ACTIVE DIRECTORY FEDERATION SERVICES

SERVER 2012

Active Directory Federation Services (AD FS) is a software component developed by Microsoft that can be installed on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries.

COMPANY A – Accounts Partner

COMPANY B – Resource Partner

Enterprise CA

DC

AD FS

tokens

AD FS

Federation Accounts Server

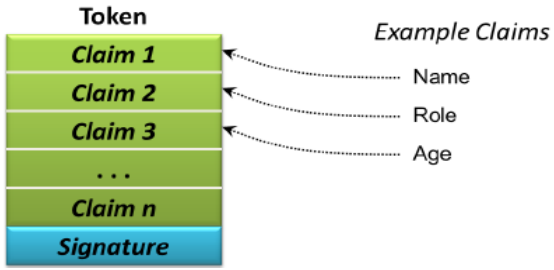
- Collecting and authenticating users credentials
- Building up claims for that user and packaging the claims into security tokens
- Presenting the tokens across a Federated Trust to enable access to Web-based resources that are located in the resource partner organization

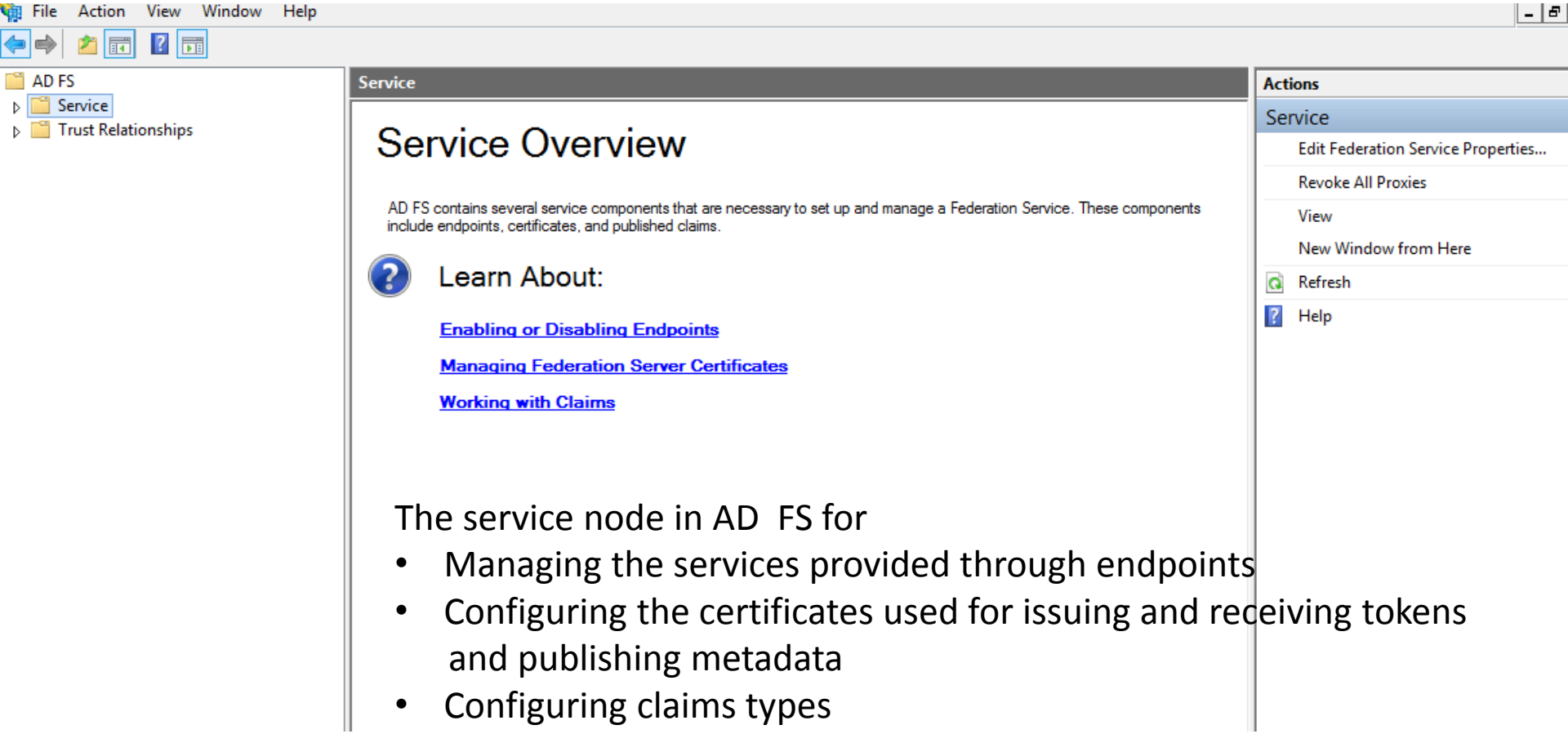
ADFS enabled Web Server (Web based Applications)

