Webinar AVG en SURFconext

HET WEBINAR BEGINT OM 12:30

Floortje Jorna, Arnout Terpstra, Raoul Teeuwen
Techniek: Teun Fransen. Communicatie: Jitse Schipper

SURF

Agenda

SURF CONEXT

Tips:

- de link naar de slides staat in de beschrijving van de opname van dit webinar – handig voor links
- zet het beeld schermvullend
- vragen mogen via YouTube of de wiki (https://wiki.surfnet.nl/display/FORUM/Privacy+related+discussions)
- disclaimer: geen juridisch advies, nuances ontbreken…

Agenda

1. De AVG en SURFconext: van aansluiten tot gebruik:
   a) De AVG en SURFconext bij het aansluiten van een nieuwe SP
   b) De AVG, SURFconext en de instelling
   c) De AVG, SURFconext en de gebruiker
2. Wat moet de instelling zelf nog doen?
3. Wat doet het SURFconext team aan de AVG?
4. Vragen
5. Handige links

SURF CONEXT

Tips:

- de link naar de slides staat in de beschrijving van de opname van dit webinar – handig voor links
- zet het beeld schermvullend
- vragen mogen via YouTube of de wiki (https://wiki.surfnet.nl/display/FORUM/Privacy+related+discussions)
- disclaimer: geen juridisch advies, nuances ontbreken…

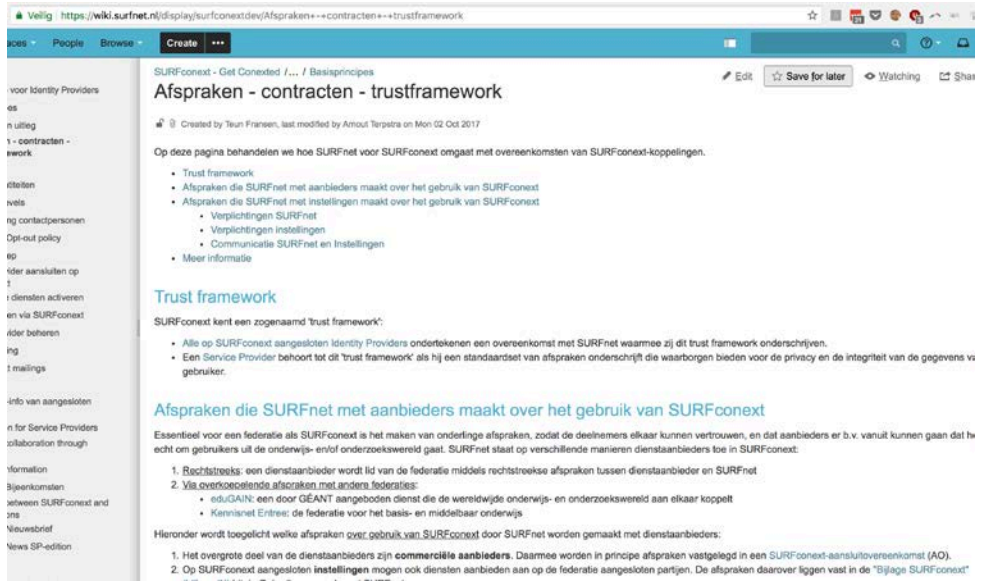
SURF

1a - De AVG en SURFconext bij aansluiten van nieuwe SP

Waar we op letten bij aansluiten van een nieuwe leverancier

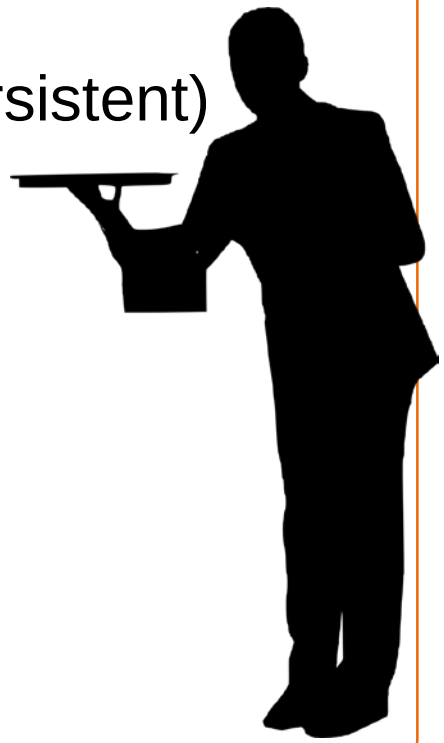
1a - De AVG en SURFconext, nieuwe SP: afspraken

