Identitymanagement, ervaringen uit het onderwijs

Drs. J. Kuipers RE RA
werkte bij KPMG, het Rijks Computercentrum en de Rabobank aan audit en gegevensbeveiliging. Met de collega's van SURF en SURFnet heeft hij SURFfederatie, de landelijke authenticatiedienst voor het hoger onderwijs, gerealiseerd. Bij DigiNotar werkt hij verder aan het realiseren van landelijke identitymanagementinfrastructuren en internet trust services. Als voorzitter van het nationaal identitymanagement- en authenticatieplatform van ECP.NL overziet hij veel initiatieven op het gebied van identitymanagement.

jaap.kuipers@surfnet.nl

Drs. Jaap Kuipers RE RA

SURFnet heeft meer dan tien jaar gewerkt aan een landelijke infrastructuur voor gemakkelijk en veilig inloggen over organisatiegrenzen heen. Dit artikel laat iets van deze geschiedenis zien. Voor het realiseren van een landelijke authenticatie-infrastructuur zijn diverse fasen doorlopen: gestart werd met chipkaarten en passwords via sms-berichten, daarna lag het accent op web single sign-on, met open source A-Select voor federatieve authenticatie (A-Select is de software onder de motorkap van DigiD). Uiteindelijk is een landelijke infrastructuur gerealiseerd gebaseerd op open source en commerciële software met nadruk op open standaarden voor identitymanagement. Identiteitenbeheer en authenticatie werden losgemaakt uit de afzonderlijke applicaties en krijgen een eigen beheersysteem dat in staat is organisatieleden ook buiten de eigen organisatie te laten inloggen.

Inleiding

De ontwikkeling naar een leven lang leren wordt op grote schaal ondersteund door ICT. Anytime, anyplace, any device, always on toegang vraagt erom dat afnemers en aanbieders van diensten met minimale hindernissen kunnen samenwerken over de grenzen van de organisaties heen. Authenticatie (bewijzen wie je claimt te zijn) en identitymanagement (beheer van gebruikersgegevens) vormen hierbij processen die steeds meer losgekoppeld worden van de individuele applicaties. Hiervoor komen systemen beschikbaar die samenwerking vergemakkelijken, met behoud van de gegevensbeveiliging. SURFnet ontwikkelde een landelijke authenticatievoorziening, in eerste instantie gebaseerd op open source-programmatuur van Alfa en Ariss. Dat is de technologie die ook door DigiD wordt gebruikt.

De ontwikkelingen gaan allang verder dan open source ter beschikking stellen: onderwijsinstellingen en dienstenleveranciers nemen deel in een landelijke SURF trustfederatie voor algemeen gebruik, waardoor werk rond identitymanagement dat de organisatiegrens overstijgt uit handen wordt genomen. Een goed voorbeeld van een trustfederatie voor specifiek gebruik bieden de banken, die het mogelijk hebben gemaakt om met de bankpas van bank A bij buitenlandse bank B contanten uit de geldautomaat op te nemen, zonder dat je eerst een rekening bij die bank B hoeft te openen.

Naadloze toegang tot een groot dienstenpalet

Door het internet is het mogelijk vanaf elke plaats op elk moment toegang te krijgen tot een scala aan diensten. Op één beeldscherm heeft de student naadloos toegang tot bijvoorbeeld:

- de elektronische leeromgeving van hogeschool A;
- de leeromgeving van universiteit B;
- artikelen uit honderden databanken van een groot aantal uitgevers;
- een landelijke beeld- en geluidbank van de omroepen;
- een gezamenlijke werkomgeving in Sharepoint waarin studenten uit binnen- en buitenland samenwerken.

Hierbij willen we de toegangsvoorziening zien als een facilitator en niet als een hindernis. Een toegangsvoorziening (identificatie, authenticatie, autorisatie) moet het gemak van naadloze toegang tot een veelheid aan bronnen bieden met behoud van beveiliging en een minimum aan administratieve lasten. Het groeiende aantal user-ids en passwords vraagt al jaren om een oplossing, SURF faciliteert een beperkte digitale sleutelbos. Verbree en Van der Hulst hebben in Compact 2005/3 al helder uiteengezet wat er technisch komt kijken bij het beperken van digitale sleutelbossen.

