RealOpen IT

Red Spider *Next Generation*: Identity Management voor gevorderden

Bert van Daalen

René Visser

Ronald Zierikzee

Red Spider
Gebruikersvereniging

RealOpen IT

OPENSOURCE OPEN MIND

Constateringen rijp en groen

- Hoge ontwikkelkosten en lange doorlooptijd nieuwe functionaliteit
- Afhankelijkheid leverancier (Novell Nederland)
- Tendens Novell > Microsoft binnen het onderwijs
- End-off live huidige generatie deelnemerinformatie systemen (nOISe en Icaris)
- Markt voor deelnemers informatiesystemen kent inmiddels meerdere – deels nieuwe- spelers (Magister – EduArte – KRD - Edictis)

Constateringen rijp en groen

- Triple A/ROC-i-partners standaardisatie berichten verkeer
- Veel instelling zijn op zoek naar een nieuw personeels informatiesysteem of hebben recentelijk een keuze gemaakt
- AAI initiatieven
- Federaties
- Wat doet de ‘concurrent’
- Security
- Shared Service Centers

Constatering vervolg

- Nieuwe onderwijs concepten
  - meer flexibiliteit
  - role based
  - over instellingen heen
  - meer integratie met het bedrijfsleven
- Service bus denken
- SOA denken
- Applicatie integratie en virtualisatie
- Self service

Wensenlijstje

- Flexibel
- Open standaarden
- Lage beheerslast
- Parameter gestuurd
- Gebaseerd op business rules
- (near) Real Time

Wensenlijstje

- Toekomstbestendig
- Geschikt voor VO
- Aandacht voor migratie- en implementatiekosten
- Concurrerend in de IDM markt
- Vereniging is eigenaar van de applicatie

Proces 1

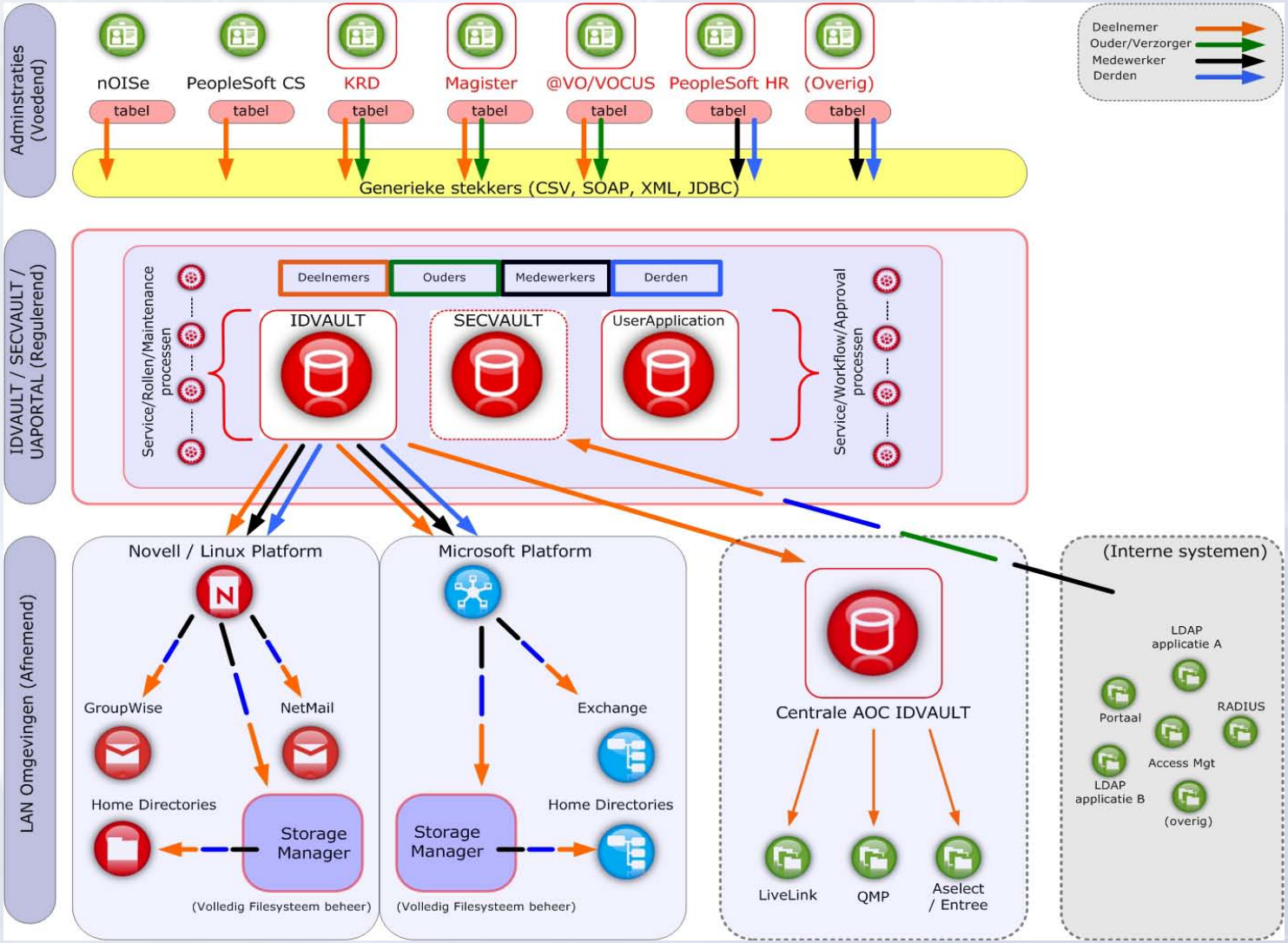
- Wensenlijstje vaststellen tijdens een ALV
- Aantal gesprekken met Novell en enkele marktpartijen
- Vaststellen offerte en besluitvormingsprocedure tijdens ALV
- Offerte traject
- Besluitvorming tijdens ALV
- Gunning aan RealOpen IT
- Vormgeven projectorganisatie

