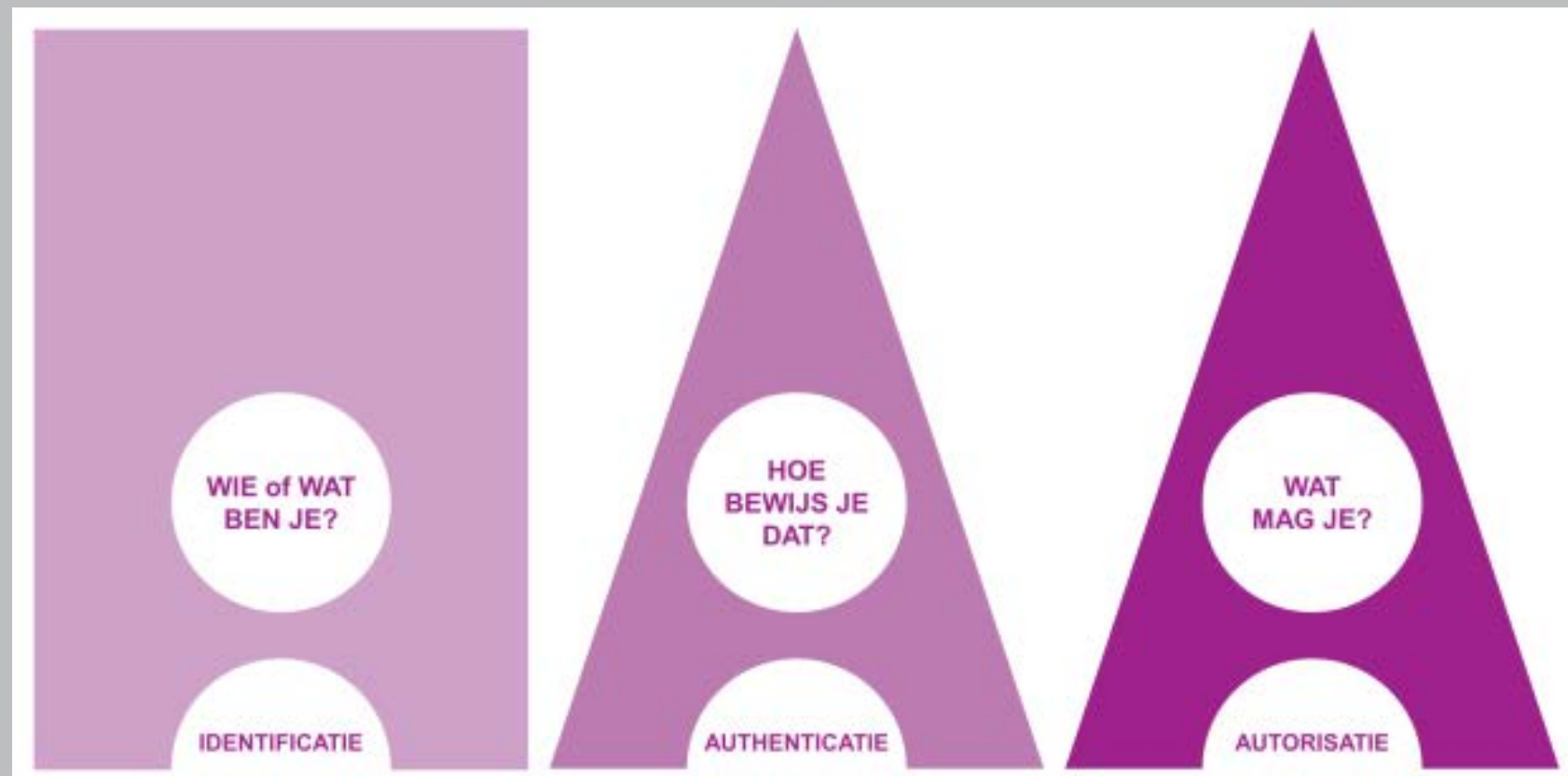


Onderwijsgroep Tilburg



► Bron: Joel de Bruijn



Identity Management Is Just An Application

Merijn van de Schoot
9 april 2019

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

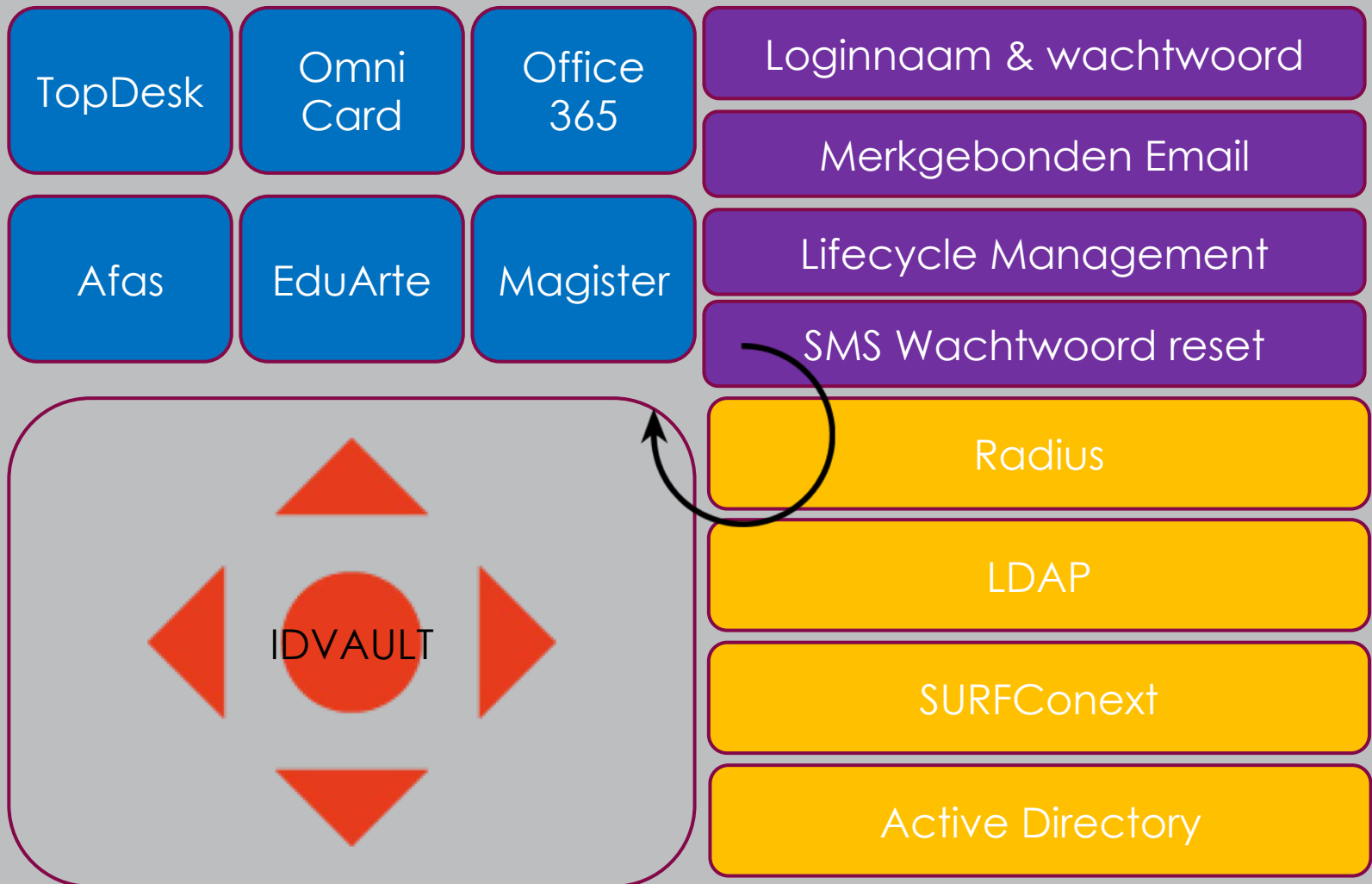
- ▶ Uit dienst? Binnen 15 minuten nergens meer toegang
 - ▶ IT systemen
 - ▶ én fysieke toegang

IDM in getallen

- ▶ Binnen 15 minuten kan je alles!
- ▶ Pasje? Binnen 1 seconden actief
- ▶ Pasfoto? Binnen 1 seconde doorgezet
- ▶ 100% sluitend met administratie
- ▶ Uit dienst? Binnen 15 minuten nergens meer toegang
 - ▶ IT systemen
 - ▶ én fysieke toegang



Architectuur



A group of five diverse students are gathered around, looking at mobile phones. A young woman with blonde hair is on the left, looking at a phone. A young man with dark hair is in the center, looking at a phone. A young woman with long dark hair is on the right, looking at a phone. A young man with glasses is on the far right, looking at a phone. A young woman with blonde hair is on the far right, looking at a phone. The background is a blurred outdoor setting.

