

Marktconsultatieverslag
Identity and Access Management (IAM)
ten behoeve van VISTA college

Aanbestedende dienst:
Datum:
Versie:

VISTA college
1 oktober 2026
Definitief



Voorwoord

VISTA college is voornemens om een aanbesteding voor Identity & Access Management (IAM) te starten. Om deze opdracht goed in de markt te kunnen zetten, heeft VISTA college informatie opgehaald door middel van een marktconsultatie. Voor u ligt het marktconsultatieverslag. Bedrijfsgevoelige informatie van de deelnemende partijen is uit het verslag gelaten.

Het marktconsultatieverslag bestaat uit een samenvatting van de schriftelijke antwoorden van de deelnemende partijen. VISTA college heeft tien aanmeldingen ontvangen en wil deze partijen bedanken voor hun input en deelname.

Algemene vragen

1.	<i>U als onderneming, zoals:</i> • <i>Naam;</i> • <i>Adres en vestigingslocatie(s);</i> • <i>Contactgegevens;</i> • <i>Korte beschrijving van de organisatie;</i> • <i>Partnerschappen of samenwerkingsverbanden.</i>
Antwoord	Tien partijen hebben gereageerd op de marktconsultatie. De deelnemers bestaan uit zowel gespecialiseerde IAM-dienstverleners en softwareleveranciers als bredere ICT-dienstverleners met specifieke IAM-expertise. De organisaties verschillen in omvang en positionering en zijn hoofdzakelijk in Nederland gevestigd of beschikken over een Nederlandse vestiging. Meerdere partijen werken samen met technologiepartners of IAM-softwareleveranciers. Andere partijen ontwikkelen en leveren een eigen IAM-oplossing. De dienstverlening varieert van advies en implementatie tot softwarelevering, migratie, beheer en ondersteuning. Een deel van de partijen benoemt specifieke ervaring binnen het onderwijs of de (semi)publieke sector.
2.	<i>Uw productportfolio:</i> • <i>Overzicht van IAM-producten en diensten</i> ◦ <i>Beschrijving van de belangrijkste IAM-oplossingen in het portfolio</i> ◦ <i>IGA, AM, PAM, SSO, SSI, Machine Identity, Authentication, Analytics</i> ◦ <i>MFA, SSO, methoden voor sterke authenticatie, passwordless, e.g.</i> • <i>Architectuur en technologie</i> ◦ <i>Architectuur en technologie</i> ◦ <i>Ondersteunde standaarden (SCIM, SAML, OIDC, OAuth2, LDAP, XACML, SOAP, REST API)</i> ◦ <i>Cloud-native, on-premises hybride of multi-cloud</i> ◦ <i>Schaalbaarheid en high availability</i> ◦ <i>Real-time provisioning, batchverwerking, workflowgestuurde provisioning</i> • <i>Integratiemogelijkheden</i> ◦ <i>Koppelingen met bronsysteem (HR, studentinformatiesystemen, etc)</i> ◦ <i>Koppelingen met doelsystemen (applicaties, cloudplatforms, ITSM, OT)</i> ◦ <i>Koppelingen met federatieve idP's</i> ◦ <i>API's, connectoren en standaardintegraties</i> • <i>Selfservice en gebruikersportalen</i> ◦ <i>Functionaliteit voor eindgebruikers, managers en beheerders</i> ◦ <i>Gebruikersbeheer (profielinformatie, wachtwoordbeheer, toegangs aanvragen)</i> ◦ <i>Rolmanagement (beheer van rollen, roltoewijzing, rolmodellering, role mining)</i> • <i>Security & compliance</i> ◦ <i>Ondersteuning voor Zero Trust, MFA, logging, auditing</i> ◦ <i>Logging- en auditfunctionaliteiten, integratie met SIEM/XDR-platformen</i> • <i>Innovaties en roadmap</i> ◦ <i>Ontwikkelingen op het gebied van SSI, AI, CIEM, etc.</i> ◦ <i>Toekomstvisie op IAM en geplande uitbreidingen</i>
Antwoord	De aangeboden portfolio's verschillen in breedte. Meerdere partijen bieden een brede IAM/IGA-oplossing waarmee identiteiten, rollen en toegangsrechten gedurende de levenscyclus kunnen worden beheerd. Daarbij worden onder meer IGA, provisioning, lifecyclemanagement, toegangsbeheer, selfservice, logging, auditing en rapportage genoemd. De markt kent zowel geïntegreerde platforms als modulaire oplossingen waarbij aanvullende functionaliteiten via andere componenten of technologiepartners worden ingevuld. Functionaliteiten zoals PAM, SSO, MFA, SSI, machine identity en geavanceerde analytics maken daardoor niet bij iedere oplossing standaard onderdeel uit van het kernproduct.



