

Bijeenkomst Overzicht van IAA in het mbo

vrijdag 7 december 2018

SURF, Utrecht

Programma



10:00 Wet Digitale Overheid, Barbera Veltkamp (Min. BZK)

10:30 Algemene ontwikkelingen IAA bij SURF & Kennisnet,
HP Köhler (Kennisnet) en Roel Rexwinkel (SURF)

11:15 Pauze

11:40 Vereniging Red Spider, Roy Dusink

12:00 Lunch

13:00 Centraal Aanmelden, Jan Bartling (saMBO-ICT)

13:20 Onderwijsgroep Tilburg, Merijn van der Schoot

13:40 Koning Willem 1 College, Jef van den Hurk

14:00 Paneldiscussie

14:45 Afsluiting met borrel



Wet Digitale Overheid: betekenis voor dienstverleners in het onderwijs

*Barbera Veltkamp
Ministerie van BZK*

SURF 7 dec. 2018



Waar gaat het over?

- Maatschappij digitaliseert; de overheid en publieke dienstverleners ook
- Verschillende wetten regelen digitalisering van de overheid (oa AVG)
- Vandaag gaat t over de WDO
- WDO regelt de *toegang* tot elektronische dienstverlening: elektronische identificatie (eID)
- Toegang tot de overheid/publieke dienstverleners





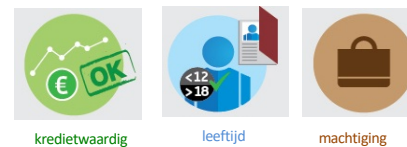
Wat is toegang?



1. Identificatie
Wie ben je?



2. Authenticatie
Hoe bewijs je dat?



3. Autorisatie
Wat mag je? Waar heb je toegang toe?



Online transacties nu

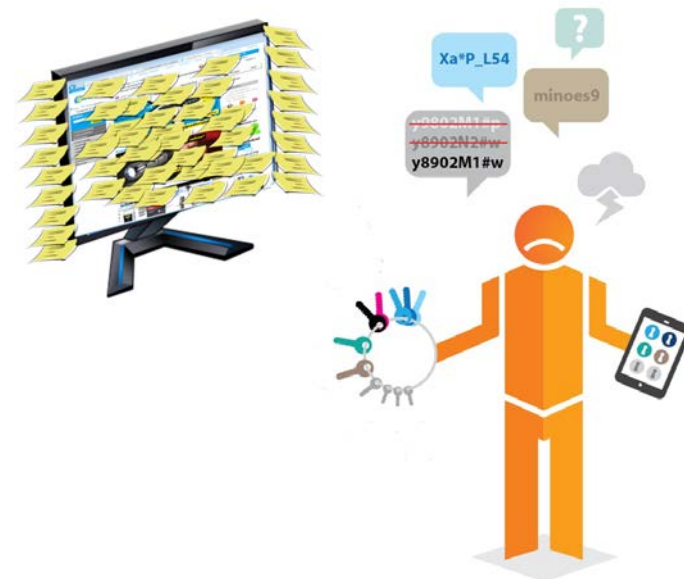
- Nu bepalen **organisaties** hoe de gebruiker zich identificeert
- Geen sprake van **standaardisatie**





Gevolgen van huidige online transactie

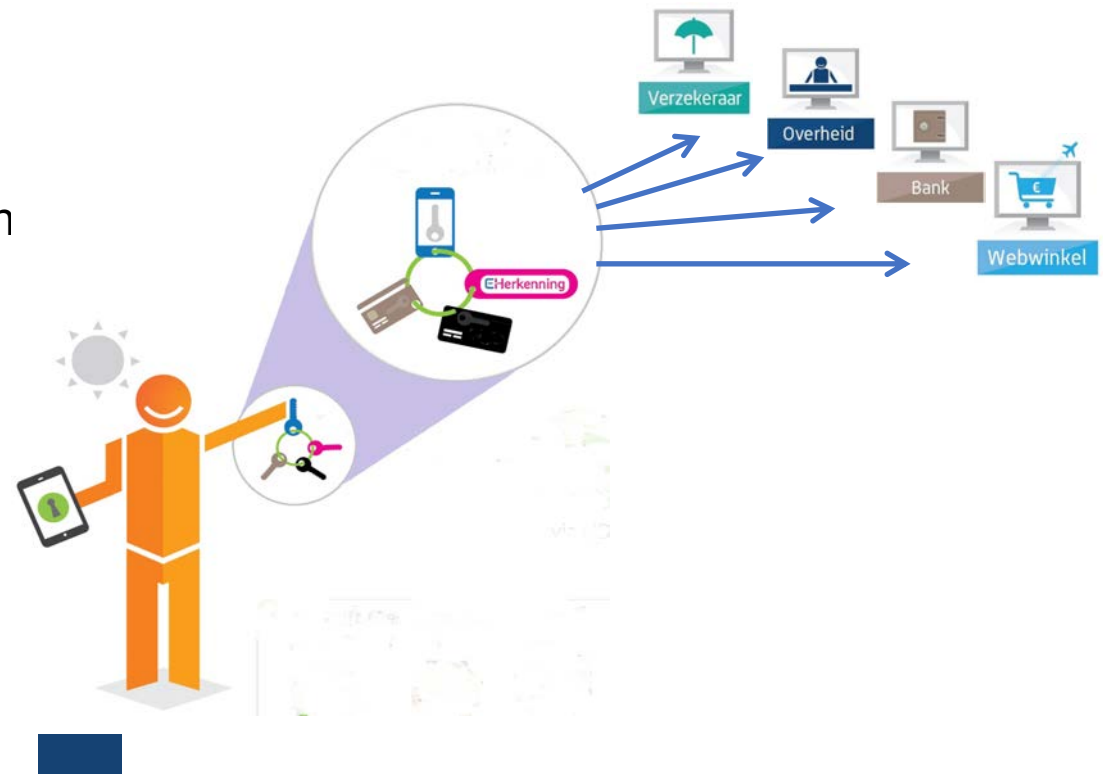
- Gebruiker moet veel verschillende gebruikersnamen en wachtwoorden gebruiken / onthouden
- Lastig en risicovol voor zowel gebruiker als voor dienstverlener





Online transacties in de toekomst

- De **gebruiker** bepaalt hoe hij zich identificeert
- Eenduidige toegang voor burgers en bedrijven





Waar gaat de WDO over?

- › Uitgangspunten: veilig, betrouwbaar, gebruiksvriendelijk, beschikbaar
- › Eenduidigheid voor gebruiker (burger of bedrijf/rechtspersoon)
- › Acceptatieplicht voor dienstverleners mbt goedgekeurde eID-middelen
- › Dwz: geen sectorale eID-middelen meer (echter: uitzondering mogelijk)
- › Dienstverleners moeten hun diensten classificeren:
 - Substantieel: bij verwerking BSN en persoonsgegevens, bijv. (centraal) inschrijven
 - Hoog: bij verwerking bijzondere persoonsgegevens, bijv. medisch
- › NB: WDO gaat *niet* over interne (ICT-)infrastructuur en identificatieprocessen





Reikwijdte WDO: voor wie geldt classificerings- & acceptatieplicht?

- Alle overheidsorganisaties en organisaties met een publieke taak
- Aangewezen organisaties w.o. zorgverzekeraars, academische ziekenhuizen, pensioenfondsen
- **Onderwijs:** NU alleen hoger onderwijs. Op termijn/gefaseerd: MBO
- Meedoen betekent ook: meebetalen
- NB: naleving standaarden (interoperabiliteit, veiligheid): voor RWT's, incl. onderwijs





Dienstverlening classificeren & eID- middelen accepteren

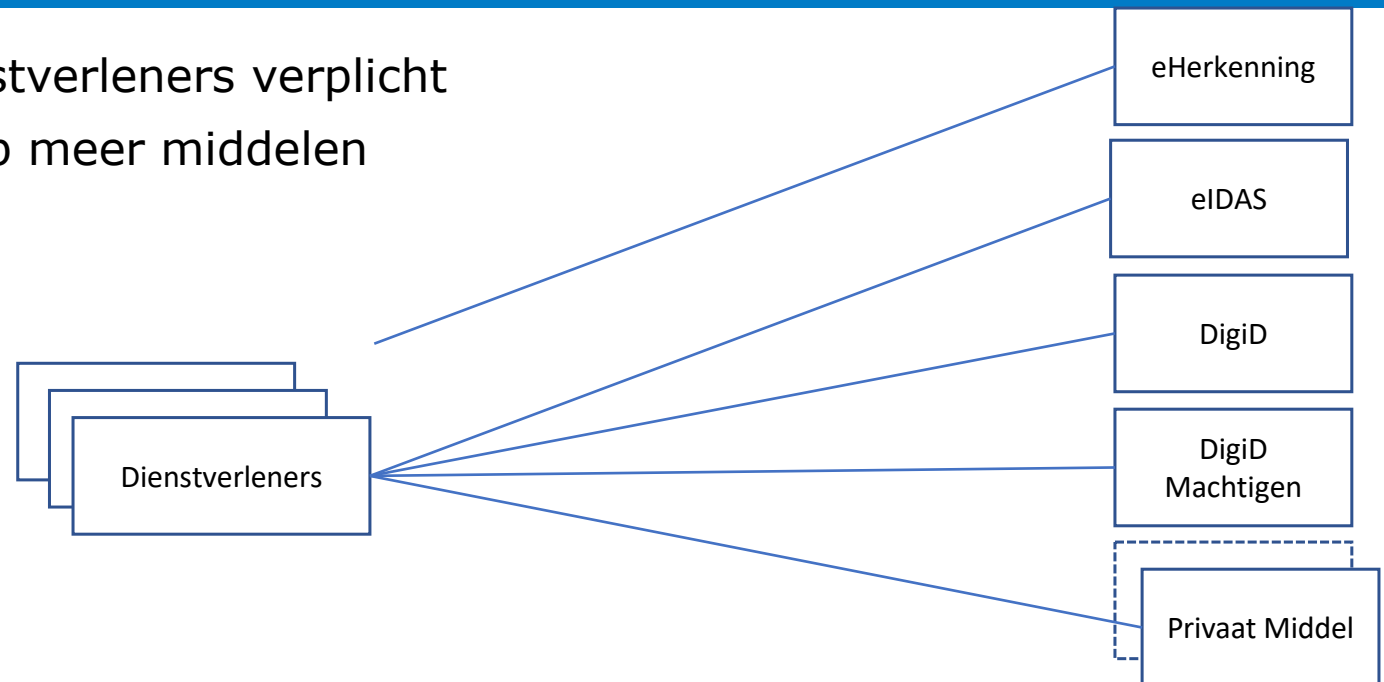
- › In lijn met Europese wetgeving: eIDAS (sept. 2018)
- › eIDAS geldt voor aanbestedende organisaties, incl. onderwijsinstellingen
- › **MAAR:** acceptatieplicht geldt alleen mbt diensten/middelen op betrouwbaarheidsniveaus *Substantieel* en *Hoog*
- › Alleen Dld heeft goedgekeurd middel





Gevolg van de WDO

- Resultaat is dat dienstverleners verplicht moeten aansluiten op meer middelen





Planning Wet Digitale Overheid (indicatief)

2019

- Behandeling WDO in Parlement
- 1/7 WDO van kracht; *niet* voor MBO
- Centraal aanmelden bepalend voor moment waarop WDO van toepassing wordt voor MBO
- OCW: voert gesprek over 'vertaling' WDO naar onderwijs (oa SAMBO, MBO-raad, Ketenregioevlg.)
- BZK: rolt ICT-voorzieningen en (publieke en private) eID-middelen uit





Kennisnet

A photograph of a classroom with several young students sitting at desks. In the foreground, a girl with long dark hair is smiling at the camera while wearing large headphones. Behind her, another girl is looking down at a tablet. To the left, a boy is also looking at a tablet. The desks are equipped with tablets on stands.

Algemene ontwikkelingen IAA KN & SURF!

Identity management als speerpunt!

H-P Köhler, Kennisnet
Roel Rexwinkel, SURF

Laat ict werken **voor het onderwijs**

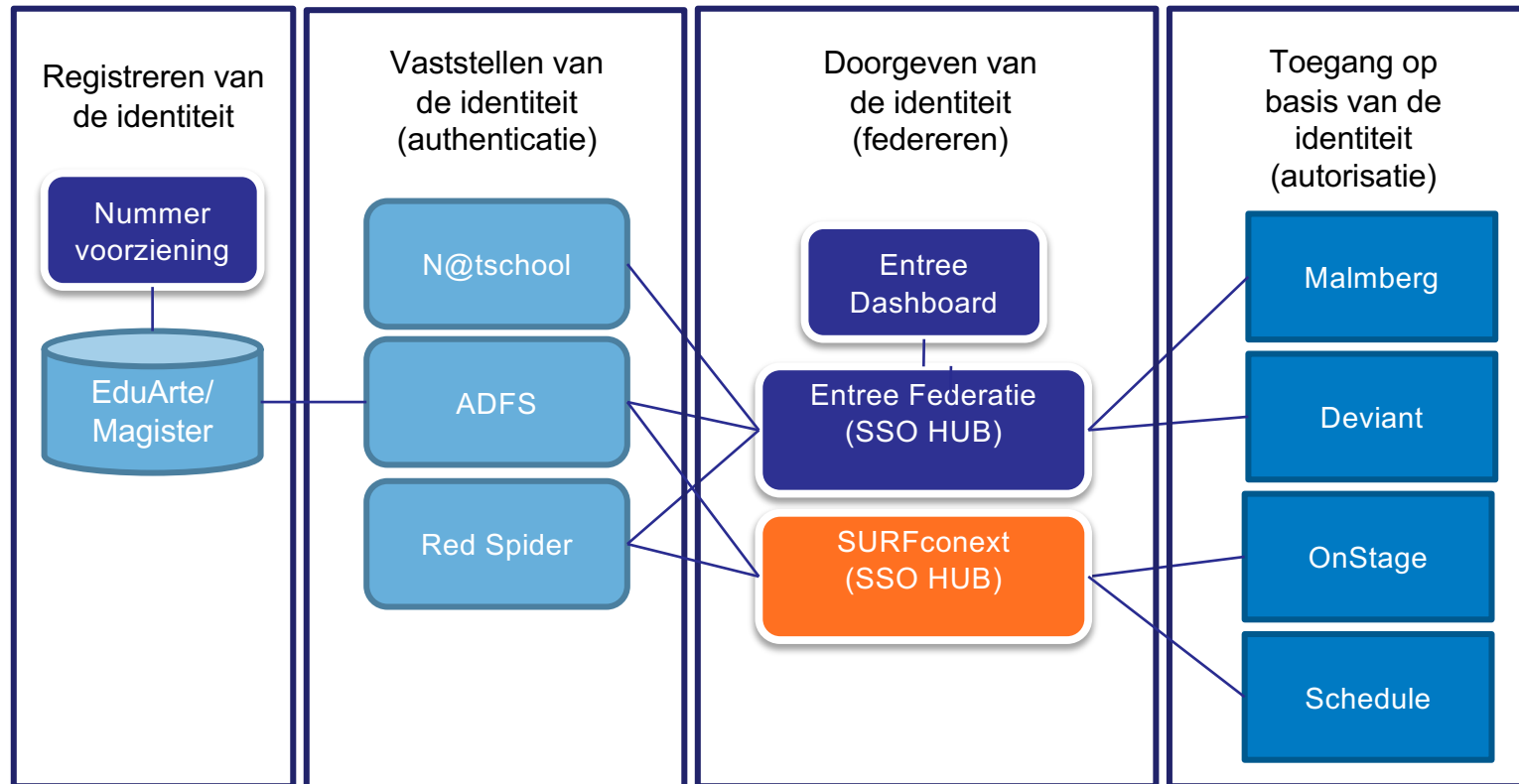
Agenda

1. Positie & Gebruik van de Federaties

2. Trends & Ontwikkelingen

- IAA in ontwikkeling
- EduID & ECK iD verschillen en overeenkomst
- Edubadges pilot
- Edumij
- Regie op Inkoop Identity Managementsystemen
- Toekomstbeeld toegang (Edustandaard)
- Kennisset ontwikkelingen zoals Mijn Entree

