Seminar What's Next @ SURFconext 24 maart 2015

Introductie

Op dinsdag 24 maart 2015 vond voor de tweede keer in samenwerking met SURFacademy het seminar What's Next @ SURFconext plaats. Tijdens dit seminar gaven verschillende leden van het SURFconext-team een update over de nieuwste ontwikkelingen rondom SURFconext. Ook was er uitgebreid ruimte voor de instellingen om met het SURFconext-team in discussie te gaan over verschillende onderwerpen.

Het was zeer positief om te zien dat het seminar leeft onder de doelgroep. Het maximaal aantal inschrijvingen was dan ook snel bereikt. In totaal waren er meer dan 70 bezoekers aanwezig op het seminar.

Ochtendprogramma

Alle presentaties (m.u.v. de discussierondes) zijn opgenomen op video. De video is te bekijken via deze link: http://surf.mediamission.nl/Mediasite/Play/e59a221a7a3842cd91e16f8f3d152d6c1d. Druk rechtsonder op de 'i' om naar een bepaalde presentatie te springen.

N.b. door een technisch probleem zijn de slides niet mee opgenomen. Je kunt de slides van de presentaties hieronder downloaden.

Update storingen, releasemanagement (Eefje van der Harst)

Eefje van der Harst gaf de eerste presentatie over de storingen van de laatste tijd, een overzicht van de platformarchitectuur en een korte vooruitblik op de roadmap voor komend jaar. Zij legde uit hoe de storingen van de afgelopen tijd zijn ontstaan en welke maatregelen zijn getroffen om deze in de toekomst te voorkomen. Vanuit de zaal was er sterke behoefte aan meer transparantie en meer informatie over releases (changes, release notes) en de roadmap van SURFconext. Hier zal in de toekomst aan worden gewerkt.

- Download de slides van deze presentatie.

Update sterke authenticatie (Eefje van der Harst)

Hierna was Eefje van der Harst wederom aan het woord met een update rondom sterke authenticatie. Er kwamen wat vragen over de gebruikte 2e factor door SURFnet (Yubikey, Tiqr, SMS), bijvoorbeeld waarom niet is gekozen voor Google Authenticator. In de toekomst kunnen zeker extra middelen worden toegevoegd maar voorlopig is in de opstartfase voor deze 3 middelen gekozen. De presentatie eindigde met een demo van het uitgifteproces van een tweede factor, deels via een selfservice applicatie.

- Download de slides van deze presentatie.

SURFconext en autorisatie? (Ton Verschuren, m7)

Hierna is het woord overgedragen aan Ton Verschuren van m7. Ton heeft op verzoek van SURFnet verschillende instellingen geïnterviewd over de vraagstukken rondom autorisatie en attributen. De resultaten van deze interviews zijn door Ton gepresenteerd.

- Download de slides van deze presentatie.

SURFconext internationaal (Arnout Terpstra & Bas Zoetekouw)

Het ochtendprogramma sloot af met twee presentaties over internationale samenwerking via SURFconext. Als eerste presenteerde Arnout Terpstra het eduGAIN initiatief, en stipte daarbij enkele belangrijke overeenkomsten en verschillen met de nationale federatie SURFconext aan. De slides van deze presentatie zijn hier te vinden.

- Download de slides van deze presentatie.

Toen nam Bas Zoetekouw het woord over om de lancering van eduTEAMs aan te kondigen; een tool om op internationaal niveau groepen en samenwerkingsverbanden te definiëren. Deze tool is via eduGAIN voor alle geïnteresseerde Identity Providers beschikbaar.

- Download de slides van deze presentatie.

Middagprogramma

SURFconext en gastgebruik (Arnout van Velzen & Maarten Wegdam, Innovalor)

Na de lunch presenteerden Maarten Wegdam en Arnout van Velzen van Innovalor (voorheen: Novay) de resultaten van hun recente onderzoek naar gastgebruik. Welke gasten zijn er eigenlijk en hoe worden deze momenteel geadministreerd? Welke mogelijkheden biedt SURFconext om dit beter in te regelen? Tijdens de presentatie werden alle deelnemers gevraagd enkele vragen te beantwoorden om de voorlopige bevindingen van het onderzoek te toetsen. Innovalor zal de uitslag van deze vragen in het eindrapport worden verwerkt.

- Download de slides van deze presentatie.

Discussierondes

De rest van de middag stond in teken van interactieve discussierondes, waarbij dieper in bepaalde onderwerpen kon worden gedoken. Hieronder volgt een overzicht van de onderwerpen die aan bod kwamen en een korte samenvatting van wat er tijdens die sessie is besproken.

