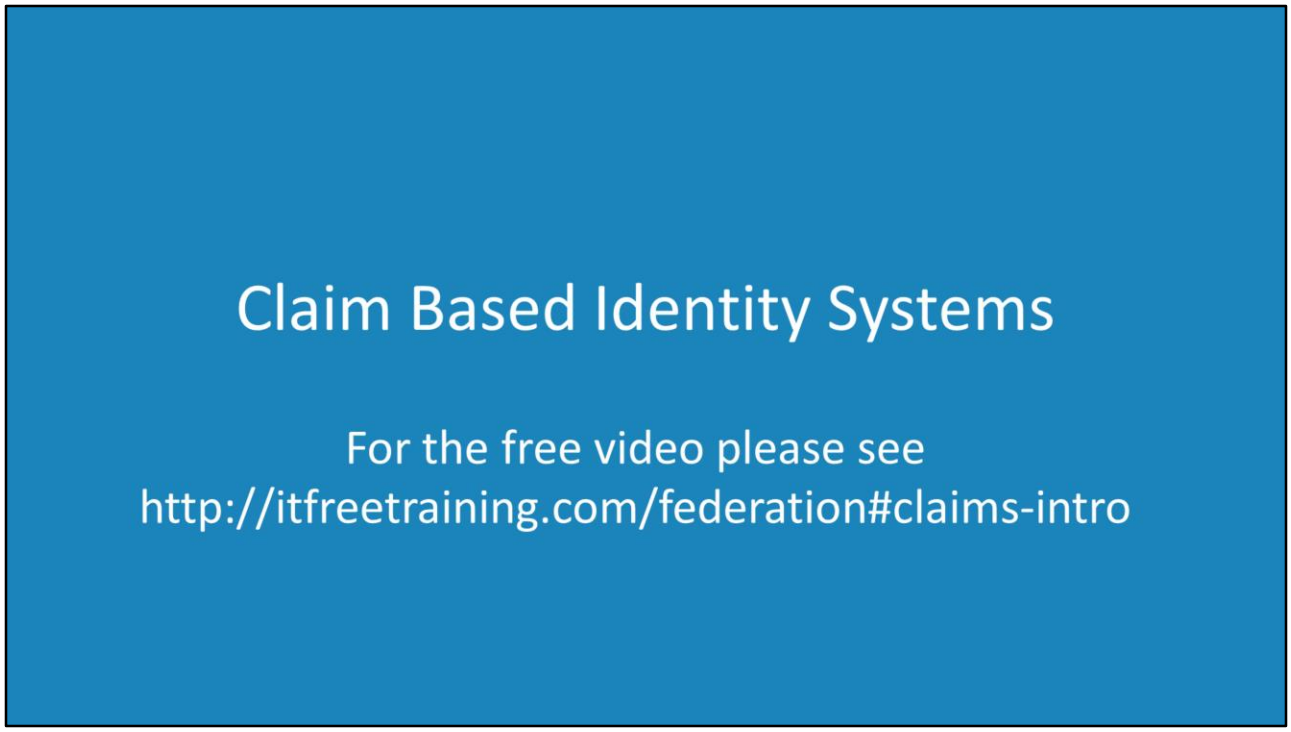
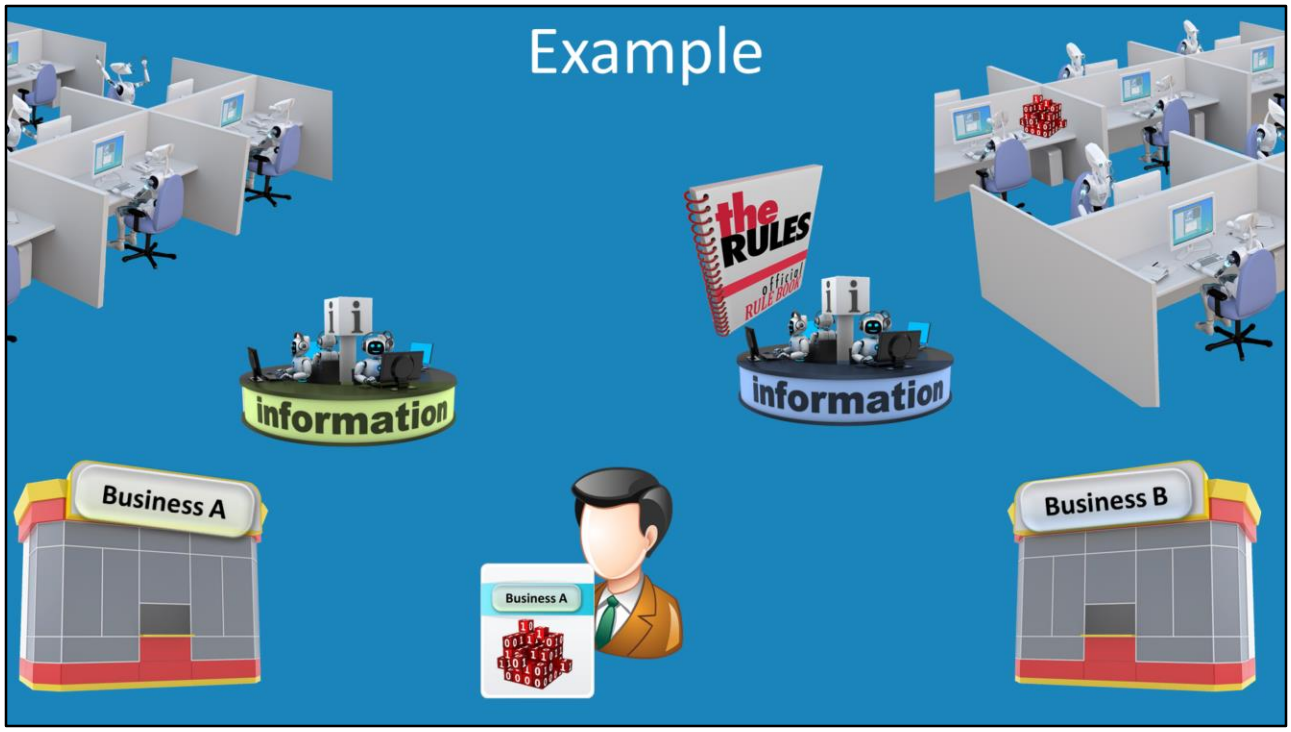
