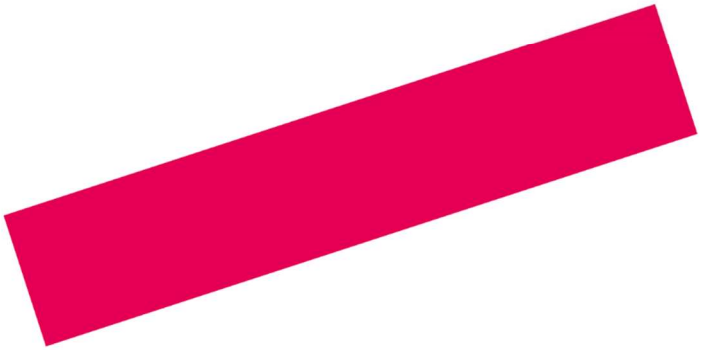
PROGRAMMA VAN EISEN_

IDM / IAM



Status definitief

Dennis Ortsen (Solution Architect), Marco de Haan (Solution Architect)

5 november 2020

1 INLEIDING

Op basis van dit document wenst Opdrachtgever middels deze marktconsultatie vast te stellen in welke mate uw oplossing kan voldoen aan de requirements voor de toekomstige Identity & Access Management omgeving van Opdrachtgever. De requirements zijn in dit document beschreven en zijn gebaseerd op de bijlages die bij deze marktconsultatie zijn opgenomen.

2 IDENTITY MANAGEMENT

Nr	Omschrijving	Voldaan? [ja/nee]	Opmerkingen
A1.	Het systeem bevat in de basis alleen identiteitsgegevens die absoluut noodzakelijk zijn voor het identiteitsbeheer. Het systeem is naar inzicht van de klant zonder kosten en maatwerk uitbreidbaar met extra kenmerken bedoeld voor identiteitsbeheer.		
A2.	Het systeem is in staat een koppeling te realiseren met het HR systeem waarbij nieuwe medewerkers geheel automatisch in het IAM systeem worden aangemaakt en beheerd conform de business logica van de HAN.		
A3.	Het systeem is in staat een koppeling te realiseren met het Studenten Informatiesysteem (SIS) systeem waarbij nieuwe studenten geheel automatisch in het IAM systeem worden aangemaakt en beheerd conform de business logica van de HAN.		
A4.	Het systeem kent voorzieningen/oplossingen voor de import van identiteiten anders dan student of medewerker. Denk bijv. aan gastdocent, alumnus, externe medewerker. Het systeem is voldoende flexibel om bronsysteem koppelingen te maken met andere systemen, zoals een CRM systeem.		
A5.	Het systeem wordt geleverd met voorzieningen/oplossingen om te koppelen met externe Identity Providers (Guest IdP) waaronder (maar niet beperkt tot) SURFconext, andere onderwijsinstellingen, social logon.		
A6.	Bij de provisioning worden alle noodzakelijke gegevens van de medewerker/student geïmporteerd zoals (maar niet beperkt tot):		

	Soort identiteit (medewerker, student, cursist, alumnus enz.), NAW gegevens, faculteit, (onder)afdeling, functie, opleiding, communicatiegegevens als meerdere emailadressen en telefoonnummers. De HAN kan zonder ontwikkelwerk vanuit leveranvier extra gegevens aan de import toegevoegen.		
A7.	Het systeem beschikt over drivers waarmee identiteiten en hun rechten vanuit IAM in zgn. afnemende systemen kunnen worden ingevoerd. Van belang zijn o.a. (maar niet uitputtend): (A)AD, Office 365, SIS, rooster- en toegangssystemen, Elektronische Leer Omgevingen (ELO's) en financiële systemen. Idealiter is reeds een flink aantal van deze drivers standaard beschikbaar of eenvoudig te realiseren.		
A8.	Het systeem staat bi-directionele koppelingen toe, zodat er naar bronsystemen kan worden teruggeschreven. Een voorbeeld is het emailadres dat de instelling uitgeeft.		
A9.	Het systeem onderkent het concept van identity life cycle: bijvoorbeeld van aanmelder naar student naar alumnus. Het Systeem modelleert voor de verschillende nader te identificeren identiteitstypes de lifecycle aan de hand van business events.		
A10.	Het systeem staat het invoeren en onderhouden van een standaard autorisatiemodel (SAM) voor autorisaties toe waarbij een hiërarchie van autorisatie mogelijk is en eenvoudig kan worden aangepast aan veranderende omstandigheden in de business.		
A11.	Het systeem ondersteunt een vorm van automatische rechtentoekenning zoals RBAC (Role Based Access Control), ABAC (Attribute Based Access Control) en Risk Adaptable Access Control (RAdAC) waarbij templates/rollen voor verschillende bedrijfsfuncties kunnen worden gedefinieerd. Toekenning van een bepaald attribuut of een bepaalde rol geschiedt automatisch op grond van bepaalde attributen zoals bedrijfsrol, academie, functie e.d. Het systeem kent alle verbonden rechten automatisch toe voor alle geconfigureerde drivers naar de afnemende systemen. Een identiteit moet meerdere rollen kunnen hebben.		
A12.	Het systeem wordt geleverd met een workflow systeem, waarmee eenvoudig en doeltreffend (extra) rechten kunnen worden aangevraagd (Self-Service). De aanvragen kunnen langs een		

