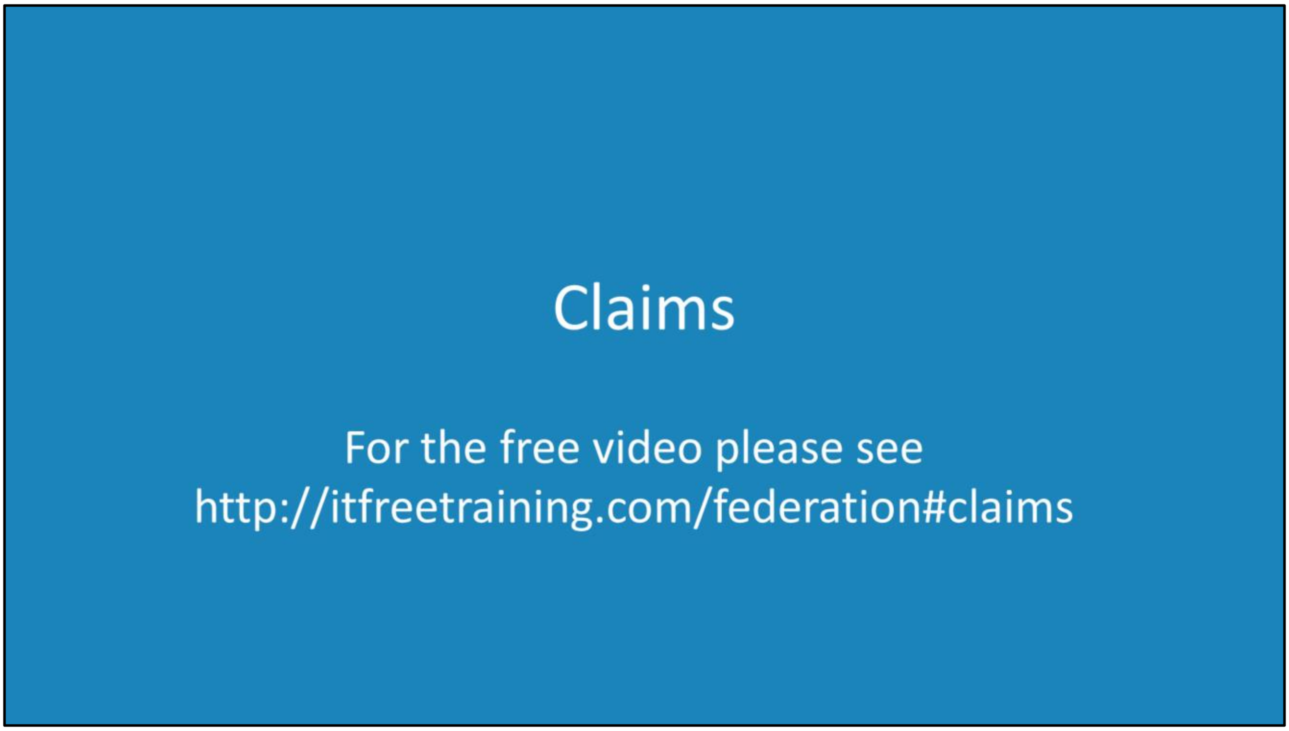
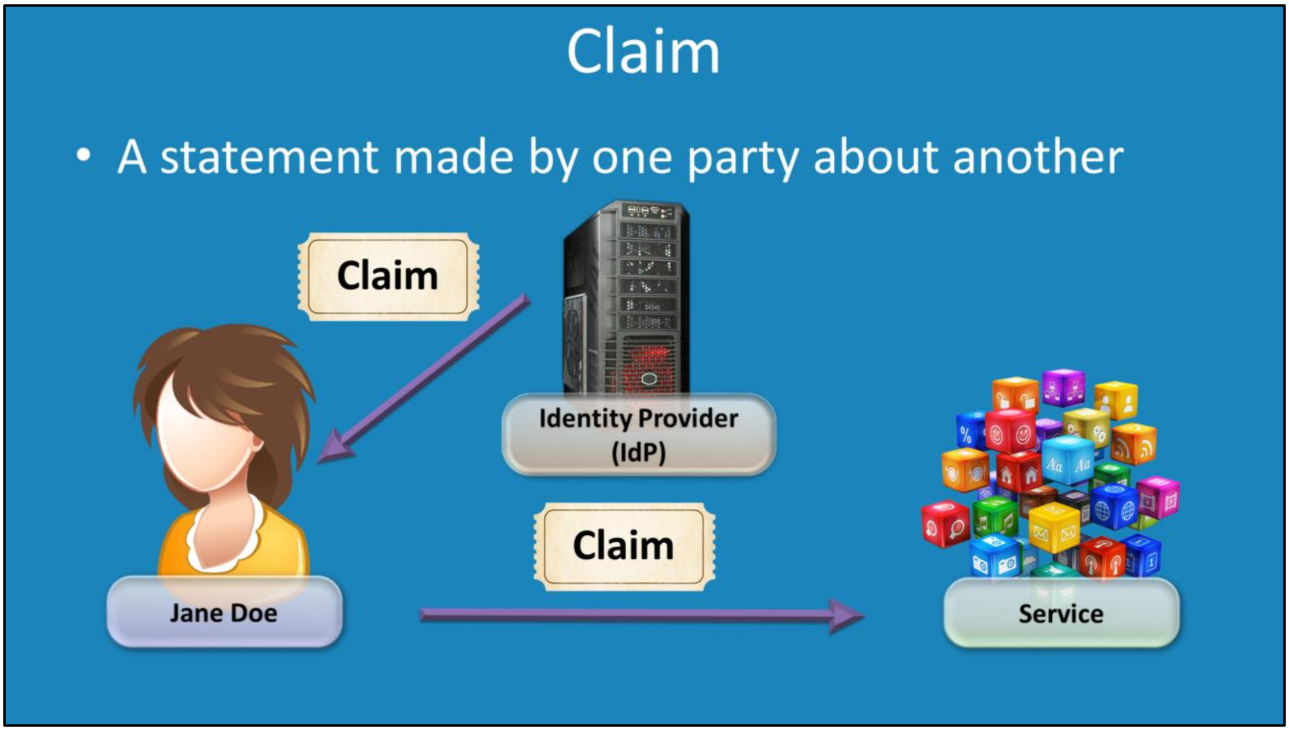


