

Toegang voor Derden bij WUR

27 september 2022, Dave Heuts

**ZORGDRAGEN VOOR
TOEGANG MET EEN
VEILIGE, FLEXIBELE,
BETROUWBARE (EN
TOEKOMSTVASTE)
IDENTITEIT**



Even voorstellen



Dave Heuts (50)



Didam



Solution Architect IAM bij WUR

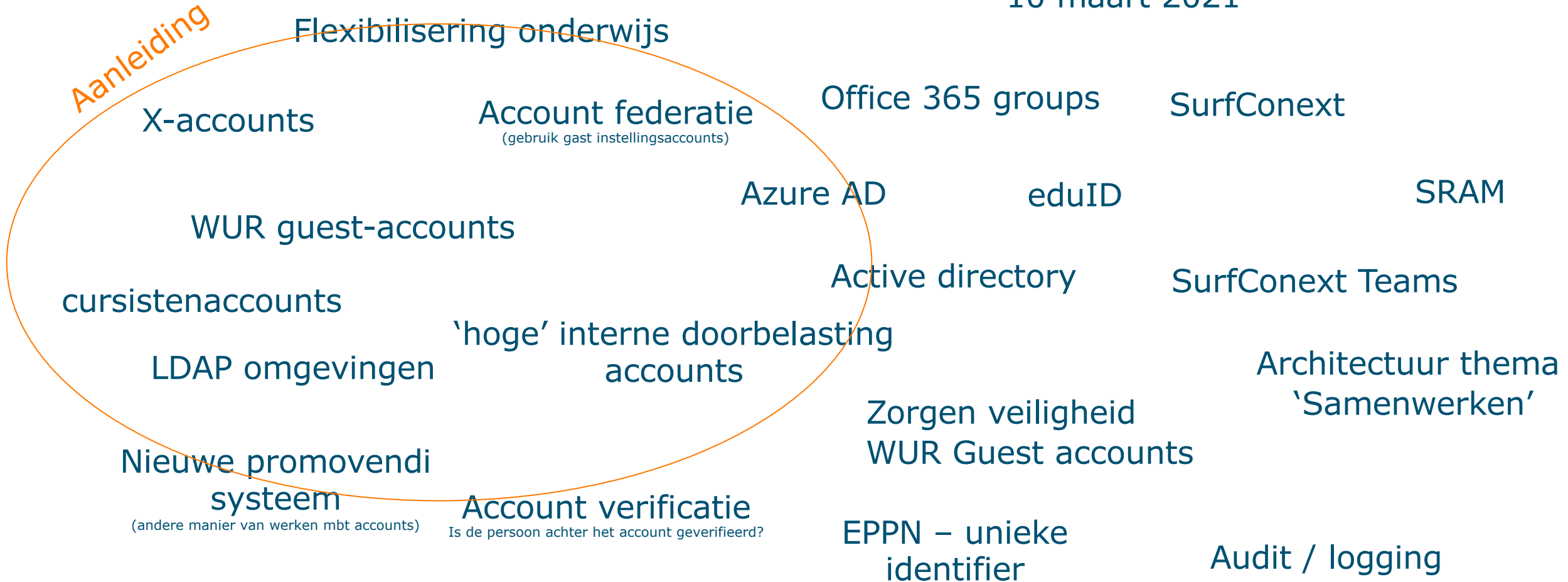
Mail: dave.heuts@wur.nl

Linkedin: <https://www.linkedin.com/in/daveheuts/>



Aanleiding en Context – Accountdifferentiatie

10 maart 2021



Business Analisten aan het werk

- Interviews met applicatie eigenaren
- Interviews met domein eigenaren
- Opstellen User stories
- Scenario's oplossingsrichting

Scenario 1:

We houden wat we hebben en maken dit veiliger.

Scenario 2:

We stoppen alles in Azure AD

Scenario 3:

We blijven in de SURF community en gaan proberen eduID en SurfConext in te zetten

Principes IAM Toegang voor derden

Derden registreren binnen WUR gebeurt op één plek en gaat conform het easy-service gedachtegoed.