- Federatie=
  1. Afspraken > overeenkomsten
  2. Techniek
- SURFnet maakt afspraken met instellingen
- SURFnet maakt afspraken met leveranciers



1a - De AVG en SURFconext, nieuwe SP: techniek

- Hoe minder (persoons)gegevens een SP heeft, hoe minder zorgen hij/zij heeft
- Federatieve authenticatie helpt:
  - geen wachtwoorden bij de SP
  - SURFconext kan pseudonieme identifiers doorgeven (transient/persistent)
  - 26 juni a.s. apart webinar!



Wat is een identifier in de context van SURFconext?

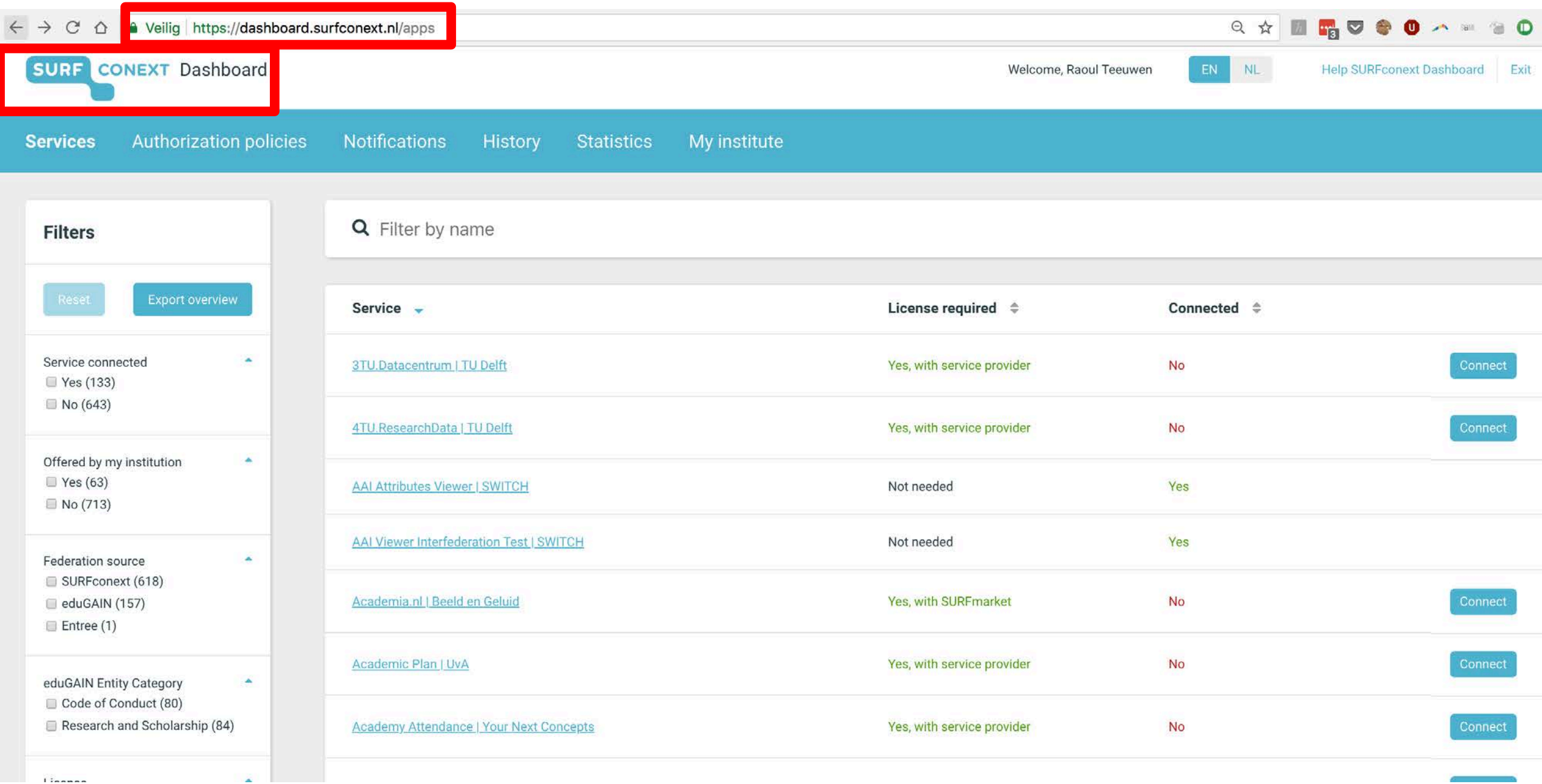
- Een “string” die een gebruiker identificeert
  - Bijvoorbeeld:
    - geesink@surfnet.nl
    - 2f2d5ed231d2c276f5f36209332e3d5c1c0f8954
    - urn:collab:person:surfnet.nl:geesink

