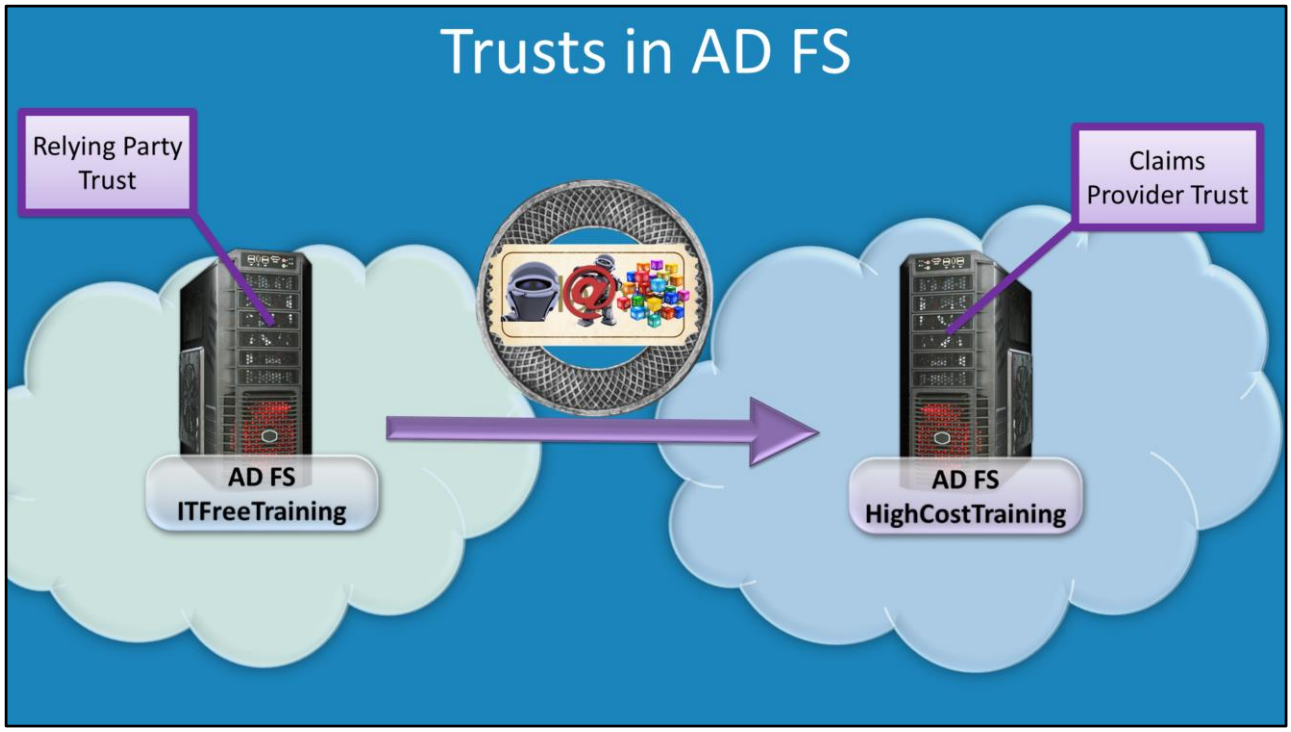
In Active Directory Federation Services there are two types of trusts. This video will look at the relying party trust which is configured on the account side. It essentially determines what information will be placed inside the claim.