Federation Resource Server

- uses the security tokens to make authorization decisions for its Web servers
- To function as an ADFS resource, Web servers must either have Windows Identity Foundation (WIF) installed or have the Active Directory Federation Services Claims-Aware Web Agent role services installed.

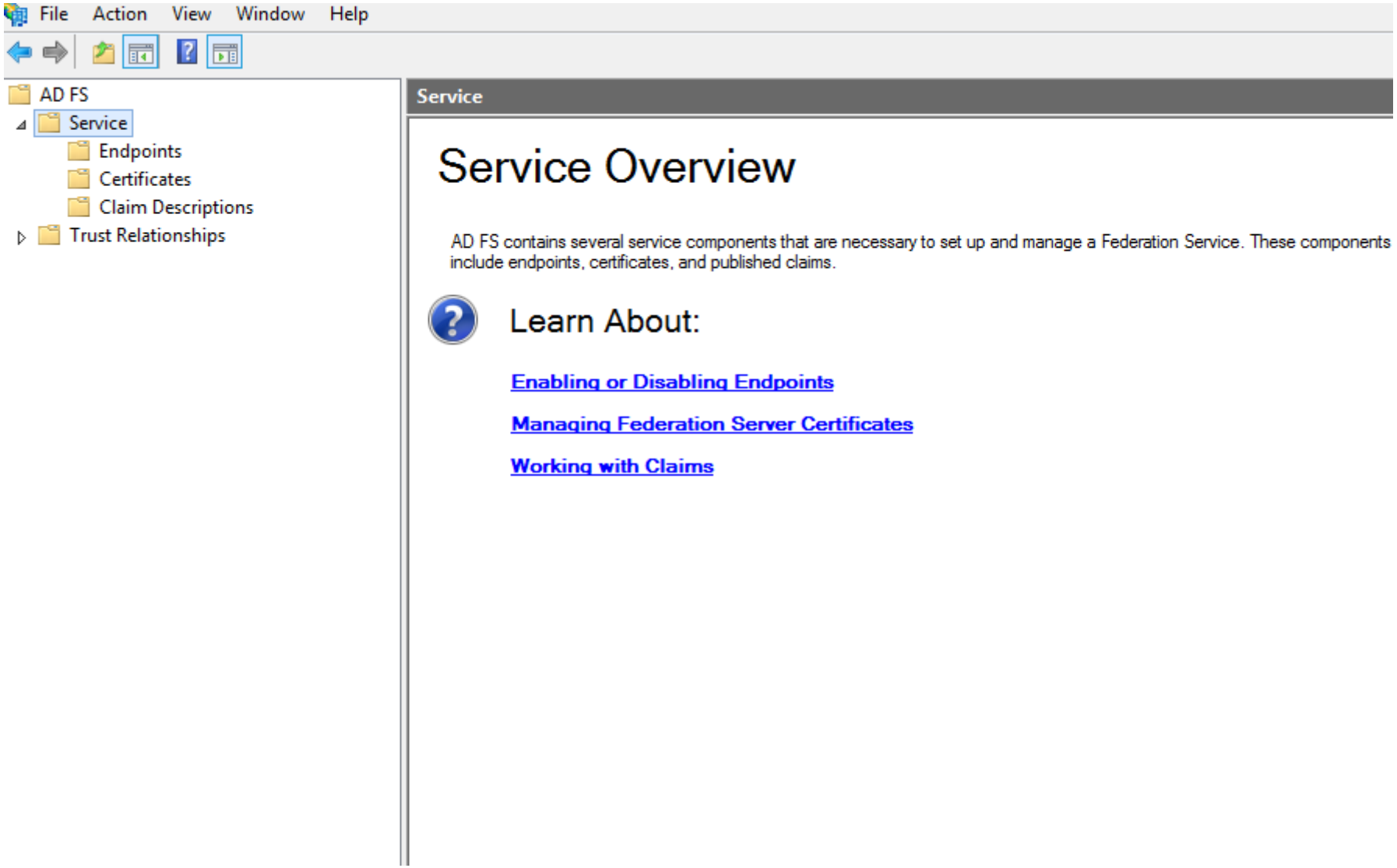
In a claims-based world, a token contains one or more *claims*, each of which carries some piece of information about the user it identifies.