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!**



**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

- ▶ Wetgeving (EU-AVG-2016/679)
- ▶ IBP Beleid en Normenkader
- ▶ Richtlijn voor gebruikersnamen en wachtwoorden
- ▶ Reglement 'Verantwoord netwerkgebruik'
- ▶ Procedure 'Autorisatie tot netwerk en kernsystemen'
- ▶ Beheerdokument per kernsysteem
- ▶ Werkinstructie per proces
- ▶ Beleid: tokens



DNA

- ▶ BIV classificatie
- ▶ Uitvoeren DPIA
- ▶ Beleid HR is de basis (ook externen)
- ▶ Beleid beheer en testaccounts (b_ en t_)
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



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 !

Active Directory

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.

De cloud provider maakt federatief inloggen met het instellingsaccount mogelijk op basis van SURFconext

1.0

De cloud provider ondersteund 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

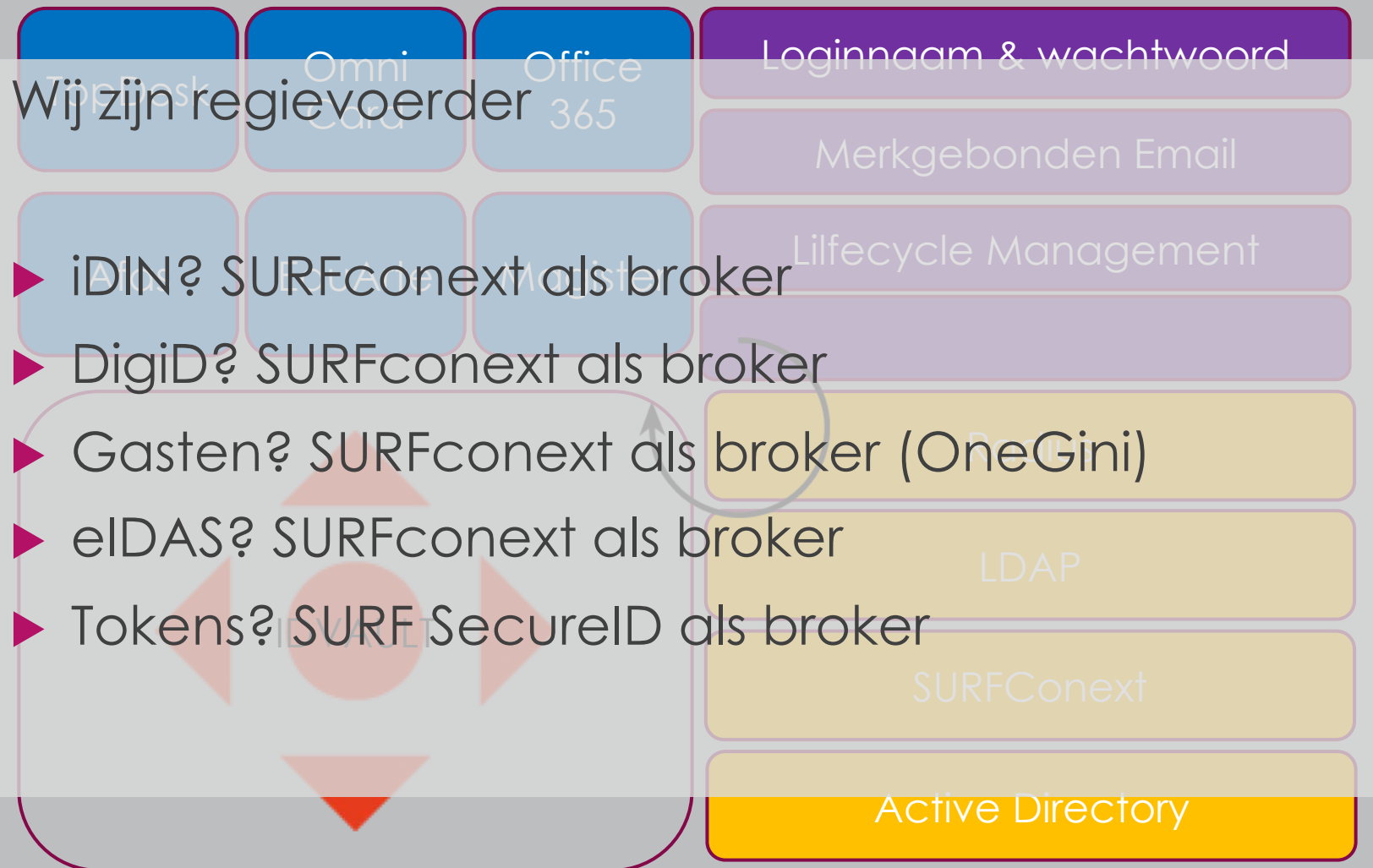
De cloud provider maakt het mogelijk dat veiligere authenticatie, naar keus van Onderwijsgroep Tilburg, afgehandeld wordt door de cloud dienst of door het SURF SecureID platform.

