityModel.Selectors.UsernamePasswordValidator in the System.IdentityModel.Selectors assembly.



**Step 4:**

The final step is in the client side, in which you just need to provide the username and the password to get the protected resource from the client.



# Refer the code attached for the further details

# Summary

In Message security, the security details were attached to every message, The service can confirm their identity by showing his certificate, Whereas the clients can confirm their identity using the windows authentication ,custom username password authentication .