Positie & gebruik van de federaties



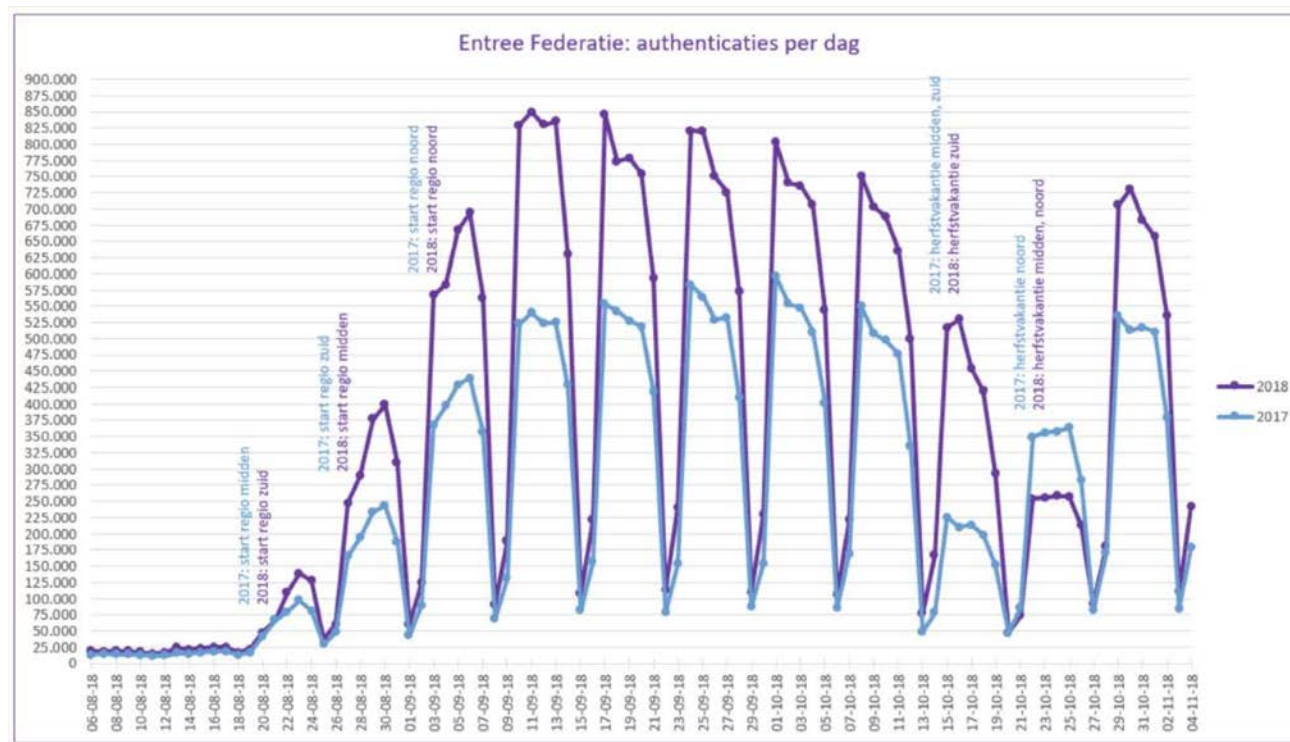
Overeenkomsten

- Centraal federatief hub model
- De school als identity provider
- SAML protocol.
- Autorisatie op basis van attributen.

Verschillen

- Attributenschema
- Aangesloten dienstverleners
- Aansluitvoorwaarden

Entree cijfers



RUIM 90 MILJOEN LOGINS MET SURFCONEXT IN 2017

net

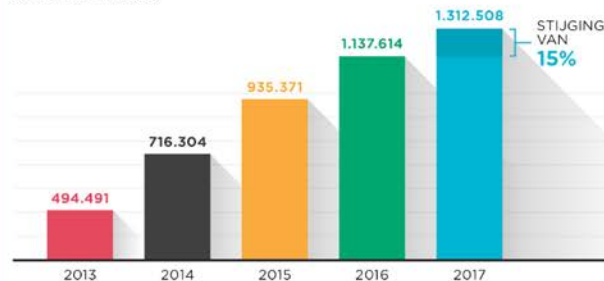
Via SURFconext loggen studenten, docenten en onderzoekers in bij clouddiensten van verschillende aanbieders. Gewoon met hun eigen instellingsaccount, veilig en gemakkelijk.

GEbruik

AANTAL UNIEKE
LOGINS

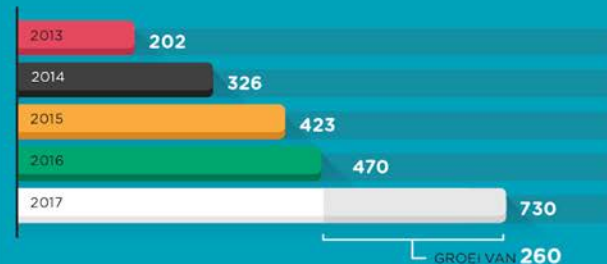


AANTAL UNIEKE
GEBRUIKERS



DIENTEN

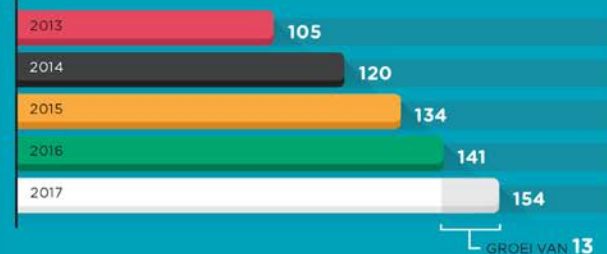
AANTAL SERVICE
PROVIDERS



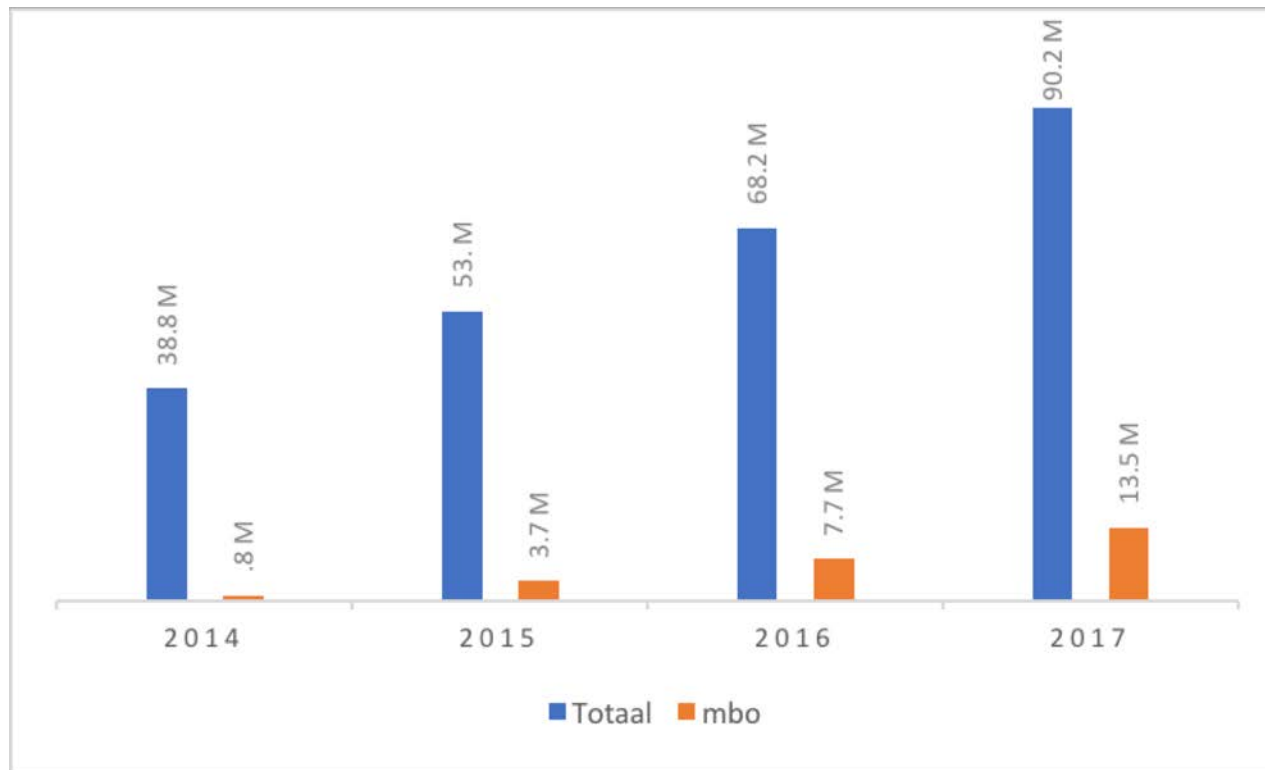
Het aantal diensten is in 2017 flink gestegen. Dit kwam met name door:

- Groei van het aantal mbo-instellingen dat SURFconext gebruikt
- Het aansluiten van een groot aantal elektronische leeromgevingen
- Toename van internationale diensten die via eduGAIN worden aangeboden

AANTAL IDENTITY
PROVIDERS



Logins SURFconext door mbo (2014-2017)



Top 10 mbo (logins in 2018)

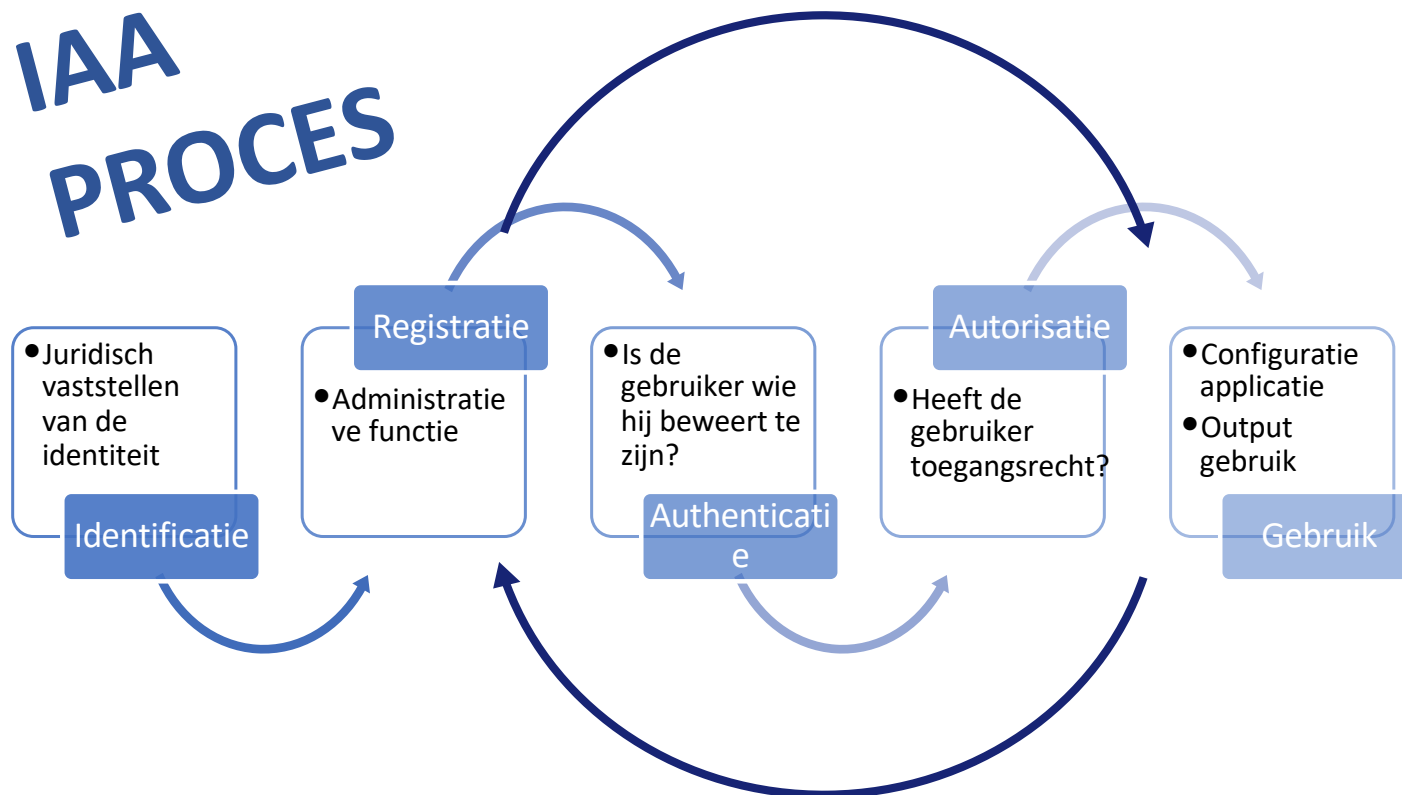
mbo	logins
ROC Midden Nederland	4.136.094
ROC Nijmegen	2.773.075
Rijn IJssel	2.525.544
ROC Aventus	1.726.336
Onderwijsgroep Tilburg	1.183.334
ROC Friese Poort	1.010.902
ROC Albeda College	1.007.074
Helicon	878.456
Clusius College	758.918
Deltion College	683.737

Diensten gebruikt door mbo met veel logins:

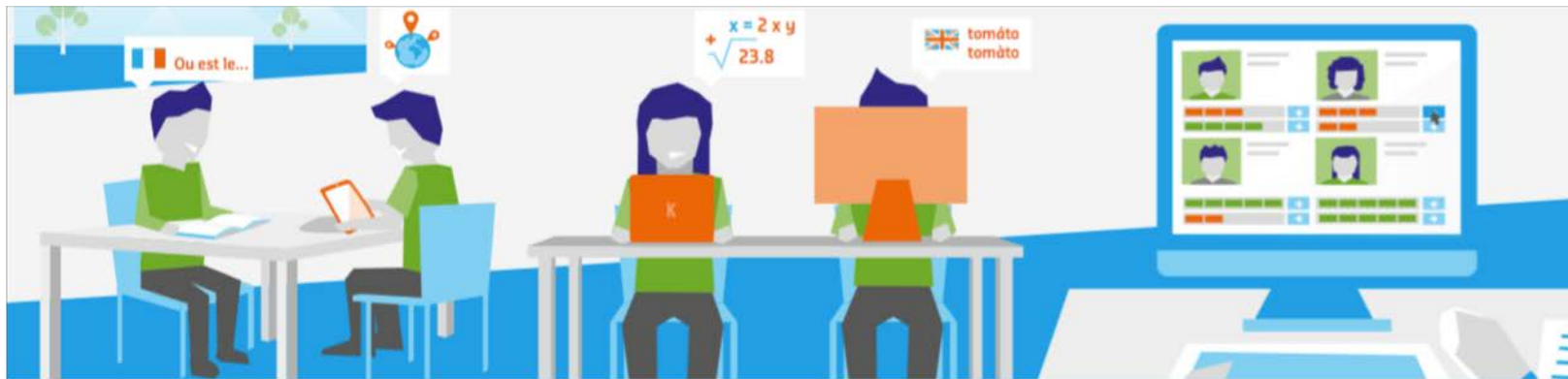
- Blackboard
- Xedule
- Education/onderwijs Online
- Trajectplanner
- EduArte

Trends & Ontwikkelingen IAA

IAA PROCES

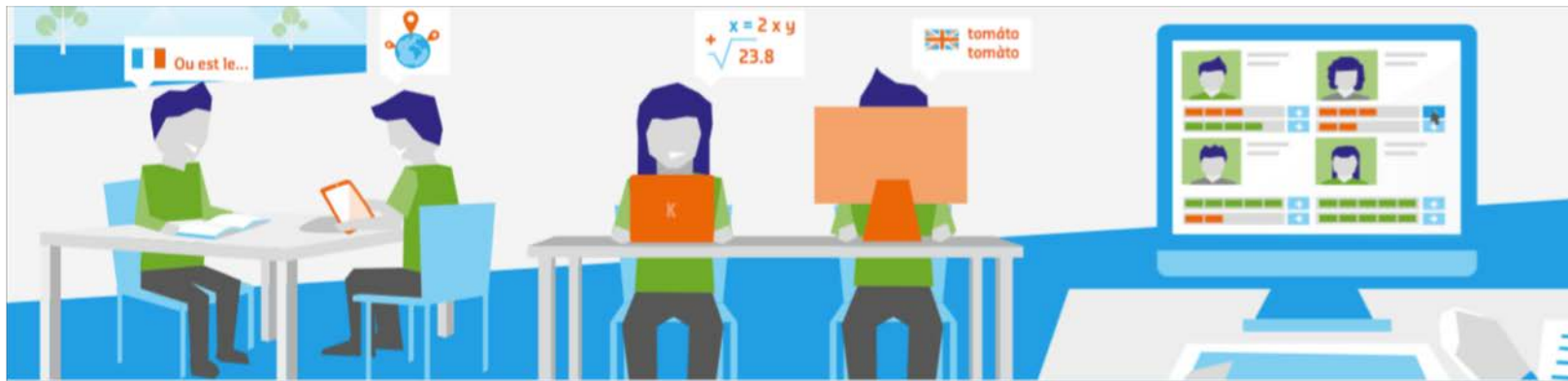


Op weg naar differentiatie



**Diversiteit dienstverlening
primaire proces neemt enorm toe!**

Privacy en beveiliging moet op orde zijn!