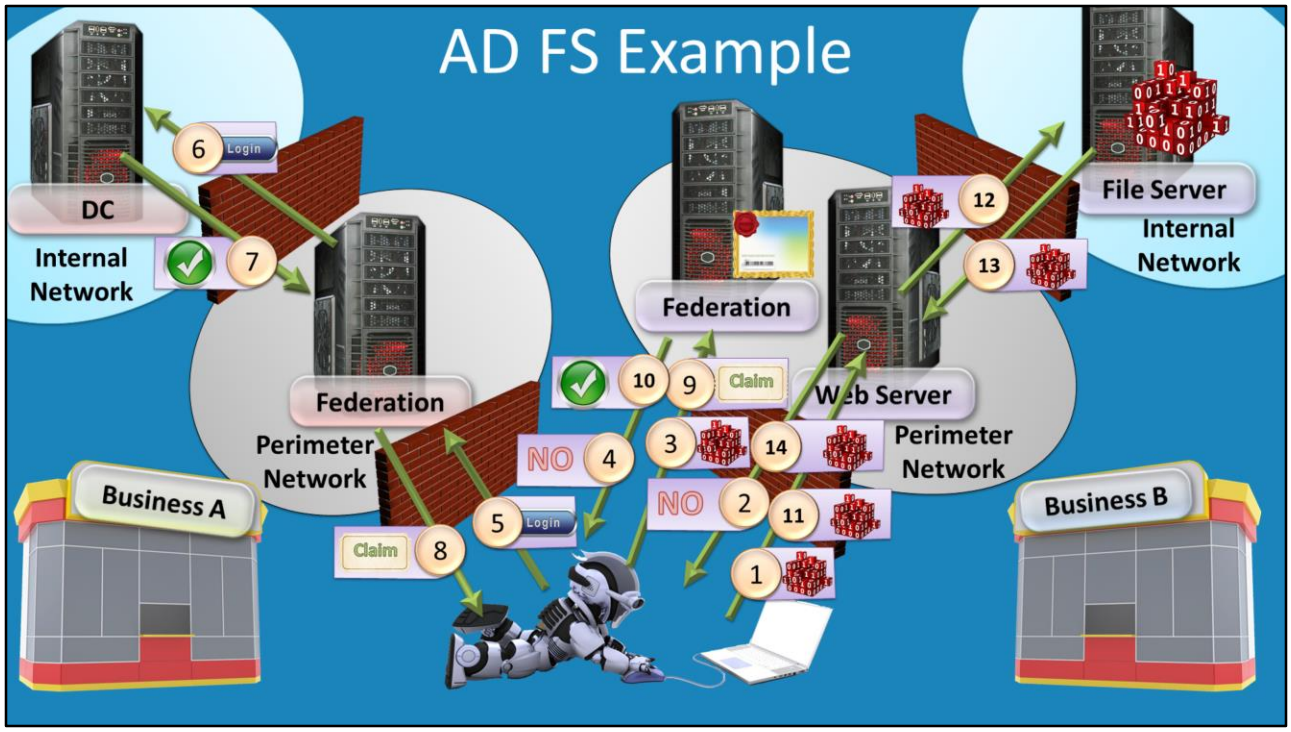