Privacy-vriendelijk

1b - De AVG, SURFconext en de instelling

Welke handige dingen op gebied van de AVG biedt SURFconext instellingen?

1 - Attributen van aangesloten diensten


Veilig | https://dashboard.surfconext.nl/apps
SURF CONEXT Dashboard
Welcome, Raoul Teeuwen
EN
NL
Help SURFconext Dashboard
Exit
Services
Authorization policies
Notifications
History
Statistics
My institute
Filters
Reset
Export overview
Service connected
Yes (133)
No (643)
Offered by my institution
Yes (63)
No (713)
Federation source
SURFconext (618)
eduGAIN (157)
Entree (1)
eduGAIN Entity Category
Code of Conduct (80)
Research and Scholarship (84)
Filter by name
Service
License required
Connected
3TU.Datacentrum | TU Delft
Yes, with service provider
No
Connect
4TU.ResearchData | TU Delft
Yes, with service provider
No
Connect
AAI Attributes Viewer | SWITCH
Not needed
Yes
AAI Viewer Interfederation Test | SWITCH
Not needed
Yes
Academia.nl | Beeld en Geluid
Yes, with SURFmarket
No
Connect
Academic Plan | UvA
Yes, with service provider
No
Connect
Academy Attendance | Your Next Concepts
Yes, with service provider
No
Connect

Overview

License

Attributes

Used by

Deactivate service

Attributes

The following attributes will be exchanged wit SURFdashboard | SURFnet. Please note: All attributes should contain the right value(s). If attributes are missing, additional steps might be needed to ensure a working connection.

Attribute	Your value*
urn:mace:dir:attribute-def:uid	raoul
urn:mace:dir:attribute-def:sn	Teeuwen
urn:mace:dir:attribute-def:mail	raoul.teeuwen@surfnet.nl
urn:mace:dir:attribute-def:givenName	Raoul
urn:mace:terena.org:attribute-def:schacHomeOrganization	surfnet.nl

* The attributes and their values for your personal account are displayed. This might not be representative for other accounts within your organization.

Veilig | https://dashboard.surfconext.nl/apps

SURF CONEXT Dashboard

Welcome, Rac

Services | Authorization policies | Notifications | History | Statistics | My institute

Filters

Reset | Export overview

Service connected
- [x] Yes (133)
- [ ] No (643)

Offered by my institution
- [ ] Yes (53)
- [ ] No (80)

Filter by name

Service	License required
AAI Attributes Viewer | SWITCH	Not needed
AAI Viewer Interfederation Test | SWITCH	Not needed
ADP Online | ADP	Yes, with service provider
Bandwidth On Demand (Acceptatie) | SURFnet	Not needed

1b - De AVG, SURFconext en de instelling

Welke handige dingen op gebied van de AVG biedt SURFconext instellingen?

2 – Antwoorden op AVG-gerelateerde vragen

SURFconext - Get Conexted / Get Conexted / Documentatie voor Identity Providers

AVG/GDPR-info van aangesloten diensten

Created by Raoul Teeuwen, last modified on Mon 23 Apr 2018

Sinds medio 2017 vraagt SURFnet leveranciers, die op SURFconext willen aansluiten of waarvan de overeenkomst verloopt en verlengd moet worden, informatie op gebied van beveiliging en privacy aan te leveren. Informatie die belangrijk is in het kader van de nieuwe AVG/GDPR. Voor instellingen kan dit helpen bij de vraag: wil ik met die leverancier gesprekken aangaan over afname van de dienst. Antwoorden van leveranciers die dit al hebben aangeleverd zijn hieronder te vinden. In de loop van 2018 zal deze informatie in het SURFconext dashboard worden getoond (waarna deze pagina vervalt).

