



Dokument	introduktionIDfed
Author	Simon Wiberg
Identifier	
Version	1.0.0
Last Modified	2006-06-26 16.10
Status	Published

Vad är en identitetsfederation?

En identitetfederation är en sammanslutning av organisationer, till exempel universitet och högskolor, som har kommit överens om att lita på varandras elektroniska identiteter i sina IT-system. Det innebär att när en person autentiserat sig mot sitt universitet så ska även de andra medlemsorganisationerna i federationen lita på att personen är den han eller hon utger sig för att vara.

En identitetsfederation är en infrastruktur som gör det möjligt att ge anställda och studenter vid ett universitet tillgång till IT-tjänster som drivs vid andra universitet. Det anses ofta önskvärt att studenter och anställda ska kunna använda Internet när de besöker andra universitet. Med en identitetsfederation är det möjligt att göra lösningar där anställda och studenter utan några speciella åtgärder kan logga in med samma användarnamn och lösenord som på sitt universitet. Det vill säga att autentiseringen delegeras från det universitet där studenten eller den anställda befinner sig till dennes hemmauniversitet. Om det inte var möjligt att delegera autentiseringen på det sättet, skulle en tjänst av den karaktären kräva att alla anställda och studenter har användarkonton (och är registrerade i koncernkatalogerna) på varje universitet. Det är inte praktiskt möjligt för ett universitet att hålla reda på vilka som är anställda eller studenter vid andra universitet.

Det krävs tekniska lösningar för att autentisering ska kunna delegeras från en plats till en annan och för att tjänster ska kunna tillhandahållas inom federationen. Däremot så består inte en identitetsfederation i sig av teknisk utrustning. Identitetsfederationen är snarare de dokument och strukturer som reglerar förutsättningarna för att medlemmarna skall kunna lita på varandras elektroniska identiteter.

Ponera exemplet med studenter och anställda vid universitet och högskolor som ska kunna använda nätet när de besöker andra universitet och högskolor. En tjänst av det slaget förutsätter att medlemmarna definierar till exempel studenter på ett likartat sätt. Identitetsfederationen förutsätter också att det finns gemensamma principer för hur tilldelningen av elektroniska identiteter går till. Reglerna för nätanvändning bör också följa samma principer hos alla medlemmarna i federationen, och medlemmarna bör ha en gemensam linje för när användare skall stängas av.

Om ett universitet skall upplåta nättillgång till studenter från andra universitet är det inte orimligt att universitetet som ställer resurser till förfogande vill kunna lita på att de som autentiseras som studenter via andra universitet verkligen är studenter. Vidare så skall en elektronisk identitet kunna knytas till en fysisk person, som kan hållas ansvarig för sitt agerande på nätet. För att det skall fungera så går det inte att tillåta att någon federationsmedlem håller låg säkerhet i sin autentisering, delar ut elektroniska identiteter hur som helst eller underlåter att stänga av medlemmar som missköter sig.

Således måste federationen ställa krav på medlemmarna. Federationens regler samlas i en federationspolicy. För att federationen ska fungera och medlemmarna kunna lita på varandras elektroniska identiteter, måste också ledningen för federationen ta på sig vissa förpliktelser. I första hand måste de se till att medlemmarna i federationen lever upp till sina förpliktelser enligt policyn. I de fall som medlemmar bryter mot reglerna måste federationens ledning vidta åtgärder - i värsta fall utesluta medlemmar ur federationen. Federationsledningens förpliktelser bör också definieras i identitetsfederationens policy.

Federationsledningens förpliktelser är viktiga för att medlemmarna ska kunna lita på de elektroniska identiteter som finns inom federationen. Men de kan också vara viktiga för att upprätthålla förtroendet gentemot externa partners.

I det ovan nämnda exemplet med nättillgång tillhandahålls tjänsten ifråga på varje universitet och högskola. Identitetsfederationen kan också användas för att dela på en applikation som drivs av någon av federationens medlemmar. Det är också möjligt att använda en identitetsfederation för att ge tillgång till externa tjänster som till exempel forskningsdatabaser eller tidskrifter. För att det skall vara möjligt att sluta bra avtal för denna typ av tjänster, så måste federationen inge förtroende i det att tillgången till resursen verkligen begränsas till den krets som avtalet avser.