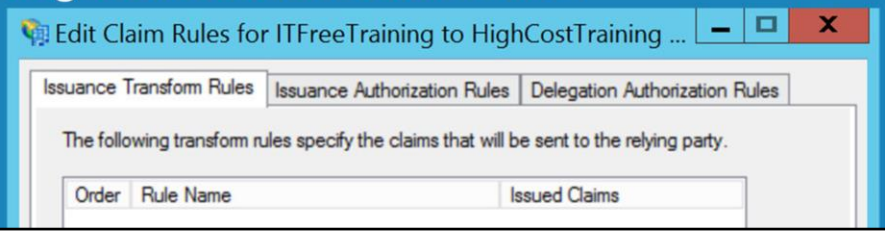


Trusts in AD FS

In this example ITFreeTraining has an Active Directory Federation Server and so does HighCost Training. On the ITFreeTraining side a relying party trust is created. The relying party trust is the configuration that is used to create a claim. It may seem that the relying party trust should be on the HighCost training side, however this is not possible. The reason for this is that ITFreeTraining creates a claim. Once this claim is created it cannot be changed. If the relying party trust was on the HighCost Training side, it would not be able to decide what data is in the claim as the claim would have already been created.

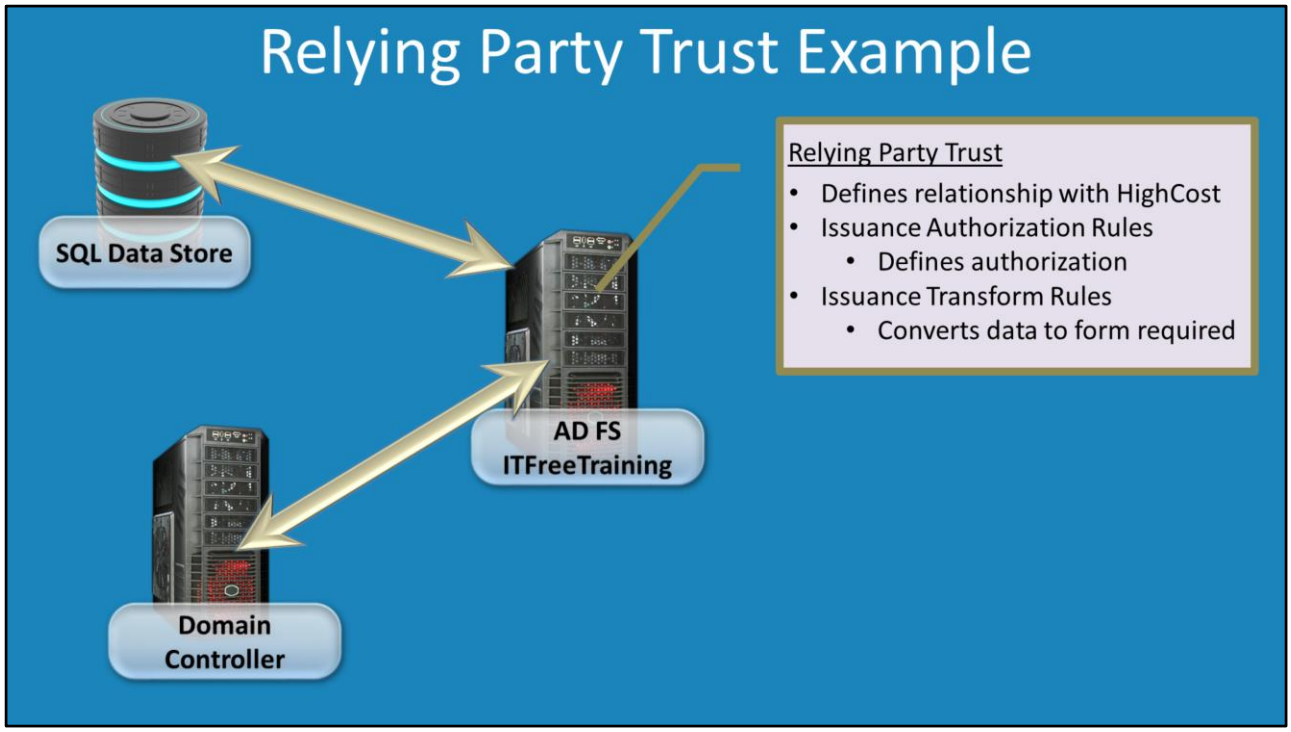
Relying Party Trust

- Defines the configuration used to create claims
  - Created in accounts partner organization
  - Federation Server to Claim Based Application
- Divided into 3 rule sets
  - Issuance Transform Rules
  - Issuance Authorization Rules
  - Delegation Authorization Rules