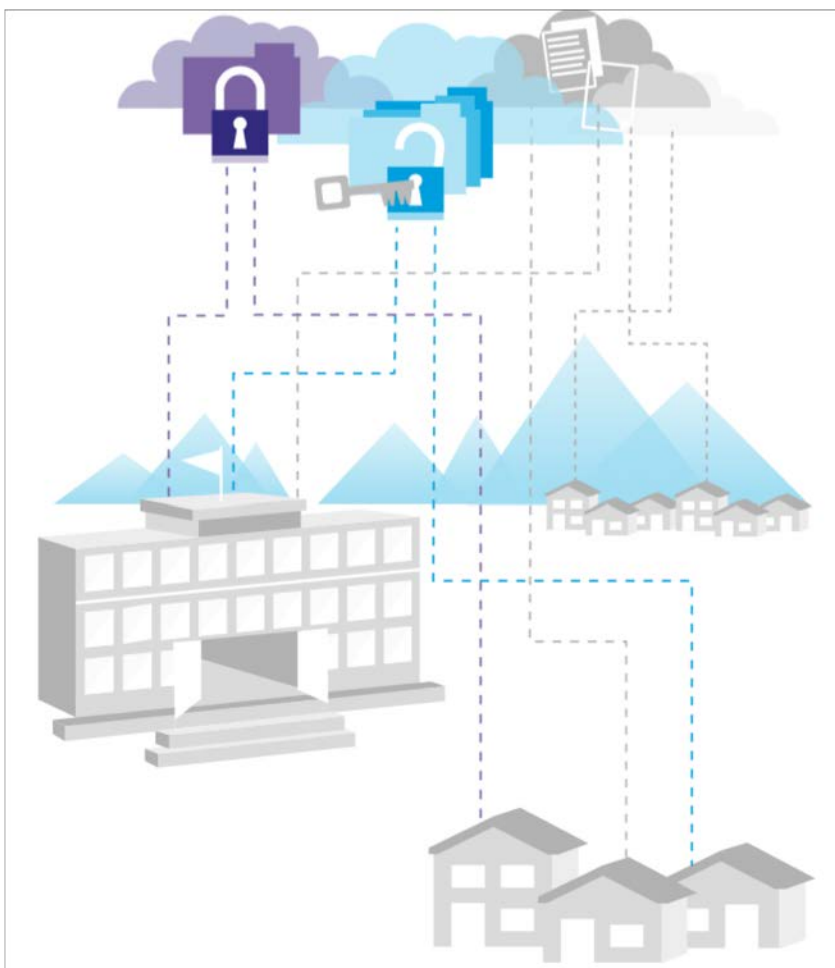


Identity management personeel & student belangrijk speerpunt...

Gezamenlijke uitgangspunten IAA



Kennisnet

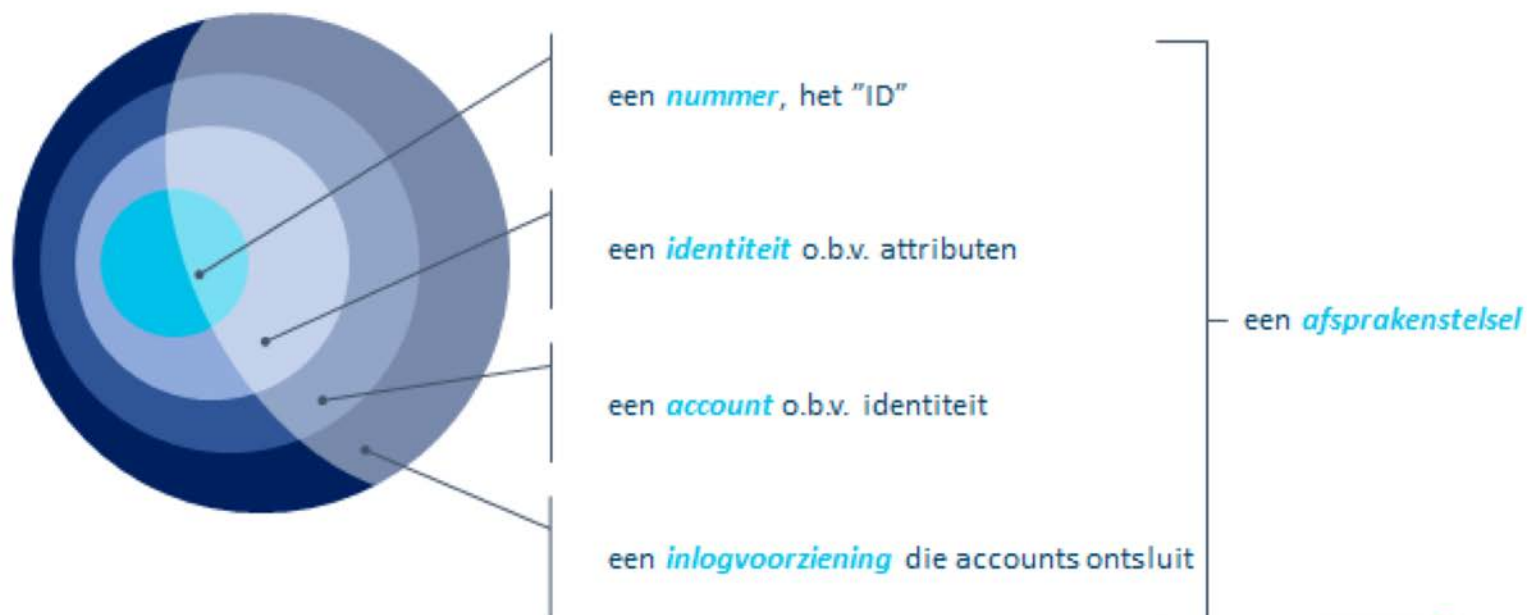


- **Gebruiker centraal/userconsent**
- **Gemakkelijk in gebruik**
- **Gemakkelijk in beheer**
- **Veilig**
- **Betrouwbaar in gebruik**
(en in de partijen die er achter zitten)
- **Privacy wordt gerespecteerd**
 - **AVG proof**
 - **Privacy by Design,**
 - **Gebruiker bepaalt**
- **Schaalbaar**
- **Betaalbaar**
- **Levenslang (wens)**
- **Niet-commercieel**
- **Ondersteunt machtigingen**
- **Belang van attributen neemt toe**

Trends & Ontwikkelingen bij SURF

- edulD verkenning (plus vergelijk ECK-ID en edulD)
- edubadges pilot 2018-2019
- eduMij- Online Persoonlijk LL Ontwikkeldossier
- Regie op Inkoop van Identity- en Access Management

Mogelijke invullingen van het eduID



Voorbeelden gebruik eduID



Vergelijk ECK-ID en eduID

	ECK-ID	eduID
Status	operationeel	verkenning
Doelgroep	PO, VO en MBO	LLL (te beginnen bij HO)
Reikwijdte	Educatieve Contentketen	ntb
Aanleiding	Privacy! Optimalisatie van de keten	studentenmobiliteit, instellingsoverstijgendID, LLL, edumij
Wat is het?	Keten- Pseudoniem	ntb

Doel proof of concept / pilot SURFnet edubadges 2018-2019

PoC Aantonen dat open badges in de HO praktijk toegepast kunnen worden en microcredentialing mogelijk kunnen maken (de keten inrichten en werkend krijgen).

Pilot Hoe organiseren we dit en maken we het toekomstvast? Welke randvoorwaarden moeten er afgesproken worden om tot dienstverlening te komen. Geleerde lessen/ervaring vanuit de PoC in de praktijk toepassen. O.a. badges duurzaam opslaan, geïntegreerd met LMS'en, signing badges etc

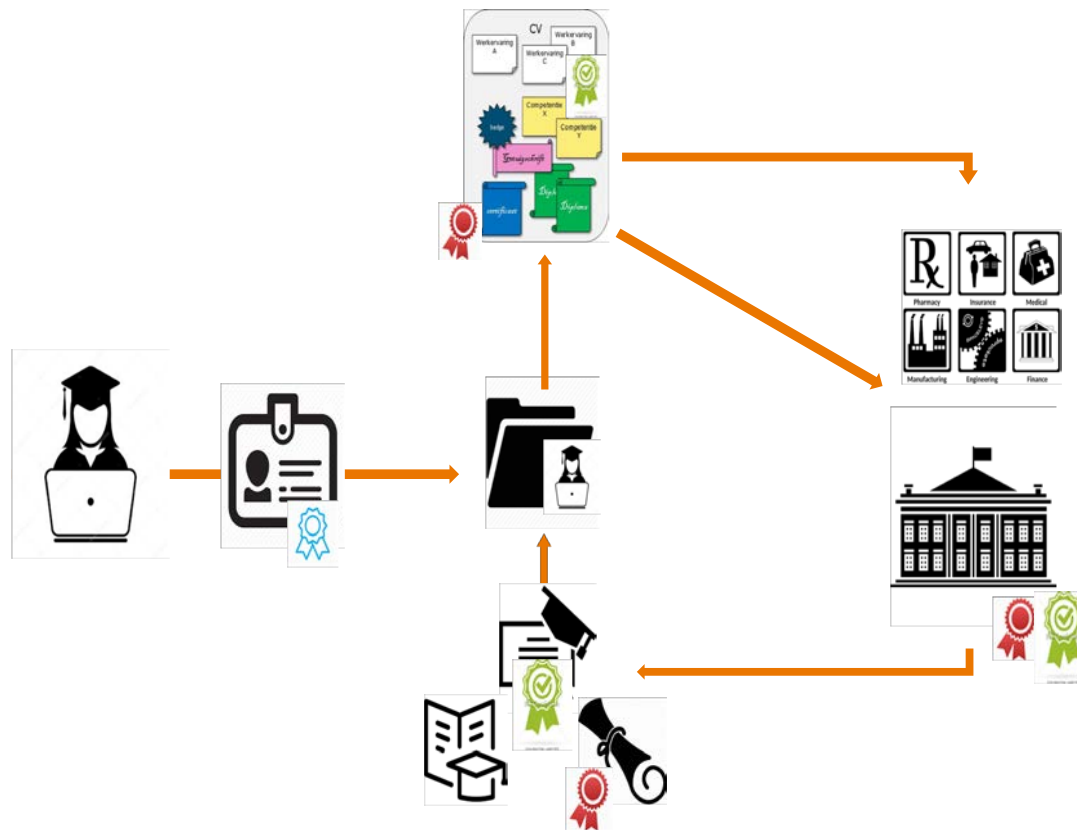
Hogerliggend doel

Met elkaar tot een standaard komen over hoe je badges waardeert (bestuurlijke borging van het bredere gebruik van microcredentialing).

Participating institutions Pilot



eduMij: een persoonlijk en levenslang educatie- & ontwikkeldossier (conceptueel)



De drie pijlers van eduMij

1) Personal Datamanagementomgeving (online opslag, folders, mogelijkheid tot delen)



- SURFdrive obv Owncloud (+ 'goedkoop' en van en door HO&O&MBO, - (nu) niet voor iedereen en ook niet LL)
- OneDrive, DropBox, GoogleDrive,..... (+: voor iedereen, -: vendorlock, privacy, prijs, ?: niet koppelbaar aan LL ID, LL)
-

2) Levenslang ID



- DigID (+: iedereen heeft t al, -: kosten, ? = wettelijke grondslag gebruik BSN ontbreekt)
- eduID (+: 'goedkoop', in potentie LL, -: is er nog niet)
- Hybride (1x DigID, daarna eduID)
-

3) Trustframework en Trusted Party/Parties om authenticiteit en integriteit te waarborgen

- Digitale certificaten/PKI
- PGP
- Edubadges/microcredentials: SURF pilot met 15 instellingen
- (non)permissioned Blockchain
- Solid by Tim Berners-Lee
- **Trusted Parties:** het Onderwijsveld (incl. koepels), OCW, DUO, SURF,.....



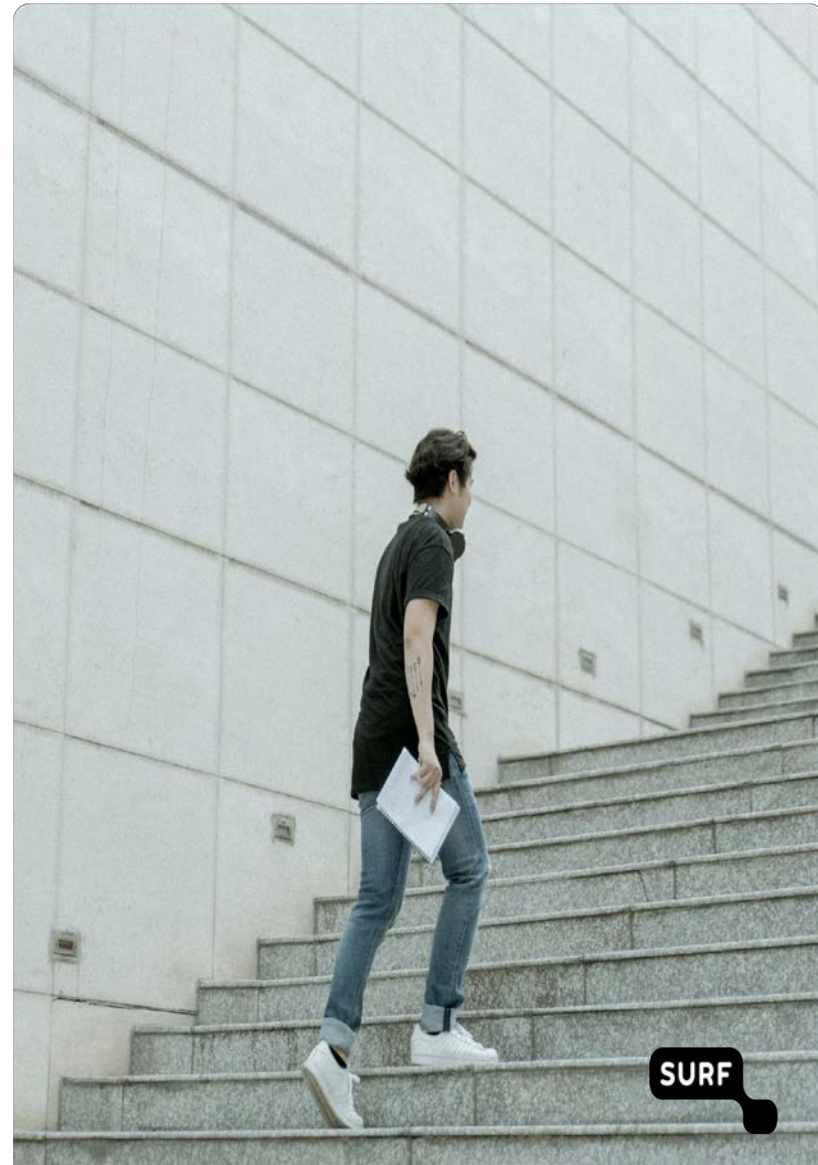
A close-up photograph of a person's hands holding a silver smartphone. The person has pink nail polish and is wearing a ring on their left hand. The phone is held over a laptop keyboard, which is partially visible. The background is blurred, showing a wooden desk and a blue object. A semi-transparent white box with a speech bubble tail is overlaid on the left side of the image, containing the title text. In the bottom right corner, there is a small black logo with the word 'SURF' in white.