1.0

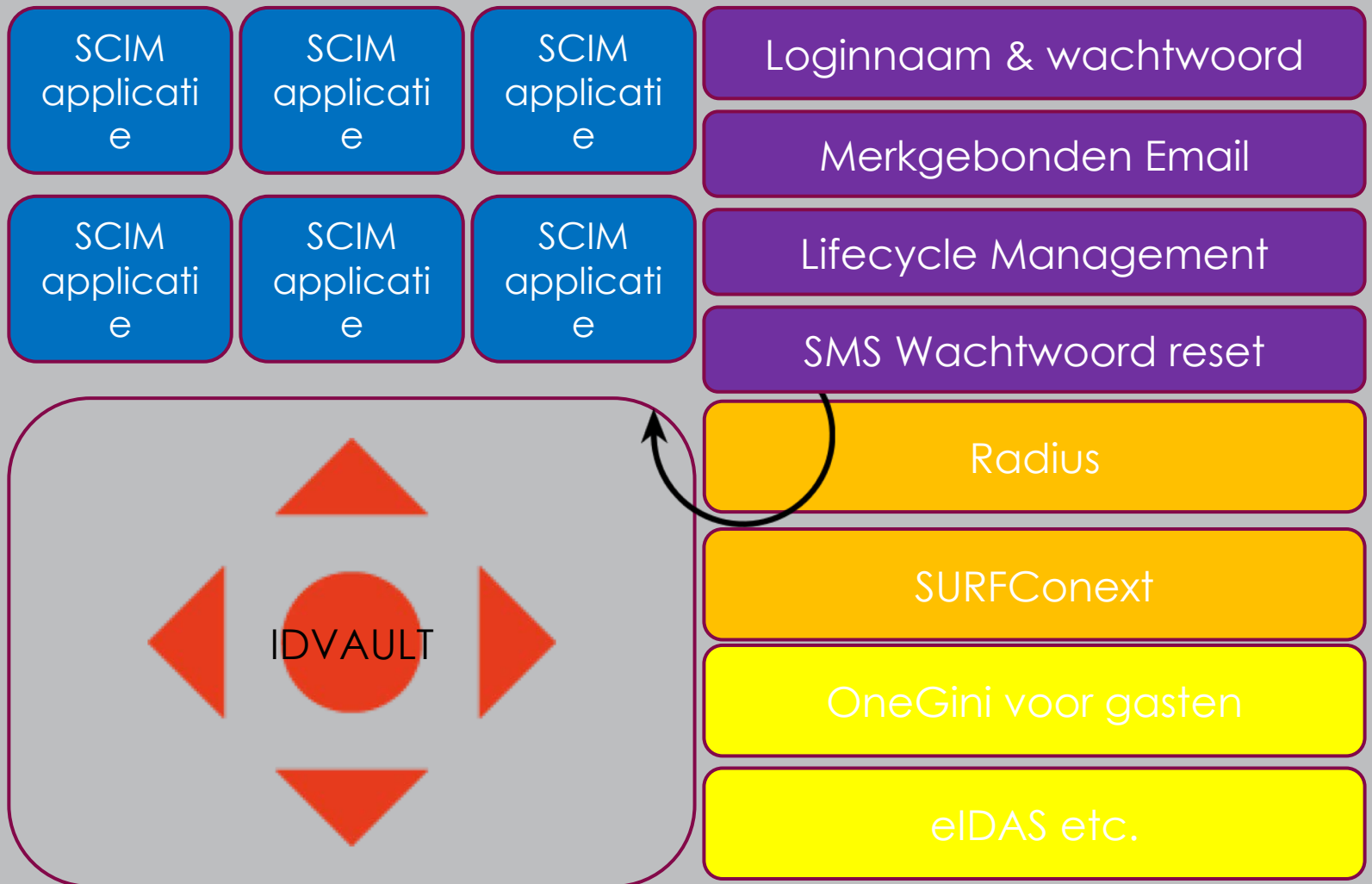
Ondersteunt u Step Up authentication op het SURF SecureID platform voor specifieke, configureerbare rollen?

