Discussierondes Seminar What's next@SURFconext 16 juni 2014

Hieronder staan de samenvattingen en opvallende punten die tijdens de discussierondes met het SURFconextteam en SURFconextcontactpersonen naar voren kwamen. Sommige punten kwamen in meerdere discussieonderwerpen naar voren en zullen dus vaker genoemd worden.

Er zijn veel vragen over wie SURFconext mogen gebruiken. De huidige policy (geen alumni, voorinschrijvers, externe beheerders etc) is in de praktijk vaak niet werkbaar. Dit punt gaan we op korte termijn bespreken binnen SURFnet en we willen onderzoeken wat de mogelijkheden zijn.

Dit document zal worden gedeeld met alle deelnemers, SURFmarket en SURFnet (SURFconext exploitatie, innovatie, stuurgroep en de account adviseurs).

Diensten afnemen - Eefje van der Harst
- een enkele instelling heeft (ondanks de gepresenteerde moeilijkheden) toch behoefte aan opt-out
- observatie instelling: eigenlijk gek dat SURFnet/ SURFmarket zich dmv licentie-check bemoeien met 'autorisatie'. Waarom die verantwoordelijkheid niet gewoon bij SP beleggen?
- er moet een oplossing komen voor gebruik SURFconext door voorinschrijvers/ alumni/ gasten/ library walk in users
- 2 contactpunten SURFnet-SURFmarket in aansluitproces is onhandig
- onduidelijkheid over wat handig is als je enige afnemer van een SP is; koninklijke route via SURFmarket? Of IdP kan zelf als SP optreden. Situatieafhankelijk, dus overleg met SURFconext team als daar vragen over zijn

Technische vragen - Pieter van der Meulen
- In twee sessies vragen over single logout. Waarom wordt dat niet ondersteund? Uitgelegd waarom het mechanisme wat in SAML beschreven staat breekbaar is en dat een niet betrouwbare oplossing met als gevolg foutmeldingen en toch ingelogd blijven ons inziens erger is dan het kwaad van het advies de browser helemaal af te sluiten. Alternatieve oplossing besproken. Het idee van een browser plugin die bijhoudt welke authenticatie cookies de browser bezit, welke site daarbij hoort en hoe je hier uit kunt loggen werd goed ontvangen. Idee voor innovatie- of afstudeeropdracht.

- Discussie over SAML koppeling Sharepoint. Sharepoint spreekt geen SAML maar WIF. Een ADFS server is de gebruikelijke oplossing om WIF te vertalen naar SAML. Voor SURFconext kan een ADFS IdP niet ook gebruikt worden om een Sharepoint te koppelen. Door instellings IT policies werd één extra ADFS server er vier: een dubbel uitgevoerde ADFS server+proxy. De aanwezigen gebruikten Sharepoint vooral voor zelf ontwikkelde sites, dat schept mogelijkheden om een alternatieve methode van koppelen te onderzoeken. Aan zelfontwikkelde software is het eenvoudiger wijzigingen te maken dan aan commerciële of kant-en-klare producten.

- Aantal SimpleSAMLphp IdP vragen van instellingen:
* Moeten wij ook nog wat down voor Heartbleed? Twee instellingen moesten zelf nog secrets moesten vervangen.
* Inlogscherm geschikt voor mobiel gebruik: Staat op onze wiki - https://wiki.surfnet.nl/display/surfconextdev/Richtlijnen+loginschermen

Rich Clients - Joost van Dijk
Drie richtingen om met het probleem om te gaan.

