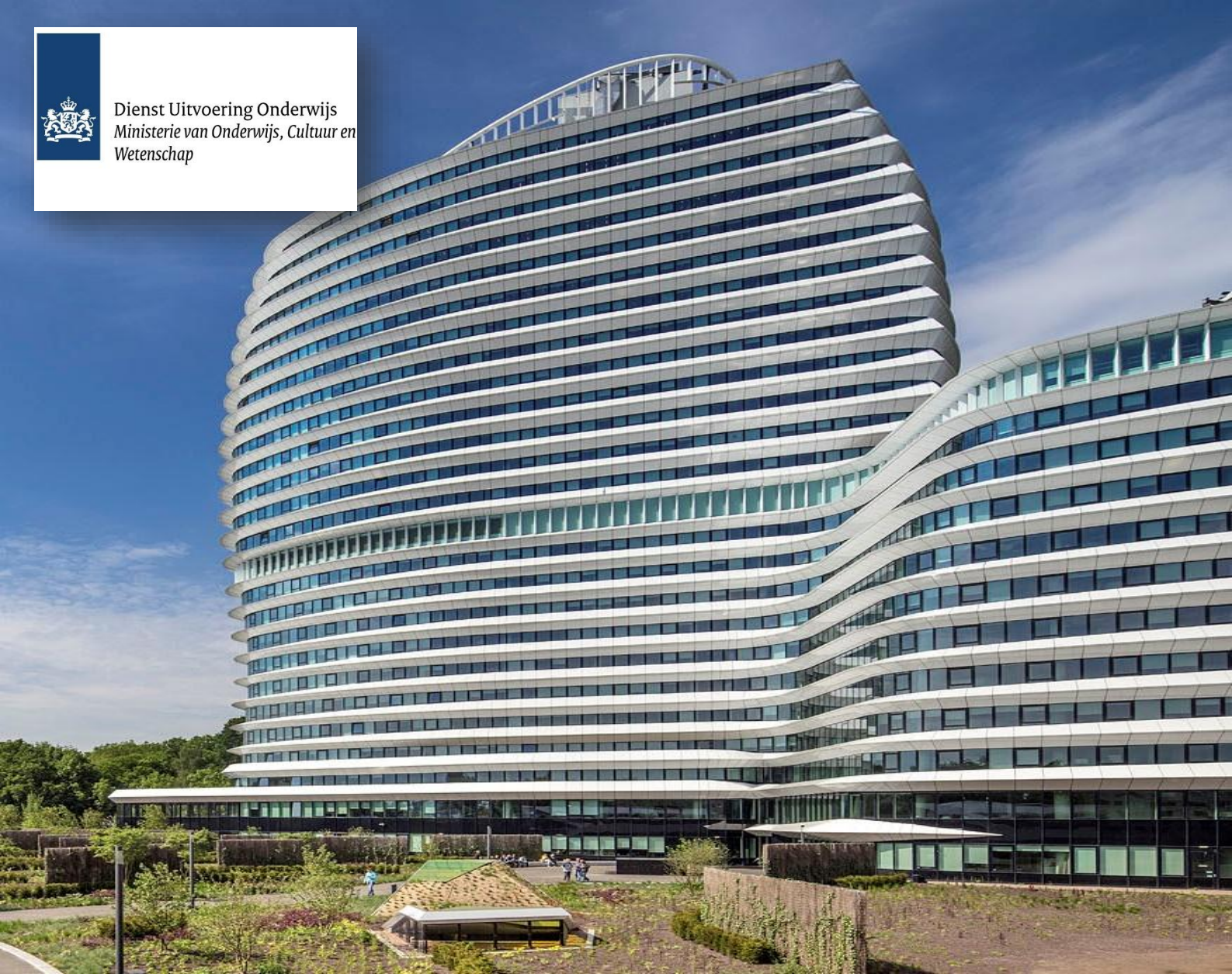
Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap



