



Samen aanjagen van vernieuwing

MVP gasttoegang met eduID

User stories en wireframes

1 Gasttoegang met eduID

Toegang tot diensten in het hoger onderwijs en onderzoek voor studenten en medewerkers is op dit moment goed geregeld middels instellingsaccounts. Er zijn echter diverse situaties waarin het verkrijgen van toegang alsnog tekortschiet. Het toegang geven van derden (gasten) tot verschillende systemen binnen de instellingen verloopt nu op veel verschillende manieren. Er is weinig overzicht in welke 'gasten' tot welke systemen toegang hebben. Het probleem is niet nieuw, het speelt al jaren.

De komst van eduID brengt de kans om dit probleem generiek op te lossen. SURF onderzoekt momenteel hoe de inzet van eduID als gast-identiteitsprovider breder ingezet kan worden.

1.1 Aanpak

Om te bepalen wat de requirements van instellingen zijn als het gaat om gasttoegang is er met een vijftal instellingen gesproken: Erasmus University Rotterdam, Wageningen University & Research, Technische Universiteit Delft, Leiden University en Koning Willem I College. De input van de instellingen is in analyse en brainstorm sessies binnen het SURF T&I team verwerkt tot user stories en een beeld van een bijpassende oplossing middels wireframes.

Dit document is bedoeld om de user stories en wireframes te toetsen bij instellingen en hierop te itereren. Na het toetsen van de uitkomsten wordt op korte termijn een Minimum Viable Product (MVP) gebouwd die aan moet sluiten op de wensen van de instellingen.

1.2 Situatie bij instellingen

De situatie per instelling verschilt sterk als het gaat om gasttoegang. Van een goed werkend gastsysteem, tot handmatige acties op basis van excel lijsten. Waar minder verschil in zit zijn de situaties die benoemd worden waar gasttoegang een rol speelt. Use cases die benoemd worden zijn o.a.: joint degrees, proefstudenten, stagebegeleiders, studenten op afstand, alumni, gastsprekers, tijdelijke bezoekers, tijdelijke medewerkers, gebruikers van cursussen en facilitaire dienstverleners.

De generieke wens die hieruit is af te leiden is om gasten gemakkelijk, online of aan een balie, te kunnen onboarden als gast. Belangrijk daarbij is dat de gast gebruik kan maken van de juiste applicaties voor de periode waarin dit noodzakelijk en toegestaan is voor die gast.

Daarnaast zijn er additionele requirements:

- Toegang tot Azure/Microsoft 365 diensten.
- Verificatie van de identiteit van gasten, afhankelijk van de applicatie/use case.
- Accepteren van instellingsvoorwaarden voor het gebruik van applicaties
- Bewijs betaling van collegegeld kunnen verifiëren

Deze additionele requirements worden meegenomen in de doorontwikkeling van het portaal voor gasttoegang, maar zijn geen onderdeel van de MVP.

2 User stories

Wanneer de wensen rond gastgebruik verder uitgewerkt wordt tot functionaliteiten die passen binnen een gaststelsel en betrokkenen die daarbij nodig zijn, ontstaat het onderstaande beeld. De specifieke requirements per betrokken 'rol' zijn uitgewerkt in user stories.

- **Uitnodiger:** nodigt gasten uit. Kan op verschillende plekken zitten. Aan een balie, docent, prompt vanuit een systeem, etc.
- **Genodigde gast:** persoon die (tijdelijk) toegang wil tot bepaalde diensten van de instelling
- **Rolbeheerder:** bepaalt welke gastrollen er aangemaakt worden en welke applicaties daarbij horen. Bepaalt wie binnen de specifieke groep uitnodiger mag zijn. (Deze persoon is bijvoorbeeld een administrator van een faculteit.)
- **Beheerder gastportaal:** Kent rechten toe aan rolbeheerders
- **Applicatiebeheerder:** Beheerder van een applicatie/dienst.