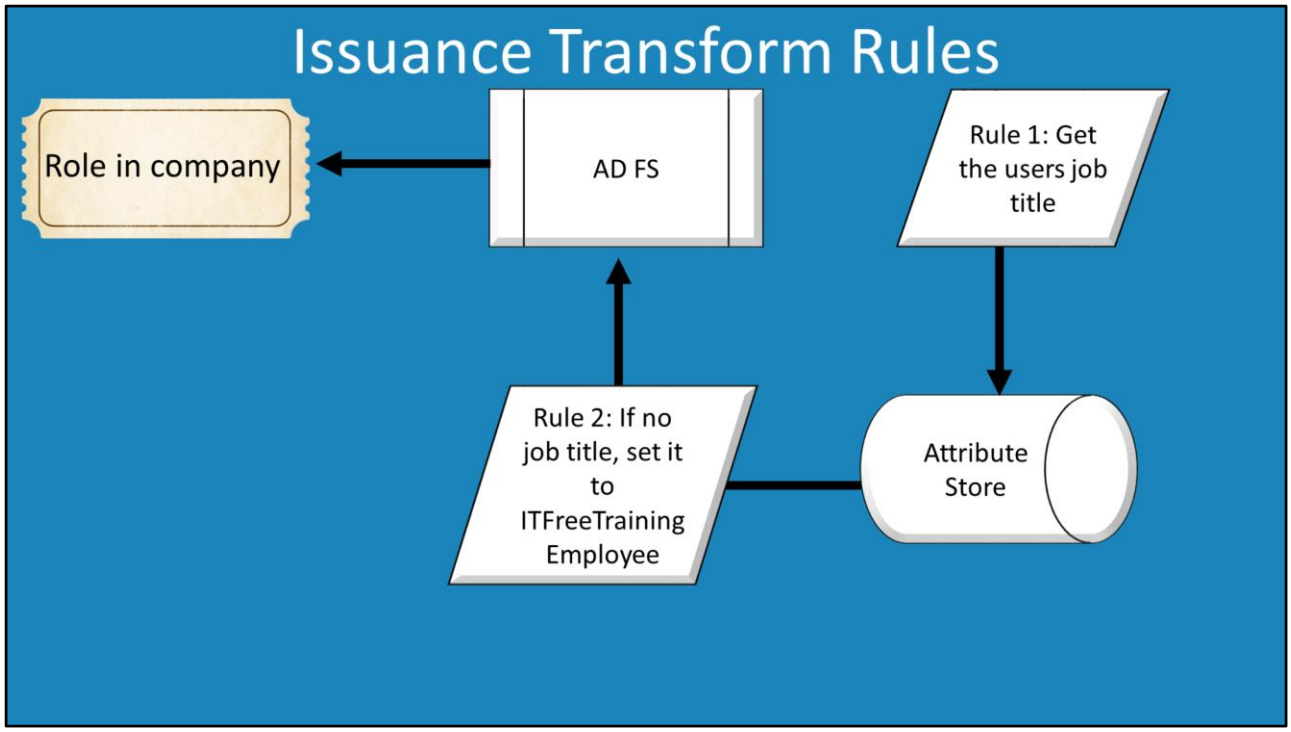
Relying Party Trust

A relying party trust is the configuration that is used in the accounts partner organization that is used to create claims. Normally it is used between the accounts partner and the resource partner but can also be used with a claims based application. When a relying party trust is created there are 3 rules that can be configured. These are, issuance transform rules, issuance authorization rules, and delegation authorization rules.



