Datum:	11 november 2014	Toestel:	0164-277374
Van:	R. van Merrienboer	Aan:	Leveranciers
Organisatie:	ICT samenwerking	Cc:	
Onderwerp:	RFI Authenticatie, Autorisatie en Auditing / Identity Management		

Inleiding en achtergronden

De BERM gemeenten: Bergen op Zoom, Etten-Leur, Roosendaal en Moerdijk zijn een samenwerkingsverband aangegaan, waarbij gezamenlijk IT-voorzieningen worden benut en gerealiseerd met behulp van een hiervoor opgericht ICT-Samenwerkingsverband. Inmiddels is begonnen met het leggen van het fundament. Het fundament bestaat uit een doelmatige informatievoorziening waardoor de BERM gemeenten in staat zijn een optimale dienstverlening te leveren met minder inspanning en tegen minder kosten. Een belangrijk onderdeel hiervan is een geconsolideerde infrastructuur van de vier samenwerkende gemeenten.

Door de ICT-samenwerking is een doelarchitectuur uitgewerkt van de nieuwe, geconsolideerde infrastructuur. ICT-Samenwerking gaat opereren als zelfstandige organisatie met een eigen centrale datacenterinrichting (redundant ingerichte hoofdlocatie en een uitwijklocatie). Gemeenten en hun gebruikers zijn klant bij de ICT-Samenwerking en nemen hiervan diensten af.