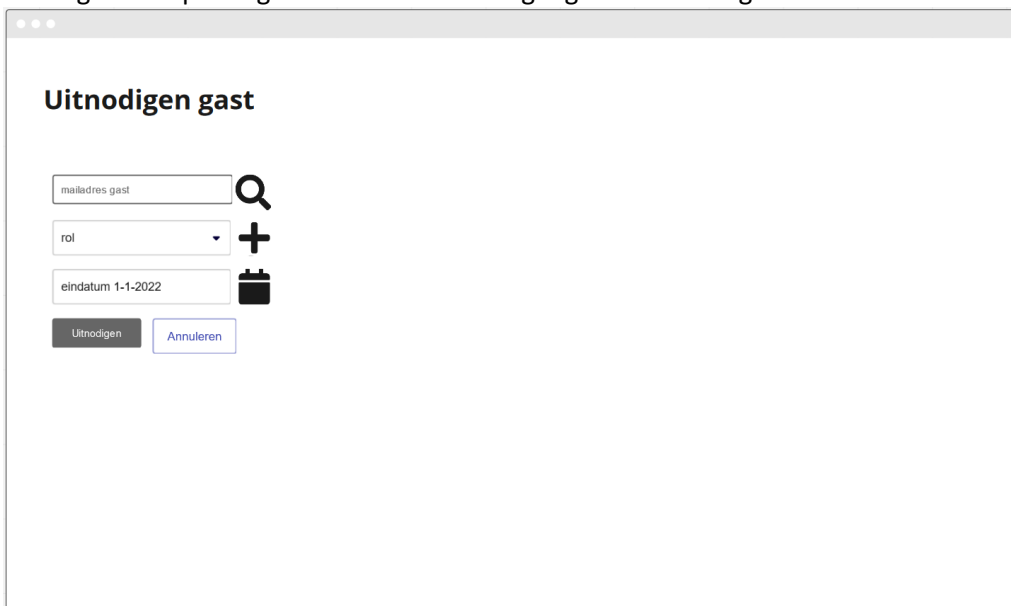
ALS	WIL IK
Uitnodiger	Mensen kunnen uitnodigen obv. e-mailadres (zodat ik dat in 1x kan regelen, waarna de genodigde toegang krijgt tot de diensten die ik heb aangevinkt)
Uitnodiger	Een (gast)rol kunnen koppelen aan de genodigde
Uitnodiger	Nieuwe rollen toekennen aan een bestaande gast
Uitnodiger	per toegangsrecht(rol) een verlooptijd kunnen instellen waarna de toegang automatisch verloopt (week/maand/jaar/specifieke datum).
Uitnodiger	Als de tijdslimiet bijna is bereikt wil ik een notificatie kunnen ontvangen. Maar dat wil ik ook (per dienst en/of per gebruiker) kunnen uitzetten
Uitnodiger	Mijn genodigden kunnen zien en beheren
Uitnodiger	Meerdere gasten in een batch kunnen invoeren (die dezelfde rol krijgen)
Uitnodiger	Kunnen zoeken op basis van verschillende kenmerken (mail, naam, rol, etc.)
Uitnodiger	Een (automatische) reminder sturen naar de genodigde gast dat een account aangemaakt kan worden
Uitnodiger	Ik wil zeker weten wie de persoon is (en wat het adres is) (online)
Uitnodiger	Kunnen zien welke rechten ik heb
Genodigde gast	Makkelijk toegang tot de applicatie/dienst waar ik voor uitgenodigd ben
Genodigde gast	Makkelijk een gastaccount aanmaken
Genodigde gast	Kunnen zien wat mijn rechten zijn, hoe lang die nog geldig zijn, etc.
Genodigde gast	Kunnen zien wie mij uitgenodigd heeft en hoe ik die kan bereiken als ik vragen heb
Genodigde gast	Verlenging aanvragen voor een applicatie/rol
Rolbeheerder	Bepalen welke rol toegang krijgt tot welke applicaties
Rolbeheerder	Toekennen wie uitnodiger is
Rolbeheerder	Toekennen welke uitnodiger welke rollen mag uitgeven
Rolbeheerder	Limieten te kunnen instellen (bijv. deze persoon mag max 10 anderen uitnodigen voor max 1 jaar)
Rolbeheerder	Kunnen zien welke rollen er zijn.
Rolbeheerder	In kunnen zien welke rechten ik heb
Rolbeheerder	Bepalen welke applicatie aan welke rol toegekend wordt
Rolbeheerder	Nieuwe rollen aanmaken en verwijderen
Applicatiebeheerder	Weten welke rollen toegang hebben tot mijn applicatie
Applicatiebeheerder	Inspraak hebben welke rollen toegang hebben tot mijn applicatie
Applicatiebeheerder	Signaleren naar de uitnodiger bij vermoedde dat er te lang/ongeoorloofd toegang is
Beheerder gastportaal	Toekennen wie rolbeheerder is
Beheerder gastportaal	Rolbeheerders verwijderen
Beheerder gastportaal	Overzicht hebben van alle rolbeheerders en uitnodigers
Beheerder gastportaal	Autorisaties van de rolbeheerders bepalen
Beheerder gastportaal	Applicaties toevoegen aan het gastportaal

3 Wireframes gastportaal

Op basis van de user stories en gewenste functionaliteiten zijn wireframes ontwikkeld. Het uitgangspunt is een gastportaal waar zowel de uitnodiger, rolbeheerder en de gast gebruik van kunnen maken. De frames zijn dan ook vanuit deze drie perspectieven vormgegeven. De perspectieven van de applicatiebeheerder en beheerder gastportaal zijn hier nog geen onderdeel van.