Toegangsbeveiligingseisen voor internen en derden zijn gelijk

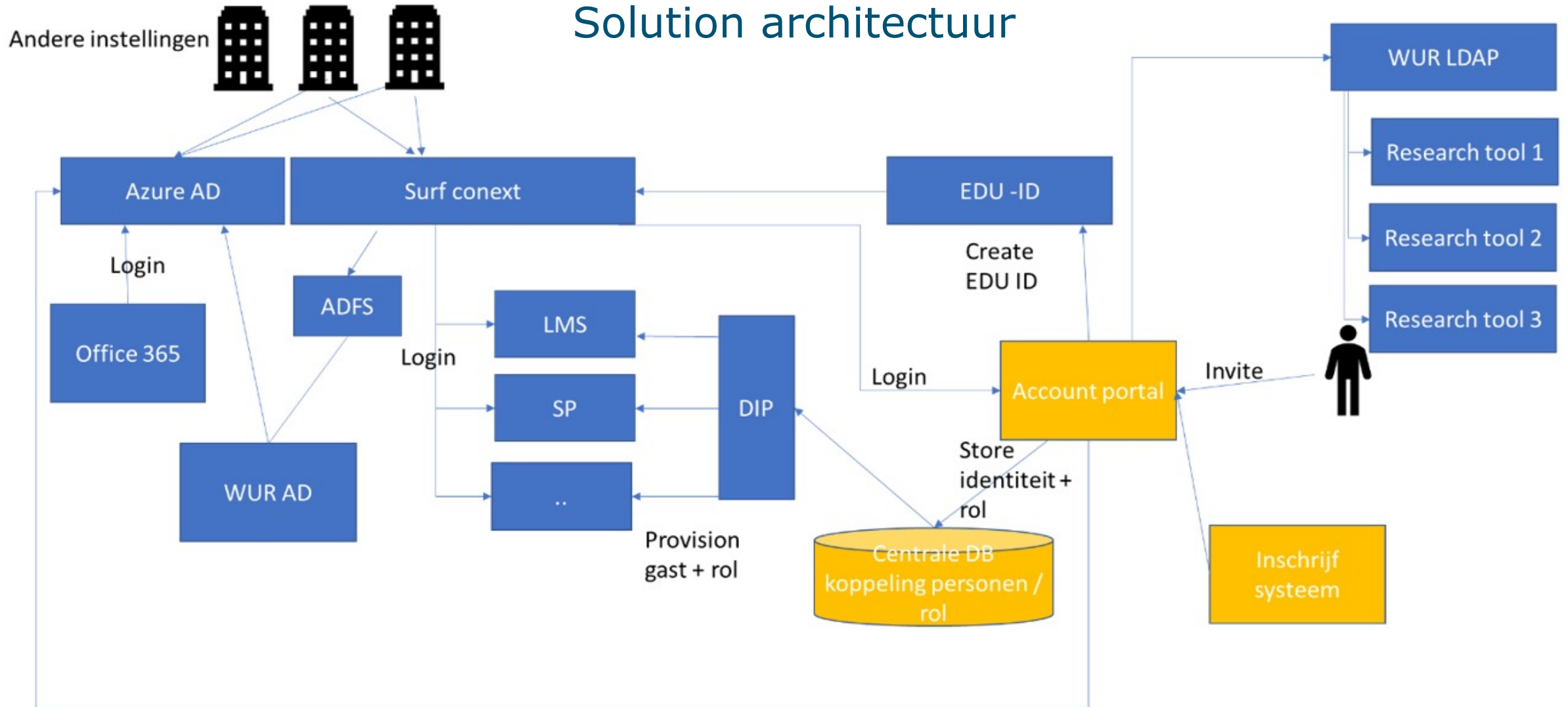
Accounts zijn gratis, rollen vormen de basis voor toegang tot WUR diensten en financiële verrekening

Processen rondom het aanmaken en afvoeren van derden zijn vastgelegd en worden gemonitord en periodiek ge-audit

Een derde moet toegang tot dezelfde systemen / bronnen kunnen krijgen als een interne

Alleen WUR medewerkers of promovendi kunnen een derde uitnodigen

Solution architectuur



Tja, en nu?