SURFnet controleert die informatie niet. Indien een instellingen gesprekken aangaat, raden we aan de informatie te verifiëren. Meer informatie over privacy en SURFconext vindt u op Privacy .

Heeft u vragen? Mail ons dan op support@surfconext.nl .

	Leverancier	Dienstnaam	AVG/GDPR informatie	Waar is de overeenkomst in te zien of op te vragen?	Versie
1	theFactor.e	Bloomreach Experience	VragenVoorSPsVoorAO2017-3-7_bloomreach_Experience.docx	SURFconext-gebruik is geregeld in een SURFconext aansluitovereenkomst, zie Contractual part	AO 2017-v1.03
2	Yard Internet	Acta Zorgnet	VragenVoorSPsVoorAO2017-3-6_Acta zorgnet-1.docx	SURFconext-gebruik is geregeld in een SURFconext aansluitovereenkomst, zie Contractual part	AO 2017-v1.03
3	Drieam	OER-Write	20171023 VragenVoorSPsVoorAO2017-3_DrieamOERWRITE.docx	SURFconext-gebruik is geregeld in een SURFconext aansluitovereenkomst, zie Contractual part	AO 2017-v1.03
4	Talking Telecom Technologies B.V.	HiHaHo Video Enrichment	VragenVoorSPsVoorAO2017-3 ingevuld HiHaHo.pdf	SURFconext-gebruik is geregeld in een SURFconext aansluitovereenkomst, zie Contractual part	AO 2017-v1.02
5	Brainstud B.V.	Brainstud eLearning	VragenVoorSPsVoorAO2017_brainstud.pdf	SURFconext-gebruik is geregeld in een SURFconext aansluitovereenkomst,	AO 2017-v1.02

SURFconext connection agreement - GDPR related questions

Fuelled by the General Data Protection Regulation, institutions have started asking certain privacy related questions about services connected to SURFconext. To prevent lots of mails, SURFnet requests the Service Provider to fill out the below questions. These will be published to provide Institutions basic GDPR related information. SURFnet plans to release an online dashboard at the end of 2017, so a Service Provider can maintain this information online. Until that moment we collect the information via this document.

Question	Answer
What kind of (personal) data is processed in the service? If you process 'Sensitive Personal Data' as mentioned in the GDPR, explicitly mention what type of data exactly.	This application provides a workflow to write Onderwijs- en Examenregelingen (OER). These documents do not contain any personal information and they will be provided to every student by the schools.
For the attributes you request via SURFconext: why do you *need* each of them/why can't you do without them?	Full name: will be shown with comments and as the writer of a document / paragraph. Email address: only used for authentication purposes and notifications.
What organisations have access to the data? Your own company? What parties you contracted?	All data will be stored in the Netherlands at TransIP. Only DevOps and our core developers have access to the production database.
Which individuals or job roles have what (read, write...) access to the user data? We assume you are limiting access. Consider both within your company as well as third parties you use.	Driem—DevOps: read and write Driem—Core developers: read and write TransIP—Engineers: physical access to the servers
In which country/countries does the data reside? Also consider any copies.	The Netherlands
List all security measures you have taken to secure the data? Also think about any encryption (during transport, in rest).	- Web service enforces HTTPS - Driem can access the servers via SSH with public key authentication - Data is stored at TransIP (The Datacenter Group), access to the servers is restricted to authorized personnel.
Can you provide a certificate like ISO27001, ISO27002, ISAE 3402 etc, including a Statement of applicability?	- No, OER Write doesn't process personal information except for the name and email address.
	- The Datacenter Group has multiple certificates: ISO 9001, ISO 27001, ISO 14001, NEN 7510.
Are you prepared to sign the SURF example Data Processing Agreement (https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2016/processing-agreement-english-october-2016.pdf), and if not, which articles would you want to discuss/negotiate with an institution interested in your service?	Yes
What is the URL of your privacy policy?	–

1b - De AVG, SURFconext en de instelling

Welke handige dingen op gebied van de AVG biedt SURFconext instellingen?

3 – Argumenten van SP’s om attributen te vragen

coin:attr_motivation:displayName	Used to display the users name within our application
coin:attr_motivation:eduPersonAffiliation	Determine permissions for the user and grant permissions within our application
coin:attr_motivation:eduPersonScopedAffiliation	Determine permissions for the user and grant permissions within our application
coin:attr_motivation:eduPersonTargetedID	Used to uniquely identify the user
coin:attr_motivation:givenName	Used to display the users name within our application
coin:attr_motivation:mail	Used for email notifications, usage data and to grant permissions within our application
coin:attr_motivation:uid	Used to uniquely identify the user

1b - De AVG, SURFconext en de instelling

Welke handige dingen op gebied van de AVG biedt SURFconext instellingen?