Claims

For the free video please see
http://itfreetraining.com/federation#claims

This video from ITFreeTraining will look at claims that are used with Federation Services. By the end of the video you will understand what are claims and what protocols are used with claims.



Claim

- A statement made by one party about another

Claims
A claim essentially is a statement made by one party about another party. This is provided by an Identity Provider. Services like Facebook are able to create a claim about a user which holds some information about the user. For example, the user can then use their Facebook login to access other sites. Let’s consider an example of a shopping center that allows free parking for those people that have travelled a long distance to shop there. In order to get their free parking, all they need to do is show their driver’s license which has their address on it. The identity provider in this case would be the institution that issues driver’s licenses. The user would be the person wanting free parking. The service would be the shopping center who has made the decision to allow free parking for people outside the area.

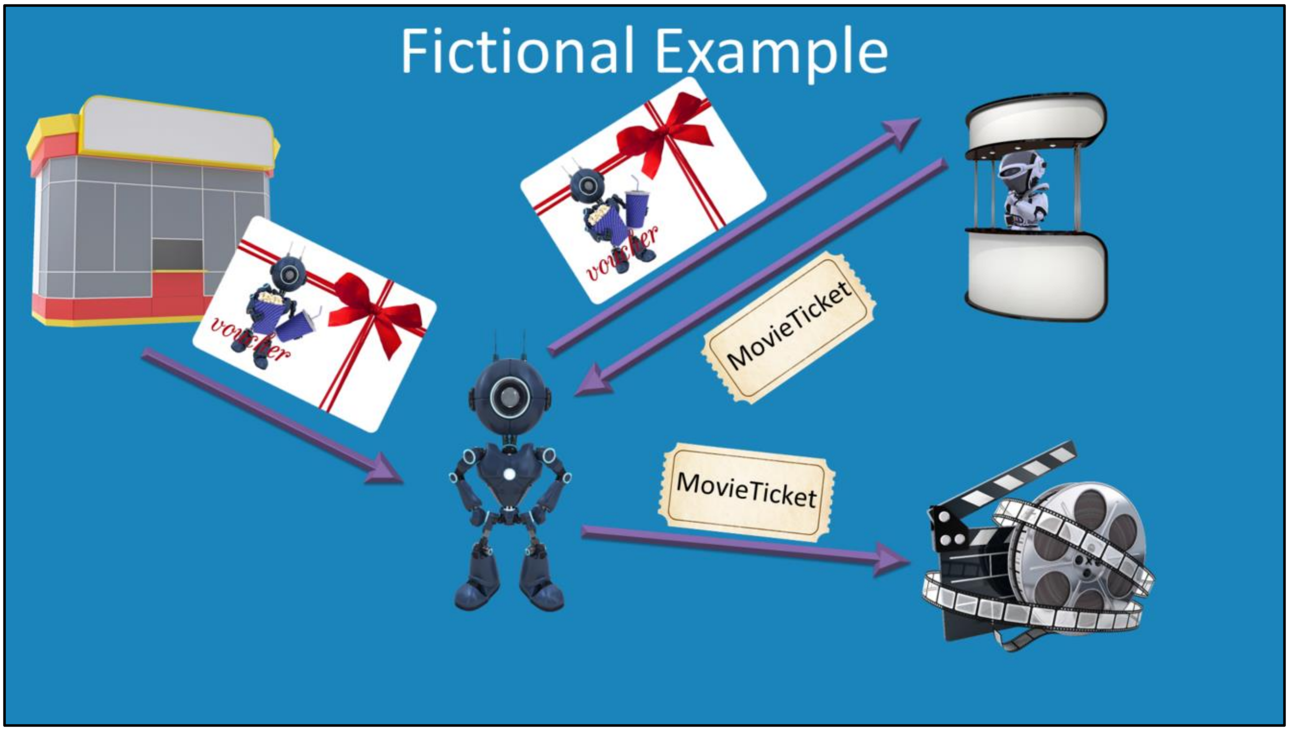
Security Token

- Claims are placed in a security token

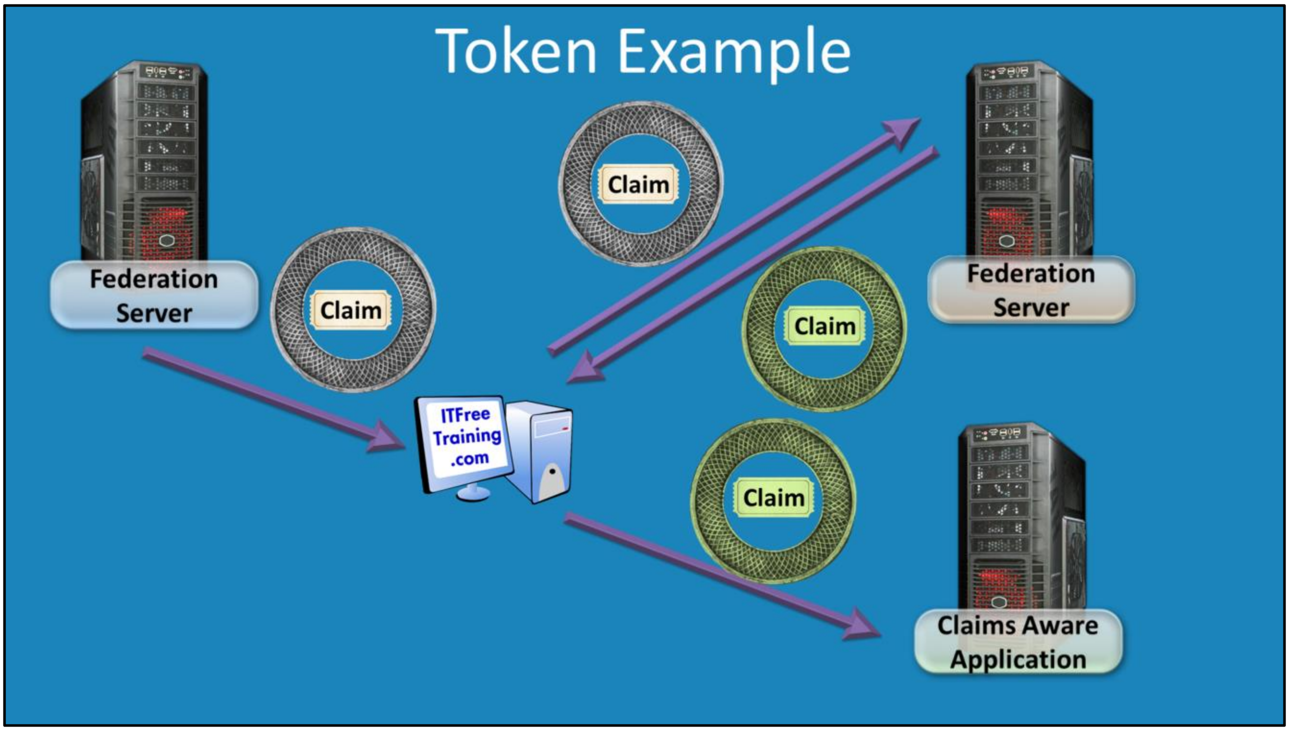