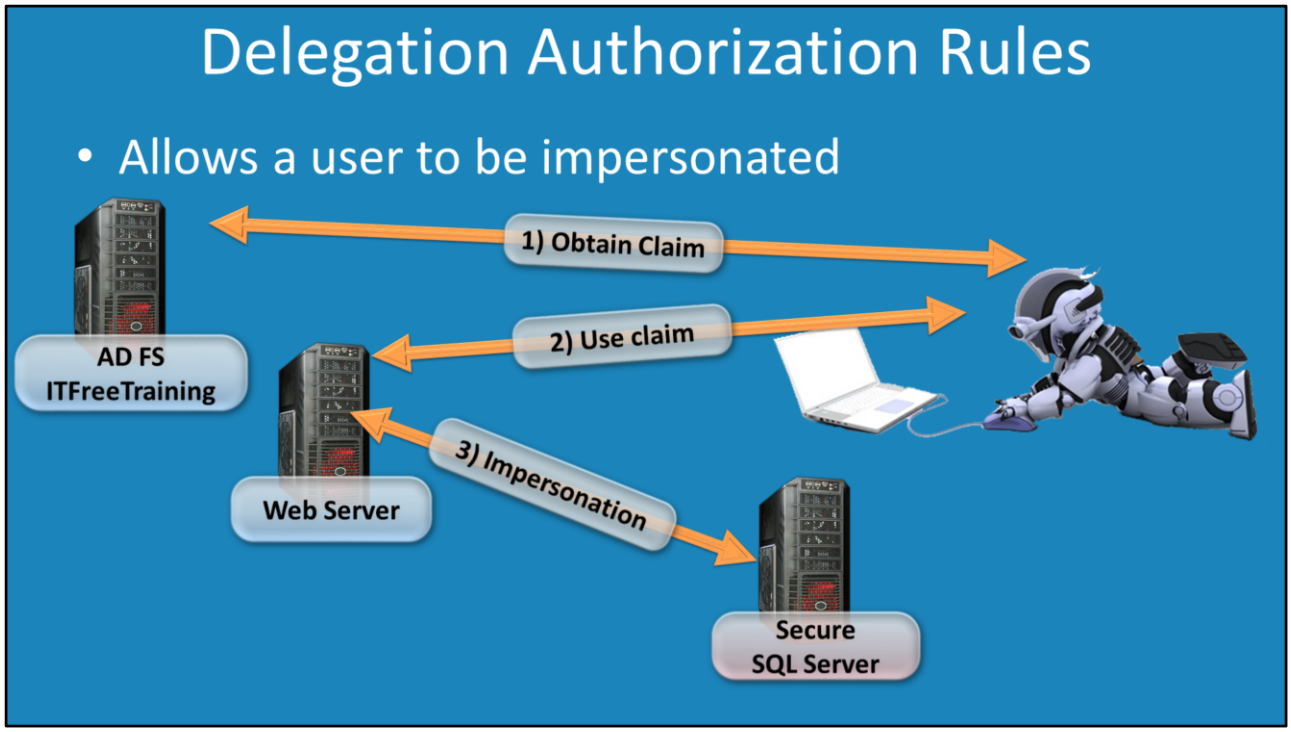
Relying Party Trust Example

In this example, an AD FS server is required to authenticate from a domain controller and obtain information from a SQL data store. When a claim is created, the AD FS federation server needs to be able determine where to get this data and which Domain Controller to authenticate with and how to output the data. In order to do this, 3 different types of rules are used. The issuance authorization rule determines how authentication will occur. In this case a domain controller is being used, however authentication could be as simple as the user having an e-mail address. Issuance transform rules define the data that is obtained and also define how it can be changed. For example, if the data obtained from the SQL Data Store was an e-mail address that ended in local, the transform rule may be defined to change this address to one ending in .com. Delegation authorization allows different users to be defined to access data. For example, delegation could be used for one user to obtain data for another user.