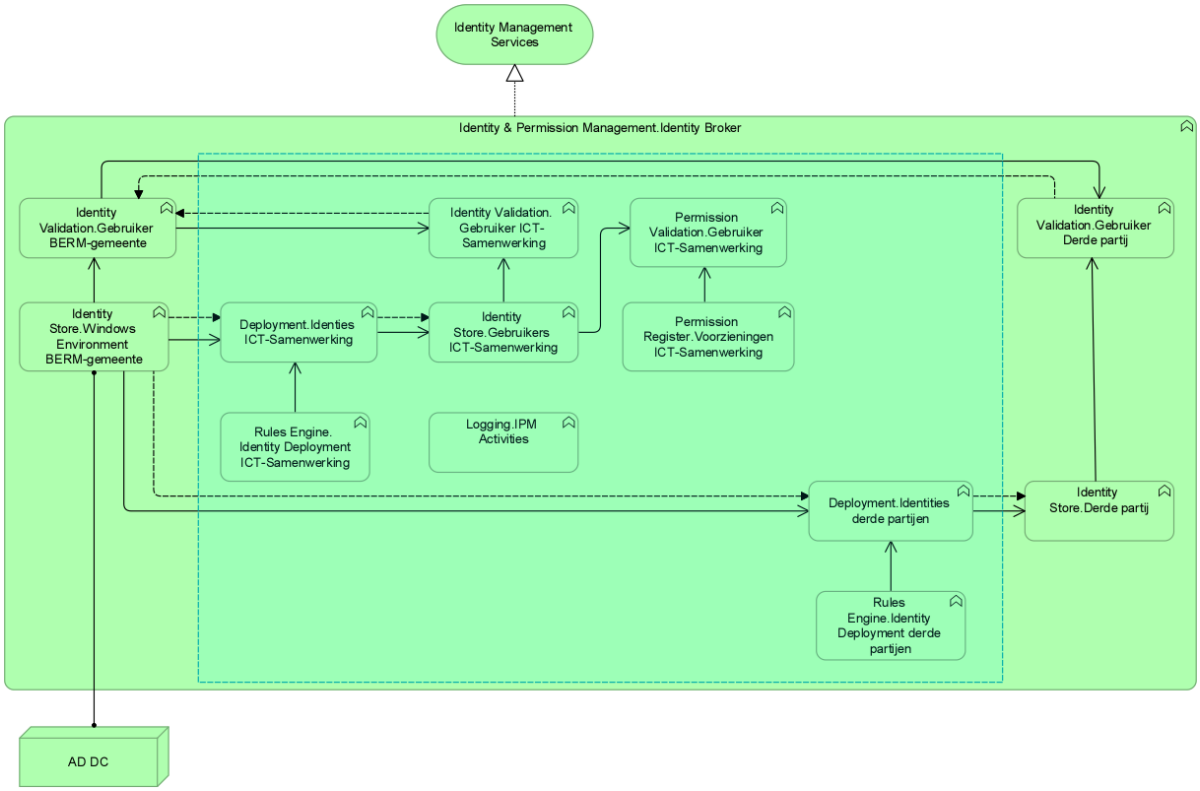
Request for Information

Eén van de ondersteunende diensten die de ICT-Samenwerking levert, is het beheer van gebruikers van haar diensten en de rechten (permissies) die zij daarvoor hebben, inclusief het auditen van acties die gebruikers uitvoeren. Daarnaast ondersteunt de ICT-Samenwerking het beheer van gebruikers bij de klantgemeenten. Dit dient op meerdere manieren te gebeuren:

1. De ICT-samenwerking voert taken uit voor het beheer van de Directory van de klantgemeenten (bij de huidige gemeenten is dit Microsoft Active Directory), waarbij overigens gemeenten zelf verantwoordelijk zijn voor deze gebruikers en hun accounts, aangezien het medewerkers van de gemeente zijn.
2. De ICT-samenwerking zorgt ervoor dat identiteiten uit de Directories van de verschillende gemeenten worden gerepliceerd richting Cloudproviders (waaronder Microsoft ten behoeve van Office365).

3. (Optioneel). De ICT-samenwerking zorgt ervoor de technische Directory van de gemeente (zoals Microsoft Active Directory) geautomatiseerd wordt gevoed en onderhouden vanuit het HRM-systeem van de betreffende gemeente. (Deze functie is niet weergegeven in onderstaand diagram).

Hieronder is de kern van de functionaliteit in een Archimate-diagram schematisch weergegeven:



De in het diagram weergegeven functies worden hieronder toegelicht:

Functie	**Omschrijving**
Identity Store.Windows Environment BERM-gemeente	Centrale opslag van gebruikers die medewerker zijn bij één van de BERM-gemeenten.
Identity Validation.Gebruiker BERM-gemeente	Valideren van een gebruiker die een dienst wil benutten bij de ICT-Samenwerking, waarbij de ICT-Samenwerking het verzoek tot validatie teruglegt bij de betreffende BERM-gemeente.
Deployment.Identities ICT-Samenwerking	Uitrol (replicatie) van digitale identities en hieraan gerelateerde attributen (waaronder credentials en groepslidmaatschappen) ten behoeve van de Identity Store van de ICT-samenwerking. Optioneel zou deze functionaliteit gebruikt moeten kunnen worden voor de replicatie van identiteit van medewerkers van BERM-gemeenten vanuit bronsystemen (zoals een HRM-systeem) richting de technische Identity Store (Identity Store.Windows Environment BERM-gemeente).
Rules Engine.Identity Deployment ICT-Samenwerking	Uitvoer van scripts/regels die de uitrol van gebruikersaccounts reguleren. Een voorbeeld is het filteren