Regie op Inkoop van Identity- en Access Managementsystemen

Stappenplan CSC's

1. Vaststellen welke oplossingen binnen Access tooling door de onderwijssectoren moeten worden opgepakt
2. Vaststellen welke oplossingen nog niet in het portfolio van SURF zitten?
3. Welke oplossingen kunnen door SURF:
 - worden aangeboden

37





Vraagstukken aan CSC's over Access

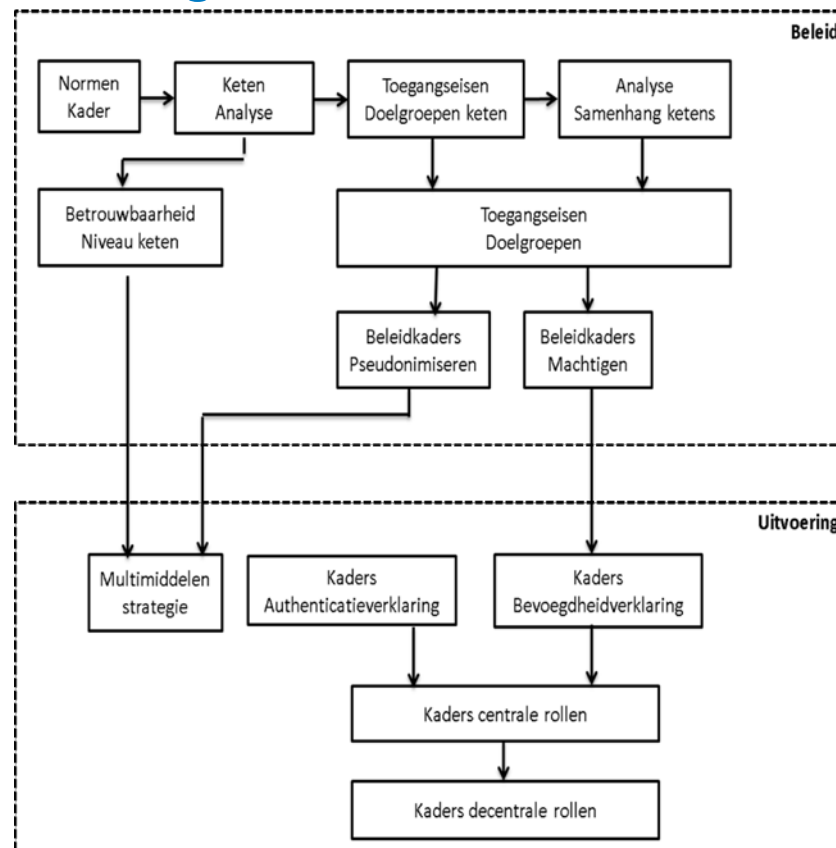
tooling aanpak

• In welke mate gaan we Identity Access Management gaan we **per onderwijssector** samen inzetten ?

- In welke mate is er behoefte aan het centraliseren van identiteiten op basis van het voorgestelde stappenplan CSCs ?
- In welke mate stelt u resources beschikbaar (i.v.m. expertise en planning) om aan deze aanpak bij

Toekomstbeeld toegang!

Alleen gaat sneller, maar samen kom je verder

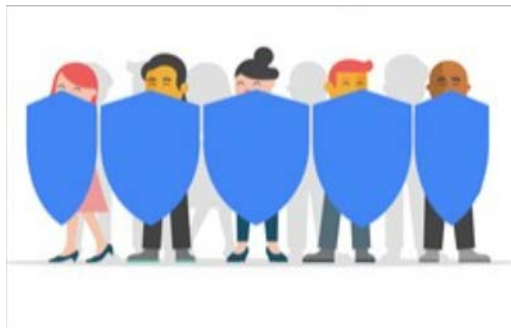


edustandaard

Scholen en leveranciers AVG

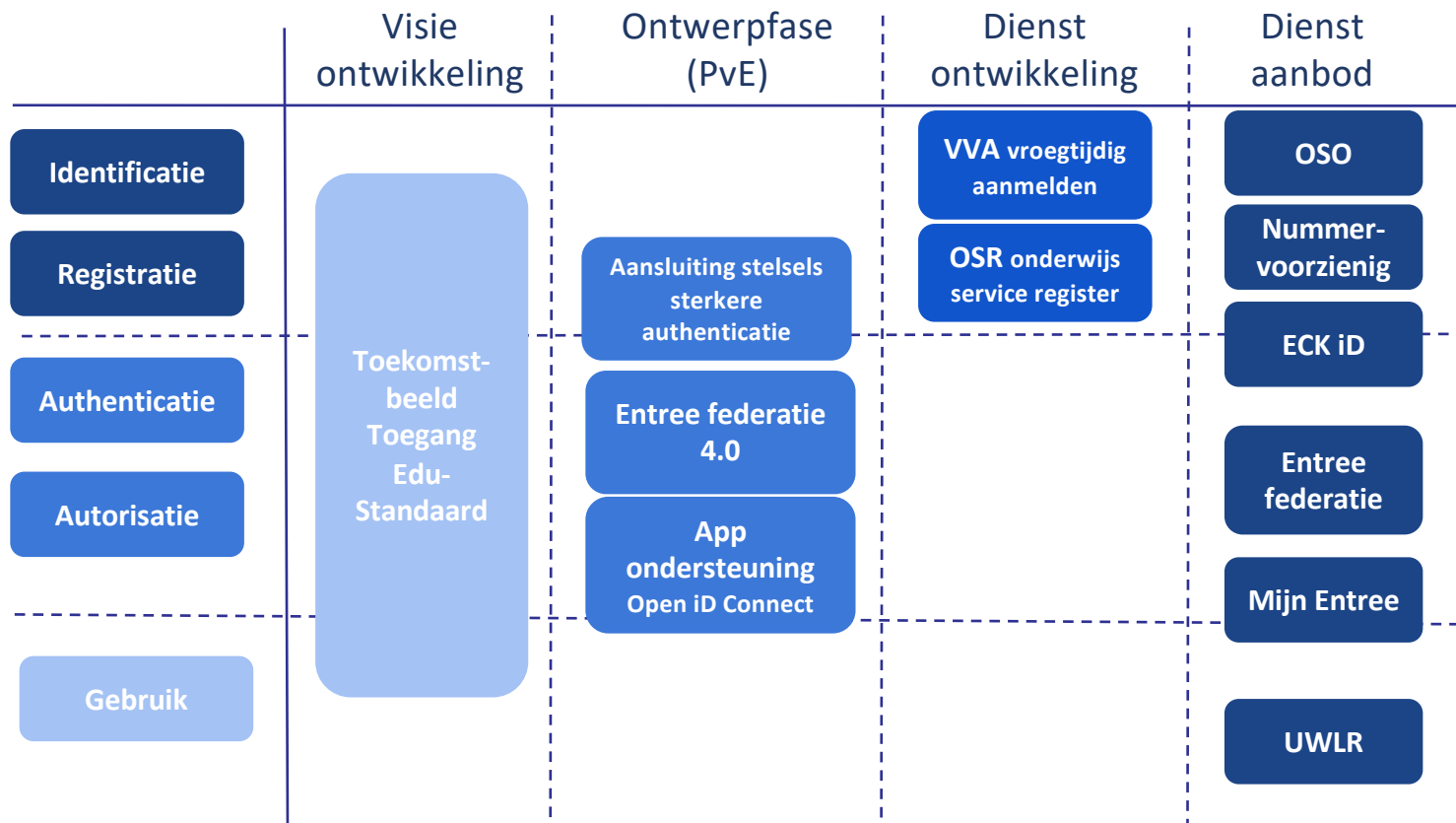
proof

Privacyconvenant



Certificeringsschema





**ENTREE**
federatie

MIJN ENTREE FEDERATIE

MIJN SCHOOL

overzicht attributen

statistieken

wijzigingsgeschiedenis

DIENSTEN

attributen vrijgeven via arp

doorgifte attributen beheren

toegang instellen

SUPPORT

uitleg

support@kennisnet.nl

0800-3212233

MIJN ENTREE FEDERATIE BETA

Doorgifte attributen beheren

Chris Tanahatoe
asdf (sdf) ▾

Elke dienst heeft bepaalde attributen (persoonsgegevens) nodig om te kunnen werken. Als je de doorgifte van specifieke attributen aan een dienst wilt wijzigen, dan kun je dat hier aanpassen.

i Let op: als je de doorgifte van attributen aan een dienst wijzigt, dan is de kans aanwezig dat de dienst onvoldoende attributen heeft om (bepaalde) gebruikers toegang te kunnen geven. Pas deze attributen daarom alleen aan als dit echt nodig is of als je precies weet wat je aan het doen bent!

Zoek de dienst

Dienst:

Zoeken **Reset**

Toon 10 resultaten ▾

DIENST(25270)	IDP / ELO	DOORGIFTE ATTRIBUTEN
dlrebd	ws-erwin-elo-org2	Bekijk doorgifte
dlrebd	ws-erwin-elo-org3	Bekijk doorgifte
dlrebd	789789789	Bekijk doorgifte
dlrebd	ws-erwin-elo-org	Bekijk doorgifte

ENTREE federatie

MIJN ENTREE FEDERATIE

MIJN SCHOOL

overzicht attributen

statistieken

wijzigingsgeschiedenis

DIENSTEN

attributen vrijgeven via

doorgifte attributen beheer

toegang instellen

SUPPORT

uitleg

support@kennisnet.nl

0800-3212233

dlrebd

IdP/ELO: 789789789

De volgende attributen worden gedeeld:

Om toegang te verlenen maken diensten gebruik van attributen: gegevens waaraan een school of gebruiker kan worden herkend. Hier kun je wijzigingen aanbrengen in welke attributen door jouw school zullen worden gedeeld met deze dienst.

Gedeelde attributen:

- ✓ givenName - Voornaam

Geblokkeerde attributen:

- ✗ nlEduPersonHomeOrganizationId - Brin instelling
- ✗ nlEduPersonHomeOrganization - Naam instelling
- ✗ eduPersonAffiliation - Rol

wijzigen

Toon 10 resultaten

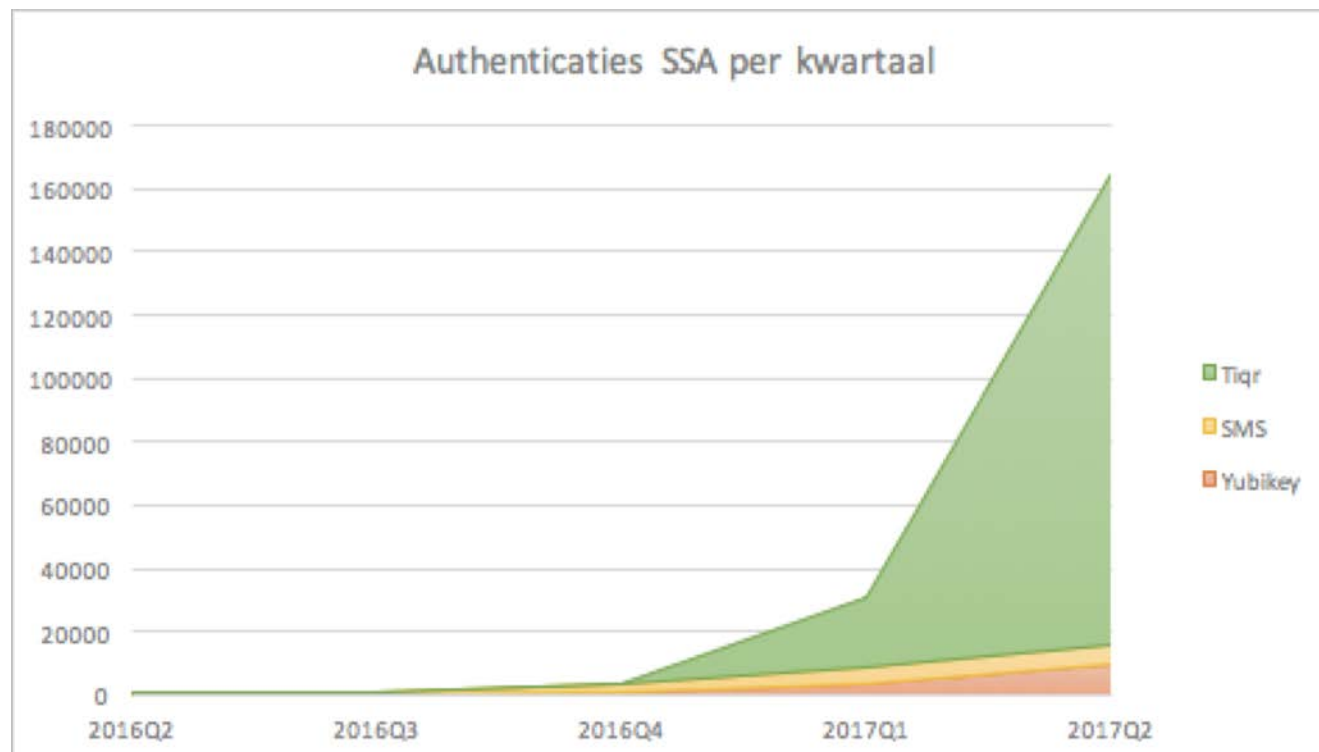
DIENST(25270)	IDP / ELO	DOORGIFTE ATTRIBUTEN
dlrebd	789789789	Bekijk doorgifte
dlrebd	JSTC6	Bekijk doorgifte
dlrebd	ws-erwin-saml-idp	Bekijk doorgifte
dlrebd	ws-erwin-elo-org2	Bekijk doorgifte

Vragen

????

Eventuele Extra (hulp)sheets

Gebruik sterke authenticatie groeit!

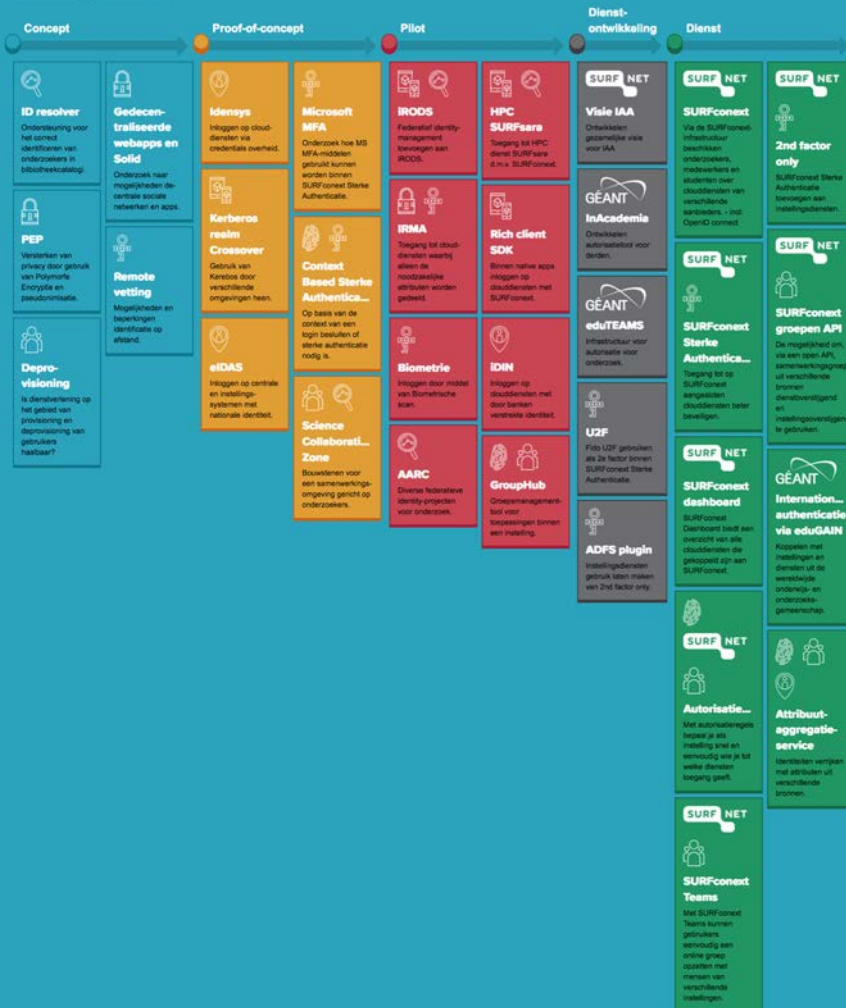


Trust en Identity

Innovatie bij SURF is een proces waarbinnen een idee zich gedurende een aantal opeenvolgende fases ontwikkelt tot een nieuwe dienst. Innovatieprojecten passen in de visie van SURF. Versie: december 2017