A vrijgeven credentials aan SPs (geen federatie dus: scenario Office 365)
B uitdelen extra credentials aan gebruikers (workaround a la Google's application specific passwords)
C wachten tot technologie toereikend is ("niets doen" totdat er iets is wat wel werkt, bv alles HTML5, moonshot, SAML ECP, etc)

Op dit moment: geen echte oplossing voorhanden, alleen workarounds

Beste workaround hangt af van specifieke dienst:
- deprovisioning vereist? (probleem voor B)
- welke mogelijkheden tot externe ww verificatie (bij A)

Beste workaround hangt af van IdP:
- credential sharing acceptabel voor sommige SPs (A), voor andere niet

En ook:
soms probleem niet groot genoeg voor bepaalde toepassingen (C). Beste benadering van het probleem is een afweging tussen security en usability

Is usability belangrijker?
Bij de deelnemers sloeg de balans vaker uit naar "security boven usability"

SURFconext Dashboard - Ivo Reints

Toegang:
Veel de vraag voor toegang tot SURFconext Dashboard. De vraag kwam onder andere van een beheerder van de ldap. Het verzoek om attributen komt nu uit tweede hand en hij kan niet verifiëren of dit correct is. Ook support van een instelling kan er niet bij terwijl er op de app pagina informatie staat die van belang is zoals e-mailadres, link naar de faq, etc. Waarom Dashboard niet voor iedereen toegankelijk maken? De ICP van de instelling kan collega's al een rol geven (SURFconext beheerder) waarmee deze gebruiker read-only rechten krijgt in het SURFconext Dashboard:
https://wiki.surfnet.nl/display/surfconextdev/Beschikbare+diensten+activeren#Beschikbarediensten activeren-Ondersteuning

SURFmarket:
Er is geen directe koppeling van een dienst naar de licentiepagina bij SURFmarket. Informatie over wie de licentiecontactpersoon(LCP) is ontbreekt nu. Licentie informatie is onduidelijk. Dit zal mee worden genomen bij de doorontwikkeling van het SURFconext Dashboard.

Statistieken:
De wens om de beschikbaarheid per dienst weer te geven. Dit zal erg lastig te realiseren zijn, omdat we alle diensten dan ook actief moeten gaan monitoren of dat we deze cijfers van alle diensten moeten ontvangen. De vraag is dan ook of dit echt de beschikbaarheid weergeeft. Dit is niet iets wat op de roadmap staat op dit moment.

Aanbod:
Diensten die op stapel staan om aangeboden te gaan worden eerder tonen of via ander weg kenbaar maken. "Binnenkort verwacht" Rubriceren van diensten op functie zoals op http://www.surf.nl/diensten-en-producten/surfconext/op-surfconext-aangesloten

diensten/index.html Hierop en op dienst en aanbieder kunnen zoeken. Overzicht op SURFconext(bovenstaande url) komt niet overeen met het aanbod in Dashboard. Bij het verzoek van bv een LCP om attributen vrij te geven is het vaak zoeken in Dashboard over welke dienst het nu precies gaat. We zullen betere zoekmogelijkheden meenemen in de doorontwikkeling.

Overig:

- Mogelijkheid om informatie uit te wisselen met andere instellingen die dezelfde services gebruiken.
- Laten zien welke instellingen welke diensten gebruikt.
- Wens van gebruikers doorgeven dat er interesse bestaat in een service. Dit kan nu al via de WAYF alleen komt dit niet bij de instelling uit.
- Mogelijkheid om in dashboard attributen toe te kunnen voegen.
- Overzicht van eigen aangeboden diensten.
- Proefperiode/testkoppeling mogelijk voor een beperkte tijd om een product te kunnen proberen. SURFmarket gaf aan dat dit veelal mogelijk is maar dan direct via de leverancier zonder gebruik van SURFconext.
- Mogelijkheid van een alert via mail is wenselijk maar dan wel instelbaar om het per bulk of per onderdeel te ontvangen.