	Open standaarden en API's worden breed ondersteund. Meerdere oplossingen zijn cloud- of SaaS-gebaseerd, terwijl ook hybride en on-premises mogelijkheden worden aangeboden. Integraties met HR-, onderwijs-, ITSM- en Microsoft-omgevingen zijn breed beschikbaar, al verschilt per aanbieder welke koppelingen standaard beschikbaar zijn en welke specifiek moeten worden ontwikkeld.
--	---

Visie en ervaring

3.	<i>Wat is uw visie op IAM Identity & Access Management (IAM)?</i> • <i>in relatie tot onderwijs en digitale transformatie?</i> • <i>In relatie tot innovaties die u voorziet in de komende vijf jaar?</i> • <i>In relatie tot het verminderen van handmatige beheertaken?</i>
Antwoord	De partijen zien IAM overwegend als een strategische randvoorwaarde voor veilige en flexibele digitale dienstverlening en niet uitsluitend als een technische voorziening voor accountbeheer. Voor het onderwijs wordt met name het geautomatiseerd ondersteunen van de volledige levenscyclus van studenten, medewerkers en externe gebruikers genoemd. Voor de komende jaren verwachten partijen verdere ontwikkeling van federatieve identiteiten en eduID, SSI en verifiable credentials, machine-identiteiten, Zero Trust, AI en meer geautomatiseerde governance en toegangscontrole. Daarnaast wordt een verschuiving verwacht van uitsluitend rolgebaseerde autorisatie naar combinaties van rollen, attributen en beleid. Vermindering van handmatige beheertaken wordt vooral verwacht door verdere automatisering van lifecycle- en provisioningprocessen, selfservice en het automatisch laten doorwerken van wijzigingen vanuit bronsystemen naar aangesloten doelsystemen.
4.	<i>Hoe speelt u met uw productontwikkeling of dienstverlening in op deze toekomstvisie?</i>
Antwoord	De partijen geven aan hun productontwikkeling en dienstverlening verder te richten op automatisering, governance, federatieve identiteiten, open standaarden, Zero Trust en nieuwe toepassingen van AI en SSI. Softwareleveranciers verwerken deze ontwikkelingen in hun productroadmaps. Dienstverleners die zelf geen IAM-platform ontwikkelen, volgen deze ontwikkelingen via hun technologiepartners en vertalen deze naar implementatie-, advies- en beheertrajecten. Daarbij wordt door meerdere partijen een gefaseerde invoering benadrukt, waarbij nieuwe functionaliteiten worden toegevoegd wanneer deze voldoende volwassen zijn en aansluiten op de behoeften van de organisatie.
5.	<i>Hoe sluit uw toekomstvisie en productontwikkeling aan op de genoemde uitgangspunten van de VISTA college?</i>
Antwoord	De partijen geven aan dat hun visie en dienstverlening in belangrijke mate aansluiten op de uitgangspunten van VISTA college. Veelgenoemde aansluitingen zijn centrale regie en governance, geautomatiseerde lifecycleprocessen, open standaarden, Zero Trust, gefaseerde implementatie en het beperken van handmatig beheer. Daarnaast wordt aansluiting genoemd op digitale soevereiniteit, federatieve voorzieningen zoals SURFconext en eduID en een architectuur die toekomstige ontwikkelingen kan ondersteunen. Meerdere partijen adviseren om continuïteit tijdens de overgang centraal te stellen en nieuwe of meer innovatieve functionaliteiten vervolgens gefaseerd toe te voegen.
6.	<i>Wat zijn uw plannen met artificial intelligence i.r.t. uw productontwikkeling? Welke mogelijkheden ziet u voor A.I., nu en in de toekomst?</i>
Antwoord	De partijen zien verschillende toepassingsmogelijkheden voor AI binnen IAM. Genoemd worden onder meer role mining en role engineering, anomaliedetectie, toegangsreviews, risicobeoordeling, analyse van toegangsdata en ondersteuning bij het opstellen en onderhouden van autorisatieregels. De volwassenheid verschilt tussen de aangeboden oplossingen. Bij sommige partijen zijn AI-functionaliteiten reeds beschikbaar of concreet voorzien op de roadmap, terwijl andere partijen AI voornamelijk als toekomstige ontwikkelrichting beschouwen. Daarbij wordt ook aandacht gevraagd voor transparantie, controleerbaarheid en passende governance bij de inzet van AI.



7.	<i>Wat onderscheidt u van andere aanbieders op de markt?</i>
Antwoord	De partijen verschillen in hun positionering en leveringsmodel. Genoemd worden onder meer verschillen in de mate van specialisatie, de inzet van eigen of externe technologie, de wijze van implementatie en de mogelijkheden om advies, implementatie en beheer integraal of afzonderlijk aan te bieden. Ook verschillen partijen in de wijze waarop hosting en samenwerking met technologiepartners zijn ingericht.

8.	<i>Wat is uw ervaring met IAM-implementaties binnen Nederland of Europa?</i>
Antwoord	De partijen geven aan ervaring te hebben met IAM-implementaties binnen Nederland en/of andere Europese landen. De ervaring varieert van implementatie en migratie tot advies, beheer en doorontwikkeling van IAM-omgevingen. Meerdere partijen benoemen ervaring bij grote of complexe organisaties en binnen de publieke of semipublieke sector. Een deel van de partijen heeft daarnaast specifieke ervaring binnen onderwijsinstellingen. De omvang en aard van de genoemde referenties verschillen per deelnemer.

Technische inrichting

9.	<i>Hoe integreert uw IAM-platform met sectorspecifieke producten zoals SURFconext en eduID?</i>
Antwoord	De meeste partijen geven aan dat integratie met SURFconext en eduID technisch mogelijk is, veelal door gebruik te maken van open en federatieve standaarden zoals SAML, OAuth2 en OIDC. De voorzieningen worden door meerdere partijen gezien als belangrijke onderdelen van het toekomstige digitale identiteitslandschap binnen het onderwijs. Verschillende partijen benadrukken dat SURFconext en eduID zich blijven ontwikkelen. Zij adviseren daarom een open en interoperabele architectuur die kan meegroeien met toekomstige ontwikkelingen, in plaats van deze voorzieningen als een statische koppeling te beschouwen.