This video looks at Claim Based/Identity Based systems using Active Directory Federation Services as an example. An example of a claim based system is where the user logs into a system like a web page using another system, for example a Facebook login.



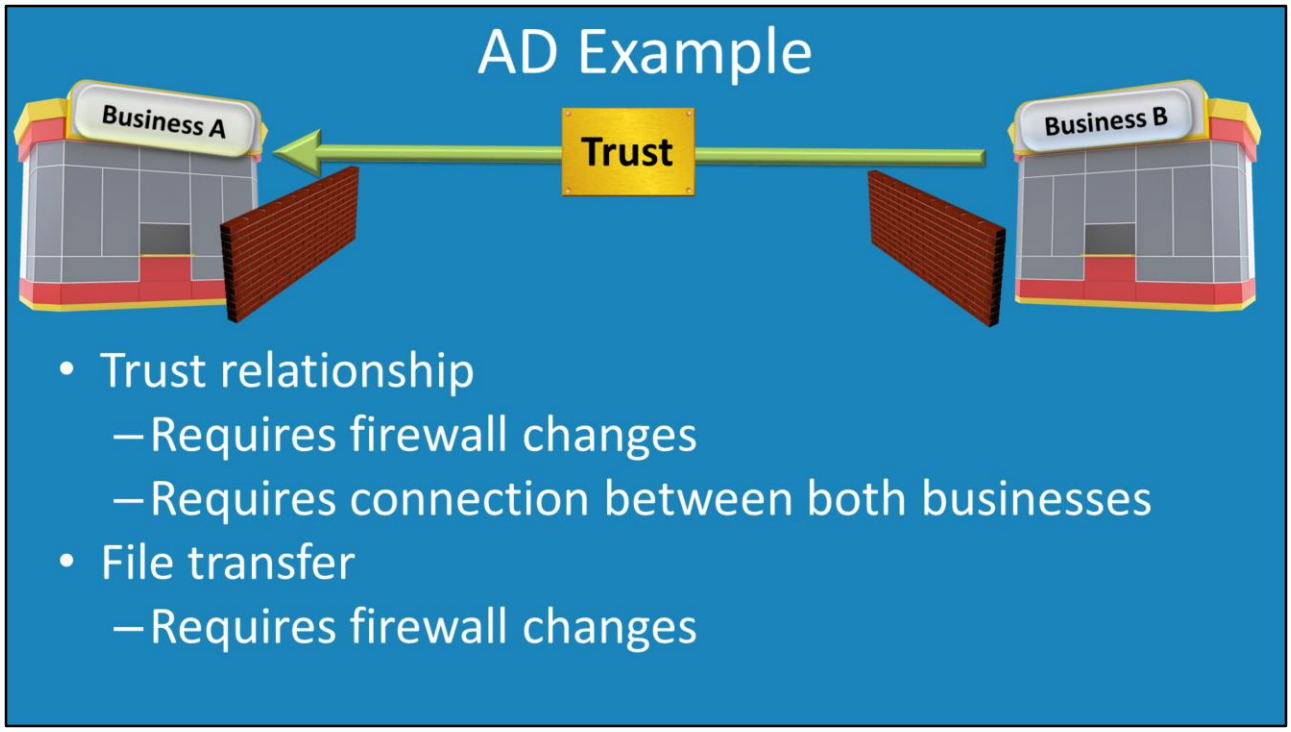
Example

In this fictional example, it shows the key points to a Federation Service. Federation Services work by a user wanting to access a system which belongs to a 3rd party. In order to do this, the first party needs to provide something the 3rd party can check to ensure the person is allowed access. It is still up to the 3rd party if they will allow them access or not. The point is that business B can check that the employee is a valid employee without having to contact business A to check.