3.1 Perspectief uitnodiger

De uitnodiger kan op basis van email adres een persoon uitnodigen. De uitnodiger kent de rollen toe die de persoon nodig heeft en hoe lang deze geldig zijn. Dit kan ook in bulk gedaan worden. De uitnodiger kan vervolgens aanpassingen maken aan de toegangsrechten van gasten.



The wireframe shows a form titled "Uitnodigen gast". It contains the following elements:

- A text input field labeled "mailadres gast" with a search icon to its right.
- A dropdown menu labeled "rol" with a plus icon to its right.
- A text input field labeled "eindatum 1-1-2022" with a calendar icon to its right.
- Two buttons at the bottom: "Uitnodigen" (dark grey) and "Annuleren" (light blue).

Het is ook mogelijk om aan een groep gasten in bulk een rol toe te kennen en uit te nodigen. Dit faciliteert bijvoorbeeld het aanmelden van een grote groep proefstudenten.



The wireframe shows a form titled "Uitnodigen meerdere gasten". It contains the following elements:

- A text input field labeled "CSV- bestand" with an upload icon to its right.
- A dropdown menu labeled "rol" with a plus icon to its right.
- A text input field labeled "eindatum 1-1-2022" with a calendar icon to its right.
- Two buttons at the bottom: "Uitnodigen" (dark grey) and "Annuleren" (light blue).

De uitnodiger kan de gasten die uitgenodigd zijn beheren. Er zijn verschillende acties mogelijk:

- verlengen van een rol,
- uitnodigen/verwijderen van rollen,
- sturen van een reminder,
- verwijderen van een gast,
- aanpassen gegevens van de gast.

Beheren gasten

Q Search Search Search

<input type="checkbox"/> naam	Rol 1 Rol 2	email adres	Vervaldatum	—
<input type="checkbox"/> naam	Rol	email adres	Vervaldatum	
<input type="checkbox"/> naam	Rol 4 Rol 6	email adres	Vervaldatum	
<input type="checkbox"/> naam	Rol	email adres	Vervaldatum	—