Historisch perspectief

Het onderwijs is niet uniek, de overheid streefde ernaar om in 2007 65% van de diensten te ontsluiten via het internet. De Belastingdienst werkt eraan om aangiftes online via het internet te kunnen laten plaatsvinden. Dit vroeg om één aanlogcode voor burgers. De vraag van de overheid naar een authenticatievoorziening in het kader van het programma 'Andere Overheid' en het aanbod van A-Select hebben elkaar via de Manifestgroep ontmoet in 2003. Dit heeft ertoe geleid dat A-Select opgenomen

Figuur 1. SURFfederatie: één sleutel voor veel diensten.

is als technologie onder de motorkap van DigiD. Een voorwaarde daarbij was dat de programmatuur als open source beschikbaar werd gesteld. De samenwerking met de overheid leidde tot een robuust en betrouwbaar systeem dat in april 2006 door 1,1 miljoen Nederlanders werd gebruikt en in 2008 door 7 miljoen gebruikers.

DigiD is nu de nationale authenticatievoorziening voor Nederland, alle overheidsdiensten kunnen voor de authenticatie (verificatie van de identiteit, bewijzen wie je claimt te zijn) een beroep doen op DigiD. DigiD geeft de aangesloten website of dienst het burgerservicenummer (BSN) van diegene die aanlogt. Wat de website of dienst vervolgens met het BSN doet hangt af van het achterliggende proces. De eerste onderwijsdienst die aansloot op DigiD was MijnIBGroep met circa 400.000 studenten. Aansluiting van Studielink op DigiD maakt het mogelijk dat aankomende studenten (die dus nog niet bekend zijn in de administratie van een universiteit of hogeschool) zich via het Internet voor het hoger onderwijs inschrijven. Het federatieve karakter van A-Select maakt het mogelijk om naast DigiD ook gebruik te maken van andere authenticatiebronnen. Ben je eenmaal ingeschreven in Studielink en heb je een user-id van je hogeschool ontvangen, dan kan je als student inloggen met zowel je DigiD als met een toegangscode van de universiteit of hogeschool.

Keuzevrijheid in authenticatiemiddelen voor gebruikers is enorm belangrijk

De naam A-Select komt van authenticatieselectie, keuzevrijheid uit verschillende bronnen en mogelijkheden om te bewijzen wie je zegt dat je bent. Keuzevrijheid in authenticatiemiddelen voor verschillende groepen gebruikers is enorm belangrijk, heeft SURF geleerd. Voorwaarde voor de keuzevrijheid is wel dat een uniek identificerend gegeven beschikbaar is.

Het vraagstuk rond toegangsbeveiliging en authenticatie, wat nu vaak identitymanagement wordt genoemd, betekende voor het onderwijs enige tijd het realiseren van een studentenchipkaart. Ten tijde van de strijd tussen Chipper en Chipknip rond 1996 was de mening dat de introductie van een studentenchipkaart de uniforme toegang tot gegevens een stuk eenvoudiger zou maken. Dat bleek moeilijker dan toen werd gedacht. Problemen met onder andere chipkaartlezers gooiden roet in het eten. Voor SURF waren de vraagstukken rond toegangsvoorzieningen en authenticatie reden om in 2001 het programma

TrustSURF te starten, dat tot doel had het bundelen en verspreiden van kennis over authenticatievraagstukken.

Het SURF Meerjarenplan 2003>6 'De kern van de zaak' formuleerde onder andere de ambitie om een landelijke authenticatiedienst voor het hoger onderwijs te realiseren. Inmiddels is door de samenwerking met de Stichting Kennisnet ICT de doelstelling verbreed naar heel het onderwijs met potentieel 3,5 miljoen gebruikers. Kennisnet biedt daarvoor de dienst Entree. Kennisnet.nl.

De moeizame inzet van een studentenchipkaart leidde binnen het Gigaport-project tot de ontwikkeling van 'pragmatische authenticatie met persoonsgebonden middelen': de bankkaart en de mobiele telefoon. Deze aanpak heeft zich bewezen, het loont om gebruik te maken van een reeds bestaande infrastructuur. De bankkaart van de Rabobank en de ABN-AMRO bank was beschikbaar binnen het onderwijsdomein voor authenticatie met voorzieningen voor internetbankieren waarover veel, maar niet alle, studenten beschikken. Het Leids Universitair Medisch Centrum (LUMC) heeft de bankkaart gebruikt om toegang te verlenen tot medische gegevens. Het onderwijs stimuleerde dat de overheid gezamenlijk gebruik zou gaan maken van deze bankauthenticatie binnen DigiD. In het rapport voor Forum Standaardisatie 'Verkenning authenticatie, roeien met de riemen die je hebt?'[1] wordt dit idee uitgewerkt.