Marktconsultatie

Secrets Management, PAM en IGA oplossing

ten behoeve van de

Dienst Uitvoering Onderwijs

Uitgevoerd door het Inkoopuitvoeringscentrum Noord

Datum	22 april 2026
Kenmerk	Feedback DUO-MACO-IUCN25100271 Secrets Management, PAM en IGA oplossing
Versie	1.0
Status	Definitief

Inhoud

1 Algemeen

1.1 Inleiding

DUO heeft op 12 december 2025 via Tenderned aan marktpartijen gevraagd die haar informatie kunnen geven over hoe zij het beste invulling kan geven aan de behoefte van een Secrets Management, Privileged Access Management (PAM) en Identity Governance and Administration (IGA) oplossing.

Op de marktconsultatie zijn reacties ontvangen van:

- Cronos
- EY Advisieurs
- Xalient/Grabowsky
- IBM Nederland
- KPMG
- KPN
- Topicus Security
- UY Holding

1.2 Doel

DUO wil voorafgaand aan een formeel aanbestedingsproces vrijblijvend en openbaar informatie verkrijgen vanuit de markt.

Het doel van deze marktconsultatie is om specifiek inzicht te krijgen in de markt en de ontwikkelingen op de markt en de verwachtingen van marktpartijen voor de toekomst. Verder beoogt DUO met deze marktconsultatie een goed beeld te krijgen van de mate van interesse en de mogelijkheden en onmogelijkheden in de markt voor deze specifieke behoefte.

De marktconsultatie levert voordelen op voor alle betrokken partijen. Voor de betrokken marktpartijen is er het voordeel dat men vroegtijdig een beeld heeft van hetgeen DUO voornemens in de markt gaat zetten en dat men invloed kan uitoefenen op de manier waarop DUO de aanbesteding gaat vormgeven.

Deze marktconsultatie kent daarnaast de volgende subdoelen:

- nagaan of de requirements van DUO haalbaar zijn;
- nagaan wat de huidige en toekomstige ontwikkelingen/innovaties in de markt zijn;
- vroegtijdig betrekken en interesseren van marktpartijen in de aanbesteding;
- beproeven van eigen uitgangspunten en aannames;
- een beeld krijgen van visies, suggesties en ideeën van marktpartijen;
- bepalen welke aanbestedingsstrategie het beste past bij de gevraagde dienstverlening.

2 De marktconsultatie

2.1 Fase 1: Schriftelijke beantwoording

Op de marktconsultatie zijn schriftelijke reacties ontvangen van:

- Cronos
- EY Advisieurs
- Xalient/Grabowsky
- IBM Nederland
- KPMG
- KPN
- Topicus Security
- UY Holding

In bijlage A is een gecumuleerd overzicht van alle reacties per vraag opgenomen.

2.2 Fase 2: Mondelinge gespreksronde

Voor de mondelinge gespreksronde zijn de volgende partijen uitgenodigd:

- Cronos
- Xalient/Grabowsky
- IBM Nederland
- Topicus Security

In bijlage B zijn de gespreksverslagen opgenomen.

Op basis van de schriftelijke reacties zijn er 29 aanvullende vragen op het gebied van aanbesteding, project en techniek gesteld en deze zijn deels teruggekomen in de presentaties. Achteraf zijn de vragen schriftelijk beantwoord door Cronos, IBM Nederland en Xalient. In Bijlage C zijn deze opgenomen.

2.3 Conclusies

Vraagstelling 1 – Hoe ziet de aanbieder de preferente implementatievolgorde?