Aktie

Beheren gast

Persoonsinformatie Rollen Historie

Achternaam

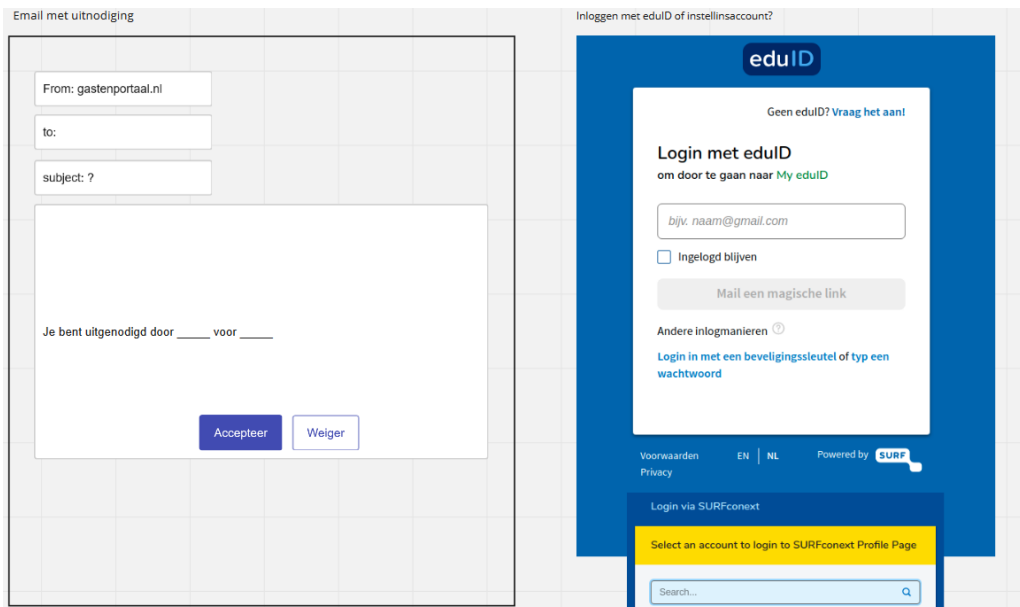
Voornaam

e-mail adres

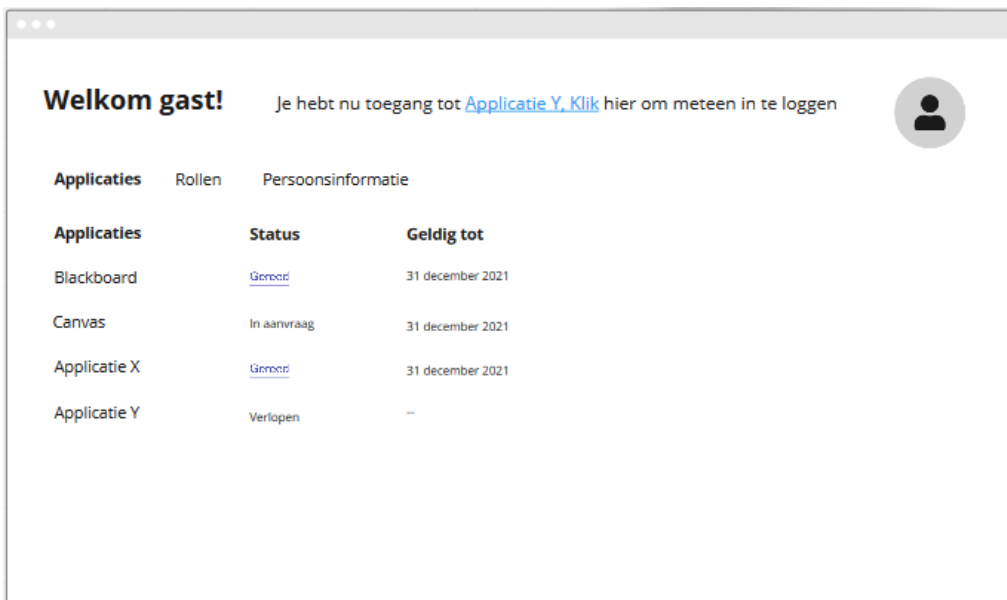
??

3.2 Perspectief gast

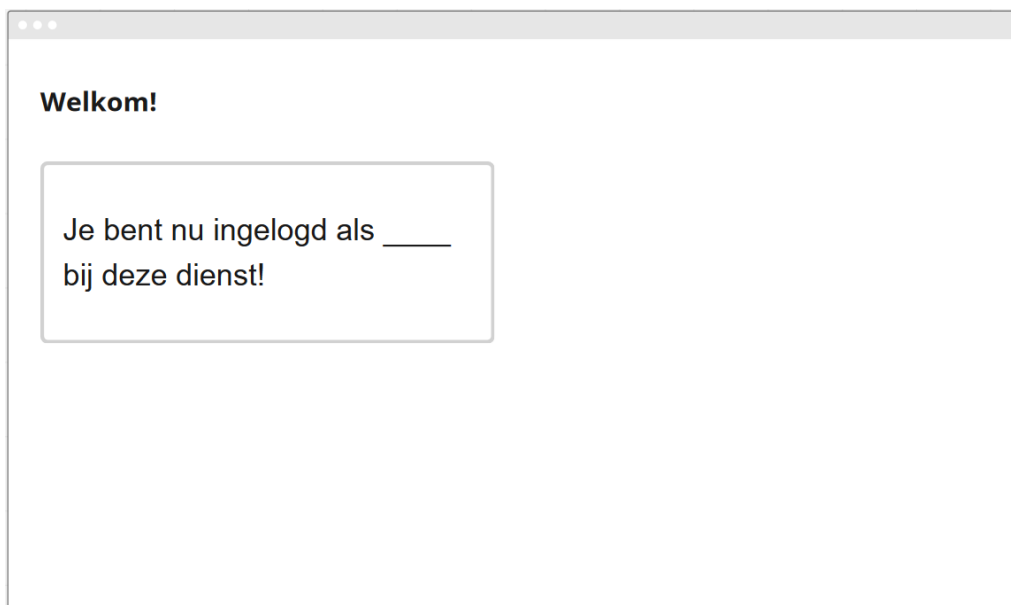
Nadat de aanvraag voor toegang is gedaan aan de balie of online, ontvangt de gast een uitnodiging per e-mail. Om de uitnodiging te kunnen accepteren wordt gevraagd om in te loggen met eduID. eduID wordt ingezet om de instelling te voorzien van de naam, emailadres en eduID identifier.