4 – Toegang beperken

SURFconext-diensten beschikbaar maken voor een beperkte groep gebruikers

Bas Zoetekouw

authenticatie, autorisatie, clouddiensten, identity provider, SURFconext, SURFconext groepen

06 MRT 2017

Vorige post Volgende post

Hoewel veel diensten die een instelling via SURFconext afneemt voor alle gebruikers van een IdP beschikbaar moeten zijn, kunnen er ook diensten worden gekoppeld die slechts voor een beperkte set gebruikers zijn bedoeld. Er kunnen verschillende redenen zijn om dit te doen, bijvoorbeeld:

- licentieoverwegingen; op deze manier kan een instelling een dienst afnemen voor een beperkte groep gebruikers (bijvoorbeeld alleen medewerkers, of alleen leden van een bepaalde faculteit);
- afscherming van gevoelige diensten; het koppelen van bijvoorbeeld beheerstools via SURFconext vermijdt het hergebruik van wachtwoorden en geeft het voordeel van single log-on; maar het is niet de bedoeling om alle gebruikers van een instelling toegang te geven;

Op deze blog beschrijf ik hoe een dienst die via SURFconext is gekoppeld, is af te schermen zodat gebruik van de dienst is beperkt tot een beperkte groep gebruikers van een instelling (bijvoorbeeld alleen studenten, of alleen medewerkers van een specifieke faculteit).

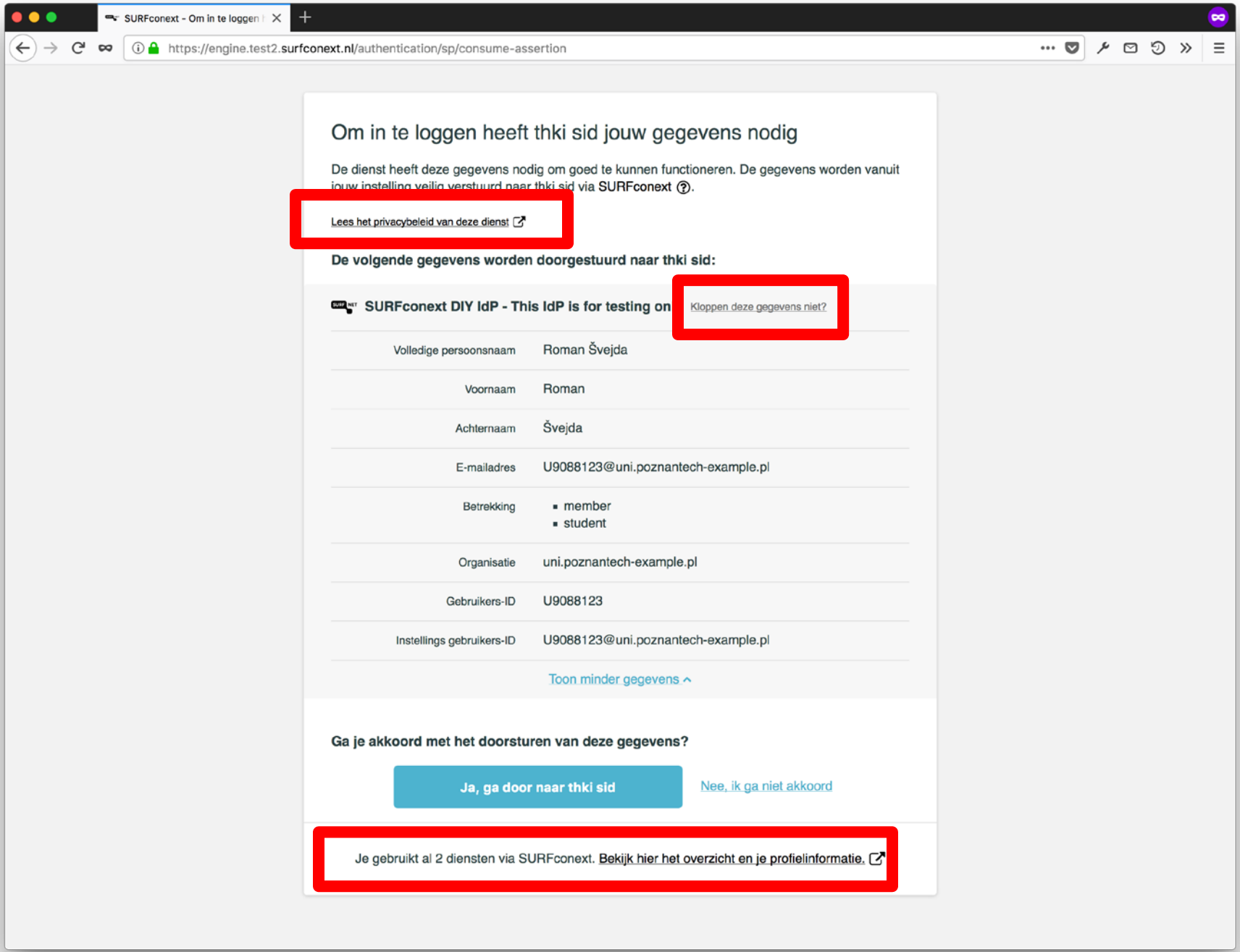
Er zijn verschillende mogelijkheden om een dergelijke afscherming te bereiken. Hieronder beschrijf ik de drie meest gebruikte methodes.