Perspectief van een rolbeheerder

eduID Invites

Logout

Home > Wageningen University & Research (WUR) (OTA)

Institution Wageningen University & Research (WUR) (OTA)

Edit

new AUP

Entity ID
https://loginota.wur.nl/federationmetadata/2007-06/federationmetadata.xml

Schac home
wur.nl

Applications

Users

Invitations

New application

Search applications

Name	Description ▼	Entity ID	Landing page URL	Provisioning
Brightspace	De applicatie voor het voorbereiden en geven van onderwijs	https://brightspace.wur.nl/s hibboleth-sp	https://wur.nltest.brightspace.com	https://wur-scim-api-test.containers.wur.nl/scim/v1

Need tips or info?
Help & FAQ

EN | NL

eduID invitation is a service by
SURF

Perspectief van een rolbeheerder

eduID Invites



Logout

[Home](#) > [Wageningen University & Research \(WUR\) \(OTA\)](#) > [Brightspace](#) > [New Role](#)

New Role

Name ⓘ

Description

Default expiry days ⓘ

Application

Cancel

Save

Need tips or info?
[Help & FAQ](#)

EN | NL

eduID invitation is a service by
SURF



Perspectief uitnodiger

eduID

Invites

Logout

Home > Universiteit van Harderwijk

Institution Universiteit van Harderwijk

Edit

new AUP

Entity ID

https://idp.uvh.nl/entityid

Schac home

uvh.nl

Applications

Users

Invitations

New invite

Search invitations

Email	Intended authority	Status	Roles
mssrikken@gmail.com	Institution admin	Open - expires 4/13/2022	
peter.havekes+verlopen@surf.nl	Guest	Expired on 1/25/2022	Gastdocent (HarderwijkELO)
peter.havekes+verlopen1@surf.nl	Guest	Expired on 1/10/2022	Gastdocent (HarderwijkELO)

Need tips or info?

[Help & FAQ](#)

EN | NL

eduID invitation is a service by

SURF



Perspectief uitnodiger

The screenshot shows the 'New invite' form in the eduID Invites interface. The form includes the following fields:

- Invites:** A header bar with the eduID logo, the word 'Invites', and a 'Logout' button.
- Breadcrumbs:** Home > Universiteit van Harderwijk > New invite
- New invite:** The main title of the form.
- Invitees:** A text input field containing 'marlies.rikken@surf.nl' with a close button (x).
- Authority:** A dropdown menu currently set to 'Guest'.
- Enforce email equality:** An unchecked checkbox.
- Invitation expiry date:** A date input field showing '18/04/2022' with a calendar icon.
- Roles:** A dropdown menu currently set to 'Kijker (Roostering)' with a close button (x). This field is circled in red.
- Role expiry date:** A date input field showing '01/03/2023' with a calendar icon and a close button (x). This field is also circled in red.
- Message:** A text area containing the message: 'Welkom bij Harderwijk! Je kunt nu alvast je rooster bekijken.'
- Buttons:** 'Cancel' and 'Send invite' buttons at the bottom.

Perspectief gast

Invitation for guest at edulD inviters

 noreply@eduid.nl <noreply@eduid.nl>
Aan:  Marlies Rikken

You have been invited to the invites website.

Click the button below to accept the invitation.

[Accept](#)

Welkom bij Harderwijk! Je kunt nu alvast je rooster bekijken.

Hi,

You have been invited by [Marlies Rikken](#) to become a **guest** at the institution **Universiteit van Harderwijk**.

