Volgende stap in identity en accessmanagement

Rick Ruumpol (ROC van Twente) - Red Spider Vereniging
Hendri Boer (Aventus) – Infrastructuur specialist

Voorstellen

Rick Ruumpol
Informatiemanager bij ROC van Twente
Bestuurslid Red Spider

Hendri Boer
Security specialist bij Aventus
Lid Wijzigingengroep Red Spider

Agenda

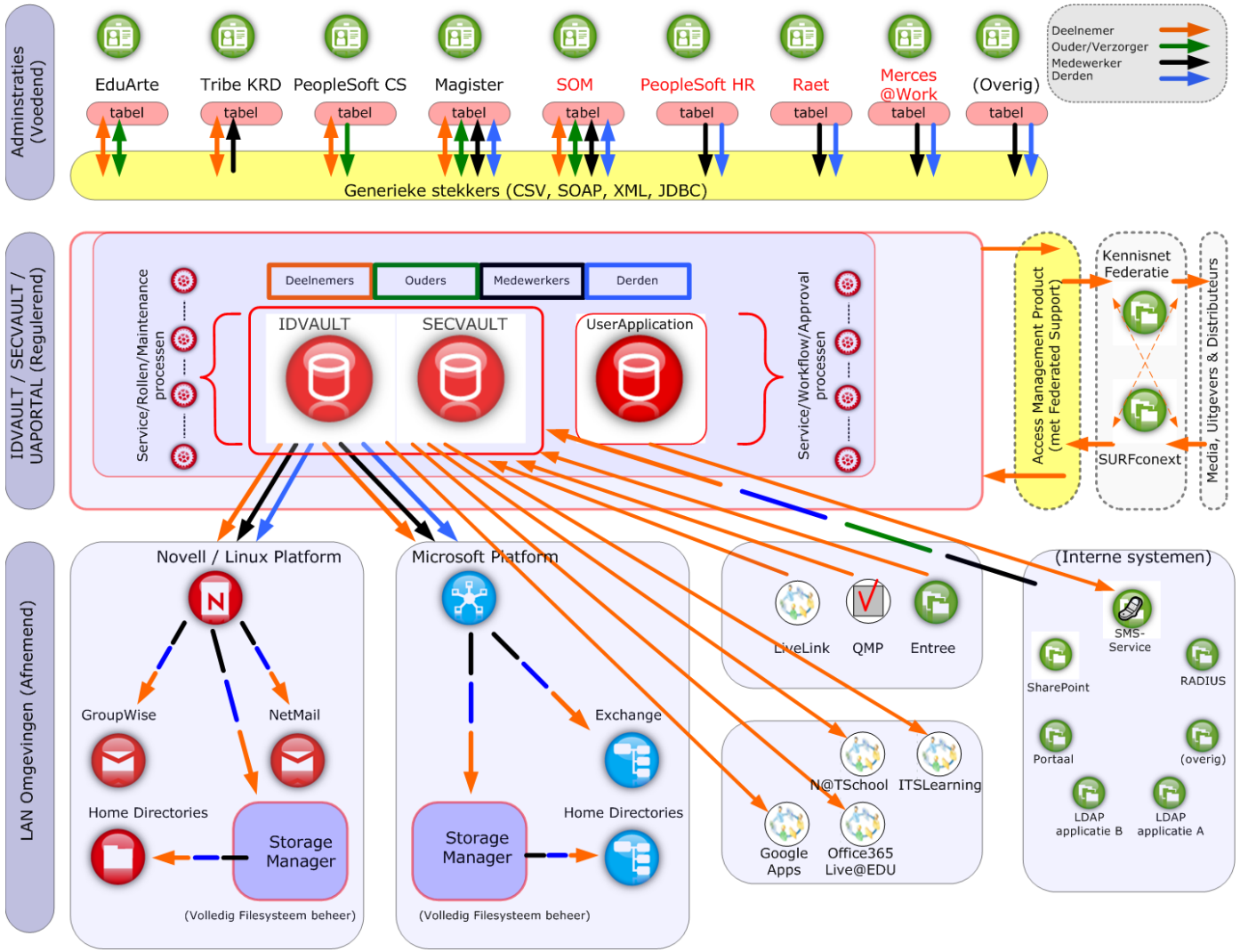
- Introductie Red Spider Vereniging
- Architectuur Red Spider aan identitymanagement
- Onderzoek naar context based access management
- Huidig vraagstuk
- Ambitie

Red Spider Vereniging

- 19 scholen (vo & mbo)
- Eén architectuur, twee implementatiepartners
- Samen ontwikkelen en onderhouden van koppelvlakken, besparing op ontwikkeling.
- Op basis van NetIQ IDM 4.6
- Koppelvlakken (de drivers) zijn van ‘ons’. Huidige set 15+
- Bestuur, wijzigingencommissie en ALV
- Jaarlijkse contributie (staffel op basis van deelnemers)