Gastgebruik (olv. Maarten Wegdam en Arnout van Velzen, Innovalor)

Innovalor heeft in opdracht van SURFnet een uitgebreid onderzoek gedaan naar de status van en uitdagingen bij gastgebruik binnen de instellingen en SURFconext. De verschillende groepen gastgebruikers die Innovalor heeft geïdentificeerd zijn voorinschrijvers, stagebegeleiders, bezoekers van (academische) bibliotheken en alumni. Tijdens de discussierondes kwam al snel naar voren dat het belangrijk is hierbij onderscheid te maken naar het type instelling. Mbo's verschillen van hbo's die weer verschillen van Universiteiten.

In de presentatie heeft Innovalor verschillende oplossingsrichtingen laten zien. Tijdens de discussierondes zijn vooral de voor- en nadelen van elke richting besproken. Het lijkt erop dat er in ieder geval niet één oplossingsrichting is die voor alle typen gastgebruik geschikt is.

De definities van de usecases werden ook bediscussieerd. Wanneer is iemand bijvoorbeeld een voorinschrijver? De suggestie in de discussiesessie is na betaling van collegegeld, je kunt dan echter ook nog van studie wijzigen. Daarbij werd gevraagd in hoeverre de definities in het afsprakenstelsel te standaardiseren zijn, wat in verband met internationale toegang (e.g. eduGAIN) wel belangrijk is. De instellingen willen misschien wel betalen voor gastgebruik, of wellicht willen of kunnen gebruikers hier zelf voor betalen.

Tijdens sessie 1 opperde iemand of je gasten niet context-based kunt identificeren; een interessant gegeven. Ondanks dat dit volgens de overeenkomsten niet is toegestaan, worden gastgebruikers soms al volgens oplossingsrichting 1 toegang verschaft via SURFconext. Hoewel werd opgemerkt dat oplossingsrichting 1 de digitale sleutelbos niet verkleint, zag men ook in dat een centrale gastaccount ook zijn beperkingen heeft.

Een vraag die werd gesteld is of de instellingen elkaars gastgebruikers ook zouden willen toestaan voor eigen lokale applicaties. De (technische) impact van oplossingsrichting 1 voor de instellingen lijkt mee te vallen, mede omdat dit niet verschilt van de huidige architectuur voor studenten en medewerkers.

Na uitleg van de inhoud van een mogelijke pilot, i.e. bestaande accounts voor voorinschrijvers ontsluiten via SURFconext, waren de reacties gematigd positief. De urgentie van gastgebruik is hoog genoeg voor verdere ondersteuning, bijvoorbeeld om niet te wachten op het eID-stelsel of een andere herbruikbare identiteit van buiten de sector.

Samengevat de achterban bevestigt de hier gepresenteerde conclusies, maar geeft iets meer nuance aan de usecases en voorziet de inrichting van attributen en autorisatie als belangrijke uitdaging.

Releasemanagement en platformarchitectuur (olv. Thijs Kinkhorst, SURFnet)

SURFconext streeft naar kleinere maar frequentere releases zodat de impact per keer ook kleiner is. Er is behoefte aan veel explicietere melding wat elke release nu precies wijzigt/oplevert, ook al is het niet per se enduser visible. Wijzigingen die wel end user visible zijn (veranderende interfaces) moeten juist langer dan een week van tevoren aangekondigd worden.

Eén instelling vraagt zijn functioneel beheerders die vinden dat SURFconext essentieel is, om zelf 's ochtends vroeg na onderhoud direct te testen zodat eventuele problemen direct helder zijn. Sommige instellingen die kritieke diensten aansluiten, vragen naar meer informatie over het creëren van een tweede inlogroute. Een instelling/dienstverantwoordelijke moet hierin zelf de afweging maken tussen extra flexibiliteit (bij storing SURFconext maar bijvoorbeeld ook als de uplink down is) en het extra werk en extra complexiteit die het met zich meebrengt. Het SURFconext-team staat overigens altijd open voor specifiek advies op maat over hoe een en ander in te richten, dus neem vooral contact met ons op voor vragen.

SURFconext Dashboard (olv. Frans Ward, SURFnet)

Tijdens de beide discussie rondes is vooral navraag gedaan welke verbeteringen er aan SURFconext Dashboard gedaan kunnen worden. Dit heeft input opgeleverd die we mee kunnen nemen in de roadmap voor doorontwikkeling.

De nieuwe interface van SURFconext Dashboard 2.0, die begin dit jaar is gelanceerd, is goed ontvangen, maar de volgende zaken kunnen beter: 'status licentie onbekend', komt nu veel te vaak voor en moet beter. We hebben aangegeven dat we hier rekening mee zullen houden bij het aanbrengen van een taxonomie (type licentie). We hebben hierbij input gekregen welke andere filteropties wenselijk zijn, zoals type dienst, voldoet aan HO-normenkader. etc.