Op basis van provisioning

1c - De AVG, SURFconext en de gebruiker

Informeren van gebruikers

De informatiepagina over vrijgeven van informatie
(geen consent)


SURFconext - Om in te loggen
https://engine.test2.surfconext.nl/authentication/sp/consume-assertion
Om in te loggen heeft thki sid jouw gegevens nodig
De dienst heeft deze gegevens nodig om goed te kunnen functioneren. De gegevens worden vanuit jouw instelling veilig verstuurd naar thki sid via SURFconext.
Lees het privacybeleid van deze dienst
De volgende gegevens worden doorgestuurd naar thki sid:
SURFconext DIY IdP - This IdP is for testing on
Kloppen deze gegevens niet?
Volledige persoonsnaam
Roman Švejda
Voornaam
Roman
Achternaam
Švejda
E-mailadres
U9088123@uni.poznantech-example.pl
Betrekking
member
student
Organisatie
uni.poznantech-example.pl
Gebruikers-ID
U9088123
Instellings gebruikers-ID
U9088123@uni.poznantech-example.pl
Toon minder gegevens
Ga je akkoord met het doorsturen van deze gegevens?
Ja, ga door naar thki sid
Nee, ik ga niet akkoord
Je gebruikt al 2 diensten via SURFconext. Bekijk hier het overzicht en je profielinformatie.

1c - De AVG, SURFconext en de gebruiker

Informeren van gebruikers

De profile pagina

SURFnet bv [NL] https://profile.surfconext.nl

Overzicht van jouw SURFconext-profiel

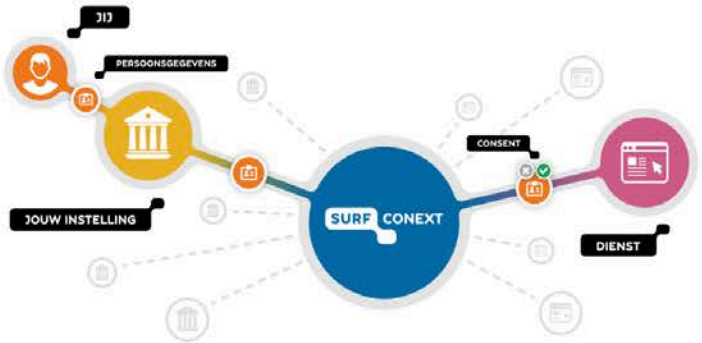
EN NL

Introductie | Mijn profiel | Mijn diensten | Mijn SURFconext | Mijn koppelingen

De profielpagina van SURFconext

Wat is SURFconext?

Jouw instelling gebruikt SURFconext zodat je met jouw instellingsaccount kunt inloggen op verschillende (cloud)diensten. Zo heb je maar één inlogaccount nodig en hoef je niet overal een apart gebruikersaccount aan te maken. Het volgende plaatje toont een schematische weergave van wat SURFconext doet:



Wat kun je op deze profielpagina?

