Bezoek A-Select dag (25 mei 2005)

Andries de Man en Martien Quaak

A-Select is een door SURFnet aangeboden authenticatievoorziening, die onder andere door Kennisnet zal worden gebruikt in het Entrada-project ter vervanging van het huidige 'Entree'. A-Select voorziet in een decentrale authenticatie, terwijl voor Entree nog een centrale database met gebruikers (authenticatie) en licenties (autorisatie) wordt gebruikt.
Momenteel zijn er zo'n 2.5 miljoen gebruikers: alle scholen, onderwijsinspectie, uitgevers plus volwassen educatie.
Doel: federatie opzetten met trustrelaties tussen onderwijsinstellingen, bibliotheken en uitgevers.

In de toekomst zal A-Select de hele 'content ontwikkeling- en distributie-keten' ondersteunen en wellicht ook een portfolio functie krijgen. Er zal dus meer aan personalisatie gedaan moeten worden en een grotere variatie in gebruikersrollen moeten worden onderscheiden. De nieuwste versie[1] van A-Select (1.4.1) zal daarom ook bij autorisatie kunnen helpen, door middel van het versturen van attributen ('identiteit') naar de server die om authenticatie heeft verzocht. De autorisatie zelf geschiedt op de ontvangende server aan de hand van de waarden van de attributen. In deze zin zal A-Select steeds meer gaan lijken op Shibboleth, dat onder andere wordt gebruikt door het AAI project van de Zwitserse organisatie SWITCH.
Versie 1.4.1 zal nog geen 'terugtransport' van attributen ondersteunen. Versie 1.4.1 ondersteunt dus wel het scenario waarin een student die op een website van een uitgever een online tijdschrift wil lezen door de onderwijsinstelling wordt geauthenticeerd en door de uitgever wordt geautoriseerd. Het uitgebreidere scenario waarin het feit dat de student een bepaald artikel heeft opgevraagd (en hopelijk gelezen) wordt opgeslagen in een door de onderwijsinstelling beheerde portfolio is nog niet ondersteund.

Zorgpunten bij A-Select zijn privacy en sessiemanagement. Als A-Select in verschillende gebieden wordt toegepast kan bij de gebruiker onzekerheid ontstaan over de hoeveelheid en aard van persoonlijke gegevens die aan een applicatie wordt doorgegeven. Dit is vooral een perceptieprobleem van de gebruiker. Het kan zich al voordoen bij de het onafhankelijk aanroepen van losse applicaties. Het probleem wordt versterkt als groepen applicaties (SSO-groepen) worden gemaakt die elkaar zonder directe invloed van de gebruiker aanroepen.
Er zit nog een addertje onder het gras: de timeout-regels van A-Select en van applicaties kunnen verschillen, waardoor de gebruiker de indruk kan krijgen dat een A-Select-sessie is beëindigd terwijl alleen maar een applicatie-sessie is beëindigd. Er kan al gedeeltelijk aan de hiervoor geschetste problemen tegemoet worden gekomen door naast single sign-on ook een duidelijke single sign-off aan te bieden.

Naast A-Select werd op de A-Selectdag ook het Engelse 'Eduserv Athens' gepresenteerd. Dit is een vergelijkbaar authenticatie-project, met als grote verschil dat er een centrale authenticatiesever wordt gebruikt. Het is grootschalig opgezet en loopt al 10 jaar. Er doen zo'n 2000 organisaties aan mee, waaronder ziekenhuizen, musea, bibliotheken en onderwijsinstellingen. Vanwege de grote verscheidenheid aan toepassingsgebieden waarin een gebruiker van dit systeem zich kan bewegen is er extra aandacht besteed aan privacy ('pseudonimity').
Een gedecentraliseerd authenticatie-model, zoals door A-Select gebruikt, heeft de voorkeur boven een gecentraliseerd model. Bij een recente implementatie van Eduserv Athens in de Verenigde Staten is een iets meer gedecentraliseerde opzet gekozen.

Voor het SCALE-project is authenticatie-door-de-onderwijsinstelling interessant, omdat dit een grote beheerslast bij SCALE zelf voorkomt. Het is echter de vraag of de attributenschema's die binnen A-Select of andere projecten ontwikkeld worden toepasbaar zijn in het SCALE project.

---

[1] ten tijde van de A-selectdag

Het feit dat er naast het internationale eduPerson-schema al een specifiek Zwitsers swissEduPerson-schema en een Fins funetEduPerson-schema zijn ontwikkeld geeft aan dat er wel degelijk behoefte is aan (lokale) variaties van zo'n schema.
De discussies over Attribute Release Policies, waarin wordt vastgelegd welke soort attributen tussen verschillende organisaties of verschillende applicaties mogen worden uitgewisseld, spelen ook in het SCALE project. Ervaringen die met A-Select op dit gebied worden opgedaan zullen waardevol zijn voor SCALE.

Op technisch vlak is er een onderscheid tussen SCALE en A-Select wat betreft de implementatie van de trustrelatie tussen servers. Bij SCALE is die implementatie zwak (referrer-based), bij A-Select wordt een sterkere implementatie voorgestaan (PKI voor langlevende trusts en SAML voor kortlevende 'payload'-trusts).

Het SCALE-project gaat in eerste instantie uit van de Elektronische Leeromgeving als server voor remote authenticatie. De bestaande A-Select Agent voor BlackBoard 6.0 kan er dus voor zorgen dat SCALE via deze omweg van A-Select gebruik maakt. Het is daarbij wel van belang dat deze Agent tijdig wordt aangepast voor nieuwe BlackBoard-versies en dat vergelijkbare agents beschikbaar komen voor andere ELO's (WebCT!).