10.	<i>Hoe wordt de technische ondersteuning voor Self-Sovereign Identity (SSI) vanuit uw productportfolio ingericht? Ondersteunt u verifiable credentials, digitale wallets, en decentralized identifiers (DIDs)?</i>
Antwoord	De ondersteuning voor SSI verschilt tussen de aangeboden oplossingen. Een deel van de partijen ondersteunt of bereidt zich technisch voor op standaarden voor verifiable credentials, digitale wallets en decentralized identifiers. Andere partijen geven aan dat SSI nog geen onderdeel is van hun huidige kernfunctionaliteit, maar dat de architectuur toekomstige aansluiting hierop mogelijk maakt. Meerdere partijen beschouwen SSI als een ontwikkeling die voor het onderwijs relevant kan worden, mede in relatie tot eduID en andere sectorale ontwikkelingen. De markt laat daarmee zien dat SSI in ontwikkeling is, maar nog niet bij alle aanbieders als volwassen standaardfunctionaliteit beschikbaar is.

11.	<i>Wat zijn de mogelijkheden om IAM te integreren met het IT service management portaal (Topdesk) van VISTA college?</i>
Antwoord	Meerdere partijen geven aan integratie met TOPdesk te kunnen realiseren. Hiervoor worden onder meer standaardconnectoren, API-koppelingen, webhooks en ticketgestuurde integraties genoemd. De mate waarin hiervoor een bestaande standaardkoppeling beschikbaar is verschilt per oplossing. Bij een deel van de oplossingen kan gebruik worden gemaakt van een bestaande integratie, terwijl bij andere oplossingen een generieke koppeling moet worden ingericht of verdere integratie nog in ontwikkeling is.

12.	<i>Hoe integreert uw oplossing met Entra ID? Is er een standaardkoppeling en kunnen wachtwoorden veilig worden uitgewisseld?</i>
Antwoord	Integratie met Microsoft Entra ID wordt breed ondersteund. Partijen noemen hiervoor standaardconnectoren, API's en federatieve standaarden. De koppeling wordt onder meer gebruikt voor provisioning, lifecyclemanagement, synchronisatie van accounts en rechten en aansluiting op authenticatie en SSO. Meerdere partijen positioneren Entra ID als de authenticatie- of directoryvoorziening naast de IAM/IGA-oplossing, waarbij het IAM-platform verantwoordelijk is voor governance en het actueel houden van identiteiten en autorisaties. De wijze waarop met wachtwoorden wordt omgegaan



	verschilt per oplossing; meerdere partijen streven ernaar wachtwoorden niet via het IAM-platform uit te wisselen wanneer gebruik kan worden gemaakt van federatie of bestaande authenticatievoorzieningen.
--	--

Identiteitsbeheer

13.	<i>Welke mogelijkheden biedt uw oplossing voor het modelleren en beheren van identiteiten op basis van doelgroepen en persona's? Denk aan:</i> • <i>automatische herkenning op basis van broninformatie</i> • <i>onderscheid tussen interne en externe gebruikers</i> • <i>validatie, reconciliatie en automatische correctie</i> • <i>één centrale digitale identiteit per persoon, matching vanuit verschillende bronnen</i>
Antwoord	De partijen geven aan dat het modelleren van verschillende doelgroepen en persona's breed wordt ondersteund. Identiteiten kunnen op basis van gegevens uit bronsystemen automatisch worden herkend en ingedeeld, bijvoorbeeld als student, medewerker, externe of gastgebruiker. Meerdere partijen ondersteunen matching vanuit verschillende bronnen naar één centrale digitale identiteit. Daarbij worden validatie en reconciliatie gebruikt om dubbele of afwijkende registraties te signaleren. Bij twijfel kan menselijke beoordeling onderdeel zijn van het proces.
14.	<i>Hoe ondersteunt uw oplossing het beheer van machine-identiteiten (bijv. API's, IoT, RPA)?</i>
Antwoord	Meerdere partijen bieden mogelijkheden voor het beheren van machine-identiteiten, waarbij onder meer eigenaarschap, levenscyclus, toegangsrechten en periodieke controle kunnen worden vastgelegd. De invulling verschilt per oplossing. Sommige partijen beschikken over specifieke functionaliteit of modules voor machine-identiteiten, terwijl andere partijen hiervoor gebruikmaken van reguliere IAM-, IGA- of PAM-functionaliteit. Uit de reacties blijkt daarmee dat machine identity een ontwikkeling binnen IAM is, maar niet bij iedere oplossing op dezelfde wijze wordt ondersteund.