Autorisatie - Bas Zoetekouw

De discussies draaien rond de volgende drie punten:
Wie heeft er toegang tot SURFconext?
Veel instellingen worstelen met het geven van toegang van niet- en semi-studenten tot hun IAM-systemen en SURFconext. Specifiek aan de orde komen de volgende groepen:
- externe beheerders
- alumni
- prospects (studenten die zich inschrijven en al voor de inschrijving start toegang moeten krijgen tot een beperkte set systemen)
- numerus-fixus studenten in een decentrale selectie (moeten voor de decentrale selectie toegang hebben tot een set diensten)

Formeel mogen al deze groepen nu geen toegang krijgen tot SURFconext, maar deze policy lijkt in de praktijk onhoudbaar.

Toegang tot dienst beperken
Een aantal instellingen heeft de behoefte om (op basis van een IdP-attribuut of een groepslidmaatschap) toegang tot diensten te beperken. Dit ook met het oog op het vorige punt.

Duidelijkheid over attributen
Er lijkt grote behoefte aan een duidelijker kader vanuit SURFconext over hoe en welke attributen doorgegeven kunnen worden aan diensten, zodat die op basis daarvan ook zelf autorisatie kunnen regelen. Er is ook behoefte aan meer generieke attributen (bv, studierichting, faculteit) dan SURFconext nu ondersteunt.

SURFconext Roadmap - Femke Morsch

Kortere termijn
Er waren veel vragen over toegang tot diensten via SURFconext voor bijvoorbeeld voorinschrijvers en alumni.

Instellingen zijn zoekende hoe ze met voorinschrijvers om moeten gaan. Als een assessmenttool voor voorinschrijvers gekoppeld kan worden aan SURFconext, dan

moeten deze mensen ook in kunnen loggen via SURFconext. SURFnet gaat kijken of we dit kunnen toestaan.

Het was ook nog niet bij iedereen duidelijk wat er allemaal mogelijk is met attributen. In SURFconext wordt een standaardset aan attributen gebruikt, maar er is ook een attribuut (entitlement) waar "vrije" waardes in kunnen komen te staan. Hierover zal wel altijd een afspraak moeten worden gemaakt met de Service Provider. Op het moment dat meerdere instellingen hetzelfde attribuut willen gaan inzetten (bijvoorbeeld voorinschrijver), dan zullen we dit gezamenlijk moeten afstemmen. SURFnet zal kijken hoe we dit kunnen gaan vormgeven. Meer informatie over attributen en SURFconext: https://wiki.surfnet.nl/display/surfconextdev/Attributen+in+SURFconext

Alumni mogen nu niet van SURFconext gebruik maken, maar een aantal diensten achter SURFconext staan dit wel toe. Dit is in de praktijk niet altijd handig. Het is bijvoorbeeld mogelijk om iemand via een attribuut aan te merken als alumni en Service Providers zouden deze mensen eruit kunnen filteren als deze geen toegang zouden mogen hebben. Op dit moment verwachten Service Providers alleen dat ze nooit een alumni aangeboden zullen krijgen en zullen ze deze filtering misschien niet doen. Op het moment dat er besloten wordt dat alumni wel gebruik mogen maken van SURFconext, zullen alle contracten moeten worden aangepast en zal iedereen binnen de SURFconextfederatie hiervan op de hoogte moeten worden gesteld.

Direct kwam de vraag of SURFconext deze filtering niet kan doen. Ook dit is technisch mogelijk, maar we zullen ons wel af moeten vragen of dit wenselijk is. De meningen van de deelnemers waren verdeeld: SURFconext moet filtering gaan toepassen tot SURFconext moet helemaal niks filteren en alles aan de Service Provider overlaten. Dit is ook een van de onderwerpen (autoristatie) die op de SURFconext roadmap staat.

<u>Lange termijn</u>
Op lange termijn zullen studenten en medewerkers vaker hun eigen ID mee gaan nemen. Dit kan een overheidsID of social ID zijn. Deze identiteit moet kan dan verrijkt worden met attributen vanuit andere bronnen. SURFnet is betrokken bij het eID stelsel, maar naar verwachting zal het nog even duren voordat we dit echt kunnen inzetten.