	leidinggevende of systeemeigenaar worden geleid. Toekenning van de rechten kan automatisch via de driver, dan wel handmatig geschieden, bijv. door de medewerkers van de Helpdesk en kunnen ook via dezelfde weg worden ingetrokken. Het is mogelijk een einddatum of looptijd te definiëren voor de extra rechten.		
A13.	Het systeem beschikt over de mogelijkheid om een beheer- en rapportagestructuur in te richten die passen bij de ondersteuningsorganisatie, bijvoorbeeld het verschil van rechten van rechten tussen een Auditer, een centrale of decentrale ServiceDesk medewerker en een goedkeurder van toegangsaanvragen voor een systeem binnen een afdeling.		
A14.	Het systeem beschikt over een standaard import en export formaat waarmee in bulk- of batchvorm rollen, attributen en identiteiten kunnen worden ingevoerd. Denk bijvoorbeeld aan fusies of reorganisaties, maar ook invoering van een nieuw IAM systeem.		
A15.	Het systeem beschikt over koppelingen (bijv. op basis van SOAP of REST api's) waarmee mutaties in het bronsysteem (HR of SIS) direct leiden tot mutaties in het IAM en de achterliggende (afnemende) systemen.		
A16.	Het systeem kan een duidelijk onderscheid maken tussen een natuurlijk persoon en een identiteit: een identiteit is altijd herleidbaar naar een natuurlijk persoon. In het geval van een onpersoonlijk account (technisch- of test account) is een identiteit herleidbaar naar een eigenaar (natuurlijk persoon)		
A17.	Het systeem is in staat om te gaan met de volgende complexe, interne wisselingen van scope, zoals de volgende situaties: - meerdere dienstverbanden bij 1 medewerker; - tijdelijke intrekking van rechten en herleving later (bijv. onderbreking studie); - overgang van type identiteit, bijv. van gastdocent naar medewerker; - docent wisselt van academie, of een staf lid dat van afdeling wijzigt; - kan omgaan met het gelijktijdig voorkomen van meerdere typen identiteiten voor één natuurlijk persoon.		
A18.	Bij de beëindiging van de relatie met een medewerker of student worden de toegangsrechten automatisch ingetrokken (de-provisioning) en doorgegeven naar de afnemende systemen. Daarbij kan een "grace period" worden ingesteld waarbij tijdens deze “grace		