Vervolgens kan de persoon zien tot welke applicaties er toegang is verleend en voor hoe lang. De gast kan gemakkelijk naar de gewenste applicatie doorklikken.

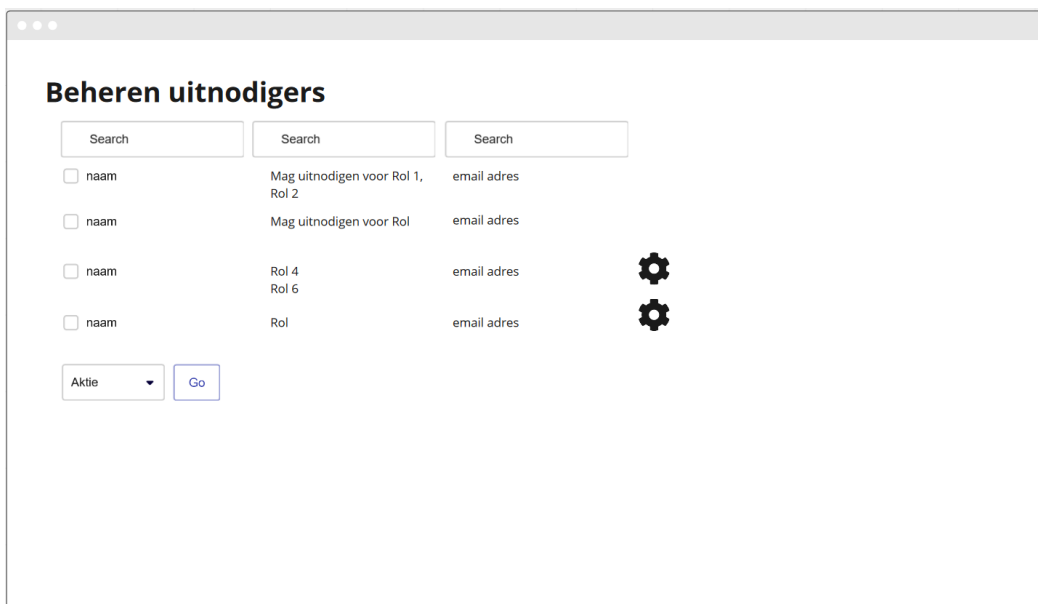


De gast krijgt vervolgens een welkomst scherm te zien en een aanduiding dat er is ingelogd.



3.3 Perspectief rolbeheerder

De rolbeheerders bepalen wie in de instelling gasten mag uitnodigen en voor welke rollen zij dit mogen doen.



De rolbeheerder maakt daarnaast rollen aan. Hierbij worden enkele keuzes gemaakt: welke applicatie is gekoppeld aan de rol, de naam van de rol en of er identiteitsverificatie van de gast nodig is wanneer deze rol toegekend wordt.

Maken/bewerken rol

Landingpage :

Provisioning :

email

Webhook

Direct beschikbaar

Moet dit email adres gebruiken bij accepteren uitnodiging

Instellingsaccount (of gelinked eduID) nodig

4 Technische opzet

SURF gaat dit gastenportaal opleveren als een API-platform. Alle functies die nodig zijn voor het realiseren van de uitnodig-flow komen beschikbaar als web-endpoints die door andere applicaties kunnen worden aangeroepen. Hierdoor kunnen instellingen dit eenvoudig implementeren in eigen portalen, IDM-processen of selfservice-tools. Onderstaande afbeelding schetst de technische opzet en het bijbehorende proces.

Daarnaast levert SURF een webapplicatie als referentie-implementatie op (zie wireframes). Deze kan direct als dienst van SURF gebruikt worden, of worden gebruikt als voorbeeld voor een eigen portaal.

4.1 Technisch proces

Na het accepteren van een uitnodiging door een gast wordt een bericht gestuurd via een API-call naar het IDM-systeem van de instelling. Vanuit dit bericht kan de eduID gebruiker worden aangemaakt in de applicatie en worden toegevoegd aan de juiste applicatierollen.

Mocht dit nog niet werkbaar zijn voor de betreffende instelling, dan kan via email een bericht gestuurd worden om bijvoorbeeld een ticket aan te maken. Als het niet mogelijk is om gastgebruikers (automatisch of handmatig) in de applicatie te koppelen, is het ook mogelijk om toegang tot de applicatie af te schermen via SURFconext; Alleen gasten met de juiste rol kunnen dan via SURFconext inloggen op de applicatie.