Architectuur Red Spider

REDSPIDER GEBRUIKERSVERENIGING



Huidig vraagstuk

- Technologie staat enigszins, wel erg complex
- Complexiteit zit in maatwerk; geen standaard product meer
- Implementatiepartners beperkt
- Access management maakt geen onderdeel uit van omgeving, belangrijker vraagstuk geworden
- Instellingen willen (deels) volgende stap maken, nieuwe vraagstukken en zoektocht naar stabiliteit

Onderzoek naar context based access management

Probleemstelling

1: Gebruikservaring authenticatie van applicaties moet beter

2: Applicaties altijd en overal beschikbaar

3: Single Sign-On grote wens voor alle diensten

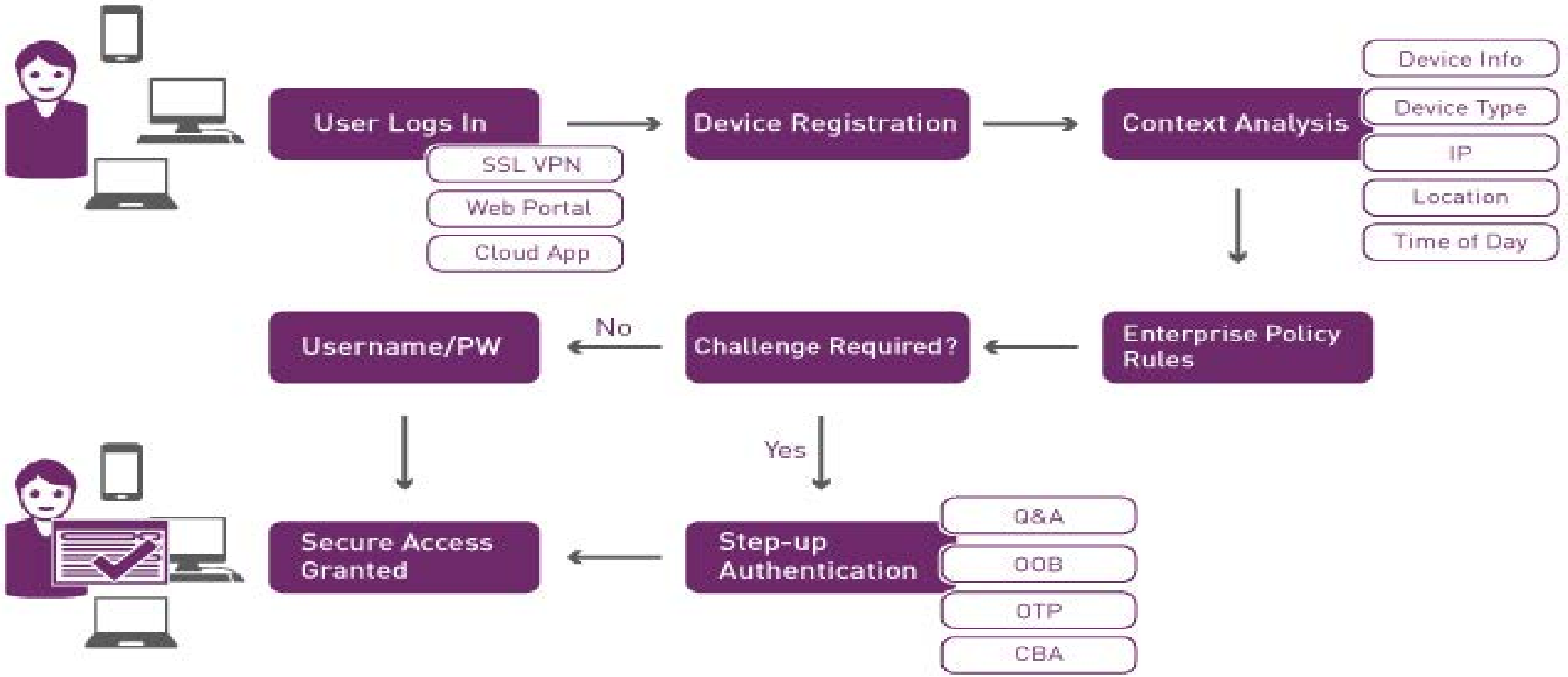
4: Nieuwe wet en regelgeving (GDPR/AVG)