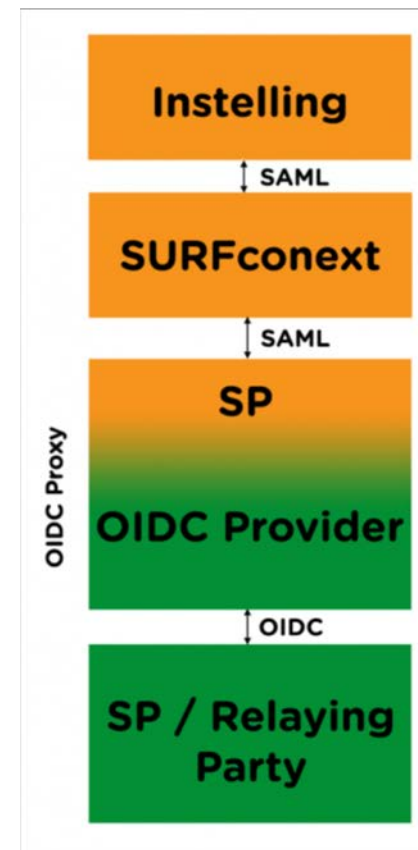
SURF

▼ Toon legenda ▼ Kies categorieën

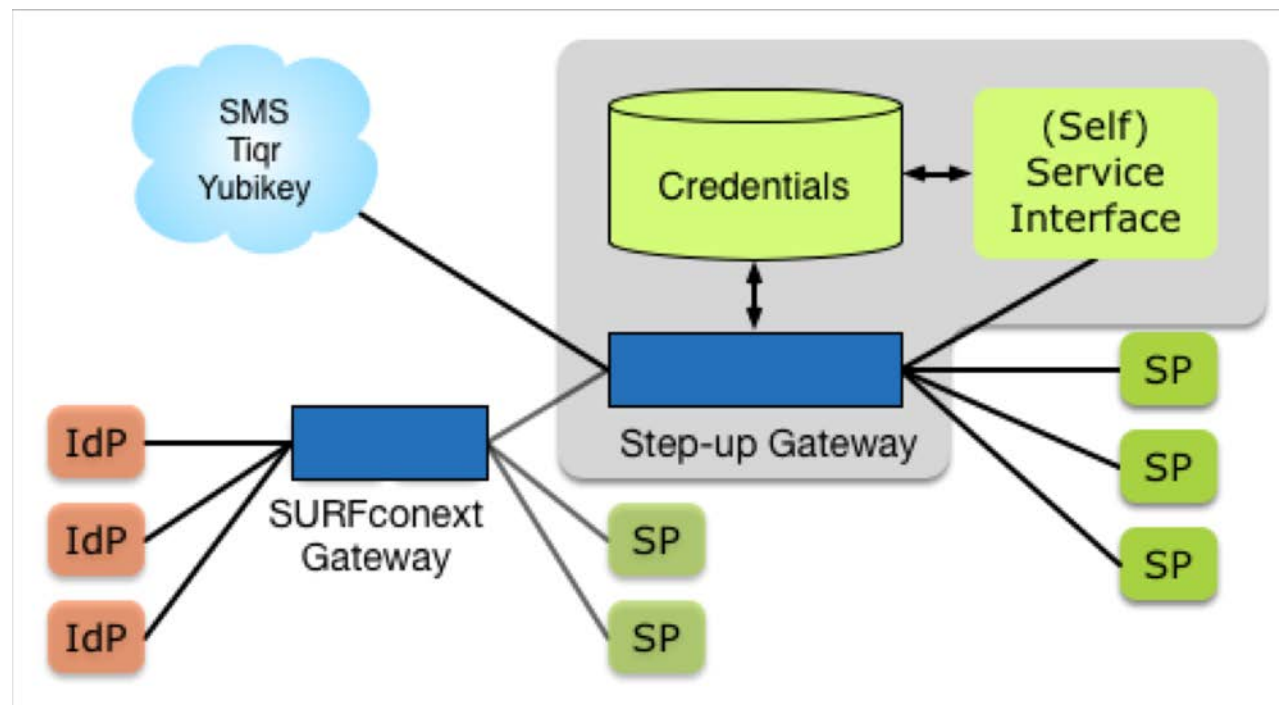


Toegang tot apps (Open ID Connect)

- SAML en Open iD connect
- Met de voordelen van de federaties kunnen we innovaties blijven ondersteunen



Strategie sterke authenticatie Surfconext



Koffiepauze



Red Spider, toekomstvisie

7 december 2018

Roy Dusink

> Agenda

- Wie zijn we?
- Architectuur
- Probleemstelling
- Uitdagingen
- Visie – waar willen we naar toe
- (Toekomst)plannen

> Wie zijn we?

- Gebruikersvereniging
- 11 instellingen (MBO & VO)
- Ontwikkelen en onderhouden Identity management oplossing met koppelvlakken
- Op basis van NetIQ IDM 4.6
- Koppelvlakken zijn eigendom vereniging
- Leden betalen jaarlijks contributie voor ontwikkeling en onderhoud

> Instellingen



ONDERWIJSGROEP TILBURG



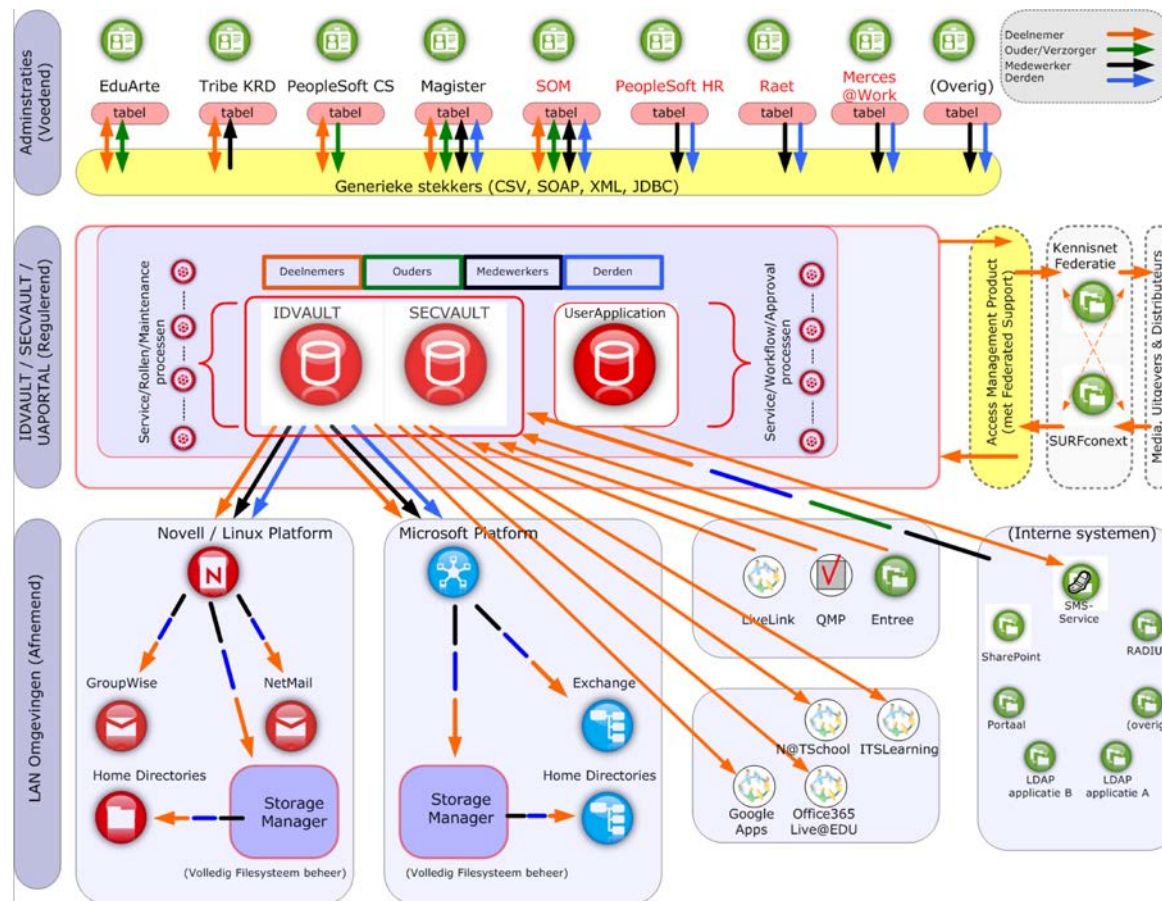
wellantcollege
II



roc van
twente



➤ Architectuur



> Kracht vereniging

- Gezamenlijk ontwikkelen en onderhouden
- Voorbeeld ECK iD
 - Technische impact -> encryptie
 - Externe datastore
 - Schooljaar 19/20 gereed
- Als vereniging:
 - Snel op kunnen inspelen
 - Met beperkte kosten voor de leden
 - Volledig aan (veiligheids)eisen voldoen



> Probleemstelling

- Technologie staat
 - 1 oplossing, 11 verschillende implementaties
 - Maatwerk
- Implementatiepartners zijn beperkt
- Access management ontbreekt vanuit oplossing, instellingen hebben eigen keuze
- Instellingen willen volgende stap maken



> Uitdagingen

- Gebruikservaring authenticatie van applicaties moet beter
- Applicaties altijd en overal beschikbaar
- Single Sign-On; éénduidig voor alle diensten
- Nieuwe wet en regelgeving (GDPR/AVG)
- ECK iD



> Visie – waar willen we heen?

Naadloze toegang	Naadloze toegang tot (cloud) diensten, ook via mobiele devices
Privacy by design	Data minimalisatie en privacybescherming. Dienstenleveranciers krijgen niet meer informatie dan nodig is voor de dienst, gepseudonimiseerd
Regie op gegevensverstrekking	De school bepaalt tot welke diensten je toegang krijgt en welke gegevens worden uitgewisseld. Inclusief het recht om vergeten te worden
Op basis van identiteit	Ontkoppeling van account en identiteit, dus geen koppeling met een specifiek (school)account
Context-based	Verrijken met attributen

> Visie – waar willen we heen?



- Context-based login
 - wie | wat | waar | wanneer | hoe
- Kenmerken van een gebruiker
 - Geografische locatie, IP-adres, tijdstip van de dag, apparaatherkenning etc.
- Wel/niet voldoen aan beveiligingsbeleid
 - Wel/niet extra verificatiemiddel

> Visie – waar gaan we heen?

Identity management

Ligt vooral bij de instelling

Koppelingen met diversiteit aan
bronsystemen

Provisioning van (cloud)applicaties

Belang neemt af

Standaardproduct uit de markt
voldoet



Access management

Ligt voor groot deel in de sector

Naadloze ontsluiting digitaal lesmateriaal
en andere diensten

Mobiele devices
Gegevensbescherming en privacy
Ontkoppeling van account

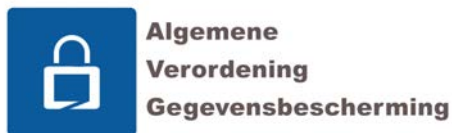
Belang neemt toe

Sectorvoorzieningen zijn cruciaal
Dit kun je niet alleen

> (Toekomst)plannen

- Wat willen we niet meer doen?
 - Directe cloud provisioning (van bron naar clouddiensten)
 - Uitwisselen van account-informatie met clouddiensten
- Wat moet daarvoor in de plaats komen?
 - Ondersteuning voor OpenID Connect (dus OAuth tokens voor anydevice)
 - Gebruik makend van de ADFS bij de instelling
 - Sectorale ondersteuning (Kennisnet Federatie/SURFconext)
 - De huidige Red Spider cloud provisioning wordt een provisioning van gegevens aan deze sectorvoorziening

> (Toekomst)plannen



> (Toekomst)plannen

- Gezamenlijke inkoop/aanbesteding voor opvolger huidig product, op basis van het (geactualiseerd) PvE
- Resultaat: geselecteerde (cloud-)product dat door elke instelling apart van een leverancier kan worden afgenomen

> (Toekomst)plannen

- We streven naar één centrale voorziening voor het accessmanagement
- Ondersteuning voor OpenID Connect en Oauth
- Generieke voorzieningen voor 2-factor authenticatie
- **Red Spider vereniging wil**
 - Actief participeren in de centrale voorziening
 - Is bereid eventueel mee te financieren voor realisatie
 - Launching customer zijn voor de introductie van nieuwe functionaliteit
 - Pilot school zijn

REDSPIDER
GEBRUIKERSVERENIGING



Lunch

Programma



10:00 Wet Digitale Overheid, Barbera Veltkamp (Min. BZK)

10:30 Algemene ontwikkelingen IAA bij SURF & Kennisnet,
HP Köhler (Kennisnet) en Roel Rexwinkel (SURF)

11:15 Pauze

11:40 Vereniging Red Spider, Roy Dusink

12:00 Lunch

13:00 Centraal Aanmelden, Jan Bartling (saMBO-ICT)

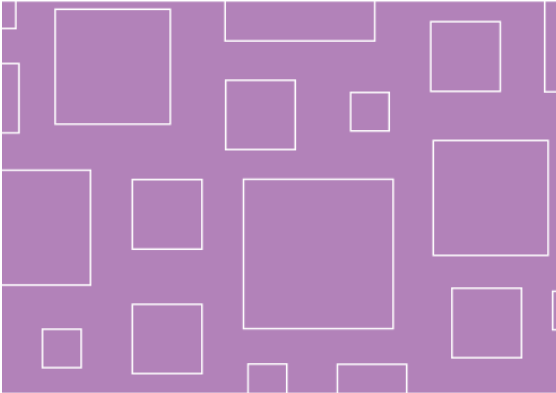
13:20 Onderwijsgroep Tilburg, Merijn van der Schoot