	van credentials bij replicatie.
Identity Validation.Gebruiker ICT-Samenwerking	Valideren van een gebruiker die een dienst wil benutten bij de ICT-Samenwerking. De validatiegegevens (account plus credentials) van medewerkers van gemeenten worden doorgezet ter controle richting de Identity Validation-voorziening bij de betreffende BERM-gemeente, omdat wachtwoorden niet worden gerepliceerd en niet beschikbaar zijn in de Identity Store van de ICT-samenwerking.
Identity Store.Gebruikers ICT-Samenwerking	Centrale opslag van gebruikers die een dienst afnemen van de ICT-Samenwerking. De gebruikersaccounts zijn gerelateerd aan de gebruikersaccounts van de betreffende BERM-gemeente door middel van replicatie. De accounts worden door de ICT-Samenwerking beheerd.
Permission Validation.Gebruiker ICT-Samenwerking	Valideren van permissies van een gebruiker in relatie tot de dienst die deze gebruiker wil benutten.
Permission Register.Voorzieningen ICT-Samenwerking	Register met permissies van gebruikers in relatie tot de diensten van de ICT-Samenwerking waar zij gebruik van maken. De permissies worden door de ICT-Samenwerking beheerd.
Deployment.Identities derde partijen	Uitrol (replicatie) van digitale identities en hieraan gerelateerde attributen (waaronder credentials en groepslidmaatschappen).
Rules Engine.Identity Deployment derde partijen	Uitvoer van scripts/regels die de uitrol van gebruikersaccounts reguleren. Een voorbeeld is het filteren van credentials bij replicatie.
Logging.IPM Activities	Logging van alle activiteiten die door het systeem worden uitgevoerd, evenals alle beheertransacties die worden doorgevoerd. Doel van deze functie is ervoor zorgen dat de voorziening goed te auditen is.
Identity Validation.Gebruiker derde partij	Valideren van een gebruiker die een dienst wil benutten bij een derde partij. De validatiegegevens (account plus credentials) van medewerkers van gemeenten worden doorgezet ter controle richting de Identity Validation-voorziening bij de betreffende BERM-gemeente, omdat wachtwoorden niet worden gerepliceerd en niet beschikbaar zijn in de Identity Store van de ICT-samenwerking.
Identity Store.Derde partij	Centrale opslag van gebruikers die een dienst afnemen van een derde partij. De gebruikersaccounts zijn gerelateerd aan de gebruikersaccounts van de betreffende BERM-gemeente.

De kernfunctionaliteit van de voorziening die de ICT-Samenwerking wil inzetten, is in een lichtblauw kader ondergebracht. Aan deze voorziening worden aanvullend de volgende eisen gesteld:

1. De voorziening maakt het mogelijk om richting BERM-gemeenten een self-service-pagina aan te bieden, zodat gebruikers hun wachtwoord kunnen resetten (binnen de eigen bron-Identity Store).
2. Ten aanzien van authenticatie dient multifactorauthenticatie ondersteund te kunnen worden.

3. Het beheer van de voorziening dient gecontroleerd gedelegeerd te kunnen worden
4. Optioneel, behorend bij het beheer van de (technische) AD van de verbonden gemeenten: Het moet mogelijk zijn om voor vaste beheeractiviteiten geautomatiseerde workflows aan te maken, zodat bijvoorbeeld verzoeken vanuit de servicedesk automatisch doorgezet worden naar de juiste beheerafdelingen.

Ten aanzien van de beschreven functionaliteit hanteert de ICT-Samenwerking de volgende richtlijnen:

1. Digitale identiteiten worden één op één gekoppeld aan Natuurlijke Personen of unieke systemen.
2. Brongegevens bevinden zich bij de juridische entiteit die verantwoordelijk is voor het beheer van de digitale identiteiten, zijnde de gemeenten. Gegevens die gerepliceerd worden vanuit de gemeenten, bevinden zich in een Mircrosoft Active Directory-implementatie.
3. Wachtwoorden worden alleen bewaard binnen de gemeenten en worden niet gerepliceerd.
4. Gebruikers van andere organisaties worden niet opgenomen in de Identity Stores van gemeenten waarin medewerkeraccounts van de gemeente zijn opgenomen.
5. Organisaties die diensten leveren zijn zelf verantwoordelijk voor beheer van gebruikersaccounts en permissies.
6. Permissies worden zoveel mogelijk rolgebaseerd ingesteld.
7. Het moet mogelijk zijn om loggingbrongegevens onweerlegbaar authentiek vast te leggen in het originele formaat.

Ten aanzien van bovengenoemde functionaliteit heeft de ICT-Samenwerking de volgende vragen:

1. Welke producten adviseert u voor de invulling van bovengenoemde functionaliteit? In welke functionaliteit kan niet worden voorzien?
2. Welke protocollen worden ondersteund voor de replicatie van identiteitsgegevens?
3. Is het mogelijk om de eigenaar van de brongegevens (in dit geval de gemeenten) de controle te geven over wat wel en niet aan accountgegevens wordt gerepliceerd?