1.0

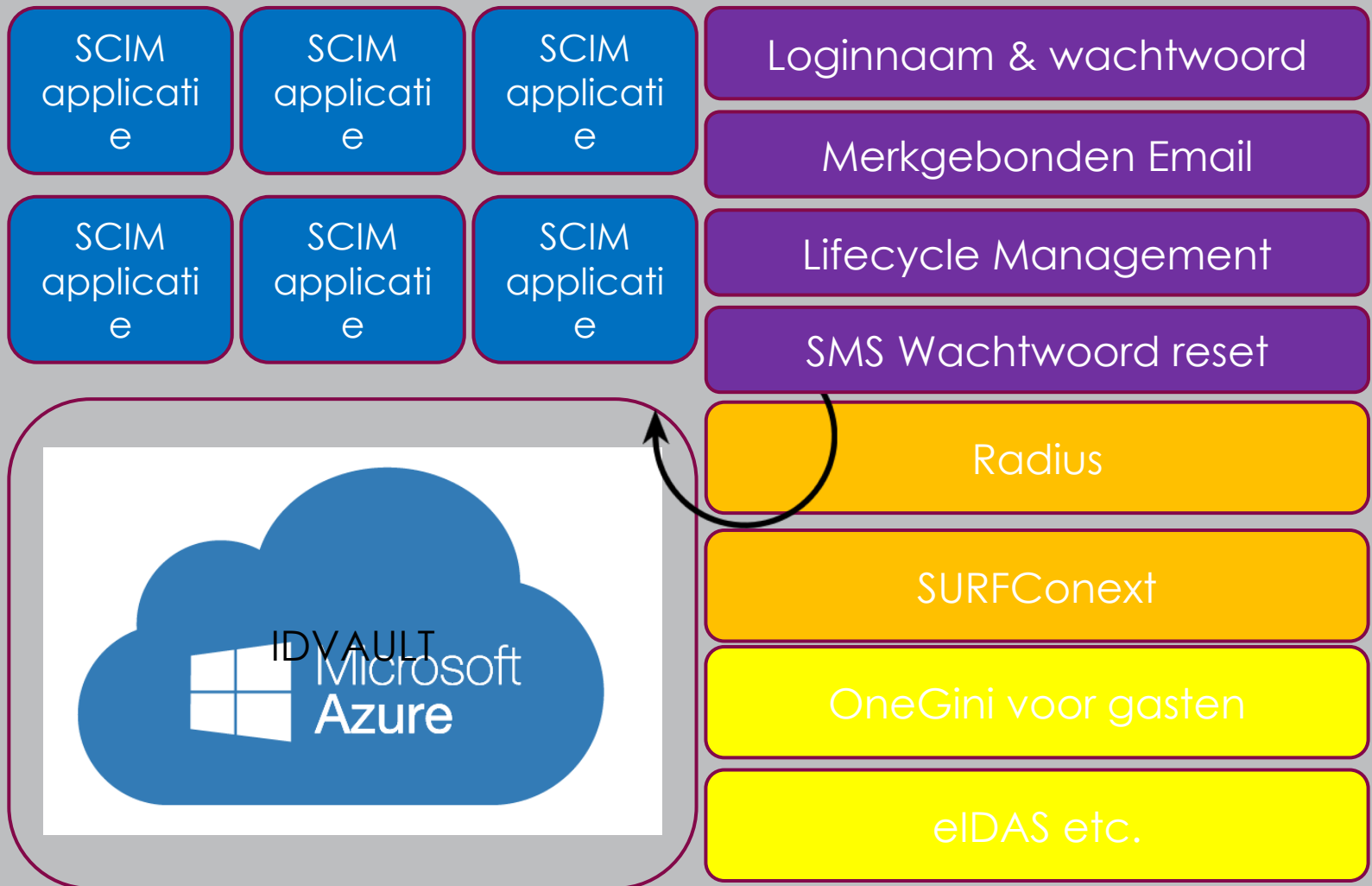
Visie



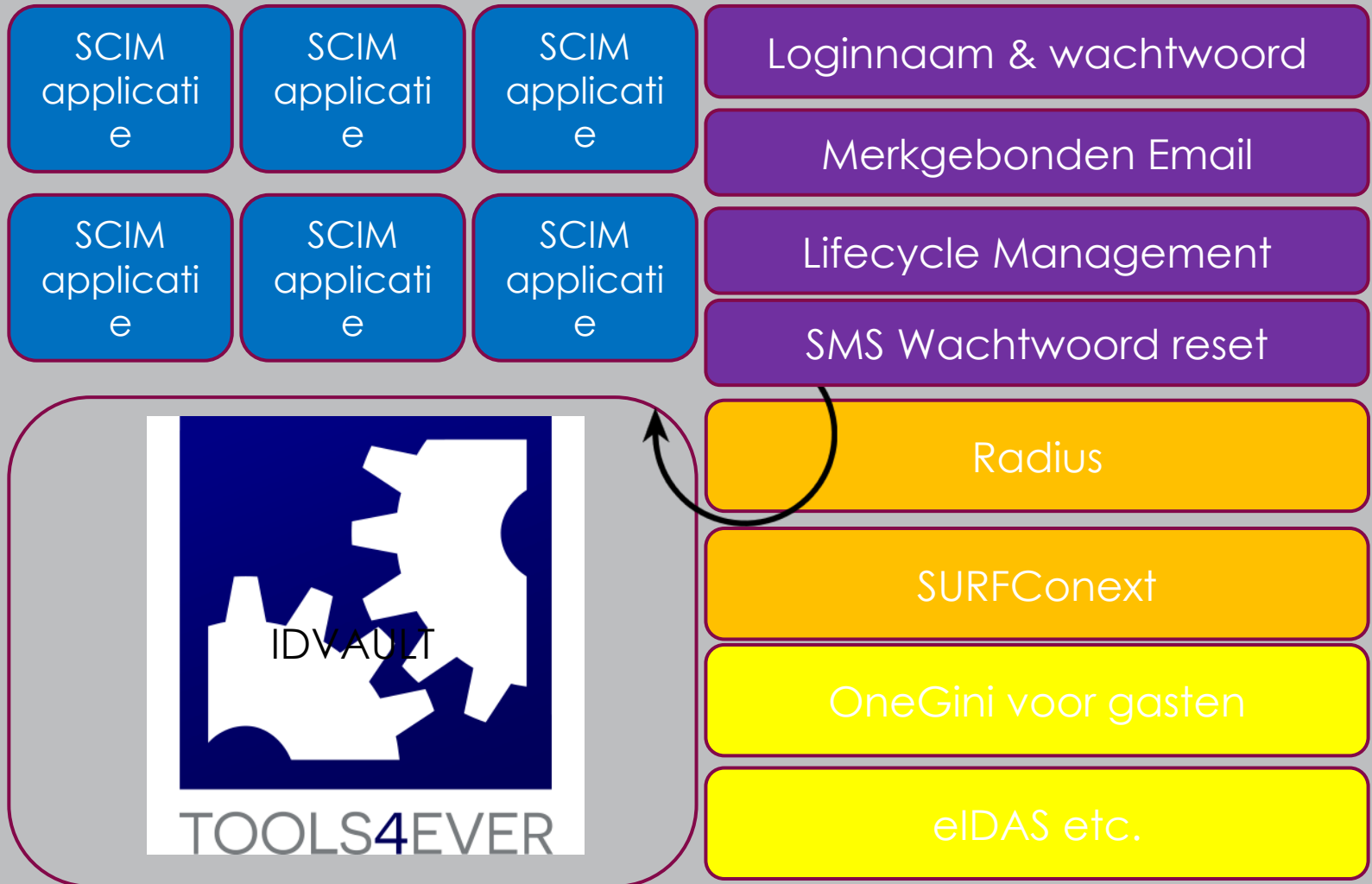