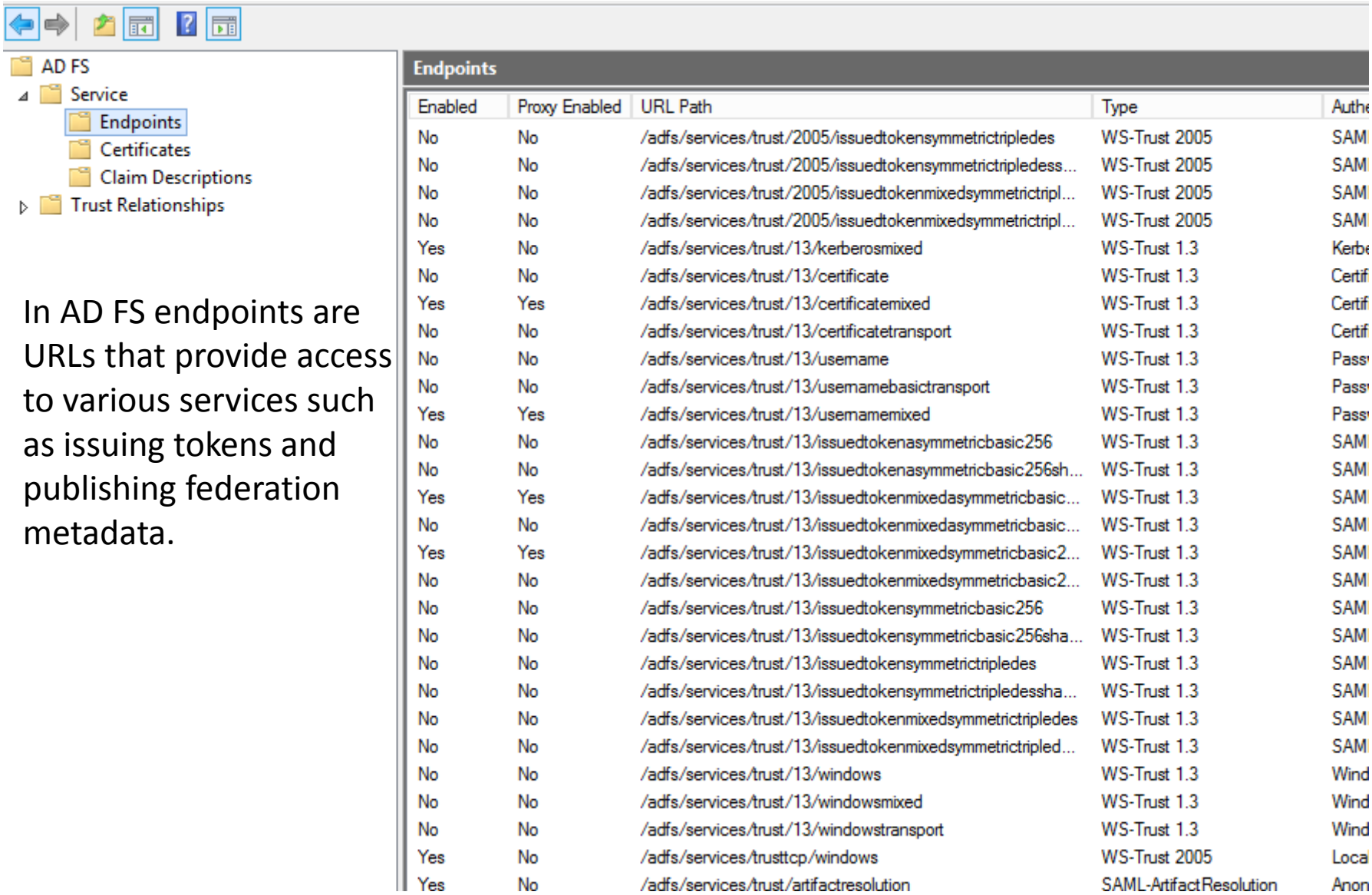




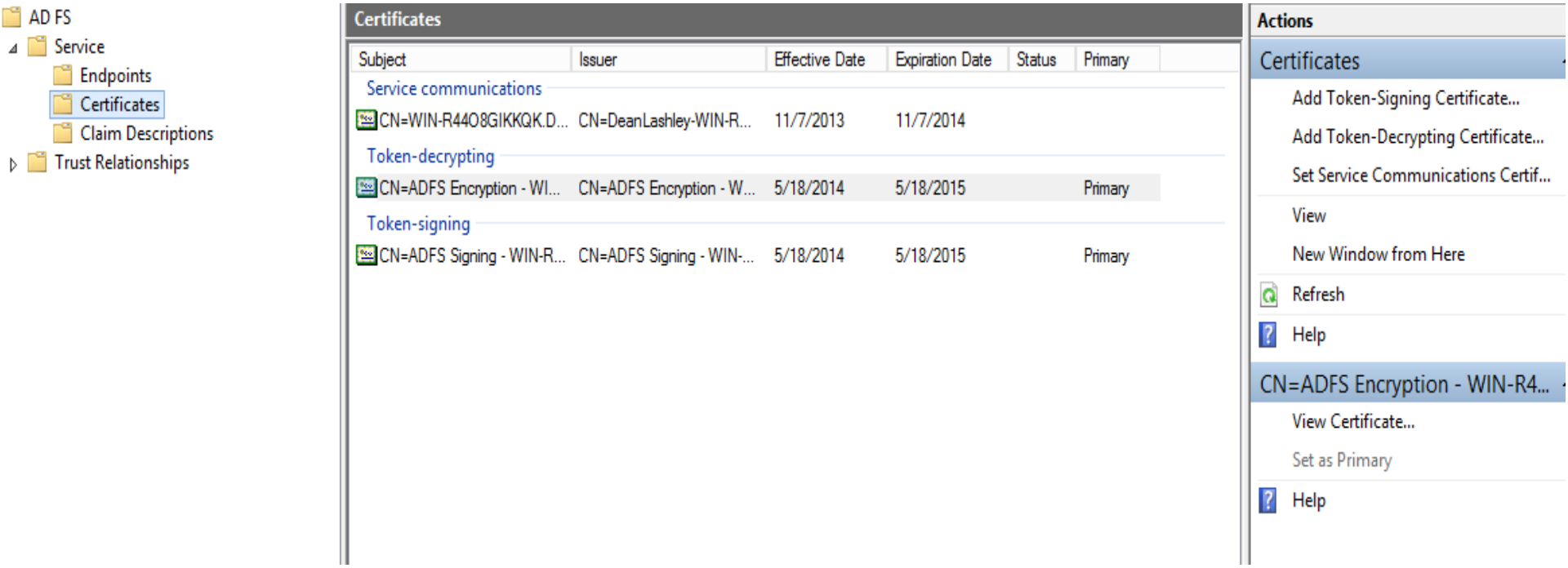
The service node in AD FS for

- Managing the services provided through endpoints
- Configuring the certificates used for issuing and receiving tokens and publishing metadata
- Configuring claims types


File
Action
View
Window
Help
AD FS
Service
Endpoints
Certificates
Claim Descriptions
Trust Relationships
Service
Service Overview
AD FS contains several service components that are necessary to set up and manage a Federation Service. These components include endpoints, certificates, and published claims.
Learn About:
Enabling or Disabling Endpoints
Managing Federation Server Certificates
Working with Claims



