[1. 验证和授权试图解决的问题 1](#_Toc463626053)

[2. WCF 部署环境 1](#_Toc463626054)

[2.1. Internal Self-Hosted Services. 1](#_Toc463626055)

[2.2. Internal Web-Hosted Services. 1](#_Toc463626056)

[2.3. Public Web-Hosted Services. 1](#_Toc463626057)

[3. 安全传输其实就是对XML 消息的加密处理 1](#_Toc463626058)

[4. Authenticate and Identify 1](#_Toc463626059)

[4.1. 验证和辨识是双方向的 1](#_Toc463626060)

[4.2. Authenticate（验证）通过Identify（辨识）来实现 2](#_Toc463626061)

[4.3. 辨识通过证书来实现 2](#_Toc463626062)

[4.3-1. transport level security 支持五种credentials 类型 2](#_Toc463626063)

[4.3-2. message level security 支持五种credentials 类型 2](#_Toc463626064)

[5. Message transfer security 3](#_Toc463626065)

[5.1. Two Mechanisms 3](#_Toc463626066)

[5.1-1. Transport Security 3](#_Toc463626067)

[5.1-2. Message Security 3](#_Toc463626068)

[5.2. Six security modes 4](#_Toc463626069)

[5.3. Binding and Security Modes 4](#_Toc463626070)

[5.3-1. Default security Mode for bingding 4](#_Toc463626071)

[5.3-2. Supported security mode for binding 5](#_Toc463626072)

[6. Authorize Clients 5](#_Toc463626073)

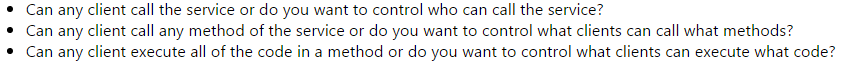
[6.1. 支持三种基本的授权模式 5](#_Toc463626074)

[6.1-1. Role-based. 5](#_Toc463626075)

[6.1-2. Identity based. 5](#_Toc463626076)

[6.1-3. Resource based. 5](#_Toc463626077)

# 验证和授权试图解决的问题



# WCF 部署环境

## Internal Self-Hosted Services.

You are self-hosting a WCF service on the corporate network. You want anyone who can log onto the network to be able to access the service. You want only certain users to be able to call particular methods.

## Internal Web-Hosted Services.

You are hosting a WCF service using Internet Information Services on the corporate intranet. Both employees and guests have access to the wireless network. You want only employees to be able to call the service. You want only certain users to be able to call particular methods.

## Public Web-Hosted Services.

You are hosting a WCF service publicly on the Internet. You want to limit access to the service to users with a valid user name and password. You want only certain users to be able to call particular methods.

# 安全传输其实就是对XML 消息的加密处理

When client applications and WCF services communicate, they do so by passing XML messages

# Authenticate and Identify

## 验证和辨识是双方向的

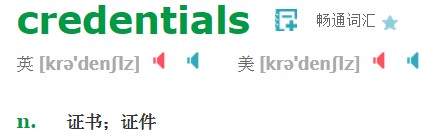
service端要验证client 端，client端同样也要验证service端

To authorize, you first need to authenticate. To do that, you must be able to identify clients. Clients can identify themselves by providing evidence such as a Windows account，a user name / password or a certificate.

Clients must also know that they are calling the service they intend to call. Services can identify themselves by providing a certificate.

## Authenticate（验证）通过Identify（辨识）来实现

Authentication enables you to identify clients and services. They identify themselves by passing credentials. 辨识通过传送证书来实现。



## 辨识通过证书来实现

### transport level security 支持五种credentials 类型

* **Windows**. The client uses a Windows token representing the logged in user’s Windows identity. The service uses the credentials of the process identity or an SSL certificate.
* **Basic**. The client passes a user name and password to the service. Typically, the user will enter the user name and password in a login dialog box. The service uses a SSL certificate. This option is available only with HTTP protocols.
* **Certificate**. The client uses an X.509 certificate and the service uses either that certificate or an SSL certificate.
* **NTLM**. The service validates the client using a challenge/response scheme against Windows accounts. The service uses a SSL certificate. This option is available only with HTTP protocols.
* **None**. The service does not validate the client.



### message level security 支持五种credentials 类型

* **Windows**. The client uses a Windows token representing the logged in user’s Windows identity. The service uses the credentials of the process identity or an SSL certificate.
* **UserName**. The client passes a user name and password to the service. Typically, the user will enter the user name and password in a login dialog box. The service can validate the user name and password using a Windows account or the ASP.NET membership provider.
* **Certificate**. The client uses an X.509 certificate and the service uses either that certificate or an SSL certificate.
* **IssueToken**. The client and service use the Secure Token Service, which issues tokens the client and service trust. Windows CardSpace uses the Secure Token Service.
* **None**. The service does not validate the client.