De markt vindt het combineren van SeM, PAM en IGA in één aanbesteding zeer ambitieus, met hoge complexiteit en veel afhankelijkheden. Er zijn twee erkende voorkeurscenario s: (1) eerst SeM en PAM realiseren voor snelle risicoreductie en daarna IGA vervangen, en (2) eerst een IGA-MVP neerzetten op basis van de HR-bron en daarna SeM en PAM inrichten, gevoed door de nieuwe IGA. Leveranciers benadrukken dat IGA-implementatie vooral een proces- en organisatietraject is, terwijl PAM en SeM vooral techniek-gedreven zijn. Een deel van de partijen adviseert om de aanbesteding zelf op te knippen (SeM los van PAM/IGA of drie afzonderlijke trajecten met één regierol) om de scope beheersbaar te houden en meer partijen te laten inschrijven. Aanbevelingen Kies expliciet één voorkeursvolgorde (scenario eerst SeM/PAM, dan IGA of scenario eerst IGA-MVP, dan SeM/PAM) en werk deze uit in een globale planning met mijlpalen als input voor het PvE; laat leveranciers afwijkingen op deze volgorde en planning onderbouwen. Overweeg om de aanbesteding op te splitsen in afzonderlijke percelen of trajecten voor IGA, PAM en SeM, met één regiepartij, om risico's te beperken en het aantal geschikte leveranciers te vergroten. Hanteer het principe think big, act small : ontwerp de totale IAM-doelarchitectuur, maar implementeer in kleine MVP-stappen per domein, met co-existentie en gefaseerde migratie. Benoem in het PvE expliciet de noodzaak van co-existentie tussen de huidige IGA-oplossing en de nieuwe omgeving, inclusief een migratiestrategie en eventuele bridge -constructies tussen oud en nieuw.

Vraagstelling 2 – Hoe schat de aanbieder de kosten in?

De afgegeven kosteninschattingen lopen sterk uiteen, van enkele tonnen voor een beperkte MVP tot totale TCO s van meerdere miljoenen euro s over een periode van vijf tot zes jaar. Leveranciers onderscheiden in hun inschattingen consequent drie hoofdblokken: licenties of abonnementen, implementatie en migratie, en doorlopende kosten voor support, beheer, hosting en doorontwikkeling. Een realistische TCO blijkt sterk afhankelijk van aantallen identiteiten, privileged users, secrets, integraties, OTAP-omgevingen en de gewenste SLA-niveaus. Aanbevelingen Vraag aanbieders om een gestandaardiseerd prijzenblad waarin de totale kosten worden opgesplitst in licentie/subscription, implementatie en migratie, en runkosten (support, beheer, hosting, doorontwikkeling), met duidelijke volumefactoren per domein SeM, PAM en IGA. Gebruik in de aanbesteding concrete scenario s en kengetallen (aantallen gebruikers, NHI s, applicaties, secrets, OTAP-omgevingen) zodat de aanbiedingen onderling goed vergelijkbaar zijn. Laat leveranciers de TCO per component (SeM, PAM, IGA) expliciet begroten, naast een integraal scenario, zodat DUO later in fasering of scope kan schuiven zonder de prijsopbouw kwijt te raken. Leg de nadruk in de beoordeling op realistische, onderbouwde kostenramingen en de transparantie van aannames, in plaats van uitsluitend op de laagste prijs.

Vraagstelling 3 – Hoe gaat de aanbieder om met het samenspel tussen leveranciers?

De meeste leveranciers vinden een multi-vendor aanpak goed uitvoerbaar, mits er één contractuele hoofdaannemer is die als centraal aanspreekpunt fungeert. De voornaamste risico s liggen bij onduidelijke verantwoordelijkheidsverdeling, vingerwijzen bij incidenten, overlappende diensten en uiteenlopende juridische voorwaarden en EULA s. Leveranciers zijn het erover eens dat governance (RACI, escalatiemodel, gezamenlijke backlog) minstens zo belangrijk is als de technische integratie tussen oplossingen. Aanbevelingen Leg in de aanbesteding vast dat DUO één hoofdaannemer

contracteert als single point of contact, met een duidelijk beschreven structuur voor onderaannemers en partners. Schrijf een gezamenlijke governance-inrichting voor met een RACI-matrix, een formeel escalatiemodel, een gezamenlijke backlog en afgestemde change- en releasetrajecten voor alle betrokken partijen. Maak EULA s en DPA s expliciet onderdeel van de aanbesteding en de contractvorming, inclusief de verhouding tot ARBIT, en vraag leveranciers hun juridische afwijkingen vooraf te benoemen. Definieer duidelijke overdrachtsmomenten (zoals oplevering van SeM/PAM-MVP, IGA-MVP, start en afronding van migraties) als contractuele ankers voor verantwoordelijkheden, acceptatie en facturatie.