Toegangs- en rollenbeheer

15.	<i>Hoe ondersteunt uw oplossing het beheer van toegangsrechten? I.r.t.</i> • <i>applicaties, werkplekken, systemen en data</i> • <i>externe gebruikers/federatieve identiteiten</i> • <i>het toepassen van RBAC/ABAC/PBAC principes</i> • <i>het toepassen van een levenscyclus voor doelgroepen/persona's</i>
Antwoord	De partijen bieden mogelijkheden voor centraal beheer van toegangsrechten voor applicaties, systemen en werkplekken en, afhankelijk van de oplossing, data. Daarbij worden rollen, attributen en beleidsregels gebruikt om rechten in aangesloten systemen toe te kennen en te beheren. In de reacties worden onder meer RBAC, ABAC en in enkele gevallen beleidsgebaseerde autorisatie genoemd. Ook externe en federatieve gebruikers kunnen worden meegenomen. De mate waarin rechten automatisch kunnen worden toegekend en ingetrokken is mede afhankelijk van de aansluiting van het betreffende doelsysteem.
16.	<i>Welke mogelijkheden kent uw product voor het opbouwen van rolhiërarchieën en roltoewijzingsregels</i> • <i>samengestelde rollen, dynamische rollen</i> • <i>periodieke (her)certificering van rollen</i>
Antwoord	Rolhiërarchieën, samengestelde rollen en dynamische roltoewijzing worden door meerdere partijen ondersteund. Rollen kunnen onder meer automatisch worden toegewezen op basis van attributen uit bronsystemen. Periodieke hercertificering van rollen en toegangsrechten is eveneens breed beschikbaar. Hierbij kan de frequentie afhankelijk worden gemaakt van bijvoorbeeld het risico of type toegangsrecht.
17.	<i>Hoe ondersteunt uw oplossing het proces van role mining en role engineering?</i> • <i>rolherkenning op basis van toegangsdata of gebruikspatronen</i> • <i>al dan niet d.m.v. machine learning/AI</i>
Antwoord	De mogelijkheden voor role mining en role engineering verschillen per oplossing. Meerdere partijen bieden analyse van bestaande rollen, toegangsgegevens en gebruikspatronen om patronen,



	afwijkingen en kandidaat-rollen te identificeren, soms met behulp van AI/ML. Andere partijen richten zich vooral op het ontwerpen, configureren en onderhouden van rollen. Daarbij wordt role mining door sommige partijen gezien als input voor role engineering, terwijl andere partijen de twee activiteiten nadrukkelijk van elkaar onderscheiden. Bij enkele oplossingen zijn role mining en/of role engineering nog in ontwikkeling of onderdeel van de roadmap.
--	--

18.	<i>Hoe ziet uw interface eruit voor de weergave van rollen? Kunnen deze grafisch worden weergegeven met bijbehorende autorisaties? Kan de impact van een wijziging in een rol voor gebruikers worden gesimuleerd?</i>
Antwoord	De mogelijkheden verschillen per oplossing. Sommige partijen bieden grafische weergaven van rollen, rolhiërarchieën en gekoppelde autorisaties, terwijl andere oplossingen deze informatie voornamelijk in tabelvorm presenteren. Ook impactsimulatie is niet bij alle oplossingen op dezelfde wijze beschikbaar. Meerdere partijen kunnen vooraf inzichtelijk maken welke gebruikers en rechten door een voorgenomen wijziging worden geraakt. Bij enkele oplossingen staat verdere grafische ondersteuning nog op de roadmap.

Selfservice voorzieningen

19.	<i>Welke selfservice-functionaliteiten biedt uw IAM-platform voor eindgebruikers, managers en roleigenaren?</i> • wachtwoordherstel • aanvragen van toegangsrechten • aanvragen van authenticatiemiddelen (MFA, Tokens) • inzien van eigen accounts en rechten • goedkeuren van toegangsaanvragen • beheren van rollen inzage in teamrechten
Antwoord	Meerdere partijen bieden selfservicefunctionaliteiten voor eindgebruikers, managers en roleigenaren. Genoemd worden onder meer het aanvragen en inzien van toegangsrechten, het goedkeuren van aanvragen, inzage in eigen accounts en rechten, rolbeheer en inzicht in teamrechten. De precieze functionaliteit verschilt per oplossing. Wachtwoordherstel en het beheer van authenticatiemiddelen worden bijvoorbeeld niet altijd vanuit het IAM-platform zelf aangeboden, maar kunnen ook via een gekoppelde identity- of authenticatievoorziening worden afgehandeld.

20.	<i>Hoe wordt selfservice ondersteund voor gastgebruikers en externe gebruikers?</i> • zelfstandig accounts of rechten aanvragen • eigen gegevensbeheer
Antwoord	Meerdere partijen ondersteunen selfservice ook voor gasten en externe gebruikers. Zij kunnen, afhankelijk van de inrichting, zelfstandig toegang aanvragen, eigen gegevens inzien en gebruikmaken van vooraf ingerichte aanvraag- en goedkeuringsprocessen. De mate waarin externe gebruikers zelfstandig accounts kunnen aanmaken of gegevens kunnen wijzigen verschilt per oplossing en is mede afhankelijk van de gekozen governance en bronsystemen.

21.	<i>Welke workflows en goedkeuringsmechanismen zijn beschikbaar binnen de selfservice-portalen?</i> • multi-level goedkeuring • notificaties en delegatie
Antwoord	Multi-level goedkeuringsworkflows worden breed ondersteund. Goedkeuringsstappen kunnen veelal afhankelijk worden gemaakt van het type aanvraag, de applicatie, het risico of de betreffende doelgroep. Daarnaast worden notificaties, herinneringen, escalaties en tijdelijke delegatie van taken genoemd. Meerdere partijen benadrukken dat workflows zodanig kunnen worden ingericht dat uitzonderingen zwaarder worden beoordeeld dan reguliere aanvragen.