# Message transfer security

client and service communicate by exchanging XML messages. You may need to secure these messages as well. Protecting messages as they are transferred from client to server and back is known as transfer security.

## Two Mechanisms

WCF provides two mechanisms for transfer security: transport security and message security.

### Transport Security

If you use transport security, security occurs at the transport level. The packets sent “on the wire” include the caller’s credentials and the message. Both of which are encrypted using whatever mechanism the transport protocol uses. For example, if you use TCP, you will likely use Transport Layer Security (TLS) and if you use HTTPS, you will likely use Secure Sockets Layer (SSL).

* 优点

It is generally faster to encrypt and decrypt messages that use transport security and you can benefit from hardware acceleration to improve performance.

* 缺点

A downside to transport security is that messages are encrypted only from point to point. Suppose a client sends a message to a service. The client encrypts the message and the service decrypts it. If the service then forwards the message to another service, the service forwarding the message will not automatically encrypt it. This is not an issue with message security because the service will encrypt the message before passing it on to another service.

### Message Security

If you use message security, the caller’s credentials are included in the message and the message is encrypted using the WS-Security specification.

* 优点

更安全

* 缺点

A downside to message security is that it requires both clients and services to support the WS-Security specification. Transport security does not have this requirement and is therefore more interoperable.

## Six security modes

WCF supports the following six security modes:

* None. Messages are not secured.
* Transport. Messages are secured using transport security. You will use this in the sample applications that demonstrate the first two scenarios (internal self-hosted and Web-hosted services).
* Message. Messages are secured using message security. You will use this in the sample application that demonstrates the first scenario (internal self-hosted service).
* TransportWithMessageCredential. Message protection and authorization occur at the transport level and credentials are passed with the message. You will use this in the sample application that demonstrates the third scenario (public Web-hosted service).
* TransportCredentialOnly. Credentials are passed at the transport level but the message is not encrypted. This option is available only if you are using the BasicHttpBinding binding.
* Both. Messages are secured using both transport level and message level security. This is supported only if you are using Microsoft Message Queue Server.

## Binding and Security Modes

### Default security Mode for bingding

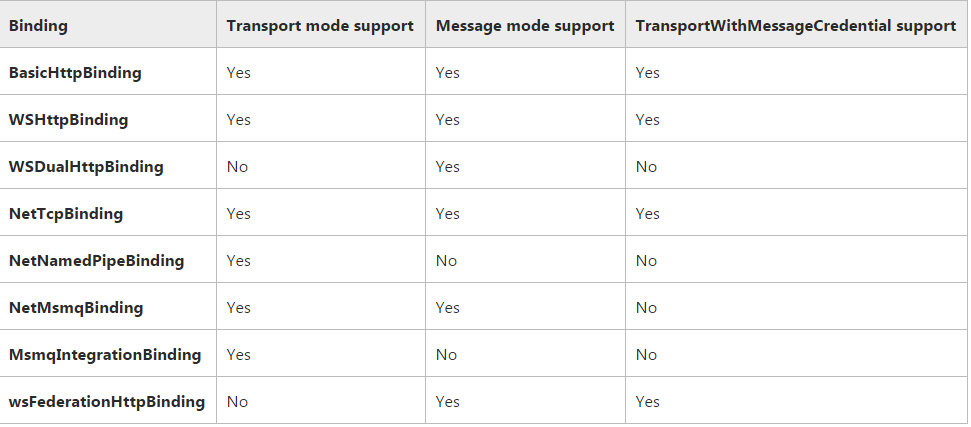
Each binding has a default set of security settings, You can modify the settings by modifying properties of the binding and by specifying service behaviors

By default, the following bindings use message security: WSHttpBinding, WS2007HttpBinding, WSDualHttpBinding, WSFederationBinding and WS2007FederationBinding.

By default, the following bindings use transport security: NetTcpBinding, NetNamedPipesBinding, NetMsmqBinding, NePeerBinding and MsmqIntegrationBinding.

By default, the BasicHttpBinding binding uses None as its security mode. In other words, message sent using that binding are not secure. This enables interoperability with ASMX Web services.

### Supported security mode for binding



# Authorize Clients

Authorization enables you to determine what operations authenticated clients can access. WCF supports three basic approaches to authorization:

## 支持三种基本的授权模式

### Role-based.

Access to a service and to operations of the service is based on the user’s role.

有三种方法确定用户的role

* Windows groups. You can use the built-in Windows groups such as Administrators or Power Users or create your own Windows groups.
* Custom roles. You can create roles that are specific to your application, such as Manager, Employee, Administrator, etc.
* ASP.NET role management. You can use the ASP.NET role provider and use roles you have defined for a Web site.

### Identity based.

Access is based on claims made within the user’s credentials. This is an extension to role-based authorization and provides a more fine grained approach. This approach will typically be used with issue token authentication.

### Resource based.

Resources, such as WCF services, are secured using Windows Access Control Lists (ACLs).