Vraagstelling 4 –Consumptiemodel: On-premises, hybride, SaaS

Leveranciers zien een duidelijke beweging naar identity-fabric-achtige architecturen en hybride consumptiemodellen: SaaS waar het kan, on-premises of sovereign cloud waar het moet vanwege soevereiniteit, dataclassificatie of legacy. SaaS wordt gezien als aantrekkelijk door snellere innovatie, automatische updates en lagere beheerlast, maar kent risico s op het gebied van datalocatie, Cloud Act, pentest-beperkingen en afhankelijkheid van de vendor-roadmap. Diverse partijen adviseren DUO om primair voor on-premises of sovereign cloud te kiezen, met SaaS als optie onder strikte voorwaarden rond datalocatie, encryptie en compliance. Aanbevelingen Leg in de aanbesteding een duidelijke voorkeursrichting vast (bijvoorbeeld primair on-premises of sovereign cloud, SaaS onder voorwaarden), inclusief harde eisen voor datalocatie binnen de EU, encryptie en naleving van relevante wet- en regelgeving. Eis dat leveranciers een toekomstvast migratiepad ondersteunen tussen on-premises en SaaS zonder onnodige vendor lock-in, inclusief voorwaarden voor data-export, logtoegang en sleutelbeheer (zoals BYOK of vergelijkbare modellen). Vraag leveranciers om een onderbouwde risico-analyse voor zowel SaaS als on-premises (inclusief pentestmogelijkheden, DPIA-effecten en soevereiniteitsrisico s) en laat hen mitigerende maatregelen uitwerken. Vraag om een duidelijke toelichting op de aansluiting van de voorgestelde oplossing op het huidige en toekomstige Rijk-cloudbeleid en op NIS2/BIO-vereisten.

Vraagstelling 5 – Prijzenblad en prijzenmodellen

Leveranciers hanteren verschillende licentiemodellen (subscription en, waar beschikbaar, perpetual) en verschillende volumemaatstaven per domein (zoals actieve identiteiten, privileged users, secrets, connectors, API-calls). Er is brede steun voor het scheiden van softwarelicenties en hosting of managed services in het prijzenblad, zodat lock-in wordt beperkt en aanbiedingen beter vergelijkbaar worden. Jaarlijkse indexatie en renewal-structuren zijn gebruikelijk; prijzen kunnen doorgaans voor meerdere jaren worden vastgezet, met vooraf afgesproken indexatiemechanismen. Aanbevelingen Ontwerp een gestandaardiseerd prijzenblad waarin minimaal wordt uitgesplitst: licenties per domein en volumefactor, implementatie en migratie, beheer en support (bijvoorbeeld per support-tier), hosting/infra en optionele modules. Vraag, waar mogelijk, zowel subscription- als perpetual-varianten op, inclusief indexatiemechanismen en voorwaarden bij verlenging, zodat DUO CAPEX- en OPEX-scenario s kan vergelijken. Laat leveranciers hun standaard prijsmodellen en licentievoorwaarden meesturen, zodat DUO eigen rekenexercities kan uitvoeren en juridische implicaties kan beoordelen. Leg als uitgangspunt vast dat softwarelicenties bij voorkeur eigendom van DUO blijven en niet onnodig worden gebundeld met hosting- en beheercontracten.