Visie



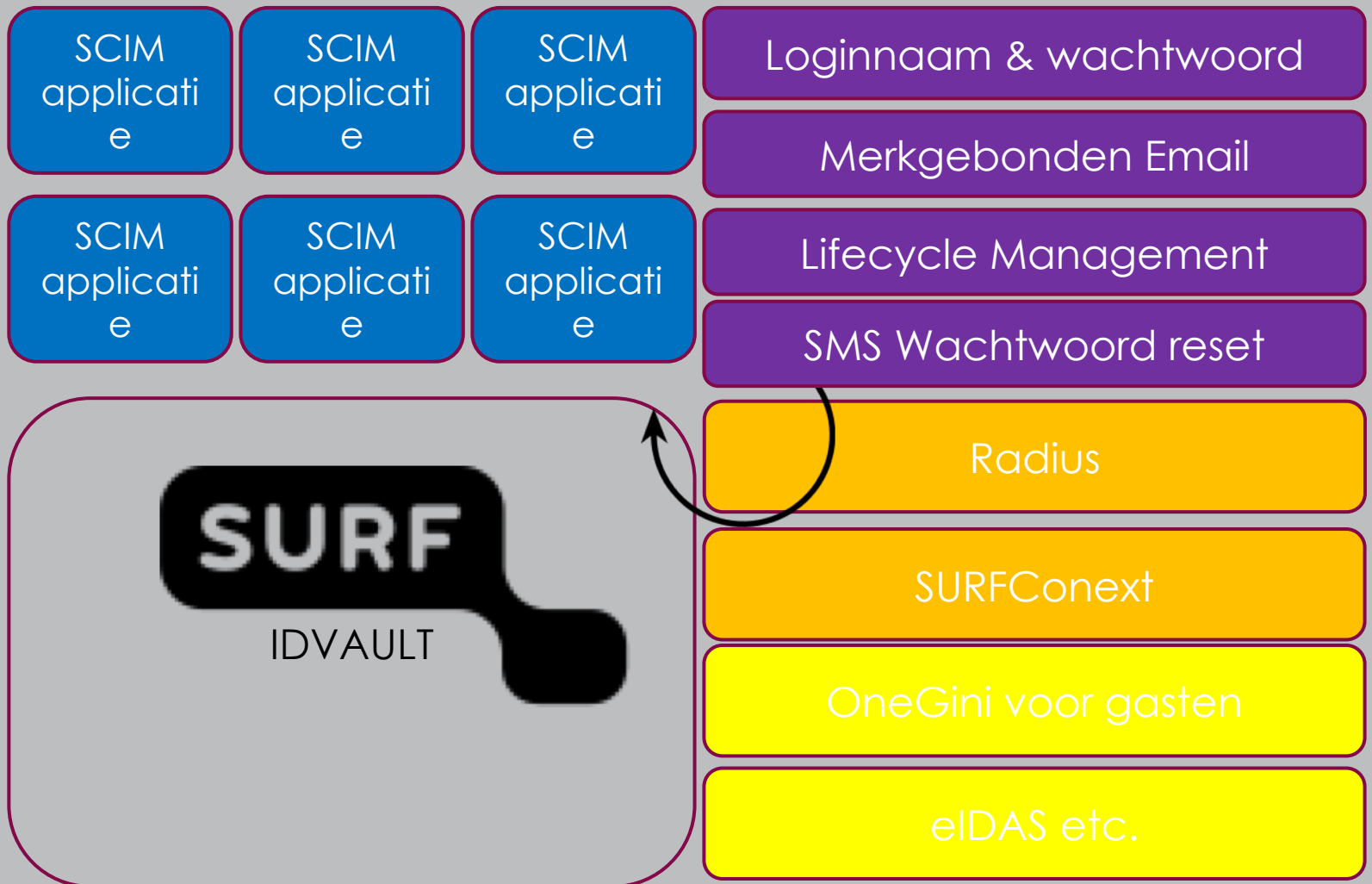
Visie



Visie



Visie



Identity Management