De mobiele telefoon werd ingezet voor het ontvangen van eenmalig geldige wachtwoorden, one-time-passwords (OTP's) via een sms. Voordeel van de mobiele telefoon als authenticatiemiddel is het intuïtieve gebruiksgemak en de combinatie van zowel het hebben van de telefoon als het weten van de pincode. Nadeel van sms-authenticatie vormen de kosten – een grote hogeschool die per dag 100.000 sms-berichten verstuurt had er een forse kostenpost bij. Een belangrijke les uit de SURF- en Gigaport-projecten was dat keuzevrijheid geboden moet worden in authenticatiemiddelen. De authenticatieselectieprogrammatuur A-Select ondersteunt verschillende authenticatievormen zoals: gebruikersnaam en wachtwoord, security tokens, authenticatie op basis van de bankkaart, sms-passwords, softwarecertificaten, hardware PKI-certificaten, authenticatie gebaseerd op het IP-adres.

Bij de keuze van een identitymanagementpakket vormt de ondersteuning van verschillende authenticatiehulpmiddelen een aandachtspunt. SURFnet maakte het mogelijk om de verschillende authenticatievormen los te koppelen van individuele applicaties. Deze ontwikkeling is vergelijkbaar met het loskoppelen van bestanden van applicaties door de komst van databasemanagementsystemen. Diverse leveranciers bieden anno 2009 pakketten voor het loskoppelen van identificatie en authenticatie.

1 www.forumstandaardisatie.nl/fileadmin/OVOS/Doc_authenticatie.pdf

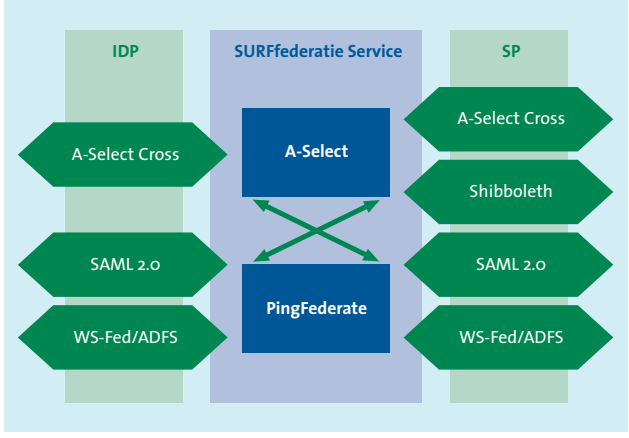
Van open source naar open standaarden

Het buitenlandse onderwijs kende gelijksoortige ontwikkelingen als het Nederlandse onderwijs, waarbij de Angelsaksische landen zich richten op het open source-systeem Shibboleth. Shibboleth is mede ontstaan uit de eis van privacybescherming volgens de Family Educational Rights and Privacy Act (FERPA). In Europa werkt het hoger onderwijs samen in de Trans-European Research and Education Networking Association (TERENA) aan het oplossen van authenticatievraagstukken. De website van TERENA (www.terena.org) bevat nuttig materiaal op het gebied van identitymanagement.

In diverse landen is gewerkt aan open source-authenticatiesystemen. Het onderwijs liep daarbij vooruit op ontwikkelingen bij de grote softwareontwikkelaars. Na 2005 werd duidelijk dat partijen als Oracle door het opkopen van nichespelers serieus werkten aan oplossingen. De vraag van het onderwijs heeft zich mede daardoor verlegd van open source naar open standaarden. Doordat ook de markt met oplossingen kwam kon de aandacht geconcentreerd worden op de standaarden.

Als we naadloos gebruik willen kunnen maken van diensten van een groot aantal partijen dan moeten we er zeker voor zorgen dat het bij elkaar kunnen inloggen gestandaardiseerd wordt. De standaard waar het meest van verwacht wordt op dit gebied, is SAML versie 2.0 (Security Assertion Markup Language). Diverse pakketleveranciers bieden ondersteuning voor deze standaard en ook de open source-pakketten zijn overgegaan op SAML. A-Select en Shibboleth spreken SAML. En ook Microsoft heeft aangegeven ondersteuning te gaan bieden.

Het College Standaardisatie werkt in het kader van het actieplan 'Nederland Open in Verbinding' van Economische Zaken aan de totstandkoming van een lijst met open standaarden. Eén van de standaarden die mogelijk opgenomen wordt op de lijst



Figuur 2. **SURFfederatie ondersteunt diverse protocollen.**

is SAML 2.0. Organisaties die nog niet van SAML hebben gehoord, doen er goed aan hier kennis van te nemen.