You will be granted access to the following applications in Universiteit van Harderwijk:

- Roostering (role: Kijker)

If you don't want to accept this invitation, just ignore or delete this message.

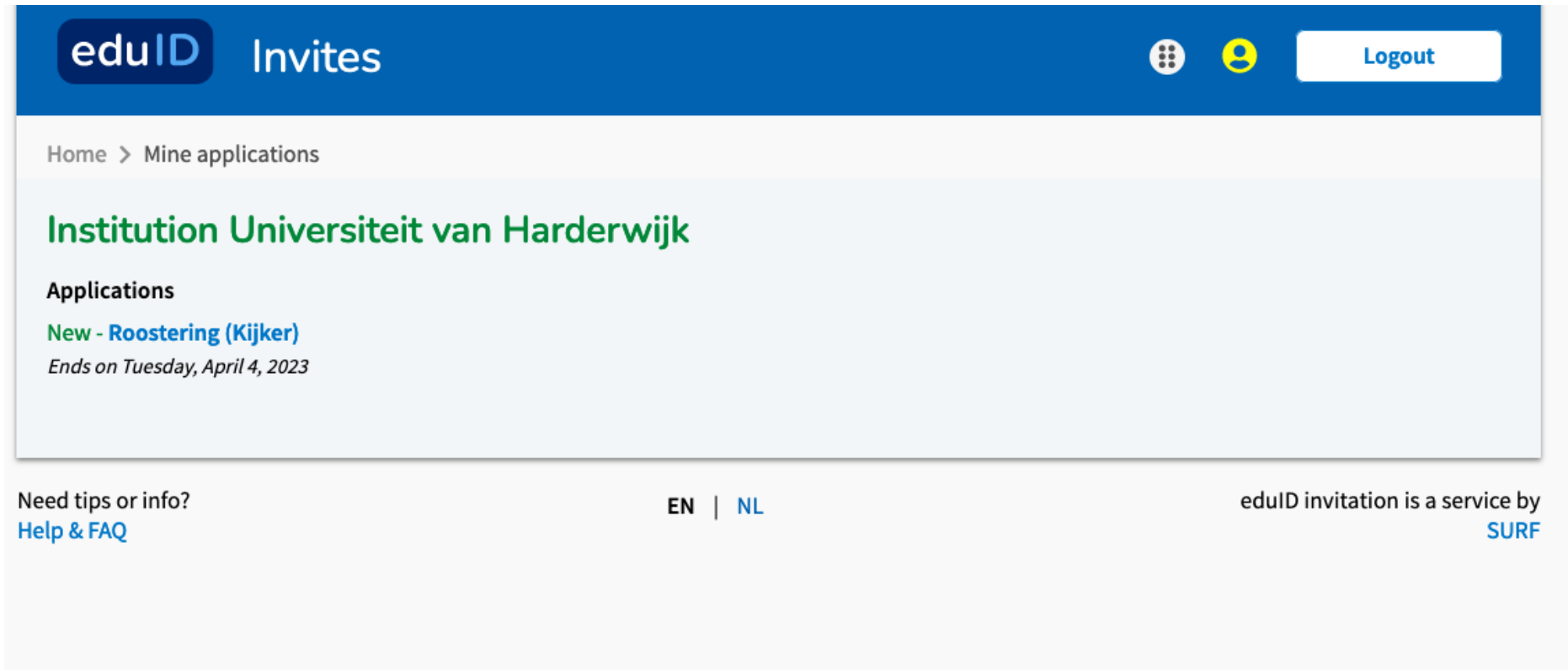
[What is edulD](#) • [Privacy Policy](#) • [Terms of Use](#)
Powered by [SURF](#)

Perspectief gast

The image shows two overlapping screenshots of the eduID web interface. The background screenshot is the 'Sign in with eduID' page, which includes a link for 'No eduID? Request one!', a login form with an email field (placeholder: e.g. user@gmail.com), a 'Stay logged in' checkbox, and links for 'Terms of Use', 'Privacy policy', and language selection (EN | NL). The foreground screenshot is the 'Request your eduID' page, which includes a link for 'Already have an eduID? Login!', a form with fields for 'Your email address' (placeholder: e.g. user@gmail.com), 'First name' (placeholder: e.g. Tim), and 'Last name' (placeholder: e.g. Berners-Lee), a checkbox for agreeing to terms and privacy policy, and a 'Request your eduID' button. The footer of the foreground screenshot shows 'Terms of Use', 'Privacy policy', language selection (EN | NL), and 'Powered by SURF'.