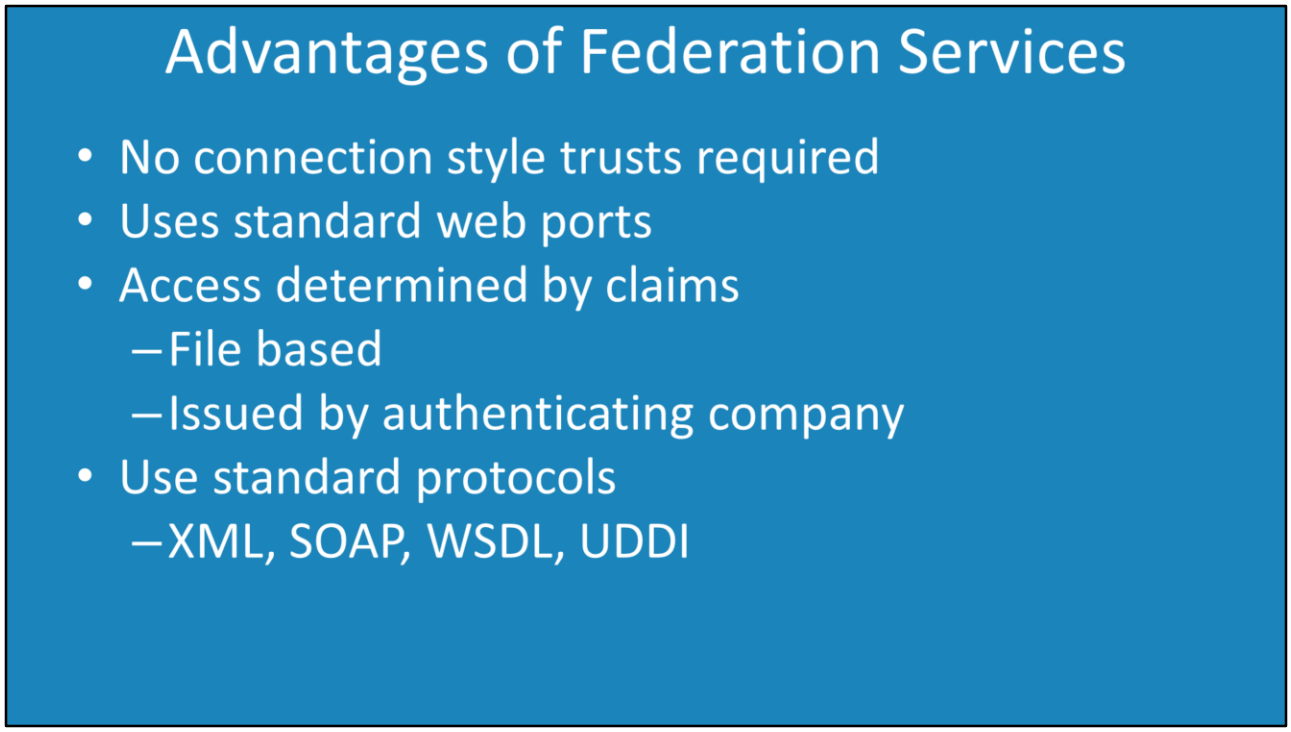
In this example, an Active Directory Federation Services model would work the following way.

1) The user contacts the web server in business B in order to obtain access to a service.
2) The web server rejects the request as the web server does not know who they are. The web server refers them to Federation Server in business B in order to get a claim in order to access the web server.
3) The user then contacts the Federation Server in the business B network.
4) The Federation Server does not know who the user is, so it says to get authorization first.
5) The user contacts the Federation Server in its DMZ and requests to be authenticated.
6) The Federation Server will pass the username and password the user provided to a Domain Controller.
7) The Domain Controller will respond back to the Federation Server that they have been authenticated.
8) The Federation Server will give the user a claim. This claim contains information indicating the user has been authenticated.
9) This claim is presented to the Federation Server in business B.
10) The Federation Server will accept the claim. Although not shown in this video, the Federation Server will often create a new claim that would be given to the user to grant them access services.
11) The user will use the claim with the web server.
12) The web server will accept the claim and connect to a file server.
13) The file server will give the information to the web server.
14) The web server will then present the information to the user.