Proces 2

- RealOpen IT inventariseert bij ROC's en AOC's
- Scope wordt bepaald, vastgelegd en geaccepteerd
- Use cases worden beschreven en goedgekeurd
- Red Spider Next Generation wordt gebouwd
- December 2009/januari 2010 testen
- Eind januari 2010 oplevering eerste release

Uitgangspunten

- Ontworpen voor alle identiteiten
- Rollen gebaseerd
- Voor meerdere bronsystemen
- Open standaarden
- Flexibel en aanpasbaar
- Lage beheerlast IT afdeling
- Geschikt voor komende drie jaar
- Geschikt voor VO
- Huidige functionaliteit mee



Features

- Aanmaken van de vier identiteiten
  - 4 generieke stekkers
    - CSV, SOAP, XML, JDBC
  - Extra : via webformulier (maken / wijzigen)
- Gebaseerd op rollen
  - kenmerken op de ID uit bron zijn sturend
  - kenmerken worden automatisch of handmatig in de Directory aangemaakt
  - kenmerken en rollen zijn Directory objecten
  - rollen leveren entitlements op

Voorbeelden van kenmerken

ID	Type	Waarde	Status	#Begin	#Eind
KRD	Identiteit	Deelnemer	A		
KRD	Crebo	%value%	A		
KRD	Lokatie	%value%	A		
KRD					

ID	Type	Waarde	Status	#Begin	#Eind
CSV	Identiteit	Medewerker	A		
CSV	Identiteit	Medewerker-Intern	A		
CSV	Lokatie	%value%	A		
CSV	Functie	%value%	A		
CSV	Afdeling	%value%	A		
CSV	Team	%value%	A		
CSV	Is-Leidinggevend	%value%	I		
CSV	Leidinggevende	%value%	%ID%		

Samenspel

1. Kenmerken registreren we in de IDVAULT als een Kenmerkgroep en een Enrolment-object. Hiermee leggen we de relatie tussen de identiteit en de aanwezige kenmerken vast.

