**Basics on WCF Security**

****

**Rameshkartik.RS**

**Table of Contents**

[Introduction 3](#_Toc392239095)

[Authentication 4](#_Toc392239096)

[Authorization 5](#_Toc392239097)

[Message Integrity 5](#_Toc392239103)

[Message Confidentiality 6](#_Toc392239104)

[Summary 6](#_Toc392239105)

**WHAT’s IN THIS ARTicle?**

* Introduction
* Authentication
* Authorization
* Message Integrity
* Message Confidentiality

# Introduction

This article is all about the basics of the WCF Security, in other words, this is the starting point of diving into the WCF Security concepts ☺ , and yes security is the most important for any technology we are working. A Decade before SOAP didn’t provide a secure message from tampering rather there was a way to encrypt the messages; all the security details were delegated to the transport layer. As a result, making SOAP an independent to the platform was a biggest challenge. Then one fine day new generation in security called WS-\* specifications was born to extend the existing SOAP specification with security capabilities for client authentication and message protection. New model for securing the messages at the message levels were also included. This SOAP specification was created in combination with the big leaders in industry such as Microsoft, IBM, and SUN among others. The following are the principles that WCF uses to secure the communication over the network

# Authentication

Authentication process normally asks two questions who are you? What is the proof you

have to get inside? For these questions the sender has to provide an answer to prove

an identity in the form of username, password or windows authentication or a token

with cryptographic information or an X509 certificate. In the other hand service should

have a mechanism of verifying/validating the evidence that were collected from the

client. For e.g. If the Custom Username and password is used, service should have logic

to validate the username and password supplied by the client. The client is successfully

authenticated only if the verification drops good results. In the following three different

scenarios the authentication would be fruitful,

* Client Authentication
* Server Authentication
* Mutual Authentication

Client Authentication is authenticated by the service to validate and verify that, are you the right person to utilize my service methods? Then what is the server authentication? Server authentication is authenticated by the client to confirm that client is talking to the right person, so the client needs to verify the service identity. Why the client needs to verify the server? Because we need to prevent the phishing attacks which is nothing but an attacker who makes available a fake service with a same signature as the original one to capture sensitive information about the user, eg: Credit card numbers, transaction passwords., we normally don’t like to provide the credit card pins to any one right? until the person is your family member or a known good friend. Final one to discuss here is Mutual authentication which is a combination of client authentication and the server authentication. Client and the server authenticate each other before any operation is made.

# Authorization

# Authorization normally decides what are all the system resources or the operations can

# be accessed by an authenticated user. WCF provides couple of mechanisms to

# implement the authorizations in the services.

* Role-Based Authorization
* Claim based Authorization and the Authorization context

# Am not going to explain in detail about the mechanisms in this article, we will discuss it

# in my series of articles in WCF Security.

# Message Integrity

It ensures that contents of the message have not been tampered or altered in transit.

Say For eg: The customer requests some amount from the bank, what if some man in

the middle attacking the message by making some change in the values.

Integrity for data in transit is generally based on some cryptographic techniques such as digital signatures.

# Message Confidentiality

It ensures that data in the message is highly confidential and private, and it does not read by unauthorized parties. It should not be seen by anyone in the network. Whereas the message integrity is the message would not be altered in the network. Without the message confidentially you cannot achieve the message integrity and vice versa. Message confidentiality is based on cryptographic techniques like data encryption.

# Summary

CIAA – Confidentiality, Integrity, Authentication and Authorization are more important in the security concepts