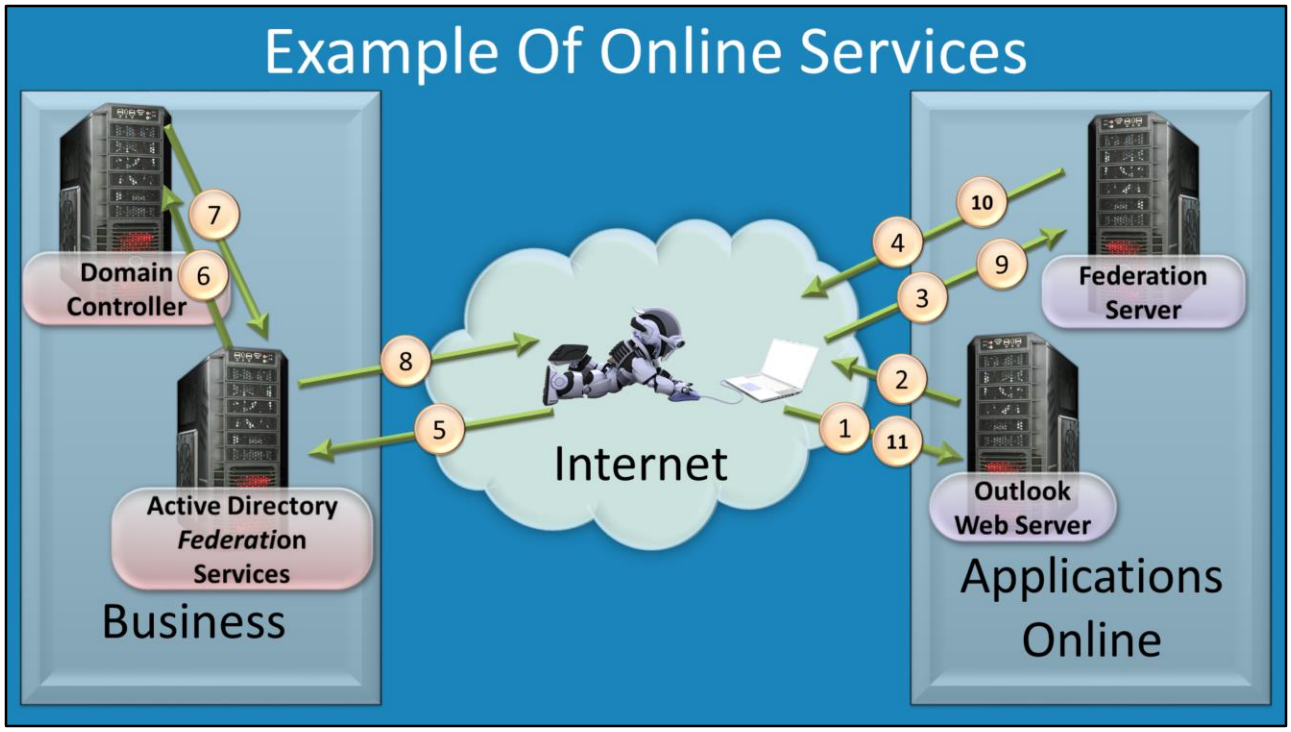
AD Example

In order to have authentication occur between two businesses using Active Directory, a trust relationship needs to be created between the two businesses. In order for this to occur, firewall changes need to made. An Active Directory trust is also connection based, which means a direct connection between the two businesses must also be present. If you want to allow services like file transfers you also need to make additional changes to the firewall. Companies often do not want to make changes to their firewall and do not want to establish direct permanent connections between different businesses.



Advantages of Federation Services

Federation Services does not require a connection style trust in order to work. It only requires a certificate to be exported and imported on the other side before the trust can be configured. Federation Services also uses standard HTTP and HTTPS protocols and thus these ports are most likely already open on the companies file firewall. Companies are more likely to agree to open these ports than open less commonly used ports. Federation Services uses standard protocols and thus can work with other systems. For example, a Windows based Federation Server can also work with a Linux based Federation Server.