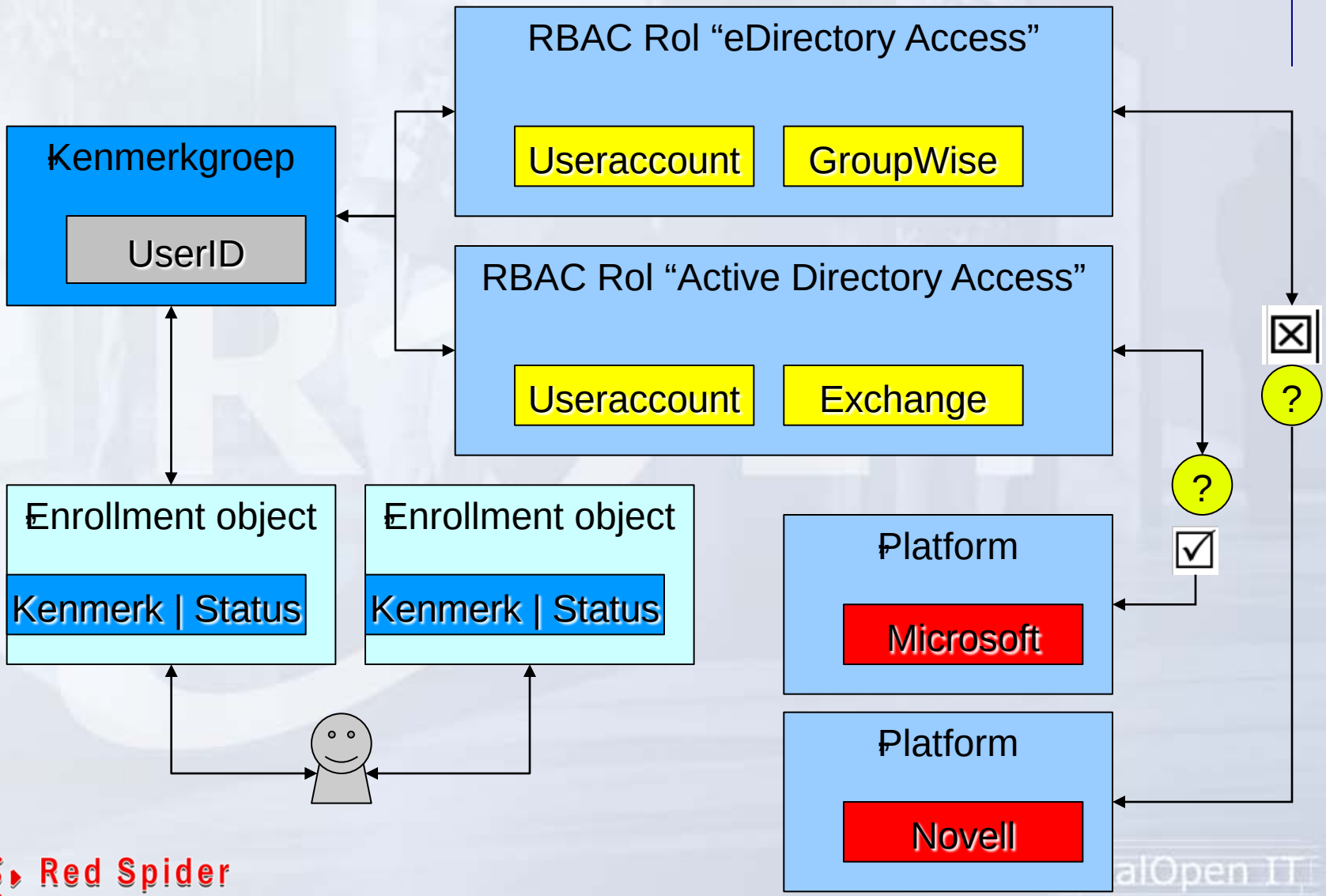
2. Deze Enrolment objecten worden later gekoppeld aan een RBAC Rolobject. Dit RBAC object bevat een Entitlement.

3. Door middel van het leggen van een relatie tussen de RBAC Rol en het Enrolment object worden de identiteiten direct geupdate met een aangemaakt Entitlement

Entitlements

- Entitlements in RBAC objecten
  - feitelijk “virtuele toegangspasjes” voor het afnemende systeem
  - Entitlements worden tijdens implementatie aangemaakt
  - Entitlements kunnen later worden toegevoegd en worden verwijderd (omgevingen veranderen immers)
  - IDM Drivers zijn/worden geconfigureerd op deze Entitlements. Toegang tot het systeem wordt hiermee geregeld.

Rolverwerking



Features

- “Open” Driver architectuur
  - voor iedere IDM partner toegankelijk
  - geen gesloten code aanwezig
  - driver code aanpasbaar
- **Multiplatform** oplossing
  - Novell (OES2 Linux)
  - Microsoft (W2003/W2008/W2008R2)
  - 32 bits/64 bits , fysiek/virtueel

Features

- Interface op Red Spider NG via de IDM UserApp
  - gemakkelijk en veilig
  - maakt gebruik van Directory rechten
- Webformulieren
  - Beheerformulieren
    - aanmaken en (beperkt) muteren ID's
    - kenmerken
    - rollen
    - toewijzingen
    - associaties
    - zoekmogelijkheden

Features

- Housekeeping / Serviceprocessen
  - loopbackdrivers
  - vertaling van kenmerken naar rollen
  - beheer van relaties tussen rollen, kenmerken en entitlements
  - beheer van default Directory attributen
- Jobs
  - beheer van inactiveren (move-to)
  - beheer van reactiveren (move-from)
  - relaties tussen objecten bijhouden
  - 'Cleanup' activiteiten

Features

- Housekeeping / Serviceprocessen
  - Advanced Logging
    - delete
    - nieuwe users
    - modificaties op de gebruikergegevens
    - modificaties op rollen/status/kenmerken
  - Password Management
    - Password Self Service / Challenge Sets
    - Per gebruikerstype in te stellen
    - Volledig bi-directioneel