Met het harmoniseren op een open standaard is een belangrijk punt bereikt in het realiseren van een naadloze mogelijkheid om gezamenlijk toegang te krijgen tot elkaars systemen. De implementatie van de standaard blijkt helaas niet altijd triviaal te zijn. Oplossingen worden nu weer gezocht in 'light' versies zoals SimpleSAMLphp die een snellere uitrol mogelijk moeten maken.

SURFnet vervult een natuurlijke rol als proeffabriek voor innovaties

SURFnet heeft intussen meegewerkt aan diverse systeemimplementaties van open source- en commerciële pakketten. Leveranciers gebruiken SURFfederatie graag als testomgeving voor hun applicaties, SURFnet vervult een natuurlijke rol als proeffabriek voor innovaties. Het open karakter van de SURFnet-organisatie houdt in dat SURFnet de opgedane kennis eenvoudig kan delen met bedrijven en organisaties.

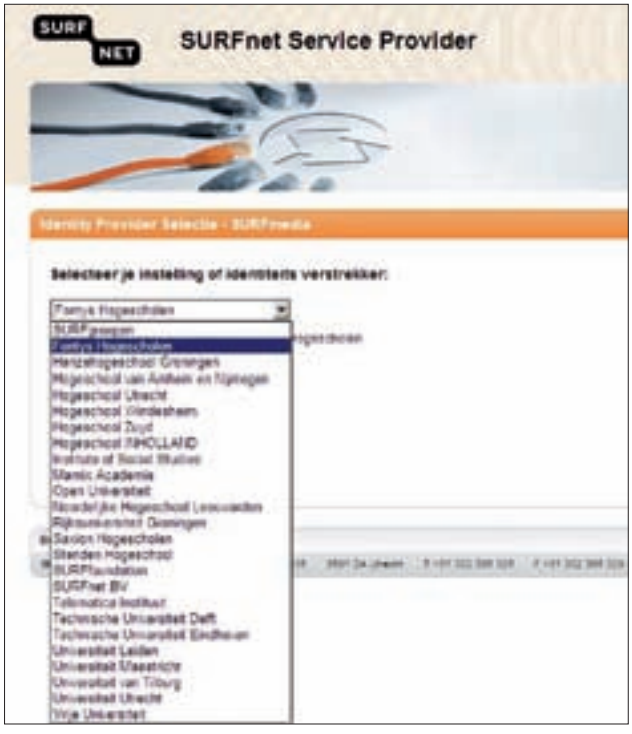
Inloggen via SURFfederatie

SURFnet heeft SURFfederatie ingericht, dat is de trustfederatie voor het hoger onderwijs en onderzoek. Een trustfederatie is een verzameling algemeen geldende technische, organisatorische en juridische afspraken die deelnemers vertrouwen bieden om gebruik te maken van lokale authenticatievoorzieningen van de aangesloten partijen voor het krijgen van toegang tot aangesloten diensten. De regels waaronder instellingen en dienstverleners samenwerken worden vastgelegd in federatievoorwaarden.

Een mooi voorbeeld van een trustfederatie met een specifiek doel bieden de banken die het rekeninghouders mogelijk maken om geld op te nemen bij een andere (bijvoorbeeld buitenlandse) bank waar klanten geen rekening aanhouden. Een voorbeeld hoe de federatie in het onderwijs wordt gebruikt is de wijze waarop studenten toegang krijgen tot de content van een uitgever zonder dat de user-ids en passwordbestanden bij de uitgever onderhouden dienen te worden. De uitgever en de federatie komen overeen dat als studenten en medewerkers lokaal geauthenticeerd zijn, dit voldoende is om op te vertrouwen. De instellingen zullen ervoor zorgen dat uitsluitend studenten die daadwerkelijk zijn opgenomen in de studentenadministratie en dus niet de reeds afgestudeerde studenten toegang kunnen krijgen tot databases van de uitgevers. Immers, afgestudeerde studenten hebben geen recht op vrije toegang tot de content van de uitgever. De uitgever moet erop kunnen vertrouwen dat als een student afstudeert deze tijdig verwijderd wordt uit de gebruikersadministratie.