Security Token

Claims are generally packaged inside a security token. This allows the details of the claim to be checked to ensure they have not been changed. When working with Federation Services you may hear the term security token and claim used interchangeable. Essentially they are referring to the claim which may be packaged in a security token.

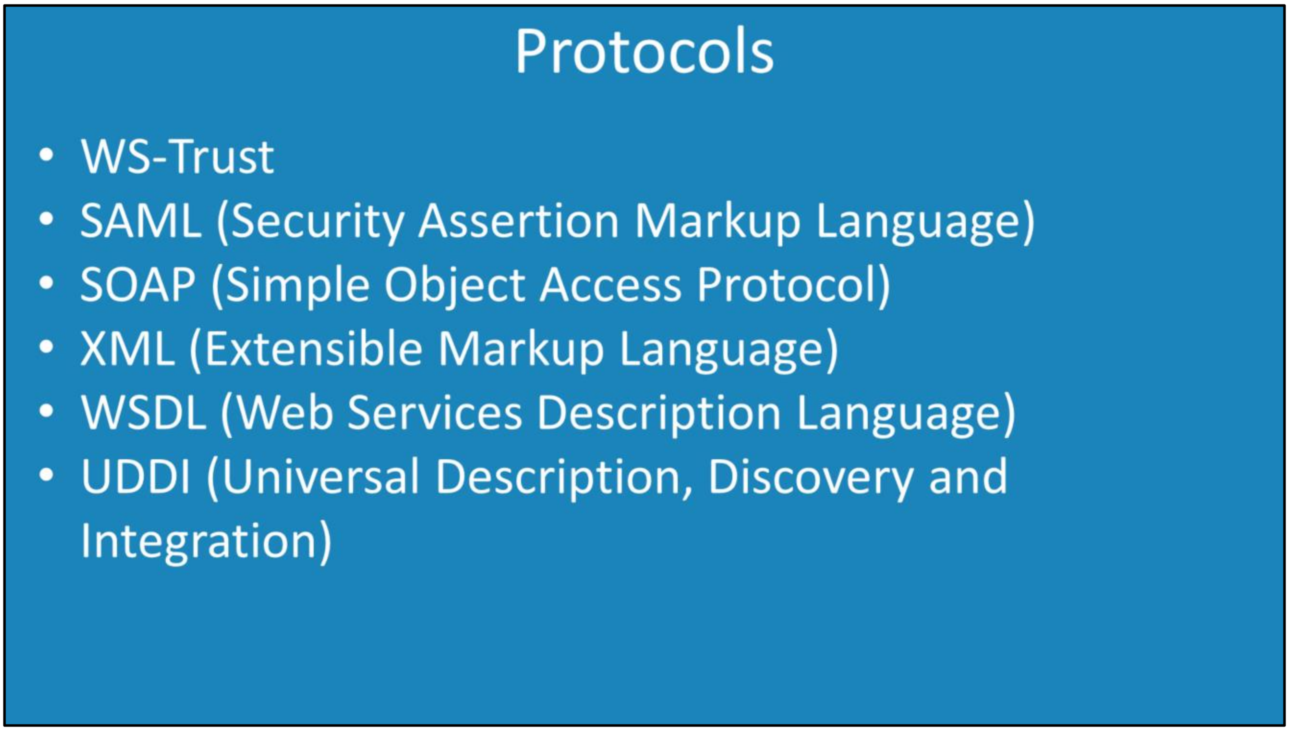
Fictional Example



Fictional Example
In this example, a person is given a voucher to a cinema in order to obtain a movie ticket. The movie ticket can then be used to enter a cinema to see a movie. Federation Services often work in a simple way.