Vraagstelling 6 – Procedure en gunning

Een meerderheid van de leveranciers adviseert een procedure met onderhandeling of een concurrentiegerichte dialoog, gezien de complexiteit van SeM, PAM en IGA en de lange looptijd. Enkele partijen wijzen erop dat een openbare procedure mogelijk is, maar dan alleen met zeer scherp geformuleerde eisen en voldoende ruimte voor vragenrondes en verduidelijkingen. De voorgestelde doorlooptijd wordt in grote lijnen haalbaar geacht, mits er ruimte is voor PoC, interne besluitvorming en eventuele DPIA s. Aanbevelingen Kies expliciet voor een procedure met dialoog of onderhandeling en onderbouw dit met de complexiteit van de opdracht, de behoefte aan verduidelijking en risicobeheersing, terwijl de niet-onderhandelbare kaders vooraf worden vastgelegd. Neem een PoC-fase op na voorlopige gunning, met een afgebakende scope en looptijd, met als doel om de aangeboden oplossing in de DUO-context te valideren, niet om opnieuw te selecteren. Definieer duidelijke gunningscriteria en weging, waarbij kwaliteit (architectuur, migratieaanpak, governance, partnership) zwaarder weegt dan prijs, naast beoordeling van TCO. Stem gestanddoeningstermijn, PoC-planning en eventueel benodigde DPIA-activiteiten op elkaar af, zodat inschrijvers hun aanbod realistisch geldig kunnen houden.

Vraagstelling 7 – Uitgesteld gebruik van een deeloplossing

Leveranciers zien in de regel geen probleem in uitgesteld gebruik of latere activatie van bepaalde deeloplossingen (zoals IGA of SeM), mits daarover duidelijke contractafspraken worden gemaakt. Er is brede steun voor het koppelen van betalingen aan concrete projectmijlpalen, in de vorm van milestone billing, in plaats van uitsluitend tijd- of kalendergebaseerde facturatie. Enkele aanbieders benoemen mogelijkheden voor opties of toekomstige afname van modules op vooraf vastgelegde voorwaarden. Aanbevelingen Leg contractueel vast dat licenties en bijbehorende kosten voor nog niet gebruikte deeloplossingen later geactiveerd kunnen worden, met vooraf afgesproken prijs- en indexatiecondities. Pas milestone billing toe als uitgangspunt, waarbij betalingen gekoppeld zijn aan oplevering en acceptatie van duidelijke deliverables, zoals MVP s en afgeronde migratiefasen. Vraag leveranciers om expliciete opties voor toekomstige afname van extra modules of uitbreidingen, inclusief prijsmechanismen en maximale indexatie.

Vraagstelling 8 – Mogelijkheden m.b.t. aansluiten specifieke platformen op SeM en PAM?

Meer algemeen Leveranciers gaan er in het algemeen van uit dat SeM en PAM redundant en hoogbeschikbaar worden ingericht over twee datacenters (twin of hot-standby), met duidelijke afspraken over failover, synchronisatie van configuratie en secrets, en testen van uitwijkscenario s. Bij een cold stand-by uitwijklocatie wordt doorgaans een soberder model gebruikt: de omgeving wordt in een minimale vorm beschikbaar gehouden en geactiveerd bij een daadwerkelijke calamiteit, wat een langere hersteltijd maar lagere kosten betekent. De markt benadrukt dat SeM en PAM zelf vaak geen directe internettoegang nodig hebben, maar dat een internetstoring wel impact heeft op federatie, externe IdP s en cloud-integraties; leveranciers zien offline-scenario s en lokale afhankelijkheden daarom als belangrijk ontwerppunt. Voor fallback en local admin accounts wordt een streng gereguleerd break-glass -model gezien als best practice: noodaccounts blijven bestaan, maar worden versleuteld opgeslagen, periodiek getest, strikt gelogd en alleen via formele procedures gebruikt, ook als een node in een cluster faalt. Aanbevelingen Meer algemeen Vraag leveranciers om een concreet HA/DR-ontwerp voor SeM en PAM over twin datacenters, inclusief gekozen architectuur (actief-actief of actief-passief), replicatiemechanismen voor configuratie en secrets en de beoogde RPO/RTO-waarden. Maak onderscheid in de eisen tussen hot-standby en cold stand-by uitwijklocaties