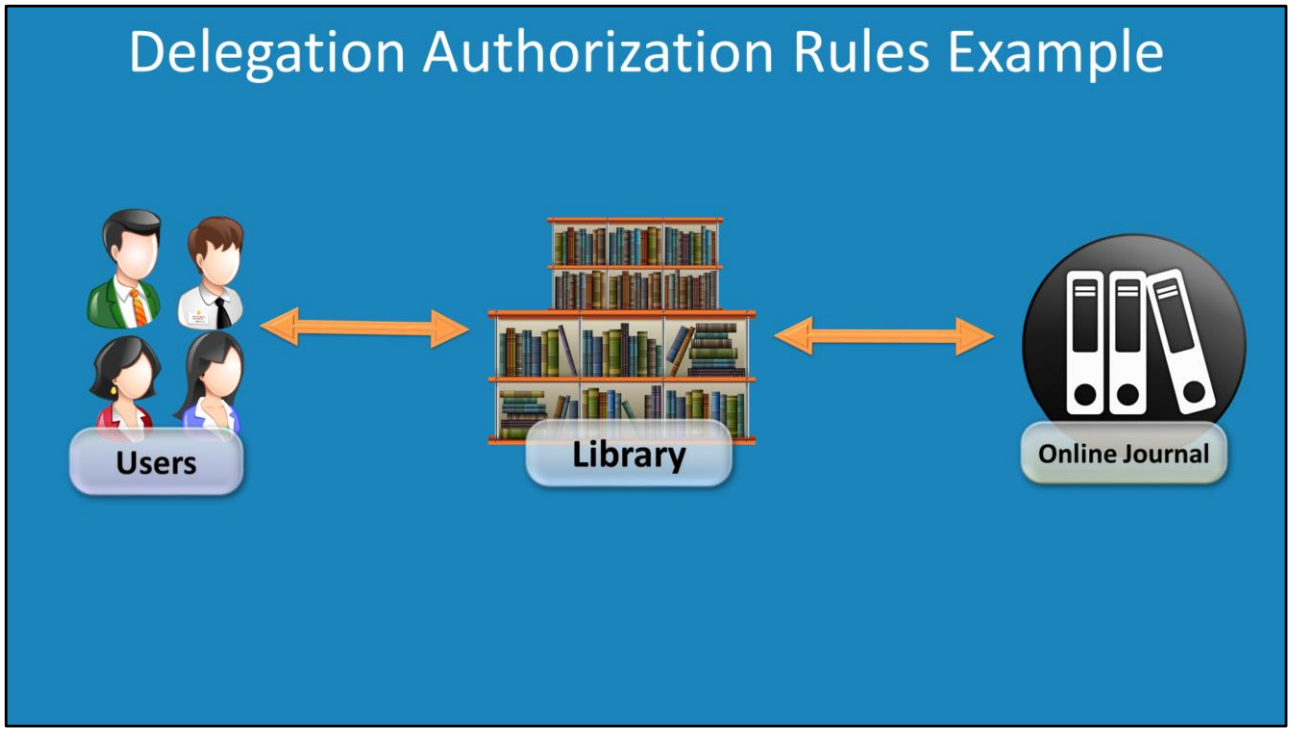
Issuance Transform Rules

In this example the job title is being added to the claim. A rule is created which defines that the job title should be obtained from an attribute store, most likely an SQL database. Once this data is obtained the job title is added to the claim. The problem is that some users do not have a job title and the claim cannot be used without a job title. The application that accepts this claim does not use the job title information in any way, however something needs to be configured, otherwise the claim will be rejected. To get around this, a second transform rule is created that configures the job title to “ITFreeTraining Employee” when no data is configured. This means that there will always be a value configured for the job title. You can see how transform rules can obtain and change data. Multiple rules can be stacked together in order to obtain the required result.