22.	<i>Zijn selfservice-functionaliteiten beschikbaar via mobiele apparaten of apps?</i>
Antwoord	De mogelijkheden voor mobiel gebruik verschillen per oplossing. Een deel van de partijen biedt een responsive webinterface die via mobiele apparaten kan worden gebruikt. Daarnaast worden mogelijkheden genoemd om bepaalde handelingen via andere applicaties uit te voeren.



	Een afzonderlijke mobiele app is niet bij alle oplossingen beschikbaar. Uit de reacties blijkt daarmee dat mobiele toegang veelal mogelijk is, maar dat de wijze waarop deze wordt aangeboden verschilt.
--	--

Geprivilegieerd toegang

23.	<i>Hoe ondersteunt uw oplossing het beheer van geprivilegieerde accounts binnen het IAM-landschap?</i> • password vault • credential rotation • check-in/check-out • sessiebeheer en -monitoring • session recording
Antwoord	De mogelijkheden voor PAM verschillen duidelijk tussen de oplossingen. Een aantal partijen biedt uitgebreide PAM-functionaliteit, waaronder password vaulting, automatische credential rotation, check-in/check-out, sessiebeheer en session recording. Andere oplossingen richten zich vooral op de governance van geprivilegieerde toegang, zoals aanvraag, goedkeuring, toekenning en periodieke controle van verhoogde rechten. Daarnaast positioneren meerdere partijen PAM als een aanvullende, gespecialiseerde component naast IGA, waarbij IGA de governance en lifecycle verzorgt en PAM de technische beveiliging van credentials en beheersessies. Sommige oplossingen bieden hiervoor gedeeltelijke functionaliteit, zoals just-in-time-activering of credential rotation, maar niet het volledige PAM-spectrum. Bij enkele partijen is volledige PAM-functionaliteit niet beschikbaar of wordt hiervoor integratie met een gespecialiseerde PAM-oplossing of de bestaande IdP voorzien.
24.	<i>Hoe sluit uw PAM-oplossing aan op het bredere landschap van VISTA college</i> • IAM-landschap (IGA, Access Manager, SIEM) • hybride omgevingen (on-premises, cloud, OT)
Antwoord	PAM-oplossingen kunnen volgens de partijen worden geïntegreerd met IGA/IAM, authenticatievoorzieningen en SIEM/XDR-platformen. Daarbij worden open standaarden, API's en standaardconnectoren gebruikt. Ook hybride omgevingen worden breed ondersteund. Hiervoor worden onder meer cloudconnectoren en lokale gateways ingezet, waardoor zowel cloud-, on-premises als in sommige gevallen OT-systemen kunnen worden aangesloten.
25.	<i>Welke rapportage- en compliance functionaliteiten biedt uw PAM-oplossing?</i> • overzicht actieve sessies • policy violations • auditlogs
Antwoord	Veelgenoemde functionaliteiten zijn realtime inzicht in actieve sessies, signalering van policy violations en uitgebreide auditlogging. Hiermee kan worden vastgelegd wie wanneer toegang heeft gehad tot een geprivilegieerd account en welke handelingen zijn uitgevoerd. Meerdere oplossingen bieden daarnaast standaardrapportages gericht op compliance en koppelingen met SIEM-platformen voor verdere monitoring en analyse.

Controles, rapportages en recertificatie

26.	<i>Hoe ondersteunt uw oplossing het uitvoeren van periodieke controles en rapportages, interne of externe audits?</i> • attestation-workflows • recertificatiecycli • automatische rapportages • reconciliatie met aangesloten systemen • privileged access • standaard auditrapportages • rapportages i.c.m. artificial intelligence
Antwoord	Periodieke attestatie en recertificatie worden breed ondersteund. De oplossingen bieden doorgaans periodieke en ad-hoccampagnes voor rollen, groepen en toegangsrechten.



	Daarnaast worden automatische reconciliatie, signalering van afwijkingen, auditrapportages en rapportage over privileged access genoemd. AI wordt bij enkele oplossingen ingezet of ontwikkeld voor risicoanalyse en ondersteuning van rapportages en beoordelingen.
--	--

Artificial Intelligence (AI)

27.	<i>Welke functionaliteiten biedt uw IAM-oplossing momenteel op het gebied van artificial intelligence of AI?</i> • levenscyclusbeheer • anomaly detection • role mining • access intelligence • authenticatie • intelligente workflows • machine accounts • chatbots • access reviews • privileged access
------------	---

Antwoord	De huidige inzet van AI verschilt sterk tussen de aangeboden oplossingen. Partijen noemen onder meer role mining, access intelligence, anomaliedetectie en ondersteuning van toegangsreviews als bestaande of beschikbare toepassingen. Andere genoemde toepassingen, zoals intelligente workflows, chatbots, ondersteuning van machine-identiteiten en AI binnen authenticatie of privileged access, zijn niet bij alle oplossingen beschikbaar. Uit de reacties blijkt daarmee dat AI-functionaliteit binnen IAM nog geen uniform volwassen functionaliteitsgebied vormt.
-----------------	---