	period" afwijkende rechten kunnen worden ingesteld. Deze "grace period" is vrij instelbaar HAN-breed, maar ook op organisatieonderdeel.		
A19.	Alle informatie in het systeem, ongeacht of deze zich in de primaire vault of een afgeleide kopie (LDAP, SQL, ...) bevindt, kan gehashed worden opgeslagen. Het gebruikte algoritme is minimaal MD5, SHA-256. Wachtwoorden kunnen bovendien salted hashed worden opgeslagen.		
A20.	Er bestaan 2 referenties met een HR systeem als bronsysteem, dat gebruikt wordt in het Nederlandse of Europese onderwijs. (zoals bijvoorbeeld SAP of PeopleSoft.)		Welke wil de HAN hier zien?
A21.	Er bestaan 2 referenties met een SIS systeem als bronsysteem, dat gebruikt wordt in het Nederlandse of Europese onderwijs. (zoals bijvoorbeeld Peoplesoft of Osiris.)		Welke wil de HAN hier zien?
A22.	Het moet mogelijk zijn om een Separation Of Duty matrix (SOD) toe te passen.		
A23.	Het systeem biedt een krachtige, gebruikersvriendelijke interface voor de beheerders, zoals een responsive webinterface met Multi Factor Authenticatie en waarbij Functioneel-, Applicatie- en Technisch Beheer en Ondersteuners zoals de ServiceDesk en (de)centraal beheerders zodat de juiste personen hierin de juiste toegang hebben.		
A24.	Het systeem biedt mogelijkheden voor zogenaamde "test accounts", in te voeren via een zij-instroom waarop dezelfde rollen of attributen toe te kennen zijn volgens zogenaamde "persona's". Op deze "test accounts" zijn dezelfde life cycles mogelijk, alsmede rapportage en deze accounts zijn altijd herleidbaar tot een natuurlijk persoon.		
A25.	Het systeem is voorzien van een portaal waar eindgebruikers wijzigingen kunnen aanbrengen en gegevens kunnen aanvullen zoals mobiel nummer, profielfoto, privé e-mailadres en challenge responseset t.b.v. wachtwoordreset. Verder biedt het de mogelijkheid om wachtwoorden zelf te resetten, om consent te geven op de voorwaarden voor het gebruik van SSO-diensten, tokens en gekoppelde apparaten.		

3 AUTHENTICATION MANAGEMENT

Nr	Omschrijving	Voldaan? [ja/nee]	Opmerkingen
A26.	Het systeem biedt mechanismen aan ten behoeve van Single Sign On authenticatie van gebruikers bij (federatief) gekoppelde systemen.		
A27.	Tenminste worden ondersteund SAML2, Oauth, OpenID (connect), LDAP, Kerberos-tickets.		
A28.	Het systeem ondersteunt een instelbare timeout tijd voor "idle" sessies, voor verschillende Service Providers. Er is ook een instelbare maximale levensduur voor sessies.		
A29.	Het systeem ondersteunt MFA langs verschillende wegen (push bericht, token, SMS enz.)		
A30.	Het systeem ondersteunt conditionele MFA (step up authenticatie), waarbij afhankelijk van user profile, geolocatie, device e.d. MFA wordt afgedwongen (risk based access). Dat gebeurt ook op grond van (afwijkend of onlogisch) inloggedrag, na een vast instelbaar aantal mislukte pogingen wordt het account geblokkeerd.		

4 ACCESS MANAGEMENT

Nr	Omschrijving	Voldaan? [ja/nee]	Opmerkingen
A31.	Het systeem is voorzien van een portaal waar eindgebruikers wijzigingen kunnen aanbrengen en gegevens kunnen aanvullen zoals mobiel nummer, profielfoto, privé e-mailadres en challenge responseset t.b.v. wachtwoordreset. Verder biedt het de mogelijkheid om wachtwoorden zelf te resetten, om consent te geven op de voorwaarden voor het gebruik van SSO-diensten, tokens en gekoppelde apparaten.		
A32.	Het systeem ondersteunt workflows die ingesteld kunnen worden door (gedelegeerde) beheerders waarmee eindgebruikers rechten kunnen aanvragen en gemandateerde personen deze kunnen goedkeuren, afwijzen of doorsturen naar een andere organisatie		

	eenheid. De eindgebruikers ervaren dit als een self-service systeem. De workflows kunnen varieren per organisatieonderdeel, zowel qua hierarchie (meer of minder lagen) als scope (meer of minder afdelingen of gemandateerden per afdeling).		
A33.	Het systeem ondersteunt Privileged Account Management (PAM). Denk aan extra policies, tijdelijkheid inlog, sessie monitoring en uitgebreide logging, indien het systeem dit niet zelf ondersteunt, dan kan het integreren met een separaat systeem zoals Azure KeyVault.		
A34.	Het systeem ondersteunt dynamische groepen op basis van attributen. Het kenmerk van een attribuut is vrij op te geven, bijvoorbeeld opleiding, minor, locatie, deeltijd/voltijd, HR-functie, organisatieafdeling (tot op teamniveau).		