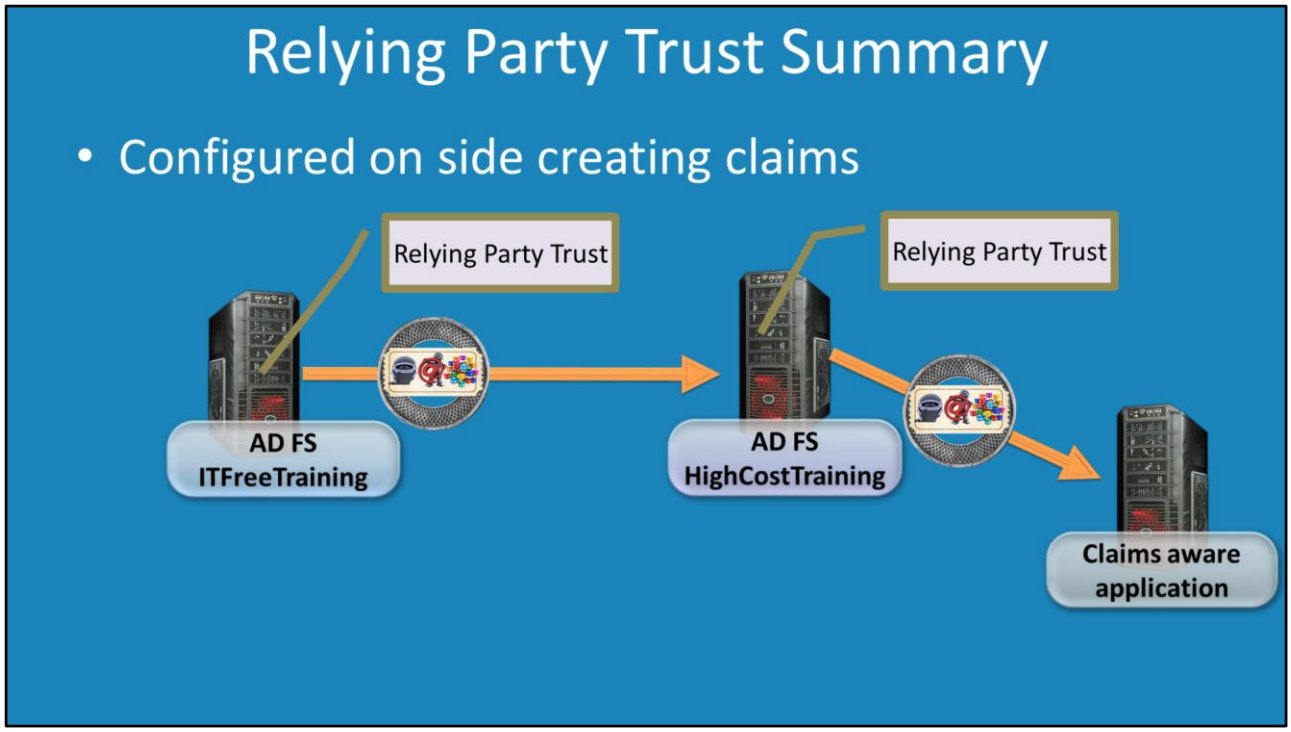


Delegation Authorization Rules

This rule essentially allows a user to be impersonated, that is, they are pretending to be someone else. In this example, the user obtains a claim from an AD FS server. They then use this claim to access a web server. The web server will then access a claim aware application using a different user name. So essentially they are performing the access as a different user than what was originally used in the claim.