28.	<i>Welke AI-ontwikkelingen verwacht u binnen IAM in de komende 2 jaar?</i> <i>Heeft u een roadmap met use cases?</i>
------------	---

Antwoord	Partijen verwachten verdere ontwikkeling van AI voor risicogestuurde toegangsreviews, anomaliedetectie, role mining en role engineering en ondersteuning van beheerders en gebruikers. Daarnaast worden toepassingen genoemd waarbij AI helpt bij het formuleren van autorisatieregels of routinematige processen ondersteunt. Niet alle partijen beschikken over een concrete of gedateerde AI-roadmap; bij enkele aanbieders is AI nadrukkelijk een ontwikkelrichting en geen huidige kernfunctionaliteit.
-----------------	--

29.	<i>Hoe waarborgt uw oplossing compliance met de EU AI Act op het gebied van AI?</i> • explainable AI (XAI) • voorkoming van bias of discriminatie • ontrecte toekenning van toegang
------------	--

Antwoord	De partijen benadrukken met name transparantie, menselijke controle, governance en traceerbaarheid bij het gebruik van AI binnen IAM. AI-toepassingen dienen volgens meerdere partijen ondersteunend te zijn en niet zonder controle zelfstandig toegangsbeslissingen te nemen. De mate waarin hiervoor reeds specifieke technische of organisatorische voorzieningen zijn ingericht verschilt per aanbieder. Ook wordt aangegeven dat de toepassing en classificatie van AI-functionaliteit mede afhankelijk is van de concrete usecase.
-----------------	---

Implementatie en migratie

30.	<i>Hoe pakt u de implementatie van uw IAM-oplossing aan binnen een complexe, decentrale organisatie zoals VISTA college?</i> • aanpak, fasering en geschatte doorlooptijd • betrokkenheid van belanghebbenden
------------	---

Antwoord	De partijen adviseren overwegend een gefaseerde implementatie. Daarbij wordt eerst de bestaande dienstverlening en continuïteit geborgd, waarna verdere optimalisatie en uitbreiding plaatsvindt. Vroege betrokkenheid van belanghebbenden, applicatie-eigenaren en beheerders wordt belangrijk gevonden. De daadwerkelijke doorlooptijd is afhankelijk van de scope, het aantal koppelingen, de kwaliteit van brondata en de complexiteit van het rollen- en autorisatiemodel.
-----------------	---



31.	<i>Welke aanpak hanteert u voor de migratie van een bestaand IAM-landschap naar uw oplossing? Hoe voorkomt u verstoring van lopende toegangsprocessen ("migratie met de winkel open")?</i>
Antwoord	De partijen adviseren een gecontroleerde en gefaseerde migratie waarbij het bestaande en nieuwe platform gedurende een periode naast elkaar kunnen functioneren. Een big-bangmigratie wordt veelal vermeden. Migratie kan plaatsvinden per doelgroep, bron- of doelsysteem. Testen, reconciliatie en validatie voordat het bestaande platform wordt uitgezet worden als belangrijke maatregelen genoemd om verstoring van lopende toegangsprocessen te beperken.
32.	<i>Welke methoden gebruikt u voor het analyseren en opschonen van bestaande identiteiten, rollen en rechten voorafgaand aan migratie?</i> • <i>role mining</i> • <i>data quality checks</i> • <i>data mapping</i>
Antwoord	De partijen noemen een combinatie van data-analyse, data quality checks, mapping, reconciliatie en in verschillende mate role mining. Het uitgangspunt is veelal dat verouderde, dubbele of niet-herleidbare accounts en rechten voorafgaand aan de migratie worden geïdentificeerd. Meerdere partijen adviseren om de kwaliteit van de onderliggende brongegevens eerst te verbeteren, zodat bestaande fouten niet ongewijzigd naar het nieuwe platform worden overgezet.
33.	<i>Welke ondersteuning biedt u bij het inrichten van bronsystemen, doelsystemen en connectoren in het nieuwe landschap?</i>
Antwoord	De partijen bieden ondersteuning bij het ontwerpen, configureren, testen en in gebruik nemen van koppelingen met bron- en doelsystemen. Voor veelgebruikte systemen zijn bij verschillende oplossingen bestaande connectoren beschikbaar. Waar geen standaardconnector beschikbaar is, kunnen koppelingen veelal worden gerealiseerd via open standaarden, API's of generieke connectorframeworks. De benodigde inspanning is afhankelijk van de technische mogelijkheden en datakwaliteit van het betreffende systeem.
34.	<i>Hoe wordt de overgang van IAM-processen (zoals provisioning, authenticatie, selfservice) gefaseerd uitgevoerd?</i> • <i>MVP-aanpak of plateaubenadering?</i>
Antwoord	Zowel een MVP- of plateaubenadering wordt door de partijen geadviseerd. Eerst worden fundamentele processen zoals lifecyclemanagement en provisioning stabiel ingericht, waarna uitgebreidere governancefunctionaliteiten en aanvullende systemen worden toegevoegd. Per fase worden duidelijke resultaten en go/no-go-momenten voorgesteld. Hiermee blijft gedurende de overgang een werkende situatie beschikbaar en kan de complexiteit beheerst worden opgebouwd.