Token Example
In some cases you will hear wording to the effect that a server consumes claims. When Federation Services are setup like this, the following generally happens. The Federation Server will issue a claim to the user. The user will then give this claim to another Federation Server. Once this Federation Server is able to verify that claim is valid, the Federation Server will destroy the claim and create a new claim. The new claim is free to change the information in the old claim and add to it. For example, it may add which servers the user is allowed to access. This kind of information is subject to change and thus the original server creating this claim does not know this information when the first claim is created.

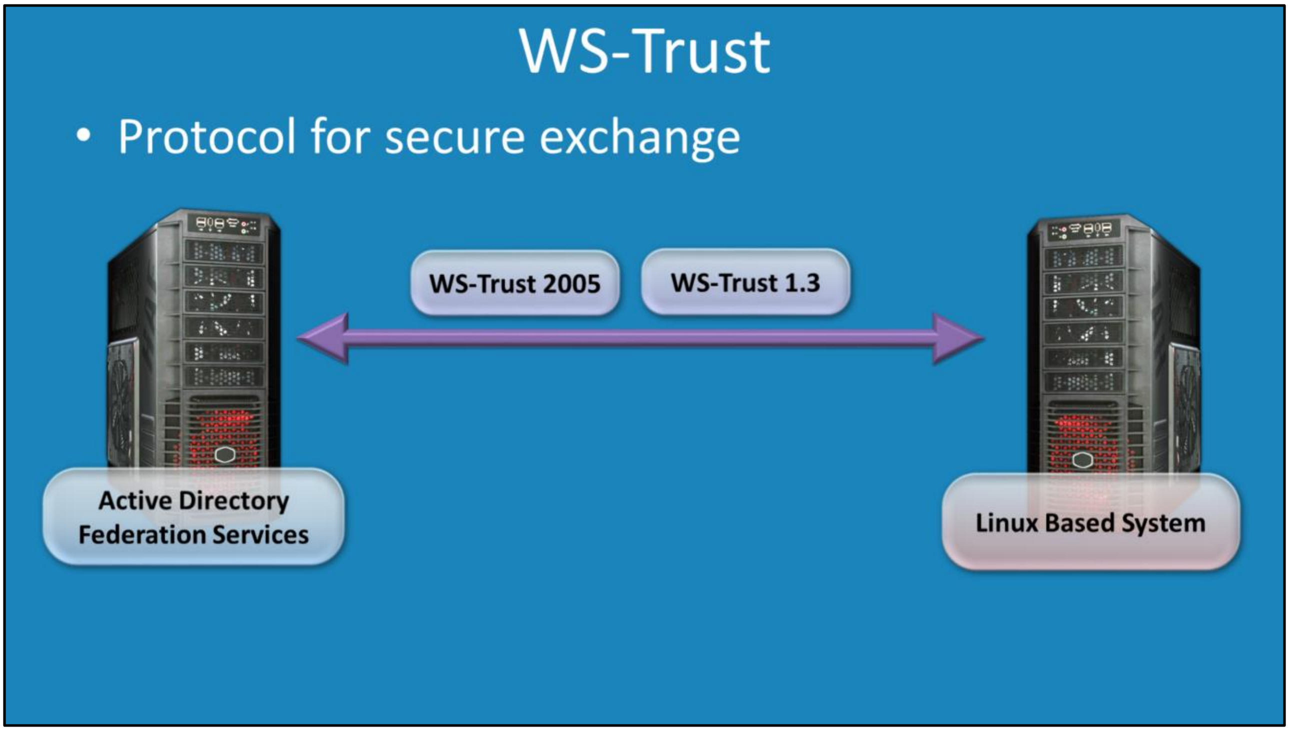


Protocols

- WS-Trust
- SAML (Security Assertion Markup Language)
- SOAP (Simple Object Access Protocol)
- XML (Extensible Markup Language)
- WSDL (Web Services Description Language)
- UDDI (Universal Description, Discovery and Integration)

Protocols

There are a lot of different protocols that make Federation Services work. Federation Services is also very customizable so even though there are some key protocols to make the system work, depending on how it is configured will determine which protocols will be used. For example, there are a number of different protocols that can be used to create a security token.