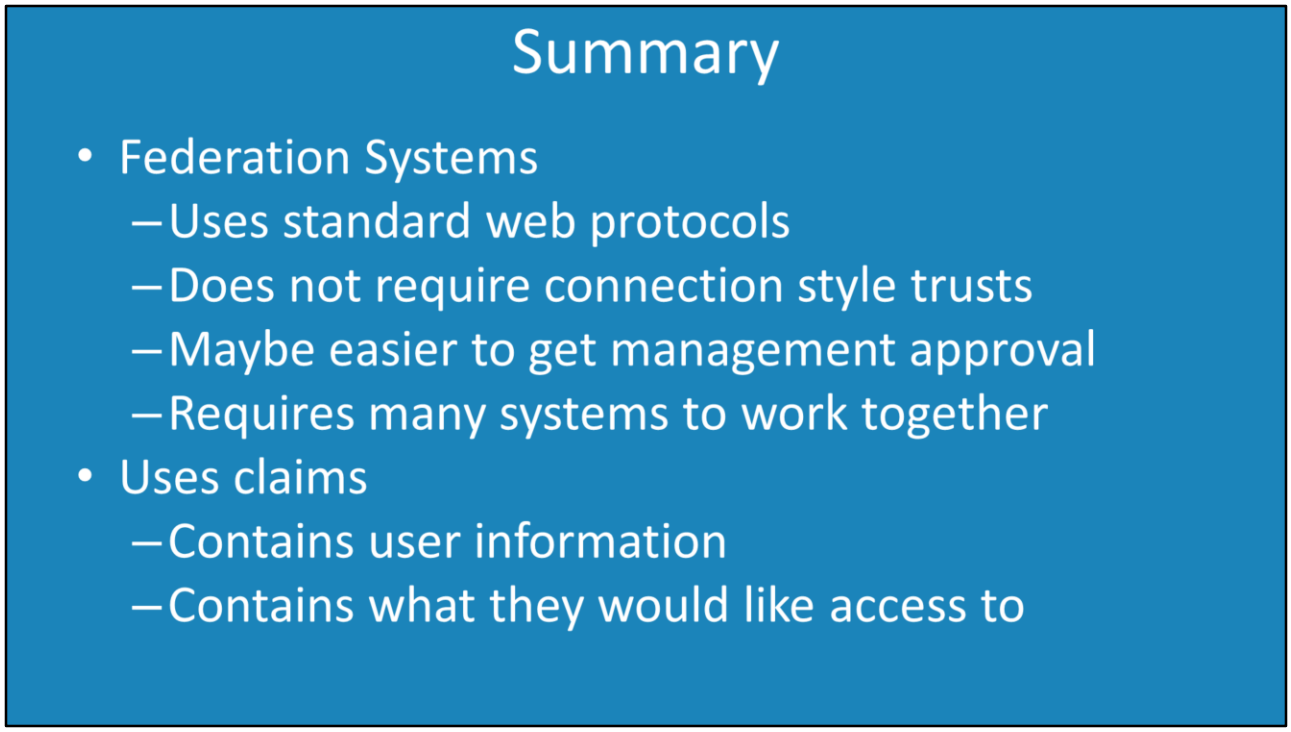


Example Of Online Services

In this example, a mobile user requires access to Exchange Services stored in the cloud using Microsoft Outlook as the client.

1) The user contacts the online Exchange Server in the cloud.
2) The server responds back that it needs a claim in order to access the service.
3) The user contacts that Federation Server.
4) The Federation Server responds back saying it will not issue a claim until they have been given a claim showing they are allow access.
5) The user contacts the Federation Service on their network with their username and password. Any authentication system could be used here. Even a system that only requires the user to present an e-mail address could be used.
6) The Federation Server contacts a Domain Controller to authenticate the user.
7) The Domain Controller responds back to the Federation Server that the user has been authenticated.
8) The Federation Server gives a claim to the user.
9) The user then gives the claim to a Federation Server.
10) The Federation Server accepts the claim and presents the user with another claim that the user can use with the online server to access the Exchange service.
11) The user then presents this claim to the online server and is now able to access the Exchange service in the cloud.

The point to remember with claim based systems is that authentication is provided by a system that is separate from the system that is providing access. This means that the first system can add and remove users as required and thus indirectly be responsible for who has access.



Summary
A Federation Service uses standard web protocols and does not require a connection style trust. For this reason these ports may already be open on the firewall and thus is generally easier to get management approval. Federation Services require many systems to work together and thus may not be that easy to get up and working. Microsoft cloud based systems are well documented. Other Federation Services solutions are not as well documented and thus may be harder to set up. Lastly a claim contains user information and what they would like access to. They use certificates to make sure the data is secure. In later videos claims will be covered in more detail.

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
"Active Directory Federation Services Overview" http://technet.microsoft.com/en-us/library/hh831502.aspx
"Federated identity" http://en.wikipedia.org/wiki/Federated_identity