Het opnemen van eduGAIN-diensten in SURFconext Dashboard wordt wel handig gevonden mits men dan wel kan zien uit welk land de dienstaanbieder komt.

Verder werd vooral aangegeven dat de statistieken duidelijker kunnen. Vooral wat betreft de informatie bij de assen van de grafieken. Men mist de oude staafdiagrammen overzicht die zo handig waren om uitgeprint te worden voor de management rapportages.

HO-normenkader & Q+A sessie SURFmarket (olv. Olga Scholcz en Raoul Teeuwen, SURFmarket)

Tijdens deze discussieronde is gesproken over de achtergrond van het HO-normenkader (Hoger Onderwijs Juridisch Normenkader Cloudservices), het belang ervan, hoe het tot stand gekomen is en hoe SURF het HO-normenkader (en onderdelen daaruit) verder aan het uitwerken is. De deelnemers aan de workshop hebben ons nuttige feedback gegeven.

Op de vraag hoe zij het liefst geïnformeerd zouden willen worden over het wel / niet HO-normenkader compliant zijn van een overeenkomst, gaven zij aan dit het liefst kort en bondig gepresenteerd te krijgen met daarbij de mogelijkheid tot het opvragen van een gedetailleerd overzicht. Ook hebben we vernomen dat het voor instellingen belangrijk is dat SURF op verschillende organisatieniveaus voor informatie over het HO-normenkader gaat zorgen. Dit zou eraan kunnen bijdragen dat de onderwerpen privacy en security binnen de instellingen hoger op de agenda komen te staan.

Mocht u vragen of opmerkingen hebben dan kunt u terecht bij Olga Scholcz (olga.scholcz@surfmarket.nl) of Raoul Teeuwen (Raoul.Teeuwen@surfmarket.nl).

- Download hier de slides die tijdens deze discussieronde zijn gebruikt.

Groepen en autorisatie (olv. Maarten Kremers, SURFnet)

Naast het federatief authenticeren (welke gebruiker logt in) leeft er bij instellingen de behoefte voor ondersteuning bij autorisatie en groepen in deze context (wat mag de gebruiker binnen een dienst en hoe kan ik gebruikers groeperen voor samenwerkingsomgevingen en autorisatievraagstukken). SURFnet werkt aan verdere voorlichting rondom autorisatie en groepenvraagstukken en is tevens aan het onderzoeken welke behoeften instellingen hebben met betrekking tot het faciliteren van autorisatie en groepen.

In de plenaire sessie zijn de eerste resultaten van dit onderzoek, uitgevoerd door Ton Verschuren, gepresenteerd. Tijdens deze discussiesessie is ingegaan op de resultaten hiervan en op de vraag welke onderdelen het meest van belang zijn.

Tijdens de discussesessies zijn de volgende onderwerpen aanbod gekomen:

Behoefte aan betere tooling voor gedistribueerde groepen, met als usecase dat een docent binnen een instelling zelf een op eenvoudige wijze groepen ("klassen, werkgroepen") kan definiëren binnen zijn instelling, en deze groepen op eenvoudige wijze kan (her)gebruiken als middel voor autorisatie in meerdere applicaties, zowel binnen de eigen campusapplicaties als cloudapplicaties.

Entitlements: deze attributen schalen tot een bepaald niveau, maar uiteindelijke zullen er bij te veel entitlements schalingsproblemen op treden. Zowel technisch (bijv. te lange verwerkingsduur), als procedureel binnen instelling (het zetten van entitlements voor kleine groepen mensen voor een bepaalde applicatie). Als oplossingsrichting is de mogelijkheid van het inzetten van meer flexibele gedistribueerde groepen (zie vorige onderwerp) en/of attribute authorities.

Een betere definiëring van het eduPersonAffiliation-attribuut. Dit attribuut geeft de relatie weer tussen de gebruiker en de instelling van de gebruiker, zoals "student" of "employee". Een SP kan/wil dit attribuut gebruiken voor een autorisatiebeslissing. Er is echter geen precieze definitie van wat elke waarde is. Dit is momenteel ter discretie van de individuele IdP, waardoor verschillen optreden (is een contractstudent bijv "student"?). Vanuit de discussiesessie kwam het verzoek aan SURF om, in ieder geval voor Nederland, hier een meer sluitende definitie voor op te stellen i.s.m. de instellingen.