en laat leveranciers per scenario de implicaties voor kosten, beheer en hersteltijden expliciet maken. Neem in het PvE eisen op voor functioneren bij internetstoringen, bijvoorbeeld het kunnen blijven werken met interne identiteiten, caching-mechanismen en duidelijke fallback-paden wanneer externe IdP s of cloud-services tijdelijk niet bereikbaar zijn. Eis een uitgewerkt break-glass-proces voor fallback en local admin accounts, inclusief: wie mag ze gebruiken, hoe worden ze beheerd en versleuteld, hoe vaak worden ze getest, hoe wordt gebruik realtime gelogd en hoe wordt dit geborgd bij cluster-falen of verlies van een individuele node.

Meer AS-400 specifiek

Conclusies AS-400 Voor AS-400 bevestigen leveranciers dat aansluiting op SeM en PAM technisch mogelijk is, maar dat dit meestal vraagt om specifieke connectoren of maatwerkachtige integratiepatronen. De user experience verandert voor beheerders en gebruikers; waar nu met één actie meerdere sessies kunnen worden geopend, zal via een PAM-oplossing vaak per sessie een aparte start nodig zijn. De complexiteit bij AS-400 zit vooral in het combineren van sterke beveiliging (PAM-sessiebeheer, credentialinjectie) met behoud van werkbare performance en beheerbaarheid. Aanbevelingen AS-400 Vraag leveranciers om expliciet te beschrijven welke standaardconnectoren of integratiepatronen zij bieden voor AS-400 en welke beperkingen of extra componenten daarbij horen. Neem in het PvE op dat de impact op gebruikerservaring en beheerprocessen voor AS-400 duidelijk moet worden beschreven (bijvoorbeeld aantal stappen per sessie en benodigde tooling). Eis dat leveranciers een migratie- en testplan leveren voor de AS-400-integratie, inclusief prestatietests en fallbackscenario s, zodat risico s op verstoringen beperkt blijven.

Meer Linux-specifiek

Voor Linux-omgevingen wordt breed aangegeven dat integratie met SeM en PAM volwassen is, onder andere via SSH-keys, agents, jump-hosts en just-in-time provisioning van accounts en sleutels. Er zijn verschillende patronen mogelijk, zoals directe SSH-toegang via een PAM-jumpserver of JIT-accounts op Linux-servers die tijdelijk worden geprovisioneerd en daarna weer worden opgeruimd. Secrets voor Linux-gebaseerde workloads (zoals microservices en containers) kunnen via SeM-oplossingen worden beheerd, met minimale aanpassingen in applicatieconfiguratie. Aanbevelingen Linux Vraag leveranciers om hun standaard Linux-integratiepatronen te beschrijven (SSH-keys, JIT-accounts, jump-hosts, agents) en daarbij helder aan te geven welke variant zij voor DUO adviseren. Leg in het PvE vast dat Linux-integratie ook de container- en DevOps-use-cases moet afdekken (bijvoorbeeld OpenShift/Kubernetes), met duidelijke beschrijving van sidecars, operators of andere koppelcomponenten. Eis dat leveranciers inzicht geven in de beheerimpact op Linux-omgevingen (bijvoorbeeld sleutelrotatie, accountopruiming, logging) en hoe dit aansluit op de bestaande beheerprocessen.

Meer netwerk-specifiek

Conclusies Netwerk Voor netwerkcomponenten (firewalls, routers, switches, NAC, Cisco ISE enzovoort) geven leveranciers aan dat integratie mogelijk is, maar vaak afhankelijk van de beschikbare API s, CLI-toegang en ondersteuning voor centrale authenticatie. Netwerk-PAM richt zich vooral op het beheren van beheeraccounts en sessies naar netwerkapparatuur, vaak via jump-hosts of proxy s die CLI-sessies afschermen en eventueel opnemen. De complexiteit zit vooral in het grote aantal verschillende typen netwerkapparatuur en versies, en in de noodzaak om bestaande beheerprocedures (ad-hoc CLI, directe logins) te standaardiseren. Aanbevelingen Netwerk Vraag leveranciers om per type netwerkcomponent (firewalls, routers, switches, NAC/Cisco ISE)