WS-Trust

- Protocol for secure exchange

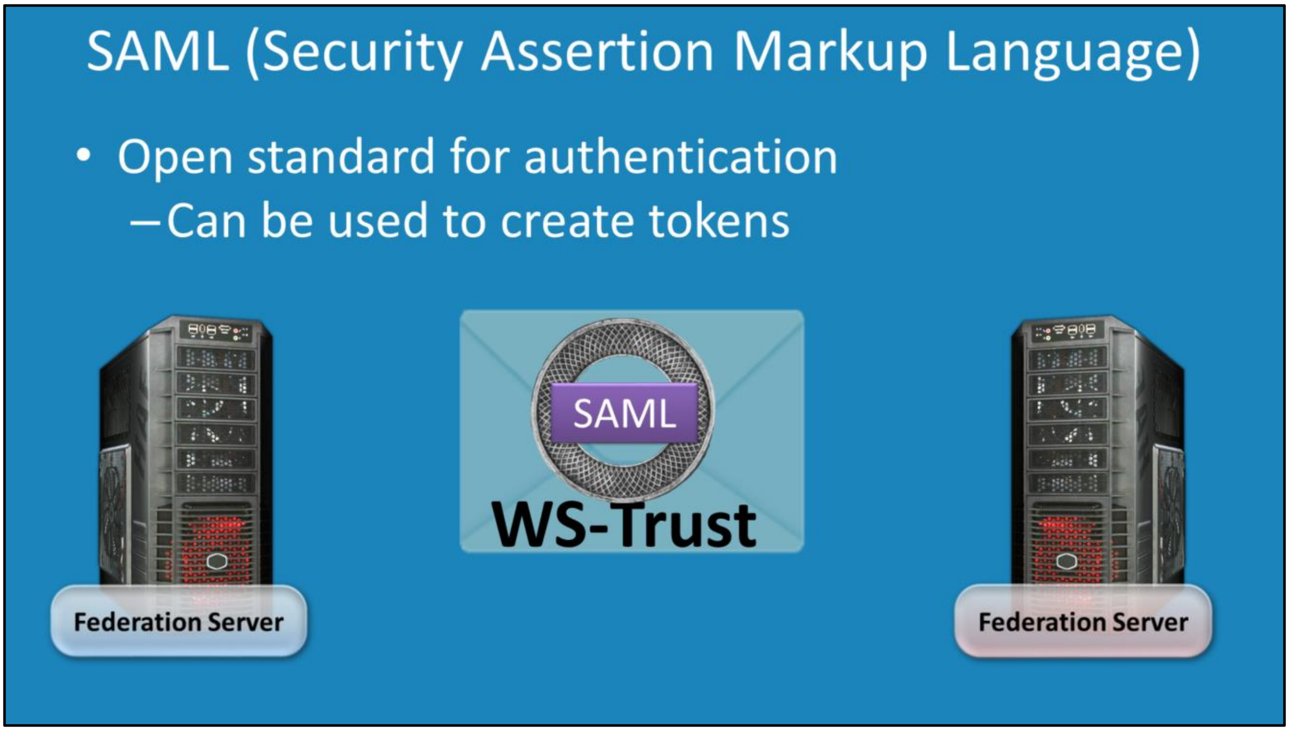
WS-Trust 2005

WS-Trust 1.3

Active Directory Federation Services

Linux Based System

WS-Trust
In order for Federation Services to exchange information between different Federation Services there needs to be a common protocol between the systems. The WS-Trust protocol is designed to allow the Federation Services to communicate with each other and exchange information like security tokens. There are a number of different versions of the protocol so it is a matter of making sure that both sides are using the same protocol.



SAML (Security Assertion Markup Language)