Op verzoek van jouw instelling geeft SURFconext een beperkt aantal persoonsgegevens door aan de dienst waar je inlogt. Soms gaat dit automatisch bij het inloggen, in andere gevallen moet jij vooraf expliciet toestemming geven voor de doorgave van jouw gegevens. Deze profielpagina geeft je inzicht in welke persoonlijke data, afkomstig van jouw instelling, via SURFconext aan welke dienst wordt doorgegeven. Ook kun je zien welke gegevens door SURFconext worden opgeslagen en bij welke diensten je in het verleden bent ingelogd via SURFconext.

Deze dienst is verbonden via SURFconext

EN NL

Help Gebruiksvoorwaarden

Informatie van jouw instelling

De tabel hieronder biedt een overzicht van de persoonsgegevens die door jouw instelling via SURFconext kunnen worden doorgegeven aan diensten. In SURFconext worden jouw persoonsgegevens "attributen" genoemd. Een attribuut kan bijvoorbeeld je naam, e-mailadres of de naam van jouw instelling zijn. Voor technische informatie over deze attributen heeft SURFconext een aparte informatiepagina ingericht: Attributen in SURFconext.

Op het tabblad "Mijn SURFconext" kan je zien welke attributen en gegevens SURFconext zelf opslaat.

Let op: jouw instelling is verantwoordelijk voor de persoonsgegevens die je hier ziet. SURFconext laat slechts de informatie zien zoals ontvangen van jouw instelling. Heb je vragen over je persoonsgegevens? Neem dan contact op met je instelling via: urfnet.nl.

Attribuut	Waarde
Volledige persoonsnaam	Raoul Teeuwen
Achternaam	Teeuwen
Voornaam	Raoul
Weergavenaam	Raoul Teeuwen
Betrekking	employee
Gebruikers-ID	raoul
E-mailadres	r surfnet.nl
urn:mace:dir:attribute-def:mobile	+31641
Gebruikers-ID bij de instelling	raou
Recht	urn:x-surfnet: ed.com:vclounge: ers urn:mace:ter onal-user urn:x-surfnet:surf
Organisatie	surfnet.nl
Organisatielidmaatschap	urn:collab:org:su
Identifier	urn:collab:person:surfnet.nl:r

SURFnet bv [NL] | https://profile.surfconext.nl/my-services

Overzicht van jouw SURFconext-profiel

EN

Introductie | Mijn profiel | Mijn diensten | Mijn SURFconext | Mijn koppelingen

Diensten via SURFconext

Dit overzicht toont alle diensten waar je tenminste één keer op bent ingelogd via SURFconext. Ook kun je zien welk deel van jouw persoonsgegevens (attributen) vanuit jouw instelling naar de dienst is doorgestuurd. Daarnaast zie je of jij zelf of jouw instelling toestemming heeft gegeven voor het doorsturen van jouw attributen:

- Toestemming door jou: bij een aantal diensten wordt vooraf aan de eerste keer inloggen, expliciet gevraagd om toestemming voor het doorgeven van een aantal persoonsgegevens.
- Toestemming door instelling: bij sommige diensten wordt niet expliciet toestemming aan jou gevraagd, maar worden de gegevens automatisch doorgegeven na inloggen. In deze gevallen heeft jouw instelling bepaald dat jouw expliciete toestemming niet nodig is.

› Google Apps.surfnet.nl | Google

› http://adfs.geant.org/adfs/services/trust

› CRM & Sharepoint

⌄ Edugroepen | 2AT BV

E-mailadres support: [redacted]
Toestemming gegeven door: gebruiker
Voor het eerst gebruikt op: 2016-06-14 05:11

Deze dienst ontvangt de volgende gegevens over jou:

Attribuut	Waarde
Gebruikers-ID bij de instelling	rad[redacted]

› https://ap[redacted]/

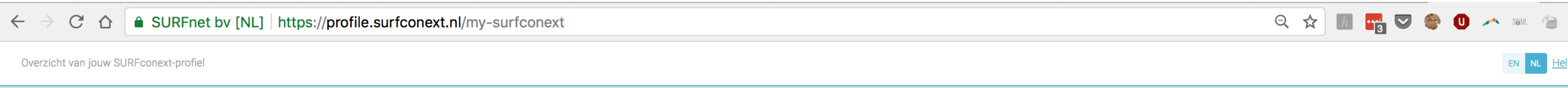
› https://at[redacted]ai.switch.ch/interfederation-test/shibboleth