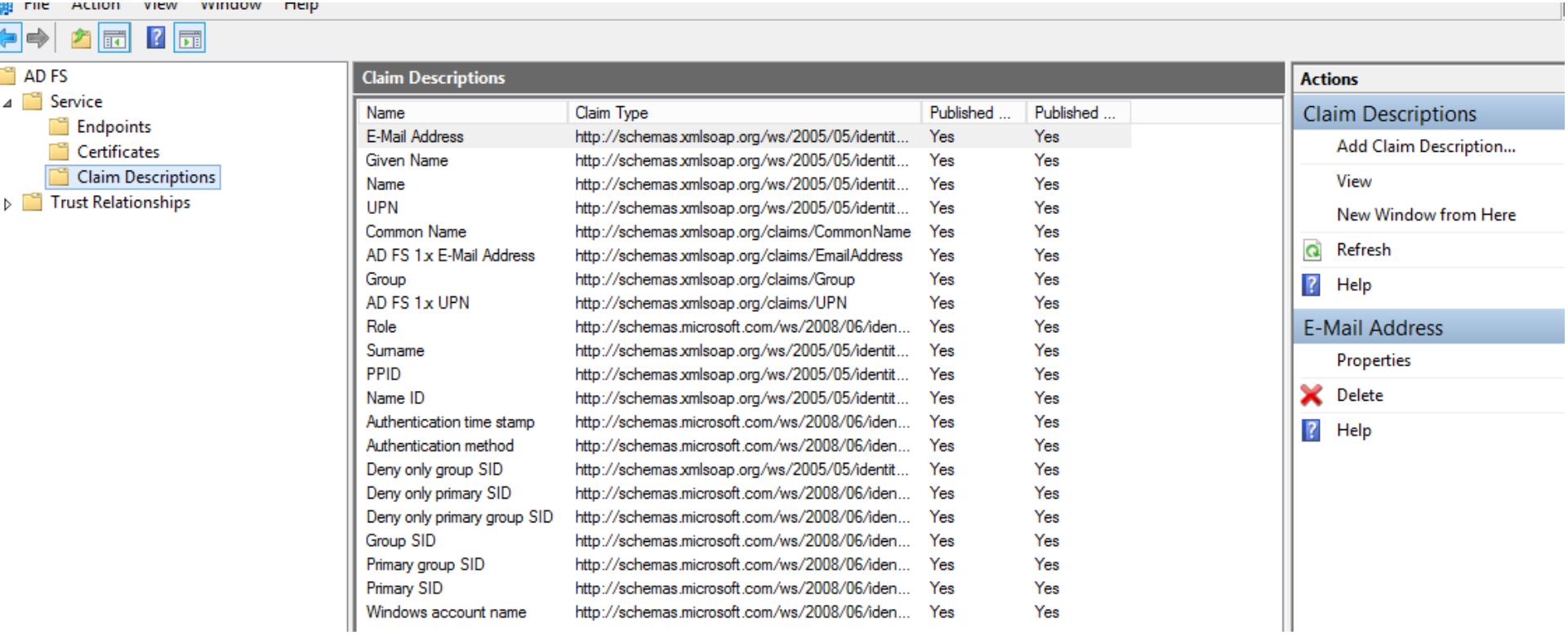
In AD FS endpoints are URLs that provide access to various services such as issuing tokens and publishing federation metadata.



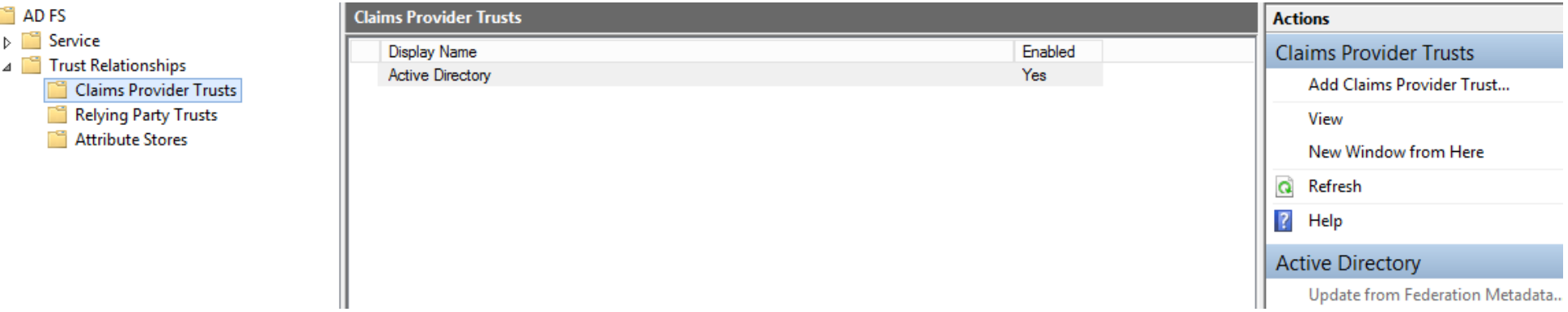
Service communications: This certificate is used for Windows Communication Foundation Message security. WCF). Before you can configure AD FS this certificate must be installed as a SSL certificate on the Default Website of the local instance of IIS.

Token-Decrypting: This is used to decrypt tokens the Federation Service receives.

Token-signing: This certificate is used to sign tokens the Federation Service issues.



CLAIMS DESCRIPTION: Through this node you can find information about the claims the local Server is currently able to assert about identities.



The Trust Relationship Node enables you to manage the trust relationships of the Federated Service. The three child nodes enable you to add and configure policies For claims providers, relying parties and attribute stores.