13:40 Koning Willem 1 College, Jef van den Hurk

14:00 Paneldiscussie

14:45 Afsluiting met borrel

Centraal Aanmelden: identificeren

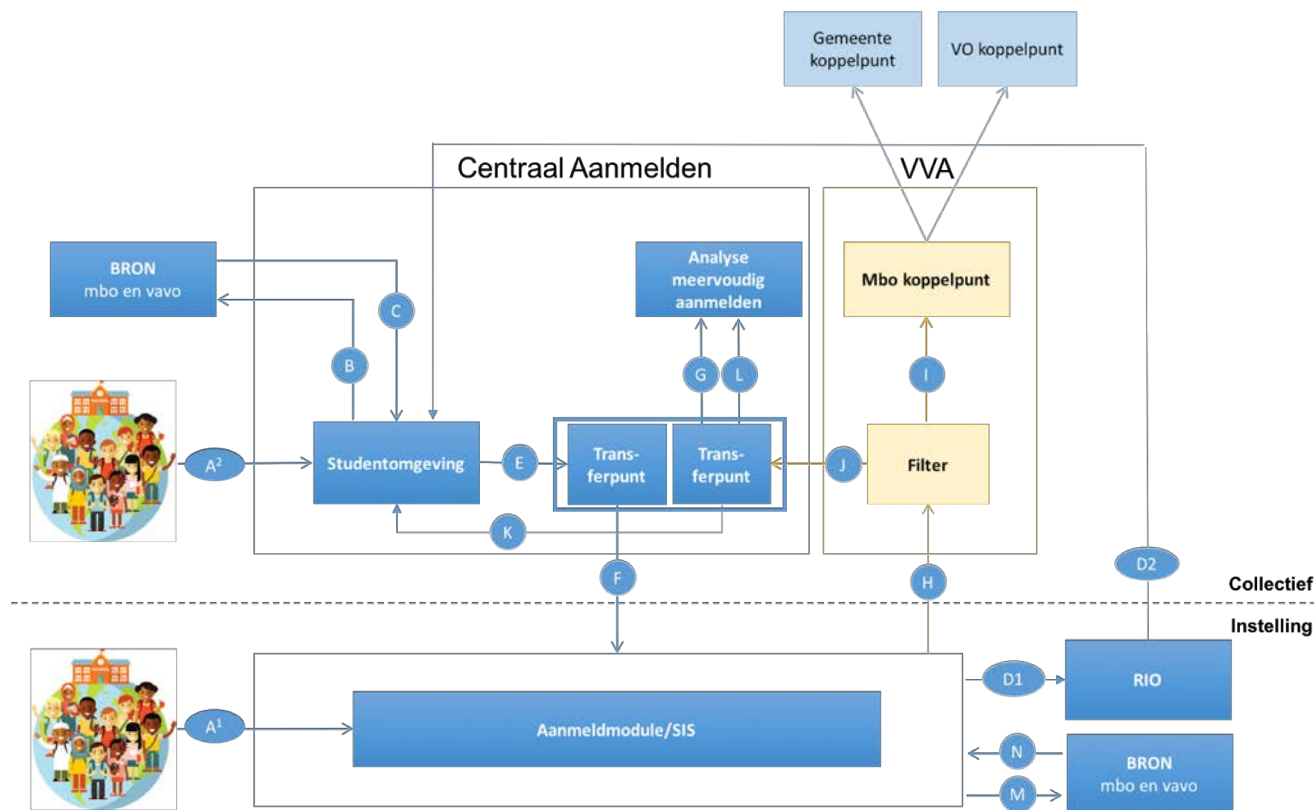


Auteur	Jan Bartling
Datum	7 december 2018

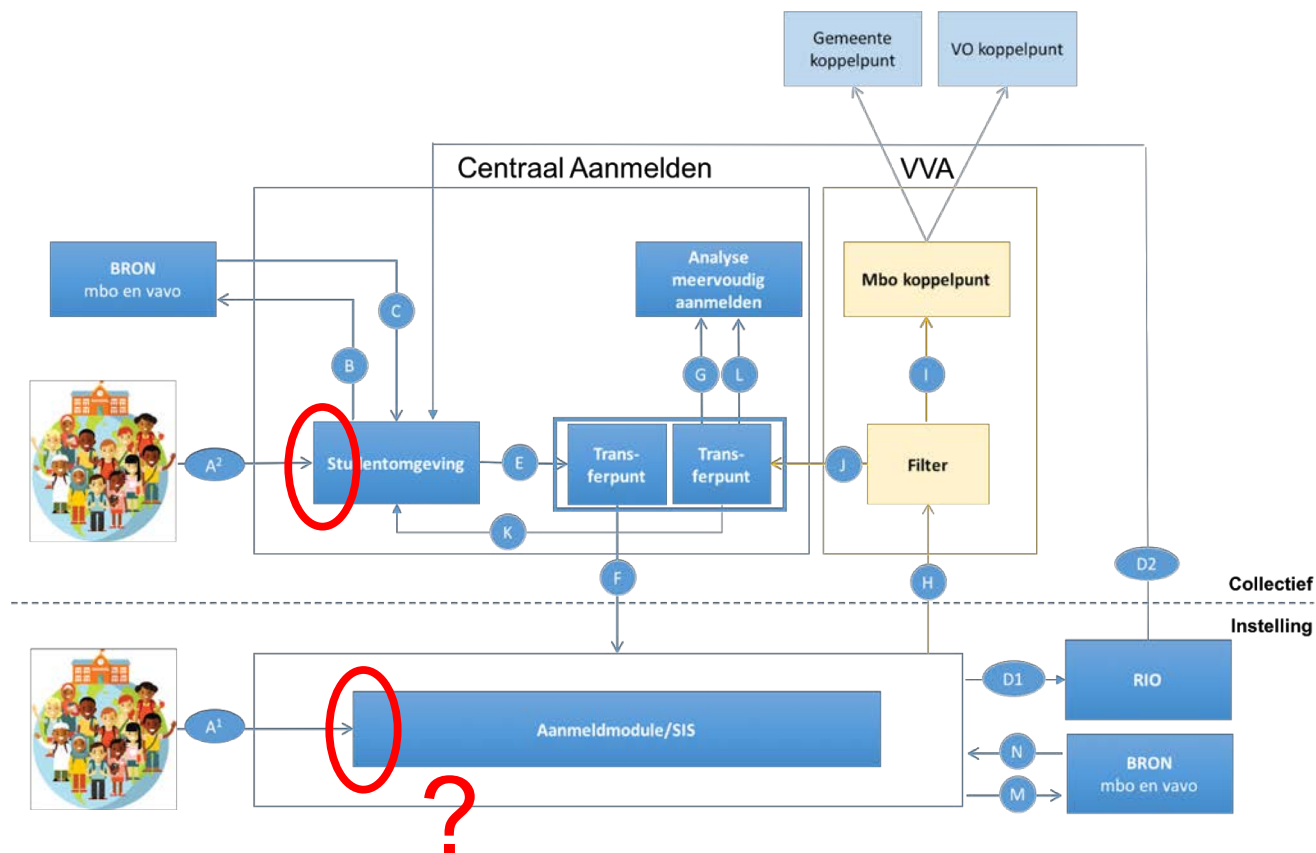
Opbrengsten centraal aanmelden

- Aanmelden heeft juridische status; centraal aanmelden levert een bijdrage aan heldere manier van aanmelden
- Aanmelden bij het MBO is/wordt uniform
- Identificatie wordt efficiënt (nl 1x) geregeld
- Inzicht in meervoudige aanmeldingen
- Centraal aanmelden is randvoorwaardelijk om op sectorniveau aantal aanmeldingen per student te limiteren

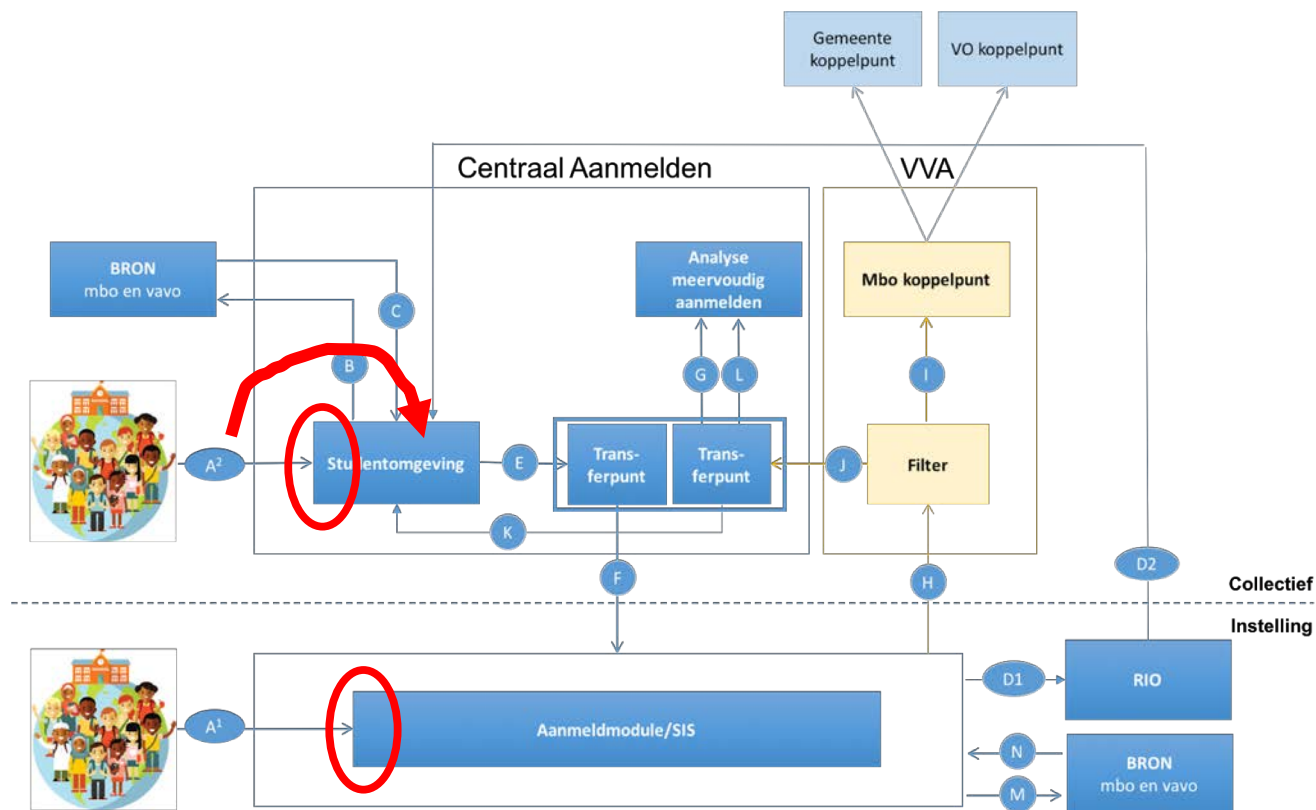
Centraal Aanmelden; schematische weergave



Centraal Aanmelden; met e-ID

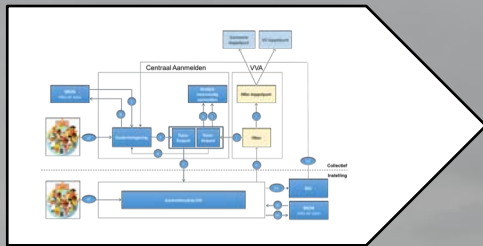


Centraal Aanmelden; zonder e-ID



Centraal Aanmelden; een begin?

saMBO-ICT



Intake

KRD

Leermiddelen

Strategische agenda mbo

saMBO-ICT



Uitdagingen identificatie

saMBO-ICT

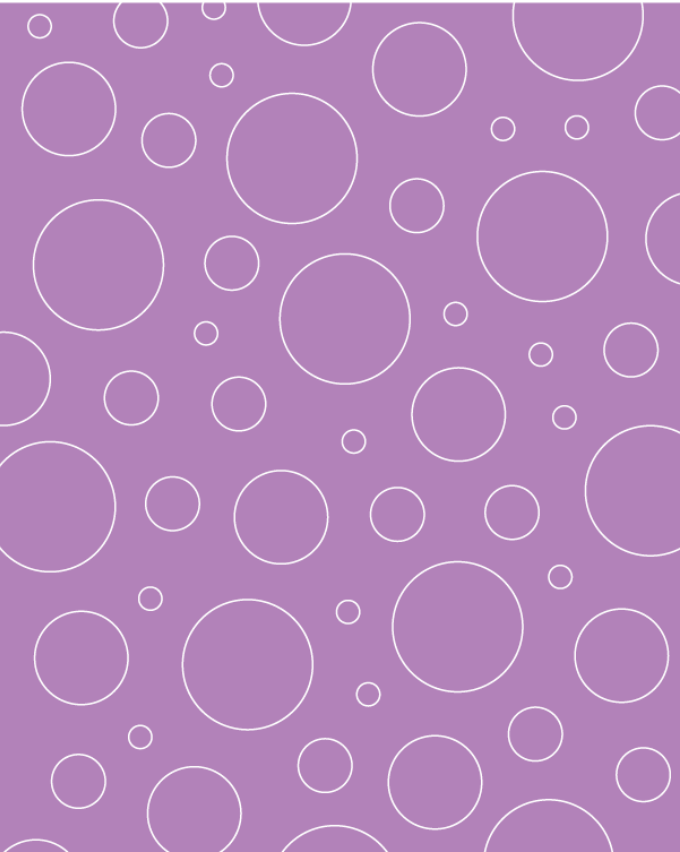
- 1 **Inhoud van het onderwijs aanpassen**
 - ➔ Werk maken van een leven lang ontwikkelen
 - ➔ Werken aan digitale burgerschapsvaardigheden

- 2 **Flexibilisering van het onderwijs realiseren**
 - ➔ Er wordt gezamenlijke regie gevoerd op leermiddelen
 - ➔ Elke student heeft een eigen dossier
 - ➔ Onderwijslogistiek maakt flexibilisering mogelijk

- 3 **Digitalisering van het leren faciliteren**
 - ➔ Docenten kunnen zich ontwikkelen en worden daarin gefaciliteerd
 - ➔ Gebruik van data-ondersteund-onderwijs

Hoe gaan we om met toekomstige ontwikkelingen?

saMBO-ICT



Jan Bartling

E Jan.bartling@sambo-ict.nl

M 0348-75 35 00

RedSpider Is Just An Application



Merijn van de Schoot
7 december 2018

Onderwijsgroep Tilburg

- 18 scholen
- 13.000 deelnemers
- 1.300 medewerkers

IDM in getallen

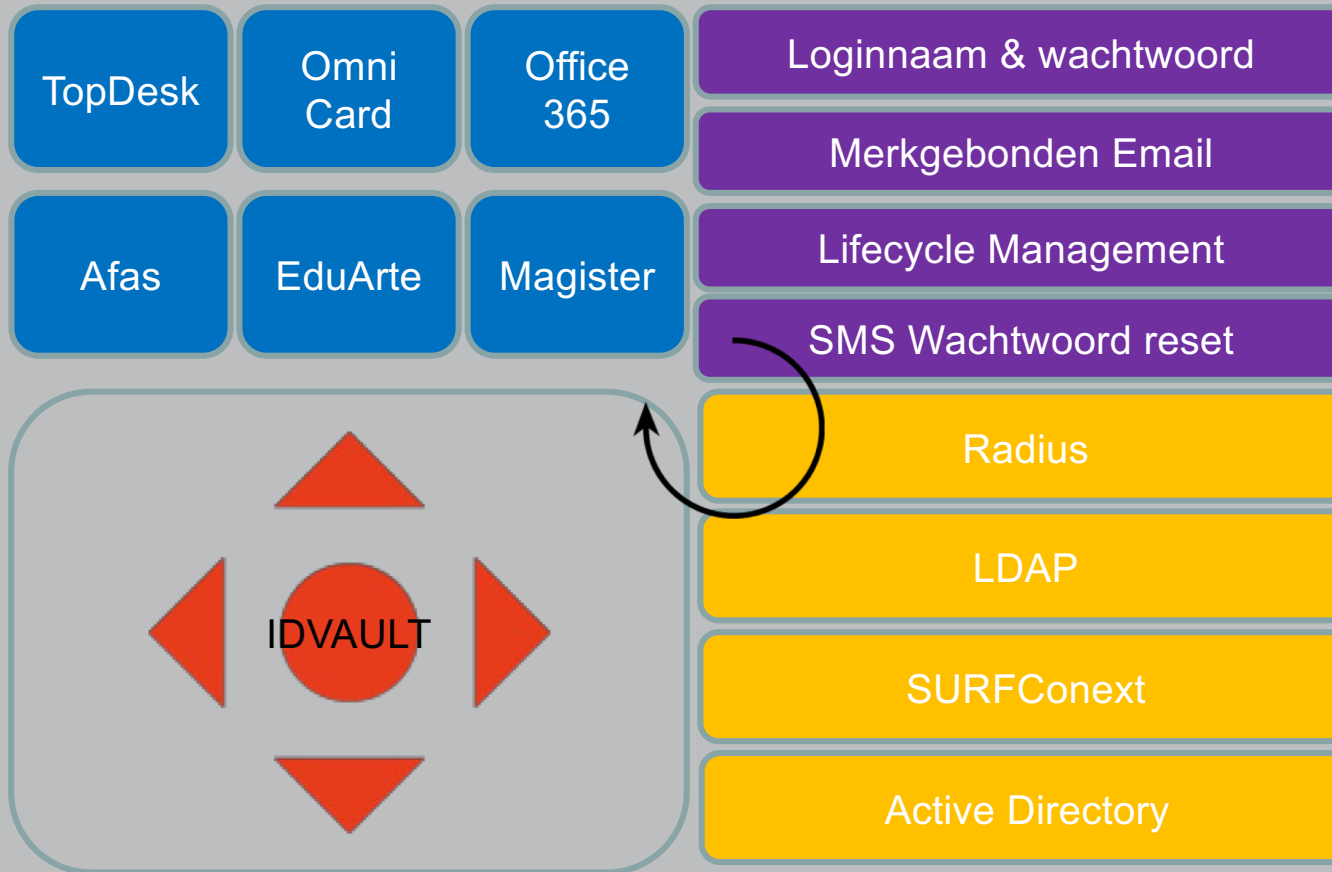
- Binnen 15 minuten kan je alles!
- Pasje? Binnen 1 seconden actief
- Pasfoto? Binnen 1 seconde doorgezet
- 100% sluitend met administratie

IDM in getallen

- Binnen 15 minuten kan je alles!
- Pasje? Binnen 1 seconden actief
- Pasfoto? Binnen 1 seconde doorgezet
- 100% sluitend met administratie



Architectuur



Één proces uitgelicht

AFAS
software



HR Proces

- ...wij zijn bijzonder
- ...standaard driver voldoet niet
- ...we hebben ook externen
- ...we hebben ook mensen niet geadministreerd
- ...'s ochtends staan er mensen op de stoep
- ...we hebben ook gasten
- ...het HR proces is zo langzaam
- ...etc

HR Proces

- Bijna 2 jaar aan het (ver)bouwen geweest
- Iedere keer zagen we iets over het hoofd
- Techniek werd onvoorspelbaar door alle uitzonderingen
- Iedereen was ontevreden
- Eindgebruiker was de dupe
- Veel geld (manuren) 'verbrand'

**If at First You
Don't Succeed
BLAME THE COMPUTER!**

barrysworld.biz

**Aanname:
over het (proces) ontwerp van de
driver is nagedacht**



HR Proces

- Waarom hebben we mensen niet geadministreerd?
- Waarom staan 's ochtends mensen op de stoep?
- Wanneer worden deze mensen gebeld?
- Wie zijn onze gasten?
- Waarom is HR langzaam?
- Wat wil (vanuit IT gezien) onze klant?
- Wat wil (vanuit HR gezien) onze klant?