standaardintegraties, ondersteunde protocollen en eventuele beperkingen te beschrijven. Neem als eis op dat beheer op netwerkapparatuur via PAM-sessies loopt (bijvoorbeeld via jump-hosts/proxy s), met logging en, waar nodig, sessie-opname voor kritieke systemen. Eis een inventarisatie- en harmonisatieplan voor netwerkbeheeraccounts en toegangspaden, inclusief stappen om huidige werkwijzen (directe CLI-toegang) gecontroleerd om te zetten naar de nieuwe SeM/PAM-oplossing.

Leveranciers bevestigen dat integratie met de genoemde platformen (zoals AS/400, Linux, netwerkapparatuur, Kubernetes/OpenShift, firewalls en NAC-oplossingen) mogelijk is, maar wijzen op de technische complexiteit en het belang van een goede discovery- en ontwerpperiode. Voor container- en cloudnative omgevingen worden moderne integratiepatronen gebruikt, zoals operators, sidecars en followers, in combinatie met open standaarden voor authenticatie en autorisatie. Certificaatbeheer wordt als nauw verwant domein gezien, maar wel met een eigen set aan requirements en prijsimplicaties, waardoor het mogelijk apart moet worden beschouwd. Aanbevelingen Vraag leveranciers om per belangrijk platform (AS/400, Linux, netwerk, Kubernetes/OpenShift, NAC, firewalls) hun standaard integratiepatronen, benodigde componenten en eventuele beperkingen te beschrijven. Maak in het PvE expliciet welke aspecten van certificaat- en PKI-beheer binnen scope van deze aanbesteding vallen en welke buiten scope worden geplaatst, om scope-uitbreiding en prijsverrassingen te voorkomen. Eis gebruik van open standaarden voor integratie (zoals OIDC, SAML, SCIM) en beperk maatwerk-agents tot situaties waarin geen standaardalternatief beschikbaar is.

Vraagstelling 9 – Hoe gaat de aanbieder om met Pas-toe-of-leg-uit standaarden?

Leveranciers geven aan in de basis goed te kunnen aansluiten op relevante (inter)nationale en Nederlandse standaarden, en zien deze doorgaans niet als belemmerend. Uitdagingen worden vooral verwacht bij specifieke legacy-koppelingen en sommige Nederlandse varianten, waar tijdelijk pragmatische oplossingen noodzakelijk kunnen zijn. Enkele partijen adviseren om open standaarden vooral functioneel te beschrijven (wat er moet worden ondersteund) en niet te veel op detailniveau van techniek en implementatie te voorschrijvend te zijn. Aanbevelingen Neem expliciet op welke Pas-toe-of-leg-uit-standaarden van toepassing zijn en beschrijf deze vooral functioneel (bijvoorbeeld gebruik van SAML2 en OIDC voor federatie, en SCIM voor provisioning). Laat leveranciers aangeven waar zij tijdelijk niet volledig kunnen voldoen, en vraag een voorstel voor mitigerende maatregelen en een migratiepad naar volledige standaardconformiteit. Neem ondersteuning van SCIM op als harde eis en koppel hieraan eisen rond compliance met BIO, AVG, NIS2 en relevante PKI-standaarden.

Vraagstelling 10 – Hoe gaat de aanbieder om met security ontwikkelingen?

Leveranciers zien Zero Trust, just-in-time en zero standing privileges, identity fabric, AI-ondersteunde detectie en voorbereidingen op post-quantumcryptografie als belangrijke ontwikkelingen in IAM.
Er is al sprake van implementatie of planning voor onder andere Shared Signals, SCIM, moderne encryptiestandaarden en een roadmap richting quantum-veilige algoritmen.
Aanbevelingen

Vraag leveranciers om concreet te beschrijven hoe hun oplossingen Zero Trust en just-in-time-principes over SeM, PAM en IGA ondersteunen, inclusief voorbeelduse-cases. Neem eisen en vragen op rond Shared Signals, SCIM en de roadmap voor quantum-veilige cryptografie, inclusief hoe en wanneer nieuwe algoritmen worden doorgevoerd.
Laat leveranciers toelichten hoe zij kwetsbaarheden managen (patchbeleid, meldingsprocedure, noodpatches) en hoe security-by-design en secure development zijn geborgd.