Contracteren en prijsvorming

35.	<i>Welke contractvormen biedt u aan voor uw IAM-oplossing? Bijvoorbeeld: SaaS-abonnement, licentieovereenkomst, managed service, open source met supportcontract.</i>
Antwoord	Meerdere partijen bieden de IAM-oplossing aan in de vorm van een SaaS-abonnement, al dan niet gecombineerd met implementatie-, support- en managed-servicesdienstverlening. Daarnaast worden on-premises licenties, beheercontracten en hybride leveringsvormen aangeboden. Sommige partijen kunnen software, implementatie en beheer integraal leveren, terwijl andere partijen hiervoor samenwerken met technologiepartners. Open source met een afzonderlijk supportcontract wordt eveneens genoemd, maar komt in de ontvangen reacties minder nadrukkelijk naar voren.
36.	<i>Welke algemene inkoopvoorwaarden acht u marktconform voor deze opdracht?</i>
Antwoord	De reacties laten verschillende voorkeuren zien. Een deel van de partijen accepteert of herkent publieke ICT-voorwaarden, terwijl andere partijen uitgaan van eigen algemene voorwaarden en hierover contractuele afspraken willen maken.



	Aandacht wordt met name gevraagd voor aansprakelijkheid, intellectueel eigendom, informatiebeveiliging, exit en transitie, gegevensoverdracht en de verhouding tussen voorwaarden van de softwareleverancier en de implementatie- of beheerpartij.
37.	<i>Welke deelopdrachten of percelen binnen deze opdracht ziet u als haalbaar voor uw organisatie?</i>
Antwoord	Uit de reacties blijkt dat de meeste partijen in staat zijn verschillende onderdelen van de opdracht gecombineerd uit te voeren, al dan niet in samenwerking met een technologiepartner. Daarnaast zijn er partijen die zich specifiek richten op onderdelen zoals advies, implementatie, migratie, softwarelevering of beheer. De reacties laten daarmee zien dat zowel een geïntegreerde opdracht als een verdeling in afzonderlijke onderdelen voor delen van de markt uitvoerbaar kan zijn. De gekozen opdrachtstructuur kan wel van invloed zijn op welke typen marktpartijen zelfstandig kunnen deelnemen.
38.	<i>Welke Service Level Agreements (SLA's) biedt u aan? Kunt u inzicht geven in beschikbaarheid, responstijden, hersteltermijnen en rapportage. Denk aan standaard support, premium support, 24/7 ondersteuning.</i>
Antwoord	De partijen bieden verschillende support- en SLA-niveaus. Veelgenoemd zijn standaardondersteuning tijdens kantoor tijden en uitgebreidere of premium ondersteuning met kortere responstijden. 24/7-ondersteuning is bij meerdere partijen mogelijk, met name voor kritieke incidenten of bij volledig beheer. Beschikbaarheid, responstijden en hersteltermijnen verschillen per oplossing en gekozen serviceniveau.
39.	<i>Welk licentiemodel hanteert u voor het beprijzen van uw IAM-oplossing?</i>
	• aantal gebruikers • afgenomen module • aantal transacties • aangesloten systemen • anders
Antwoord	De gehanteerde licentiemodellen verschillen per oplossing. Meerdere partijen hanteren het aantal gebruikers of identiteiten als grondslag voor de licentiekosten. Daarnaast worden modellen genoemd waarbij de prijs mede afhankelijk is van afgenomen modules, functionaliteiten of het aantal aangesloten applicaties. Bij sommige oplossingen gelden aanvullende kosten voor specifieke modules, connectoren of dienstverlening. De reacties laten daarmee geen uniform licentiemodel zien waarmee alle aangeboden oplossingen rechtstreeks op dezelfde grondslag kunnen worden vergeleken.
40.	<i>Welke omstandigheden kwalificeren volgens u als overmacht bij het leveren, implementeren of beheren van de IAM-dienstverlening, en welke omstandigheden beschouwt u als regulier leveranciersrisico?</i>
Antwoord	Partijen maken in algemene zin onderscheid tussen omstandigheden buiten de redelijke invloedssfeer van de leverancier en gebeurtenissen die behoren tot de normale bedrijfs- en leveranciersrisico's. Tot regulier leveranciersrisico worden onder meer beschikbaarheid van de eigen oplossing, voldoende capaciteit, softwarefouten en het nakomen van SLA-afspraken gerekend. Als mogelijke overmacht worden bijvoorbeeld grootschalige externe verstoringen, overheidsmaatregelen en uitval van voorzieningen buiten de invloedssfeer genoemd. De exacte afbakening wordt bij voorkeur contractueel vastgelegd.
41.	<i>Zijn er kosten verbonden aan het toevoegen van extra gebruikers, rollen of systemen? Zijn kortingen mogelijk, bijvoorbeeld in de vorm van staffels.</i>
Antwoord	Bij meerdere oplossingen kunnen extra gebruikers of identiteiten leiden tot aanvullende licentiekosten. Verschillende partijen bieden daarbij staffels of volumekortingen aan. Het toevoegen van rollen leidt volgens de reacties niet altijd tot afzonderlijke kosten. Voor het aansluiten van aanvullende systemen kunnen wel eenmalige implementatie- of connectorkosten en, afhankelijk van de oplossing, terugkerende kosten gelden. De kostenstructuur verschilt daarmee per aangeboden licentiemodel.