DNA

- Gebruikersnaam en wachtwoord beleid
- Beleid: tokens
- Beleid: BIV
- Beleid: PIA
- Beleid: HR is de basis (ook externen)
- Beleid: b_ en t_ accounts
- Beleid: gastaccounts



Gasten

Gasten hebben alleen behoefte aan wifi

Eduroam Visitor Access zorgt voor deze toegang

Enthousiast ontvangen door de organisatie,
selfservice door medewerkers

100% sluitend met administratie,
accounts zijn binnen 1 seconden actief

APPROVED

HR in hun kracht!

- Spinoff: nieuwe medewerkers kunnen selfservice in het HR portaal alles regelen
- Spinoff: schooldirecteur geeft akkoord met één muisklik
- IT garandeert inloggen binnen x periode
- HR is geen administratieve typemiep (meer)
- HR heeft zicht op al het personeelsverloop
- HR adviseur in dialoog met directeur (bijvoorbeeld melding einde contract)
- Schooldirecteur is autonoom en zelfstandig

Wat gaat er fout?

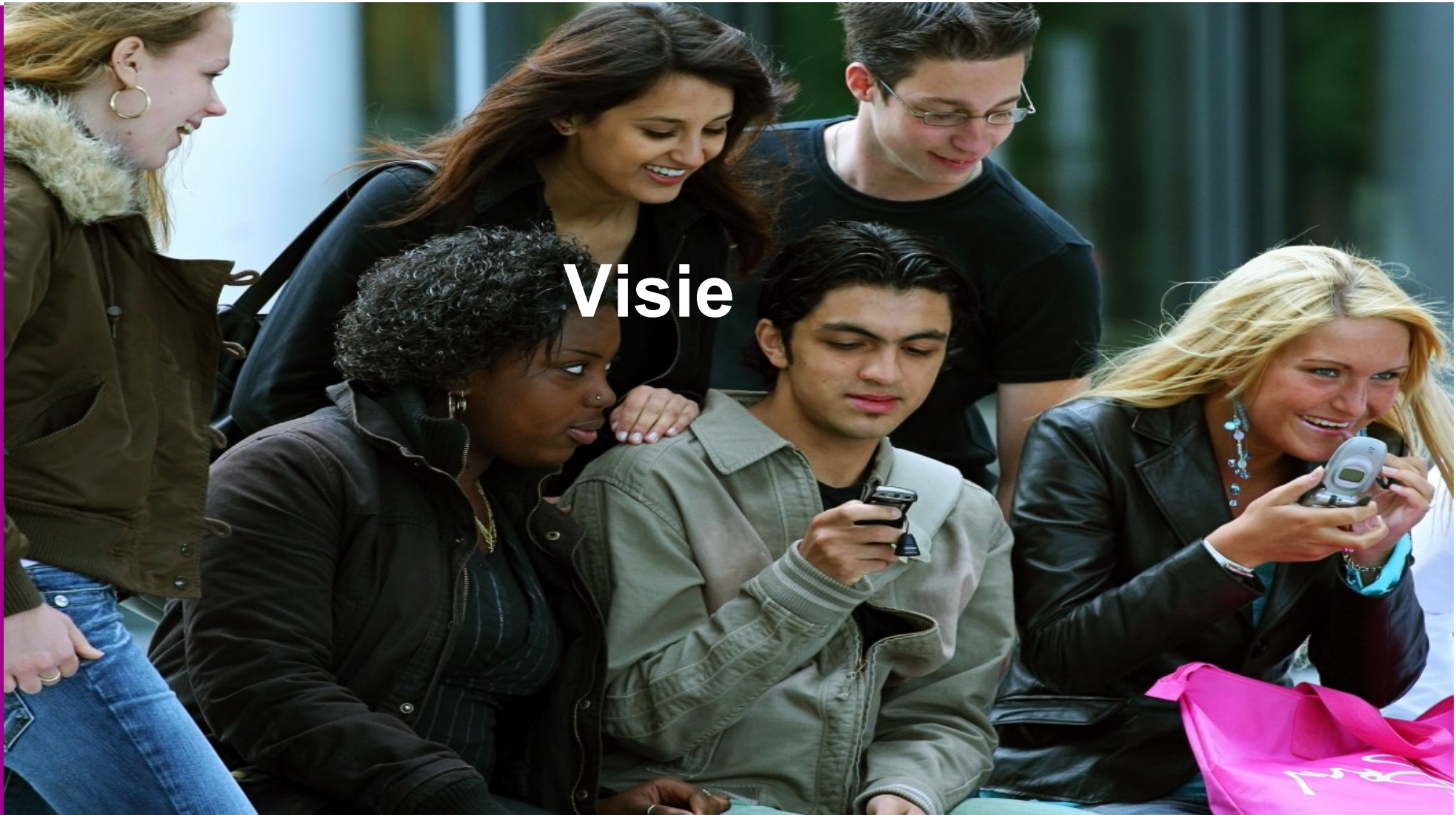
- Medewerker kon op 3 december niet meer inloggen.
Reden: schooldirecteur was vergeten nieuw contract te accorderen binnen HR systeem.
- Schoonmaakpersoneel had per 1 september geen toegang meer tot gebouwen.
Reden: verantwoordelijke was vergeten binnen HR systeem (externen) contract te verlengen.
- **HR is altijd leidend. Zonder uitzondering.**



Over het (proces) ontwerp van de
driver is nagedacht:
wij zijn niet bijzonder

Ook jullie zijn niet bijzonder

Visie

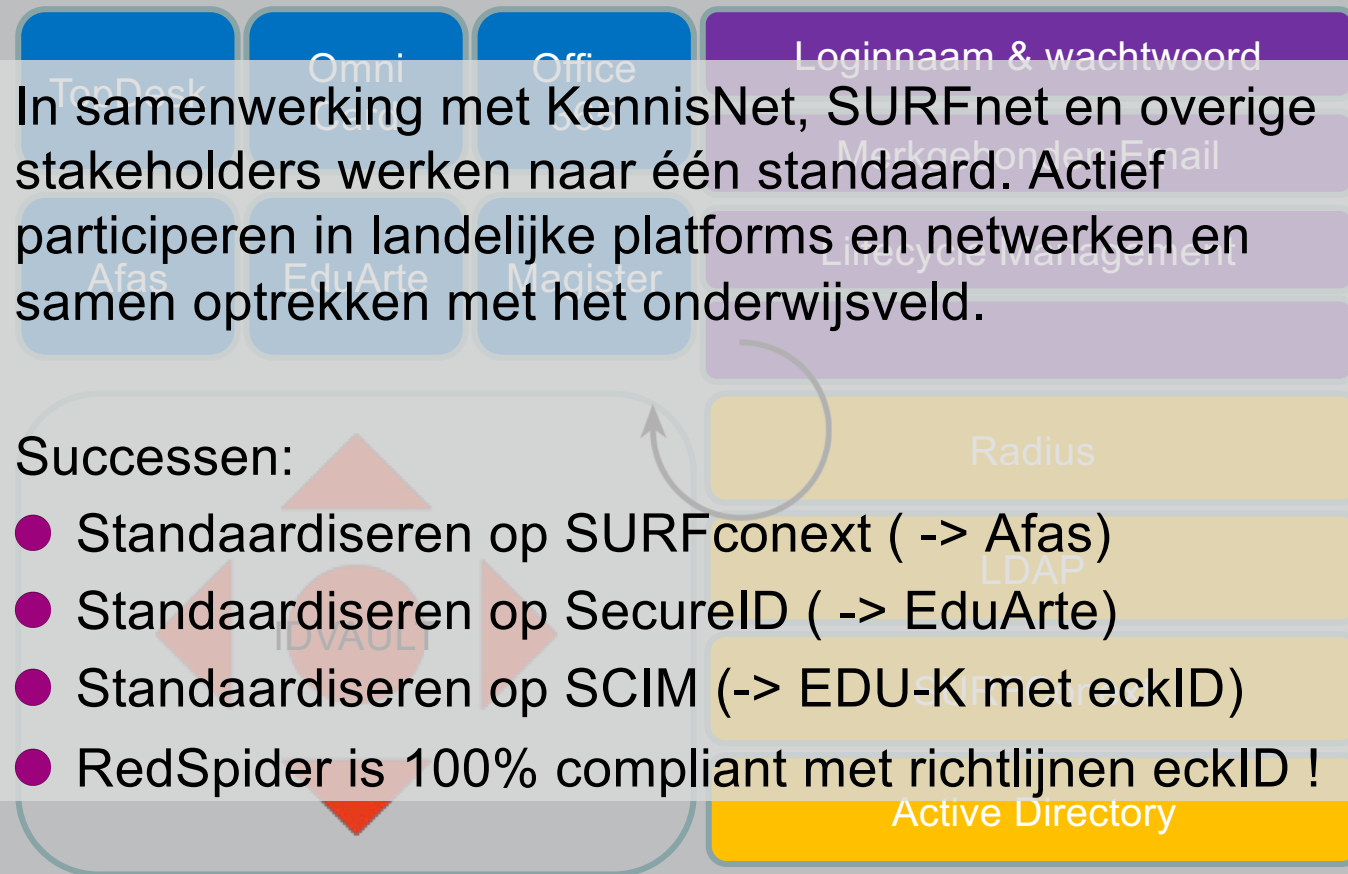


Visie

In samenwerking met KennisNet, SURFnet en overige stakeholders werken naar één standaard. Actief participeren in landelijke platforms en netwerken en samen optrekken met het onderwijsveld.

Successen:

- Standaardiseren op SURFconext (-> Afas)
- Standaardiseren op SecureID (-> EduArte)
- Standaardiseren op SCIM (-> EDU-K met eckID)
- RedSpider is 100% compliant met richtlijnen eckID !



Visie

Stelling	Versie
Voor het inloggen wordt aangesloten op SURFconext. Het systeem maakt, indien gewenst door de Onderwijsgroep Tilburg, gebruik van onze IDVAULT voor het ophalen van identiteits-attributen. Hierdoor wordt single sign on en het vullen middels RedSpider mogelijk.	1.0
De cloud dienst ondersteunt zowel het IPv4 als het IPv6 protocol.	1.0
Kan de cloud dienst volledig functioneren op een door Onderwijsgroep Tilburg te bepalen domeinnaam?	1.0
Kunnen updates en upgrades in productie worden uitgerold en zijn daarvoor geen service windows nodig (continuous delivery)?	1.0
Voldoen aan de norm van min. 3 t.a.v. het volwassenheidsniveau waar het mbo normenkader van toepassing is.	1.0
De cloud provider maakt federatief inloggen met het instellingsaccount mogelijk op basis van SURFconext	1.0
De cloud provider ondersteunt IDP initiated login.	1.1
De cloud provider maakt het mogelijk om veiligere authenticatie te doen met een extra authenticatiemiddel, zoals SMS dienst, One-Time-Password (OTP) tokens en Smart Phone apps	1.0
De cloud provider maakt het mogelijk dat veiligere authenticatie, naar keus van Onderwijsgroep Tilburg, afgehandeld wordt door de cloud dienst of door het SURF SecureID platform.	1.0
Ondersteunt u Step Up authentication op het SURF SecureID platform voor specifieke, configureerbare rollen?	1.0

Visie

Wij zijn regievoerder

- iDIN? SURFconext als broker
- DigiD? SURFconext als broker
- Gasten? SURFconext als broker (OneGini)
- eIDAS? SURFconext als broker
- Tokens? SURF SecureID als broker