Is Just An Application

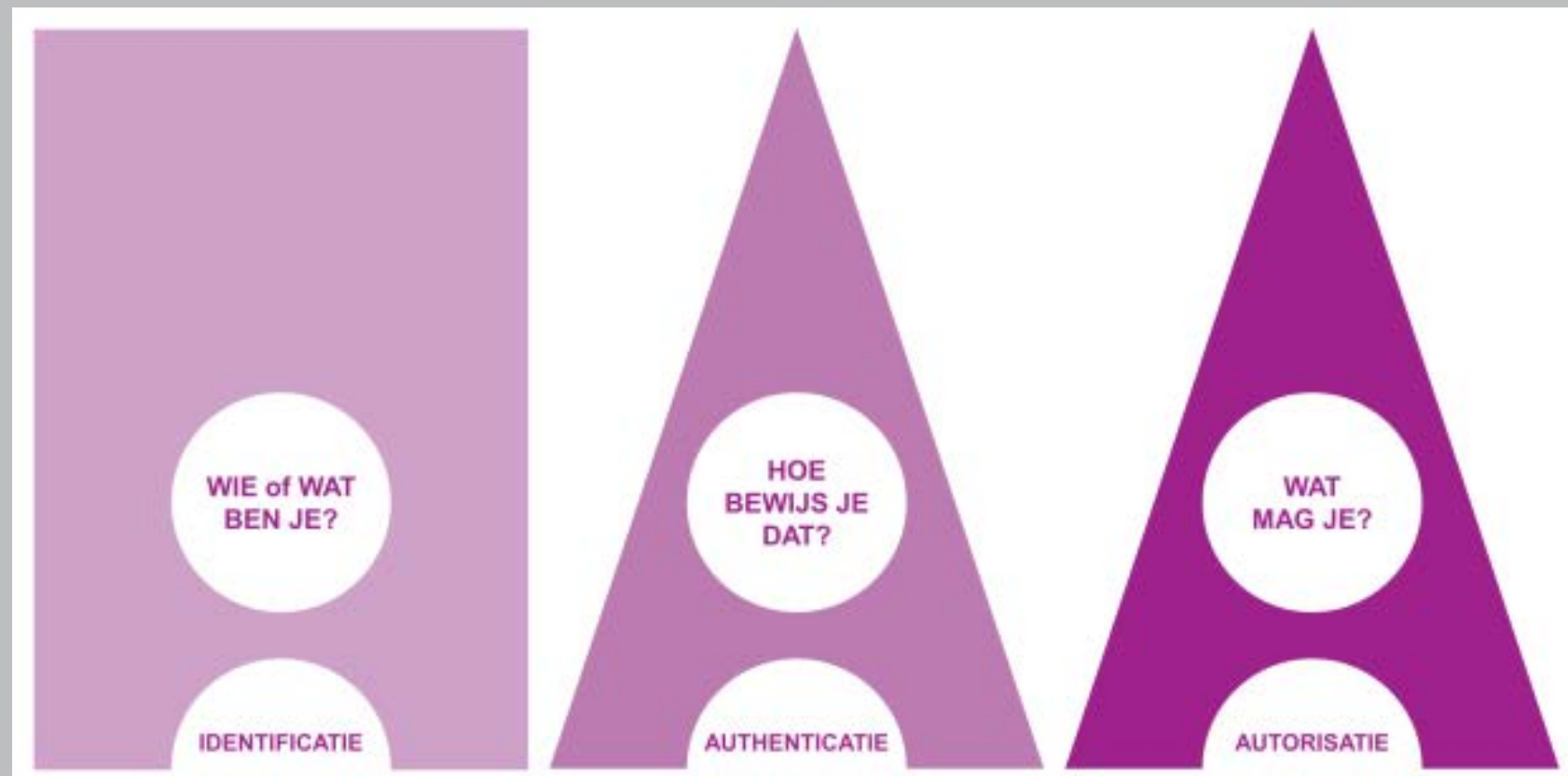
Merijn van de Schoot
mvd schoot@onderwijsgroep tilburg.nl





Vragen?

Onderwijsgroep Tilburg



► Bron: Joel de Bruijn