The image is a screenshot of the 'eduID Invites' page. At the top, it says 'Hi marlies.rikken@surf.nl,' followed by a message: 'You have been invited to accept the following role: **Kijker** (application **Roostering**) at the institution Universiteit van Harderwijk'. Below this is a yellow box with the text 'We are ready to create your profile.' The next section is 'Acceptable use policy', stating 'By logging on the Invite app, you become a user and agree to the [term and conditions of our AUP](#).' There is a checkbox that is checked, with the text 'I hereby certify that I have read the AUP and that I accept them'. At the bottom right is a blue 'Proceed' button. The footer includes 'Need tips or info? [Help & FAQ](#)', language selection (EN | NL), and 'eduID invitation is a service by [SURF](#)'.

Perspectief gast



The screenshot shows the 'eduID Invites' web interface. The top navigation bar is blue with the 'eduID' logo and the word 'Invites'. On the right side of the bar are icons for a grid of applications and a user profile, followed by a 'Logout' button. Below the navigation bar, a breadcrumb trail reads 'Home > Mine applications'. The main content area has a light blue background and features the text 'Institution Universiteit van Harderwijk' in green. Underneath, the section 'Applications' is shown, with a link 'New - Roostering (Kijker)' and a note 'Ends on Tuesday, April 4, 2023'. The footer contains a link 'Need tips or info? Help & FAQ', language options 'EN | NL', and a statement 'eduID invitation is a service by SURF'.

eduID Invites

Home > Mine applications

Institution Universiteit van Harderwijk

Applications

[New - Roostering \(Kijker\)](#)

Ends on Tuesday, April 4, 2023

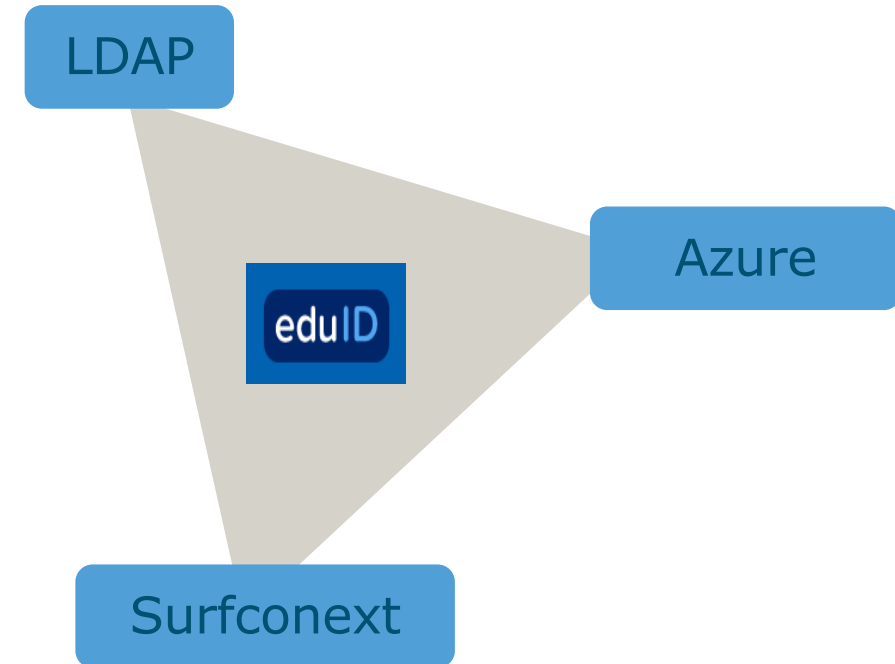
Need tips or info?
[Help & FAQ](#)