Loginnaam & wachtwoord

Merkgebonden Email

Lifecycle Management

Radius

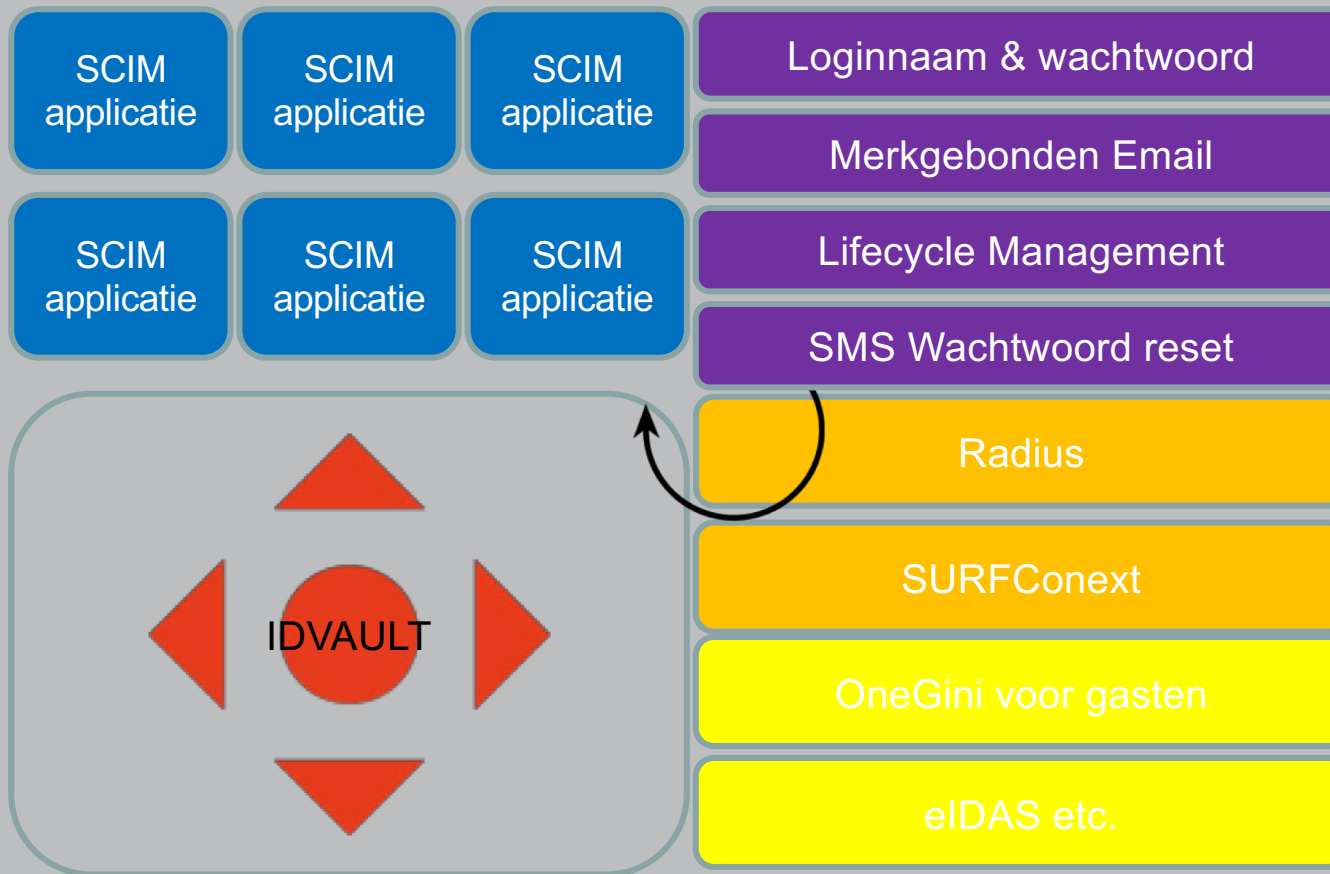
LDAP

SURFConext

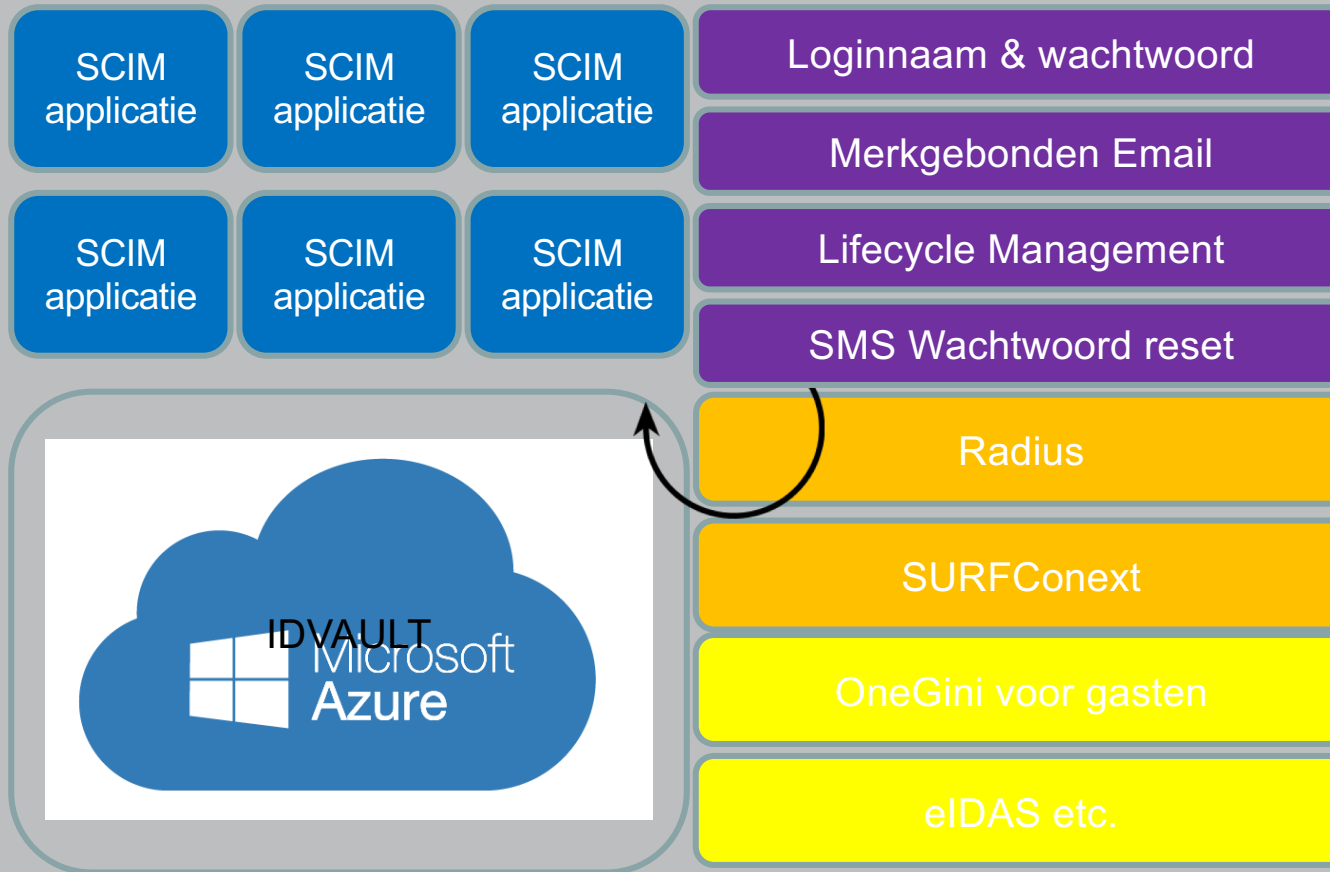
Active Directory

IDVAULT

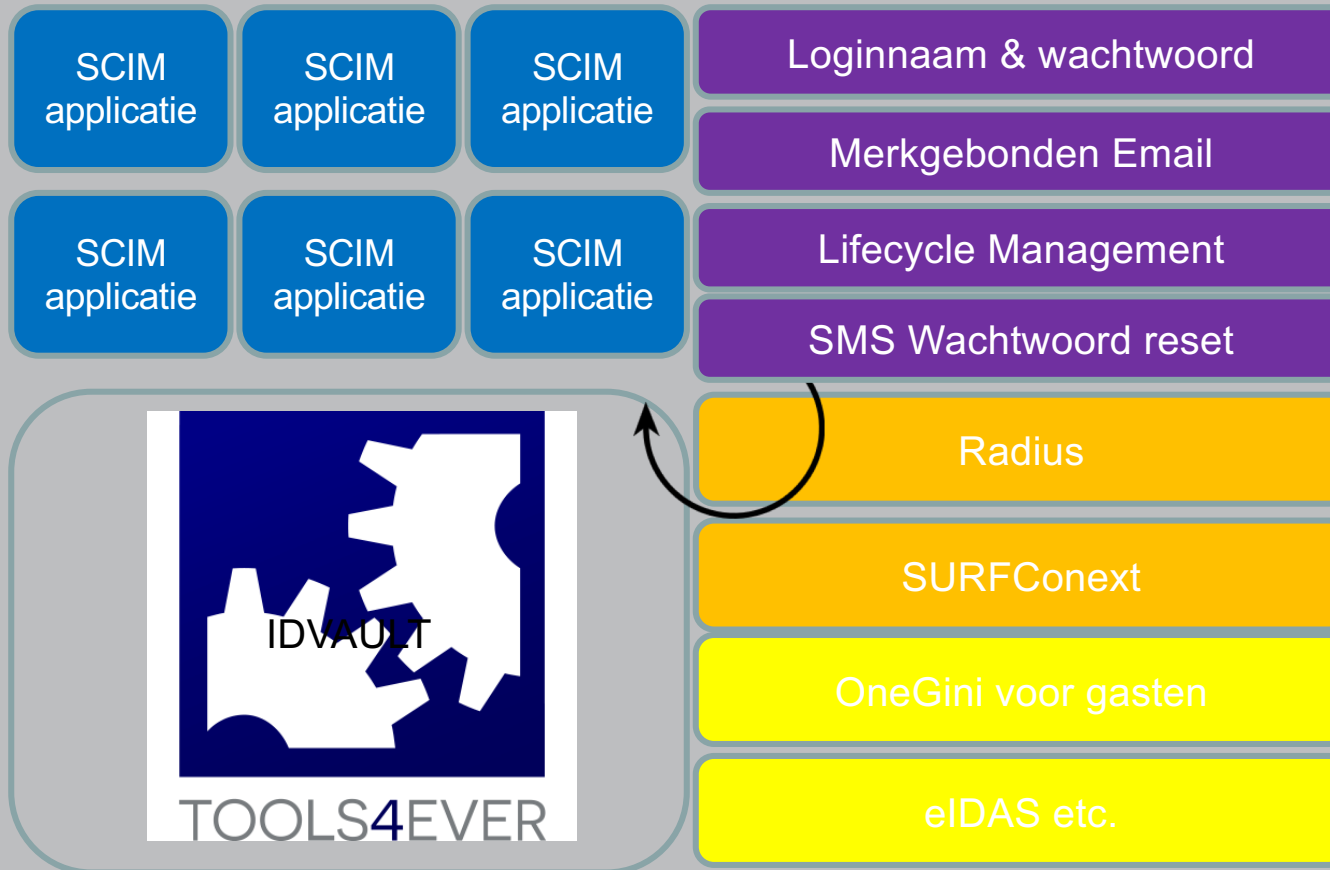
Visie



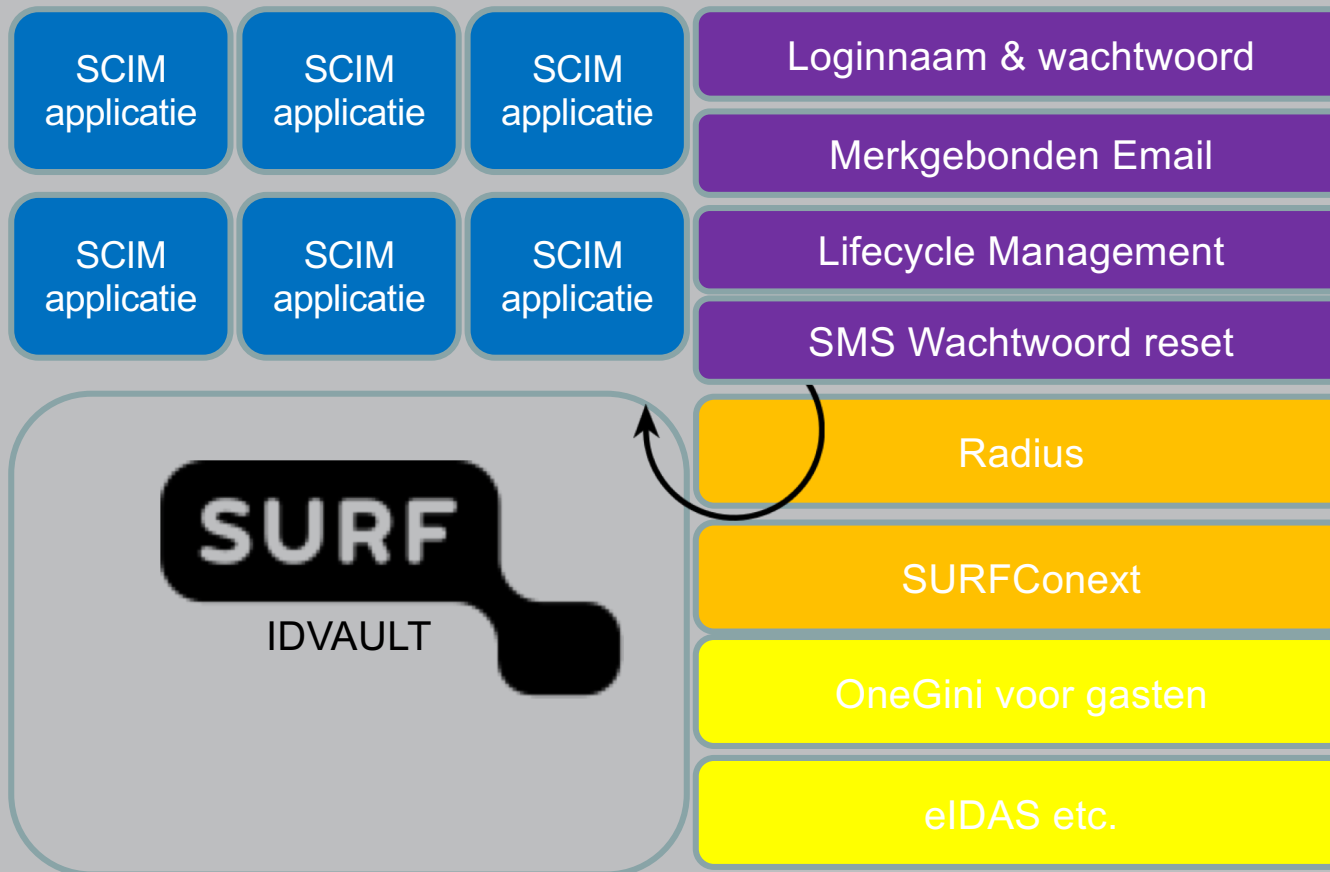
Visie



Visie



Visie



RedSpider Is Just An Application



Merijn van de Schoot
7 december 2018



Identity & Access Management

Jef van den Hurk | 7 december 2018

Koning Willem I College

- 13.000 studenten / leerlingen / cursisten
- 1.200 medewerkers
- 14 locaties in Den Bosch, Rosmalen, Boxtel en Oss
- Informatie architectuur principes
 - Hybride omgeving (deels cloud – deels ‘on premise’)
 - Replicatie van bronsystemen naar KW1C Integratieplatform
 - Microsoft tenzij



Waarom IAM – Doelstelling organisatie

Aanleiding: Het KW1C voldoet niet aan de strengere eisen van deze tijd op het gebied van Identity- en Accessmanagement, o.a. als gevolg van IBP en AVG. De complexiteit van het applicatielandschap stelt hogere eisen aan de beheerbaarheid en beheersbaarheid van toegang, rollen en rechten.

Het project draait om ***Toegang tot voorzieningen***

Doel: Het project realiseert een éénduidige manier waarop betrokkenen bij het Koning Willem I College toegang krijgen tot:

- locaties,
- systemen en
- voorzieningen

op basis van een identiteit en rolgebaseerde autorisaties.

Access Management

Authenticatie

- Single Sign On
- Sterke authenticatie
- Sessie Management

Autorisatie

- Rolgebaseerd
- Op basis van regels
- Op basis van attributen
- Autorisatie op afstand

Identity & Access Management

De juiste mensen krijgen de juiste toegang op het juiste moment

User management

- Gebruikers- en rollenbeheer
- Provisioning
- Wachtwoordbeheer
- Selfservice

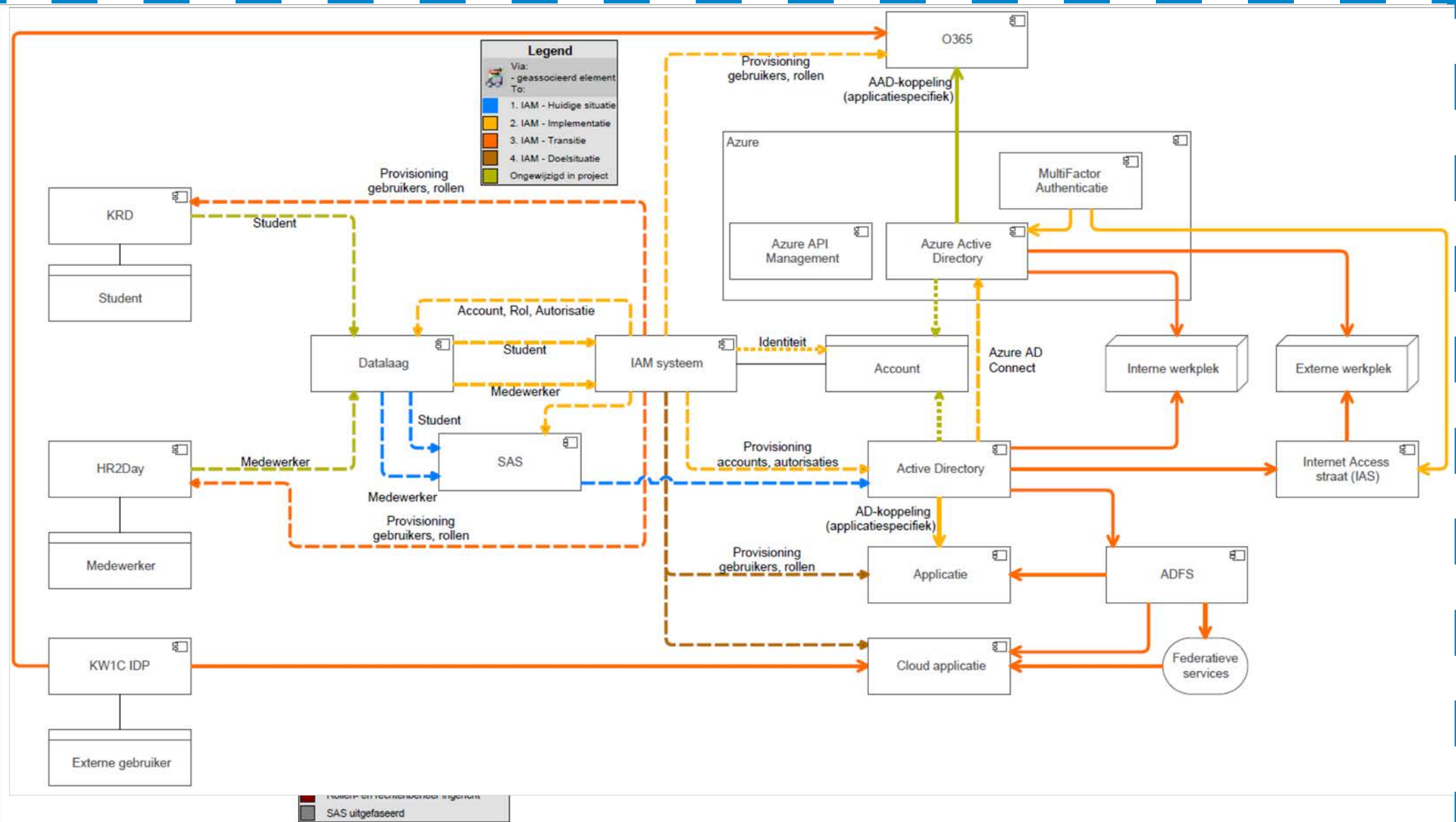
Centrale gebruikers repository

- Directory
- Data synchronisatie

Identity Management

Doelen

- Centrale voorziening ter vervanging van het huidige *Software Autorisatie Systeem* (SAS – zelfbouw)
- Inregelen geautomatiseerde flows voor toekennen van accounts en autorisaties op basis van verandering in status, rol of andere kenmerken
- Inregelen rollenbeheer – Selfservice voor management voor aanpassen / toekennen autorisatie rollen
- Multifactor authenticatie
- KW1C Identity Provider (profielwerkstuk leerlingen)
- Azure API Management
- Bring your own Identity



Actuele situatie

- Visie op Toegang geformuleerd
- Projectstartarchitectuur opgesteld
- Use cases uitgewerkt
- Aanbesteding uitgezet (gunning staat voor de deur)
- Extra beheer geregeld
- Vanaf januari implementatietraject (voor 1 jaar uitgestippeld)
- Verwachte duur > 2 jaar



Paneldiscussie met:
Jan Bartling (saMBO-ICT)
Roy Dusink (Redspider)
Martijn Nachtegaal (Kennisnet)
Femke Morsch (SURF)