SURFspot (olv. Hans-Peter Ligthart, SURFmarket)

Veel deals bij SURFspot komen tot stand door centrale onderhandelingen met commerciële aanbieders ten behoeve van de hele onderwijsmarkt. Hierdoor ontstaat een aanbod dat scherper is dan wat de markt aanbiedt. Je kunt educatielicenties ook bij Adobe kopen, maar bij ons zijn ze voordeliger. Dat komt enerzijds door de volumecontracten en anderszijds door afspraken voor thuisgebruik binnen de campusovereenkomst van de onderwijsinstelling. Geen onderwijsinstelling = geen aanbod.

Waarom zie je na inloggen bij SURFspot niet je naam of e-mailadres? ARP staat voor Attribute Release Policy. Met andere woorden welke gegevens ontvangt SURFspot van je instelling na het inloggen. SURFconext zorgt voor federatieve authenticatie, zodat gebruikers met hun instellingsaccount veilig toegang hebben tot SURFspot. SURFconext heeft voor elke dienst (Service Provider; SP) en instelling (Identity Provider; IdP) een contract. In dat contract worden afspraken gemaakt over de informatie die een dienst ontvangt en wat deze dienst met die informatie mag doen. SURFspot is een dienst aangesloten op SURFconext. Om SURFspot te laten functioneren hoeven we alleen te weten of degene die inlogt, werkt of studeert bij een aangesloten instelling. Bovendien hanteert SURFconext het principe van "minimal disclosure". Een dienst krijgt alleen die informatie die strikt noodzakelijk is om de dienst aan de klant te kunnen verlenen. Hieruit wordt een Attribute Release Policy (ARP) vastgesteld. De ARP voor SURFspot is dusdanig ingesteld dat wij geen gegevens meekrijgen van de instellingsdatabase. Eindgebruikers moeten zelf aangeven wie ze zijn en op welk e-mailadres ze de producten willen ontvangen. Hiervoor kunnen en mogen wij dus geen gegevens van de instelling gebruiken. SURFspot gebruikt de attributen affiliation en organization om het specifieke aanbod te kunnen tonen. Alleen gebruikers met affiliation employee of student krijgen toegang tot SURFspot.

SURFconext internationaal (olv. Niels van Dijk, SURFnet)

N.a.v. de presentatie over eduGAIN kwam al gauw een praktijkvoorbeeld naar voren, van een Service Provider die momenteel contractonderhandelingen met SURFmarket voert, maar ook reeds beschikbaar is via eduGAIN (lynda.com). Wat betekent dit precies? Stel dat de onderhandelingen met SURFmarket niet worden afgerond, kan een Identity Provider dan alsnog gebruik maken van de dienst, via eduGAIN? Dat is uiteraard mogelijk, maar dan moet de Identity Provider wel beseffen dat de strenge eisen van de SURFconext-federatie niet automatisch gelden. Het is ook denkbaar dat SURFmarket of de Identity Provider zelf onderhandelt met de Service Provider over licenties en voorwaarden, terwijl de technische koppeling via eduGAIN loopt. Dit staat dus los van elkaar (technische koppeling vs. administratieve afspraken).

Daarnaast is het onderwerp dataprotectie uitgebreid besproken. Waar iedere federatie wel duidelijke afspraken maakt over de voorwaarden waar je als partij aan moet doen om lid te worden van de federatie (noot: deze afspraken zullen per federatie verschillen), geldt dit niet voor dataprotectie. De wetten op het gebied van privacy en informatiebeveiliging kunnen per land sterk uiteenlopen. Daarom is de GÉANT Data Protection Code of Conduct in het leven geroepen. Dit document bevat principes voor dataprotectie gebaseerd op de Europese wetgeving. Service Providers die hieraan voldoen hebben dataprotectie op eenzelfde niveau ingeregeld.

De Code of Conduct bevat echter geen principes over Level of Assurance (LoA). Wellicht dat eduGAIN in de toekomst uitgebreid kan worden om ook sterkere authenticatie op internationaal vlak te ondersteunen.

Als laatste kwam voorbij dat eduGAIN het beste vergeleken kan worden met een telefoonboek (wie kan ik waar vinden), en niet met een centraal technisch koppelvlak (zoals SURFconext).

Tot slot

Afsluitend gaf Eefje van der Harst een overzicht van de roadmap van SURFconext in 2015. Deze slide is te vinden in deze presentatie.

De volgende What's Next @ SURFconext meeting zal in het najaar van 2015 worden gehouden. Het is gebleken dat de ruimte in het kantoor van SURF niet groot genoeg is om voor iedereen plaats te bieden. We zullen daarom bekijken of we beter kunnen uitwijken naar een andere locatie, met meer capaciteit. Wordt vervolgd dus!