EN | [NL](#)

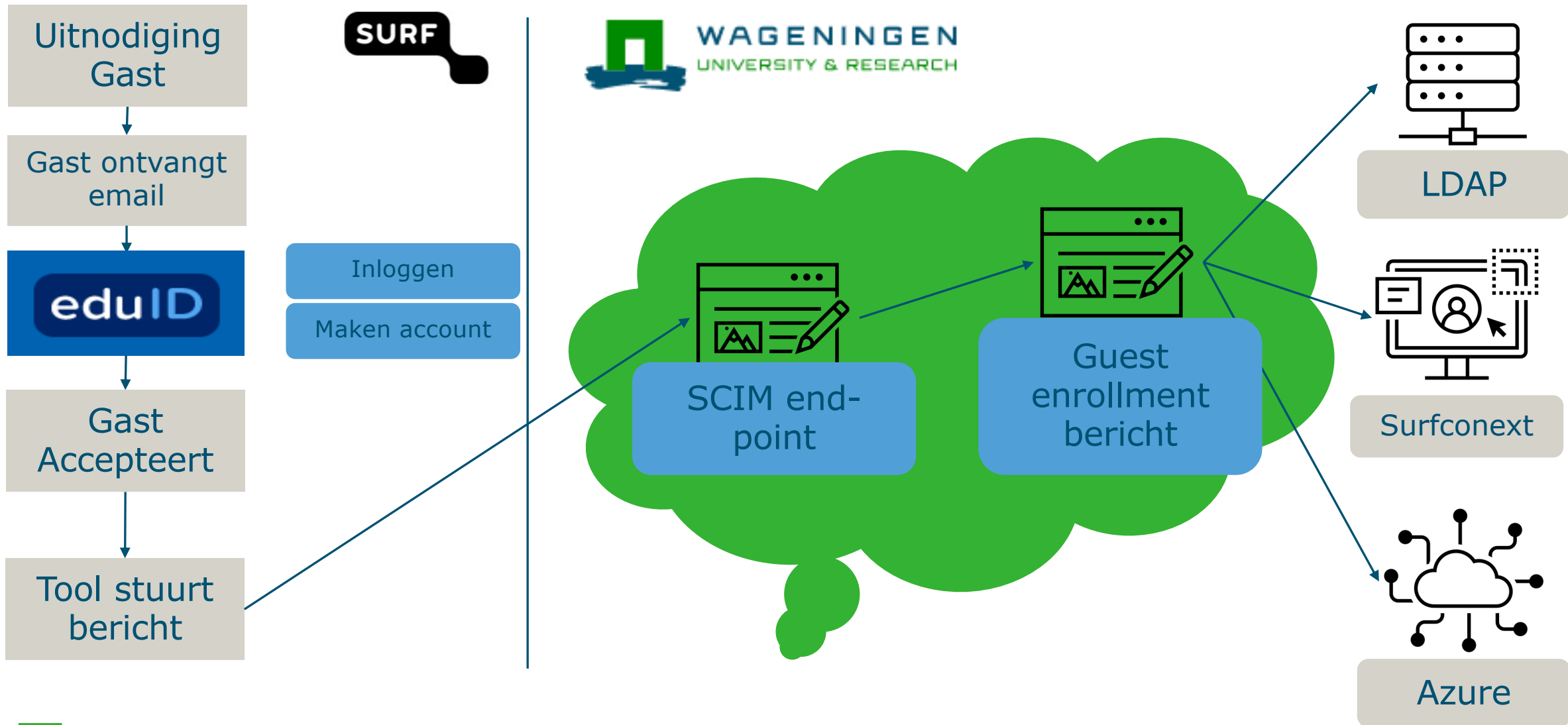
eduID invitation is a service by [SURF](#)