- Open standard for authentication
  - Can be used to create tokens

Federation Server

SAML

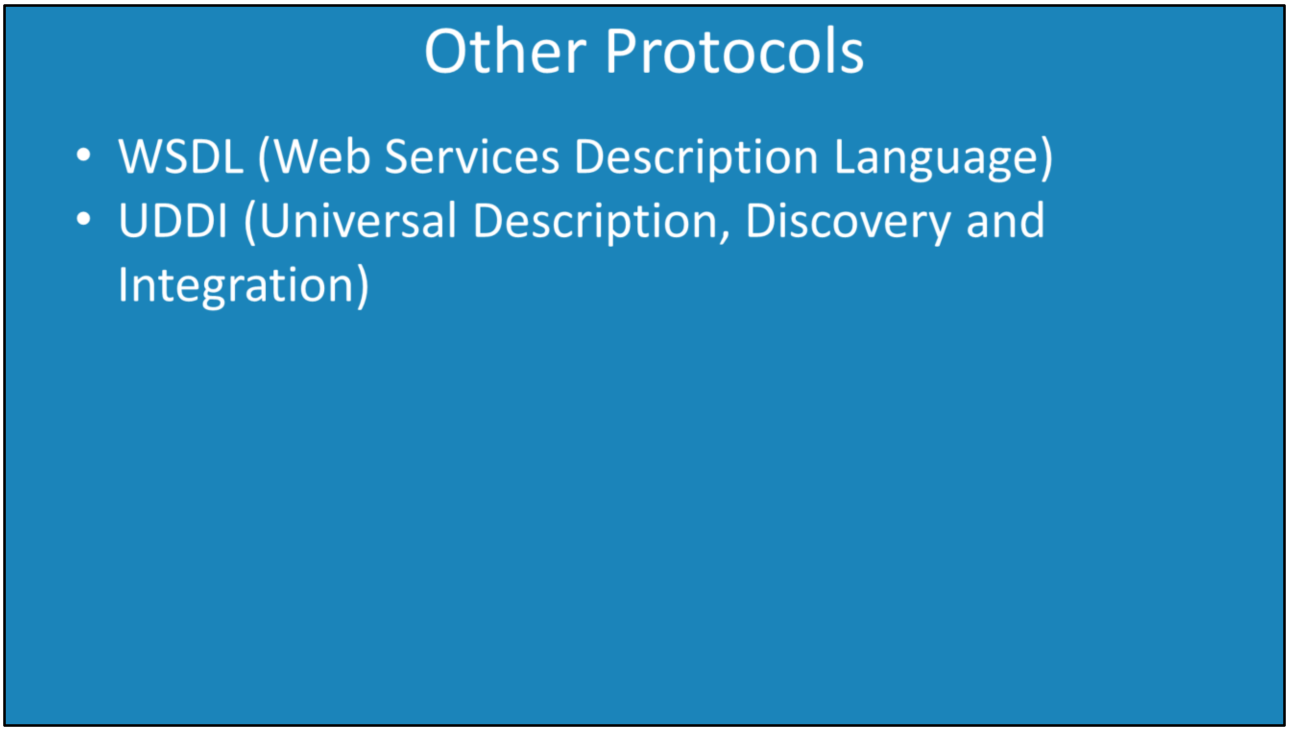
WS-Trust

Federation Server

SAML (Security Assertion Markup Language)
SAML is one of the protocols that can be used to create security tokens. It is an open standard for authentication but can be used to create tokens. Once the token is created, it is transported to the other server using WS-Trust. It is possible to use other protocols however this one is the most common. What the server will accept and not accept is referred to as an endpoint.

Endpoint
If you open AD FS Management on a server that has Active Directory Federation Services installed and configured, this will show all the different types of connections that server can accept. To access EndPoints, expand services and then open the container EndPoints. This container shows all the EndPoints this server will accept. For example, if you select one and it says the type is WS-Trust 2005 and authentication type is Certificate, this EndPoint will only accept WS-Trust 2005 connections that use certificates. In order to use this server with another Federation Server, both Federation Servers must have the same end point configured in order to allow communication to occur.

Configuration information about the server is also available under Metadata. If you need to access the configuration information for the server you only need to open this URL in a web browser. This information can be saved to a file and read on the other server if required. If this information is not available, it can be manually entered in on the other server.



Other Protocols

- WSDL (Web Services Description Language)
- UDDI (Universal Description, Discovery and Integration)

Other Protocols
There are a lot of protocols that make Federation Services. The Web Service Description Language (WSDL) and Universal Description Discovery and Integration (UDDI) are low level protocols that are used with Federation Services. For this reason you may not come across these protocols directly as they are used with other protocols.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
“Web Services Description Language” http://en.wikipedia.org/wiki/Web_Services_Description_Language
“WS-Trust and WS-Federation”
“WS-Trust” http://en.wikipedia.org/wiki/WS-Trust