Oplossingsrichting

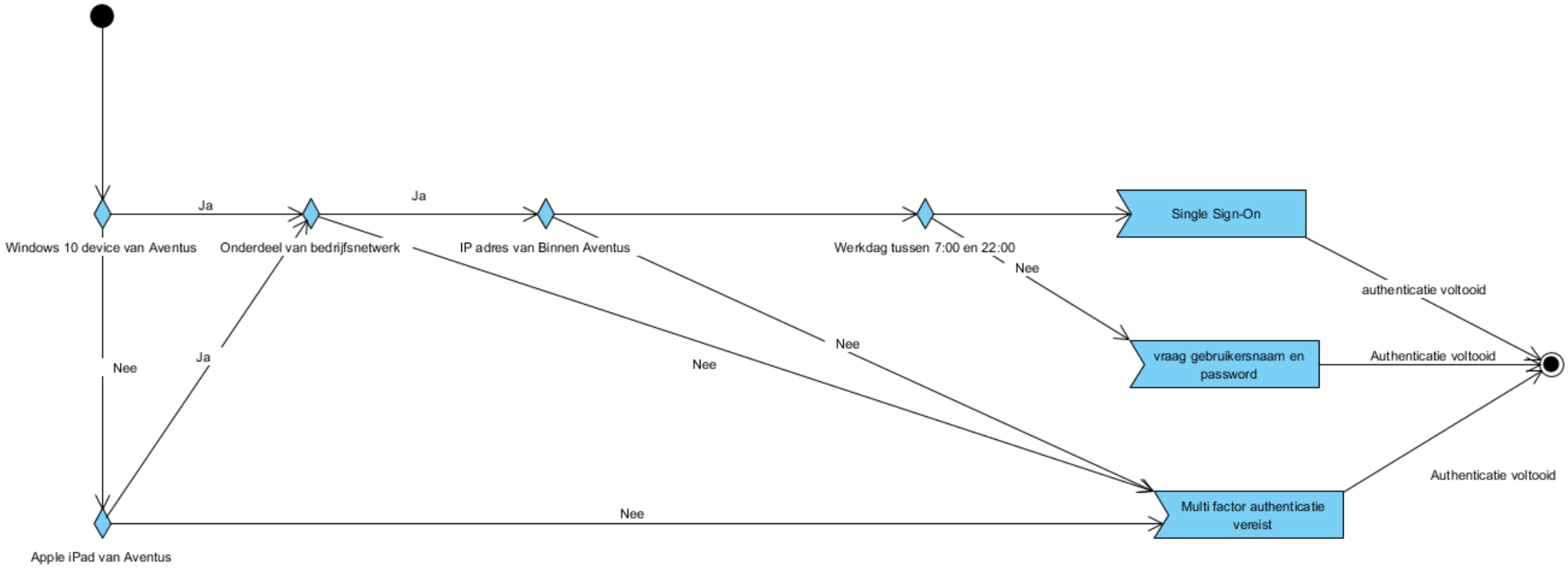
Context based login / authenticatie

Wie, wat, waar, wanneer, hoe?!