Doelsituatie toegang voor derden

- Eén portaal waarin gasttoegang wordt geregeld
- Autorisaties worden verstrekt via rollen
- Faciliteren zelfinschrijving (proef student)
- Inzet van SURF diensten voor toegang derden
- Geen WUR-specifieke gastidentiteit benodigd door inzet EduID



Workflow Surf Guest Invitetool



Uitgangspunten → Aansluitvoorwaarden



Applicatie waartoe
derden toegang moeten
krijgen (vb.
Brightspace)



Moet gebruik maken van
Surf Conext als
authenticatie middel



Moet naast WUR
identiteiten ook EduID
als Identity Provider
kunnen gebruiken

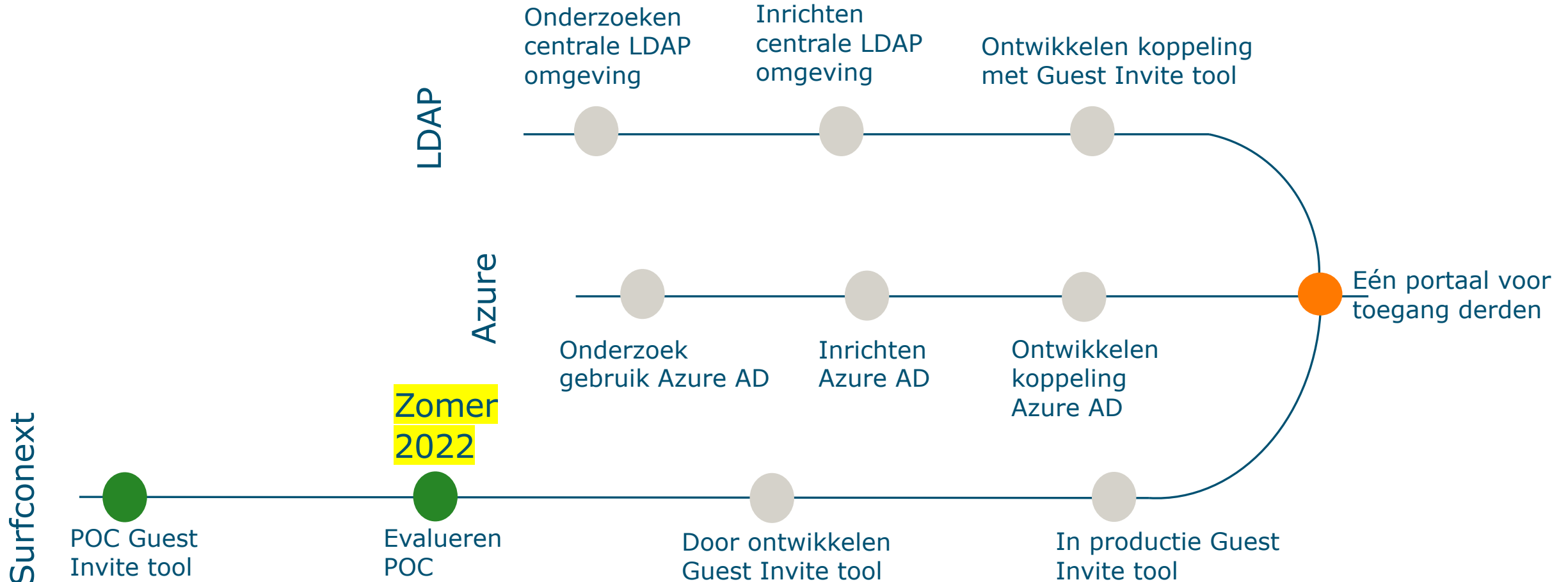
Identifier

**EPPN – EduPerson
Principal Name**

Gebruikersbeheer in applicatie

**Integratieplatform -
guestEnrollment event**

Roadmap ontwikkeling toegang voor derden



**Werkt dit ook
voor jullie?**