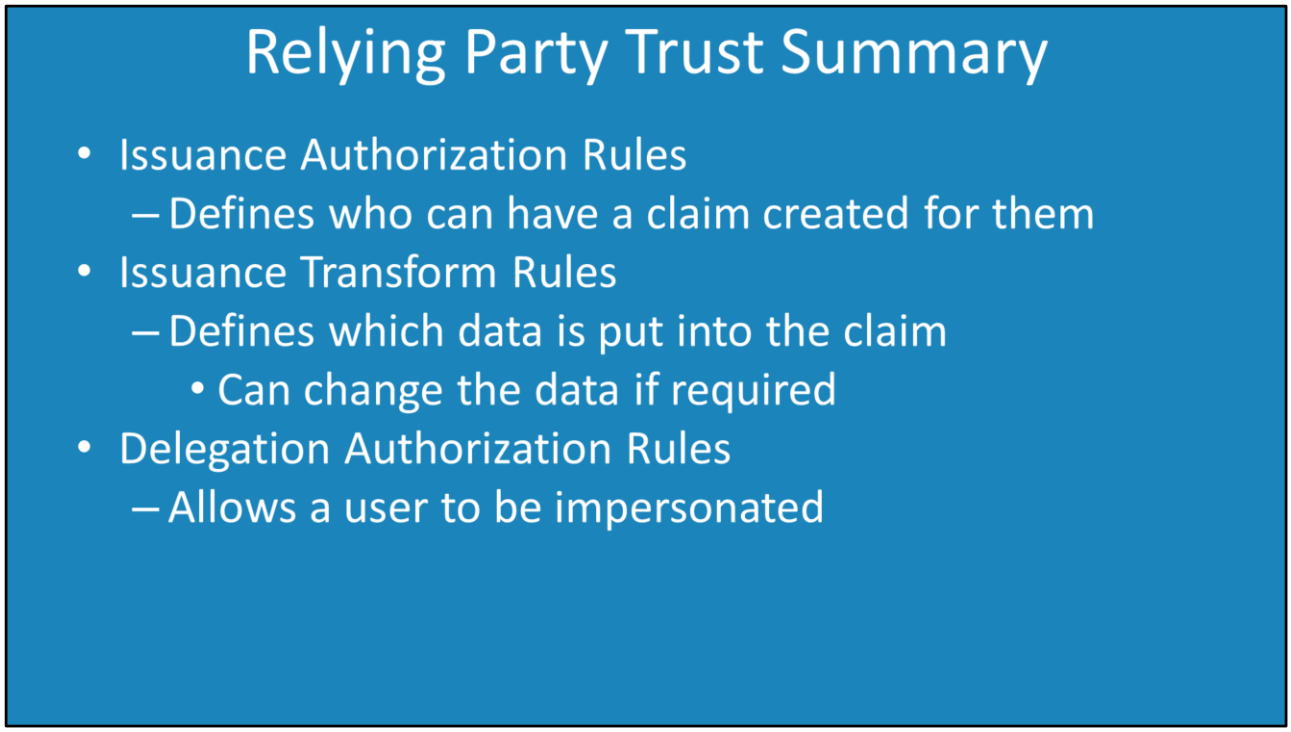


Delegation Authorization Rules Example
In this example, a library has purchased access to an online journal for their students. The online journal license agreement states that is can only be used by students who are members of that library. If the library was to give the users the username and password to access the online journal they would lose control. This is because a user could stop being a member of the library and still have access or they could give the username and password to other people to use. To keep control of the online journal, the users connect to the library using their username and password and are authenticated. This allows the library to confirm that they are members of the library and their access is still valid. The library then accesses the online journal using their username and password on behalf of the student. This is an example of delegation authorization rules where a different user is being used to access information rather than the original user that accesses the system.



Relying Party Trust Summary

A relying party trust is created on any Federation Server that is required to create claims. Since a claim cannot be changed after it is created, the relying party trust must be created on the server creating the claims although this may seem the opposite to the way it should be done. Any server that creates claims needs to have a relying party trust created. For example, if a federation server has a trust between it and another server that has a claims-aware application running on it, a relying party trust needs to be created on the federation server.



When a relying party trust is created, 3 different rules can be created in the relying party trust.
Issuance authorization rules: This determines who is allowed to have a claim created and also how the authentication of that person will work.
Issuance Transform Rules: This rule defines which data is put into the claim. The data that is put into the claim can also be changed as required.
Delegation Authorization Rules: This allows a user to be impersonated, or put another way, allows the Federation Server to masquerade as someone else.

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
"The Role of Claim Rules" http://technet.microsoft.com/en-us/library/ee913586.aspx
"Claims Transformation and Custom Attribute Stores in Active Directory Federation Services 2" http://www.syfuhs.net/post/2010/09/14/Claims-Transformation-and-Custom-Attribute-Stores-in-Active-Directory-Federation-Services-2.aspx
"When to Use Identity Delegation" http://technet.microsoft.com/en-us/library/dd807122.aspx