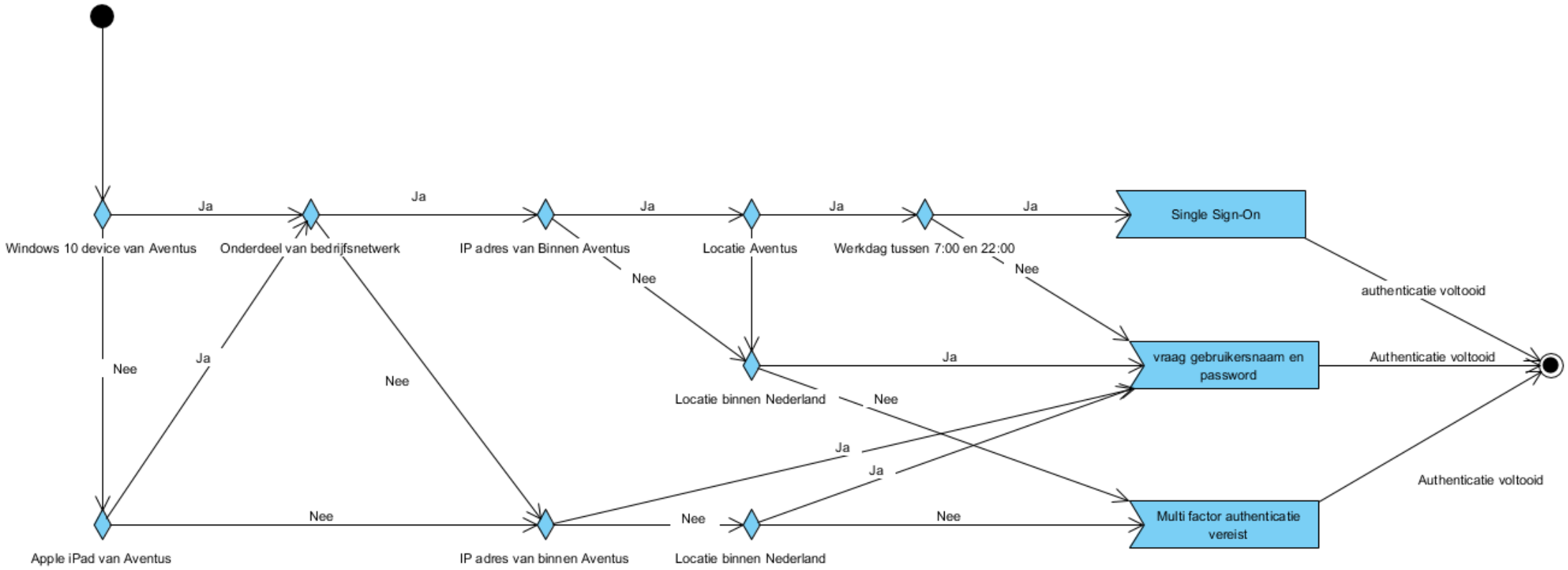
Oplossingsrichting



Afhandeling van toegang: voorbeeld



Afhandeling van toegang: voorbeeld



Conclusie

Context based login / authenticatie

Wie, wat, waar, wanneer, hoe?!

Gerealiseerd op Microsoft ADFS platform, SURFconext en Kennisnet federaties

Red Spider - toekomst

Verkenning

- 2015: Marktverkenning op basis van ‘nieuw’ plan van eisen, geen keuze gemaakt en vervolg gegeven. Wel constatering dat de markt de vraag kan beantwoorden.

- 2017: Nieuwe start verkenning toekomst en rapport ‘visie op IDM’ bij Kien ICT

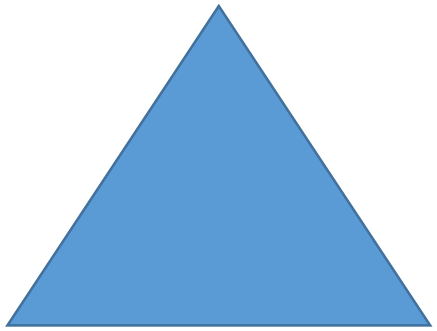
- 2018: Samen met Bas Kruiswijk (TG) en Mark de Jong (zelfstandige) nieuwe visie en voorstel voor vervolg

Visie

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

Visie

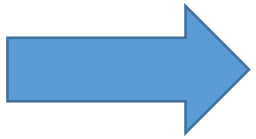
Identiteit
(Gebruiker in een bepaalde rol)



Account
(Manier om identiteit aan te tonen)

Claim
(Toegangsrecht)

VAN
Eén account verschaft je toegang tot alle diensten
Alle diensten gebruiken hetzelfde gebruikersprofiel
Ruime complete gegevenslevering,
zowel vooraf, op moment van gebruik als later (updates)



NAAR
Gepseudonimiseerd toegang tot diensten
Op basis van claims gekoppeld aan een identiteit
Minimale en gecontroleerde gegevensverstrekking,
op het moment van gebruik (JIT)

Visie

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 apparaten
- Gegevensbescherming en privacy
- Ontkoppeling van account
- Context gebaseerde toegangscontrole
- Sectorvoorziening: dat kunnen we niet alleen!

Conclusie

- Geen grote noodzaak tot vernieuwing bij de instellingen
  - Elk gangbaar IAM-product voldoet
  - Zolang ADFS, OpenID Connect en Oauth maar worden ondersteund
- Wel noodzaak om het gebruik en de inrichting te wijzigen
  - Geen directe (cloud) provisioning meer
  - Aansluiten op nieuwe sectorvoorzieningen
  - Gericht op context gebaseerde toegang
- De uitdaging ligt in de sectorvoorzieningen
  - Sectorale ondersteuning voor OpenID Connect en Oauth
  - ECK-ID en attributenbeleid is eerste stap, maar niet het eindpunt

Vervolg

- De gebruikersvereniging krijgt andere rol, huidige leden moeten nog instemmen
- Eventueel samen verkennen van IAM-product, voorkeur voor Microsoft
- Samen met sectoren, Kennisnet, SURF en saMBO~ICT optrekken voor sectorvoorziening
- Aandachtspunt: huidige voorzieningen en vo en mbo leden Red Spider

Nieuwe leden welkom! Samen aan de slag Kennisnet, SURF en saMBO~ICT !

Vragen?

Rick Ruumpol
rruumpol@rocvantwente.nl

Hendri Boer
h.boer@aventus.nl