5 ANALYTICS & MONITORING

Nr	Omschrijving	Voldaan? [ja/nee]	Opmerkingen
A35.	Het systeem biedt logging op verschillende niveaus, welke eenvoudig ontsloten kan worden voor verschillende profielen waaronder (maar niet beperkt tot) Security Officer (CISO), Security Manager, Data- of Systeemeigenaar, Auditor. Logging blijft ten minste 6 maanden bewaard en/of kan worden doorgestuurd naar een centraal systeem zoals een Security Information & Event Management systeem (SIEM)		
A36.	Het systeem leert en herkent gebruikelijke patronen bij authenticatiepogingen en notificeert bij (significante) afwijkingen.		
A37.	Het systeem herkent - aan de hand van in te stellen periodes - ongebruikte accounts en rapporteert daarover.		
A38.	Het systeem biedt de mogelijkheid om kengetallen te genereren zoals hoeveel accounts, hoeveel wachtwoord resets, hoeveel mislukte inlogpogingen, hoeveel ongebruikelijke locaties.		
A39.	Het systeem biedt rapportage op CPU-gebruik, wachtrijen, algehele performance, doorlooptijden, responsetijden, uptime. Hierbij moet signalering mogelijk zijn zoals verzending van een SMS of e-mail wanneer de gemonitorde dienst binnen een bepaalde tijd (een aantal		

	keer) faalt, of de toegangsaanvraag langer dan een bepaalde tijd blijft liggen.		
A40.	Het moet mogelijk zijn om een groep van 10.000 accounts binnen een uur bij te werken bij een resource-uitbreiding van een rol. Hierbij moet het systeem een realistische sizing kennen.		
A41.	Het product moet Identity Governance and Administration (IGA) rapportages ondersteunen zoals overzichten met toegekende rechten, zoals per user of per systeem, maar ook kengetallen over het gebruik van het selfservice systeem voor eindgebruikers om toegang aan te vragen, maar ook kwartaarlijkse controle van rechten voor bedrijfskritische applicaties, reguliere rechten voor natuurlijke personen en onpersoonlijke (systeem-)accounts eens per half jaar goedgekeurd door leidinggevende (middels een review functionaliteit).		

6 NON-FUNCTIONALS

Nr	Omschrijving	Voldaan? [ja/nee]	Opmerkingen
A42.	Het IAM systeem moet redundant on premise gedraaid kunnen worden en kan als as-a-service worden aangeboden. Hybride oplossingen worden ondersteund.		
A43.	Er zijn bij de leverancier of partners minstens drie technische consultants beschikbaar in Nederland die kunnen ondersteunen bij de implementatie en het functioneel en technisch beheer van het systeem, gedurende de gebruiksperiode bij de HAN. Er bestaan Nederlandstalige helpdesks bij de leverancier en diens partners, gedurende de gebruiksperiode bij de HAN.		
A44.	Het systeem heeft als Identity Provider (IdP) een koppeling met SURFconext, of deze koppeling is eenvoudig te realiseren.		
A45.	Het systeem wordt ge-update middels continuous delivery of frequente minor upgrades. Het is eenvoudig om actueel te blijven		

	met het systeem, ook bij gebruik van meerdere modules van het product, of bij hosting on premise.		
A46.	Op basis van 3 referenties - van bij voorkeur vergelijkbare klanten - moet getoetst kunnen worden dat het product de gewenste kwaliteit heeft.		
A47.	Alle betrokken partijen moeten - daar waar toepasbaar - voldoen aan eisen inzake informatiebeveiliging en privacy (ISO27001, GDPR, data binnen EER etc.). Qua verwerkersovereenkomst wordt de SURF-standaard gebruikt.		
A48.	Het systeem moet redundant uitgevoerd kunnen worden, waarbij er een 24*7 beschikbaarheid geldt met een 99% uptime (inclusief gepland onderhoud) voor wat betreft authenticatie.		

OPEN UP NEW HORIZONS.

HAN_UNIVERSITY
OF APPLIED SCIENCES