42.	<i>Wat kunt u aangeven over mogelijke kosten die zijn verbonden aan het inrichten van uw product, gegeven de omvang van VISTA college? Waar moeten we budget-technisch rekening mee houden?</i> • <i>kosten voor configuratie, integratie, migratie, training en projectmanagement.</i>
Antwoord	De eenmalige implementatiekosten bestaan volgens de partijen voornamelijk uit configuratie, integraties en connectoren, migratie, training en projectmanagement. De uiteindelijke kosten zijn sterk afhankelijk van het aantal bron- en doelsystemen, de beschikbaarheid van standaardconnectoren, de kwaliteit van bestaande data en de complexiteit van het rollen- en autorisatiemodel. Meerdere partijen geven daarom aan pas na nadere inventarisatie een betrouwbare prijs te kunnen bepalen.

43.	<i>Welke jaarlijkse operationele kosten zijn van toepassing?</i> • <i>onderhoud, support, updates, hosting (indien SaaS), monitoring.</i>
Antwoord	Jaarlijkse kosten bestaan voornamelijk uit licenties of abonnementen, onderhoud, support, hosting en eventueel aanvullende beheerdiensten. Bij SaaS-oplossingen zijn onderhoud, updates en hosting vaak geheel of gedeeltelijk in het abonnement inbegrepen. Premium support, uitgebreid beheer of aanvullende applicaties kunnen afzonderlijk worden geprijsd.

Duurzaamheid, publieke waarden en soevereiniteit

44.	<i>Welke certificeringen heeft uw organisatie en/of IAM-oplossing op het gebied van informatiebeveiliging en privacy? (ISO/IEC 27001, 27701, SOC 2, ISAE 3000, NEN 7510)</i>
Antwoord	De aanwezige certificeringen verschillen per partij en oplossing. ISO/IEC 27001 wordt door meerdere partijen genoemd. Daarnaast worden onder meer ISO 9001, SOC 2 en andere assurance- of privacykaders genoemd. Niet iedere partij beschikt over alle in de vraag genoemde certificeringen. Ook wordt in de reacties onderscheid gemaakt tussen certificeringen van de dienstverlener, de softwareleverancier en eventueel de hostingpartij.

45.	<i>Welke maatregelen neemt u om de ecologische voetafdruk van uw platform en dienstverlening te beperken?</i> • <i>groene datacenters, CO₂-compensatie, of circulaire IT-principes.</i>
Antwoord	De partijen noemen verschillende duurzaamheidsmaatregelen, waaronder energiezuinige of groene datacenters, gebruik van hernieuwbare energie, CO₂-reductie of -compensatie en beperking van reisbewegingen door remote dienstverlening. Daarnaast worden duurzaamheids- en ESG-programma's, elektrische mobiliteit en het verminderen van ongebruikte accounts en digitale resources genoemd. De mate waarin duurzaamheid formeel wordt gemeten en gerapporteerd verschilt per partij.

46.	<i>Hoe draagt uw oplossing bij aan de autonomie van gebruikers?</i> • <i>selfservice</i> • <i>controle over eigen gegevens</i> • <i>ondersteuning voor Self-Sovereign Identity (SSI).</i>
Antwoord	De oplossingen ondersteunen autonomie voornamelijk door selfservice, waarmee gebruikers zelf toegang kunnen aanvragen, eigen rechten kunnen inzien en bepaalde handelingen zelfstandig kunnen uitvoeren. De mate waarin gebruikers zelf hun persoonsgegevens kunnen wijzigen is doorgaans beperkt wanneer de gegevens afkomstig zijn uit een leidend bronsysteem. Ondersteuning voor SSI verschilt; bij sommige oplossingen is dit reeds voorzien of voorbereid, terwijl het bij andere partijen vooral een toekomstige ontwikkelrichting betreft.

47.	<i>Hoe wordt privacy-by-design toegepast in uw IAM-platform?</i> • <i>dataminimalisatie</i> • <i>doelbinding</i> • <i>bescherming van persoonsgegevens</i>
------------	---



Antwoord	Dataminimalisatie, doelbinding en bescherming van persoonsgegevens worden door de partijen als belangrijke uitgangspunten genoemd. Veelal worden alleen die gegevens vanuit bronsystemen verwerkt die noodzakelijk zijn voor identiteits- en toegangsbeheer. Daarnaast worden onder meer instelbare bewaartermijnen, encryptie, pseudonimisering, logging en beveiligde gegevensoverdracht genoemd. De precieze technische invulling verschilt per oplossing.
48.	<i>Hoe ondersteunt uw oplossing inclusiviteit en toegankelijkheid?</i> • <i>meertalige interfaces</i> • <i>toegepaste middelen voor gebruikers</i> • <i>ondersteuning voor verschillende doelgroepen</i> • <i>naleving van WCAG-richtlijnen</i>
Antwoord	Meerdere partijen bieden meertalige interfaces en mogelijkheden om de gebruikersinterface en selfservice af te stemmen op verschillende doelgroepen. Daarbij wordt onder meer aandacht besteed aan eenvoudige bediening en begrijpelijke interfaces. WCAG wordt door meerdere partijen genoemd in relatie tot digitale toegankelijkheid. Uit de reacties blijkt echter niet dat iedere aangeboden oplossing aantoonbaar aan hetzelfde WCAG-niveau voldoet. De mate van conformiteit en de beschikbare onderbouwing verschillen per oplossing.