› https://at[redacted]ai.switch.ch/shibboleth

› https://au[redacted]omation.surf.net/shibboleth

› https://au[redacted]fconext.nl/shibboleth

› https://au[redacted].nl/shibboleth



Introductie Mijn profiel Mijn diensten Mijn SURFconext Mijn koppelingen

Details van jouw SURFconext-profiel

SURFconext slaat gegevens op om je eenvoudig en veilig in te kunnen laten loggen bij verschillende (cloud)diensten en om jou inzicht te geven waar je allemaal bent ingelogd. Jouw instelling bepaalt welke diensten voor jou toegankelijk zijn via SURFconext. De meeste diensten die je via SURFconext benadert krijgen een klein deel van jouw gegevens. Sommige diensten hebben helemaal geen persoonsgegevens nodig. Als je wilt zien welke dienst welke gegevens krijgt, kijk dan bij Mijn diensten.

Accountgegevens

SURFconext kan (cloud)diensten een privacyvriendelijke identifier (nummer) geven waarmee jij herkend kan worden als je opnieuw inlogt bij een dienst. Om dit te kunnen doen, moet SURFconext jouw Gebruikers-ID en de naam van jouw instelling opslaan.

Gegevens en herkomst: Gebruikers-ID en de naam van jouw instelling + nummer gegenereerd door SURFconext

Bewaartermijn: Tot 3 jaar na laatste inlog.

Loggegevens

SURFconext bewaart tijdelijk wanneer en vanaf welk IP-adres je gebruik maakt van SURFconext en bij welke diensten je hebt ingelogd. Dit is nodig voor het beheer en de beveiliging van SURFconext.

Herkomst: Gegenereerd door SURFconext

Bewaartermijn: 6 maanden. Na 6 maanden worden de logbestanden geanonimiseerd.

Toestemmingsgegevens

Bij de meeste diensten moet je, voordat je voor de eerste keer inlogt, expliciet toestemming geven om jouw attributen te delen met de dienst waar je wilt inloggen. SURFconext slaat op wanneer en voor welke dienst je deze toestemming hebt gegeven. Meer over welke gegevens je per dienst heb gedeeld, vind je onder Mijn diensten.

Herkomst: Gegenereerd door SURFconext

Bewaartermijn: Tot 3 jaar na laatste inlog.

2 – Wat moet je als instelling zelf nog doen?

Wat moet de instelling zelf nog doen? (in de SC-context)

- Bepaal de rolverdeling. Is de leverancier een verwerker:
  - Verwerkersovereenkomst instelling <> SP (opstellen &) tekenen
  - SURF heeft een model verwerkersovereenkomst
  - SURFmarket dienstverlening
  - Deprovisioning (afspraken)
  - SURFconext is slechts doorgeefluik
- Hou beveiliging IdP actueel(zie ook de What's Next 2018 presentatie daarover)
- Dring bij SP's aan op dataminimalisatie & gebruik van SC pseudonieme identifiers
- Gebruik waar mogelijk federatieve authenticatie (ook in mobiele apps!)

3 – Wat doet SURFnet mbt SURFconext en de AVG

Wat doet het SURFconext team aan de AVG?

- Gegevensminimalisatie intern
- Gegevens niet langer bewaren dan nodig
- Beperken van toegang & regelmatig controleren
- Privacy by Design
- Security audits
- Kwaliteitsmanagement: processen gedocumenteerd + geaudit
- SURFconext AVG-ready

Vragen

Handige links (staan ook de in beschrijving onder de video)

- Wat is SURFconext: https://www.surfconext.nl/
- Welke afspraken maakt SURFnet rond SURFconext: https://wiki.surfnet.nl/display/surfconextdev/Afspraken+-+contracten+-+trustframework
- De profielpagina: https://profile.surfconext.nl/
- Het info/'consent'-scherm: https://wiki.surfnet.nl/display/conextsupport/Het+Consent-scherm
- Sterkere authenticatie? > SURFsecureID > https://www.surf.nl/surfsecureid
- Toegang beperken: https://blog.surf.nl/surfconextdiensten-beschikbaar-maken-beperkte-groep-gebruikers/
- SURFconext & privacy > https://wiki.surfnet.nl/display/surfconextdev/Privacy
- Discussieer door op https://wiki.surfnet.nl/display/FORUM/Privacy+related+discussions

Einde van het webinar. Dank voor uw belangstelling.