Een belangrijk voordeel van federatief identitymanagement is dat de privacy van studenten en medewerkers verregaand kan worden beschermd. De mogelijkheid bestaat om af te spreken dat een uitgever toegang geeft tot specifieke databanken louter op basis van het feit dat de instelling verklaart dat het daadwerkelijk een student of medewerker is. De uitgever hoeft niet te weten welke individuele student een bepaalde databank raadpleegt, alleen dát het een student is van de specifieke instelling. Mogelijk kan de verklaring specifieker worden: dit is een student chemie in de laatste fase van de opleiding. Het definieren en registreren van de attributen studierichting, studiefase stelt extra eisen aan het administratieve apparaat. De standaardisatie van attributen zal de nodige inspanning vergen, hoe kom je bijvoorbeeld internationaal tot een werkbare definitie van studierichtingen. Authenticatie op basis van attributen, de eigenschappen van een gebruiker, maakt nieuwe wijzen van zakendoen mogelijk.

Een belangrijke proef met federatief inloggen vond plaats bij de Universiteit van Tilburg in samenwerking met uitgever Elsevier. Deze universiteit host de infrastructuur inmiddels. Eind 2007



Figuur 3. **Keuzemenu vergelijkbaar met iDeal.**

ging SURFfederatie in productie en begin 2009 zijn 53 instellingen en diensten, 410.000 studenten aangesloten op SURFfederatie. Het aantal instellingen en diensten zal in 2009 groeien naar 80, met 500.000 studenten. In 2010 zal het hoger onderwijs vrijwel geheel zijn aangesloten. Een dienst die geleid heeft tot een versnelling in het aansluiten op SURFfederatie is de videohost van SURFnet met beeldarchief van de omroepen en video-opnames van colleges. Als studenten deze dienst thuis willen gebruiken, moeten zij bijna altijd aanloggen via de federatie. Een populaire extern gehoste applicatie helpt enorm bij de adoptie van federatief identitymanagement.

Authenticatie op basis van attributen maakt nieuwe wijzen van zakendoen mogelijk

In Europa en Amerika zijn diverse onderwijsfederaties ingericht en buiten het onderwijs gebeurt ook het nodige. Covisint is een mooi voorbeeld van een federatie voor bedrijven. In het kader van landelijk lenen en een landelijke bibliotheekpas werken openbare bibliotheken al geruime tijd samen. De overheid werkt aan een federatie van ministeries onder de naam Rijksweb en biedt MijnOverheid.nl. In de zorg werkt VECOZO aan een single logon-oplossing voor 90.000 zorgverleners en 20 verzekeraars. DigiNotar biedt een federatieve oplossing voor onder andere de advocatuur en accountancy en algemeen voor consumenten. Veel partijen ontmoeten elkaar via ECP.NL, het platform voor eNederland dat precompetitieve samenwerking op het gebied van identitymanagement faciliteert. ECP agendeert hierbij diverse ontwikkelingen zoals eHerkenning (authenticatie) voor bedrijven richting overheid, een OpenID-pilot en onderzoek naar identitymanagement en beveiliging binnen social networking-omgevingen.

Vertrouwen door audit van aansluitvoorwaarden

SURFfederatie biedt het gemak dat een deelnemer, bijvoorbeeld een uitgever die een vaste prijsafspraak heeft gemaakt met een aangesloten universiteit, de authenticatie voor zijn systemen uitbesteedt aan een onderwijsinstelling. De deelnemer vertrouwt dat het authenticatiesysteem van de andere deelnemers, waar hij geen zicht op heeft, in orde is. Voor een betrouwbare federatie is het uiteindelijk vereist te kunnen bouwen op een betrouwbare infrastructuur van alle aangesloten partijen. Om deze te realiseren zullen alle aangesloten onderwijsinstellingen hun beveiliging op orde moeten houden en hierbij is een rol weggelegd voor de informatiebeveiligingsfunctionarissen. In het hoger onderwijs treffen de informatiebeveiligingsfunctionarissen elkaar regelmatig in het SURF-informatiebeveiligersoverleg (IBO). SURF stimuleert dat de aansluitvoorwaarden voor SURFfederatie onderwerp van een lokale audit worden.

Voor een auditor betekent de ontwikkeling naar federatieve authenticatiestructuren meer samenwerking met derden (SAS 70, third party-mededelingen).

Conclusie

De conclusie van de ervaringen uit het onderwijs is dat het mogelijk is om een grootschalige identitymanagementfederatie in te richten waarbij derden vertrouwen op de infrastructuur van de aangesloten partijen. Hierbij is standaardisatie van het samenwerkingsprotocol en de uit te wisselen gegevens van groot belang. De regels voor samenwerking zullen in de praktijk moeten worden getoetst. SURFnet heeft veel ervaringskennis verworven en deelt deze kennis als proeffabriek voor innovatie graag met derden.