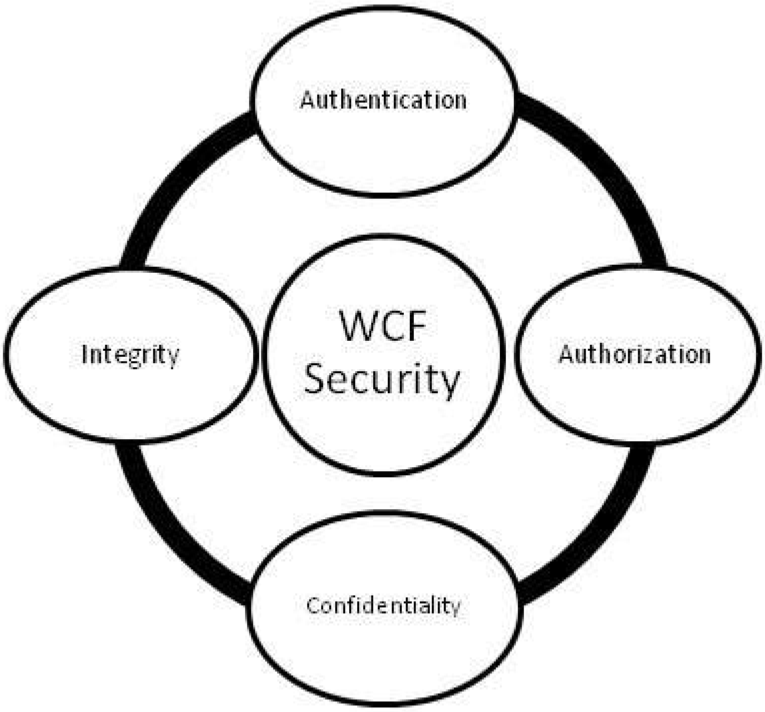
# WCF - SECURITY

http://www.tutorialspoint.com/wcf/wcf_security.htm Copyright © tutorialspoint.com

A WCF service boasts of a robust security system with two security modes or levels so that only an intended client can access the services. The security threats that are common in a distributed transaction are moderated to a large extent by WCF.

## Key Security Features

WCF service has four key security features as depicted in the figure below.



- **Authentication** - Here, authentication is not limited to identifying the sender of the message, but is mutual, i.e., authentication of the message receiver is required to rule out the possibility of any kind of middleman attack.

- **Authorization** - This is the next step taken by a WCF service to ensure security and it is here determined whether the service should authorize the caller to proceed further or not. Although authorization is not dependent on authentication, it normally follows authentication.

- **Confidentiality** - The exchange of information between a caller and a service is kept confidential to restrict its interpretation by others for whom the message is not intended. To make this possible, encryption is used along with a wide variety of other mechanisms.

- **Integrity** - The final key concept is maintaining integrity, i.e., offering the assurance that the message has not been tampered by anyone in its journey from the sender to the receiver.

## Transfer Security Mode

WCF offers the following transfer security modes to ensure a secured communication between a client and a server. The diverse transfer security modes are mentioned below.

- **None** - This mode does not guarantee any kind of message security and the service does not get any credentials about the client. This mode is highly risky, as it may allow message tampering and hence not recommended.

```
<wsHttpBinding>
   <binding name="WCFSecurityExample">
      <security mode="None"/>
   </binding>
```

```
</wsHttpBinding>
```

- **Transport** - This mode is the easiest way to achieve a secured transfer of message via the use of communication protocols such as TCP, IPC, Https, and MSMQ. This mode is more effective when the transfer is point-to-point and is used mostly in a controlled environment, i.e., intranet applications.

```
<wsHttpBinding>
   <binding name="WCFSecurityExample">
      <security mode="Transport"/>
   </binding>
</wsHttpBinding>
```

- **Message** - The security mode allows mutual authentication and offers privacy to a great extent as the messages are encrypted and can be transported through http, which is not considered as a secure protocol. Here the security is provided end-to-end without considering how many intermediaries are involved in a message transfer and whether there is a secured transport or not. The mode is used typically by internet applications.

```

<wsHttpBinding>
   <binding name="WCFSecurityExample">
      <security mode="Message"/>
   </binding>
</wsHttpBinding>
```

- **Mixed** - This security mode is not used frequently and client authentication is offered only at the client level.

```

<wsHttpBinding>
   <binding name="WCFSecurityExample">
      <security mode="TransportWithMessageCredential"/>
   </binding>
</wsHttpBinding>
```

- **Both** - This security mode comprises of both transport security and message security to offer a robust security cover, but often results in overloading the overall performance. This one is supported by only MSMQ.

```

<netMsmqBinding>
   <binding name="WCFSecurityExample">
      <security mode="Both"/>
   </binding>
</netMsmqBinding>
```

All WCF bindings except BasicHttpBinding have some extent of transfer security by default.

## Message Security Level

Message level security is not dependent on WCF protocols. It is employed with message data itself by encrypting the data by using a standard algorithm. A number of client credentials are available for different bindings for the message security level and these are discussed below.

### Client credentials for message level security in WCF

**None** : Here, encryption is used to secure the message, whereas no client authentication is performed which means that the service can be accessed by an anonymous client. Except for BasicHttpBinding, all WCF bindings support this client credential. However it should be noted that for NetNamedPipeBinding, this client credential is not available at all.

- **Windows** - Here, both message encryption and client authentication take place for a real-time logged-in user. In this case too, unlike all other WCF bindings, NetNamedPipeBinding is not available and BasicHttpBinding does not lend its support.

- **UserName** - Here, messages are encrypted as well as secured by offering a UserName, and clients are authenticated as they need to offer a password. BasicHttpBinding just like the above two client credentials, does not support UserName and it is not available for NetNamedPipeBinding.

- **Certificate** - Along with message encryption, both the client and the service get an authentication with certificate. This client credential is available and is supported by all WCF bindings except NetNamedPipeBinding.

- **IssuedToken** - Issued Tokens from an authority like Cardspace are used to authenticate the messages. Encryption of messages are also performed here.

The following code shows how client credentials are configured in the WCF message security level/mode.

```
<netTcpBinding>
   <binding name="WCFMessageSecurityExample">
      <security mode="Message">
         <message clientCredentialType="None"/>
      </security>
   </binding>
</netTcpBinding>

<netMsmqBinding>...</netMsmqBinding>
</bindings>
<behaviors>...</behaviors>
```

Here, it must be noted that the transport security mode has an edge over the message security level, as the former is faster. It does not require any additional coding and offers interoperability support, and thus does not reduce the overall performance.

However, from security point of view, the message security mode is more robust and is independent of protocols and offers end-to end security.