**Microsoft ADFS (Active Directory Federation Services)**

* Einführung: Februar 2006
* Wurde dauernd weiterentwickelt: Anfangs war es nur eine Technik, um die Anmeldung an Web-Applikationen zwischen den AD (Active Directory)-Umgebungen zu erleichtern
* Heutige Entwicklung: wichtige Industriestandards (z.B. SAML, oAuth 2.0) auch herstellerübergreifend unterstützen -> leider unübersichtlich (Dokumentation sehr mager)
* Optional bei Windows Server Version 1.1 und 2.0, weiter WS 2012 aber integriert
* Grundkonzept: Zugriffskontrolle basierend auf Anmeldetoken; Single-Sign On bei Web-Applikationen
* Trennung zwischen den Applikationen (Zugriff auf den Webserver und Verwaltung der Benutzer – auch Cloud-Service möglich, Kontrolle durch Unternehmen)
* Komponenten:
  + Kunde, der die Benutzerkonten verwaltet (Identity Provider)
  + Anbieter der Applikation, der die Anmeldungen akzeptiert (Application Provider)
* Ablauf:
  + Austausch von Security Tokens
  + Benutzer bestätigt seine Identität und weitere nötige Infos
  + XML-Dokument wird genutzt
  + Application Provider entschlüsselt den Token und kann davon ausgehen, dass es von einem vertrauenswürdigen IdP kommt.

Quelle: https://www.faq-o-matic.net/2014/04/02/adfs-grundlagen-und-architektur/