Vraagstelling 11 – Communicatie m.b.t. wijzigingen techniek en diensten

De markt benadrukt het belang van duidelijke SLA's per component, inclusief beschikbaarheid, responstijden, hersteltijden en eisen voor hoogbeschikbaarheid en disaster recovery.
Leveranciers vinden een integraal beheer- en governancemodel met vaste overlegstructuren, transparante rapportage en duidelijke rapportages over incidenten, wijzigingen en roadmaps cruciaal. Onvoldoende operationele kennis en onduidelijk eigenaarschap binnen de organisatie worden gezien als belangrijke risico's voor een stabiele beheerfase.
Aanbevelingen
Leg in het PvE concrete SLA-eisen per domein vast (SeM, PAM, IGA), inclusief eisen voor HA/DR, escalatiepaden, root cause analyses en toegang tot gespecialiseerde support bij kritieke incidenten.
Eis een integraal beheer- en supportmodel met heldere rolverdeling, periodieke rapportages en vaste overlegmomenten op operationeel, tactisch en strategisch niveau.
Vraag om een uitgewerkt opleidings- en kennisoverdrachtsplan met trainingspaden per rol, documentatie en runbooks, en een RACI-overzicht voor beheer en eigenaarschap.

Vragen gericht op de voorgenomen aanbesteding

De markt adviseert overwegend een procedure met dialoog of onderhandeling, met een sterke focus op kwaliteit, visie en lange-termijnsamenwerking in plaats van primair op prijs. Een gedetailleerde beschrijving van de huidige situatie (architectuur, identiteitsstromen, aantallen, applicatielandschap, cloudstrategie) wordt als randvoorwaardelijk gezien voor goede inschrijvingen. Het onderscheidend vermogen van leveranciers ligt vooral in integrale architectuur, Zero-Trust-benadering, soevereiniteit en de migratie- en implementatieaanpak, niet zozeer in losse productfeatures. Aanbevelingen Beschrijf in de aanbestedingsdocumenten zeer concreet de huidige IAM-architectuur, identiteits- en autorisatiestromen, aantallen gebruikers en NHI s, het applicatielandschap, cloudstrategie en een financieel kader. Formuleer gunningscriteria waarin integratiearchitectuur, migratie- en adoptieaanpak, governance en partnerschap en soevereiniteit zwaar meewegen naast TCO. Neem use-case-gebaseerde demonstraties en/of een PoC op in de beoordeling, gericht op integratie en Zero Trust, en ga niet alleen uit van papieren beschrijvingen.

Vragen gericht op de Functionaliteit

Leveranciers benadrukken het belang van maximale inzet van standaardfunctionaliteit en standaardkoppelingen en het zo veel mogelijk vermijden van maatwerk. De behoefte van DUO aan decentrale bevoegdheden en eigenaarschap, gecombineerd met centrale governance en compliance, wordt door de markt als logisch en haalbaar gezien. Aanbevelingen Leg vast dat standaardfunctionaliteit en standaardkoppelingen leidend zijn en dat maatwerk alleen in uitzonderingsgevallen wordt toegestaan met duidelijke businesscase en exitstrategie. Vraag

leveranciers expliciet hoe hun oplossing decentrale autorisatie en eigenaarschap combineert met centrale governance, rollenmodellen, scheiding van functies en periodieke certificering. Neem vereisten op voor rapportage, auditability en compliance (zoals BIO, AVG, NIS2) als integraal onderdeel van de functionaliteit.

Vragen gericht op Beheer en Onderhoud

De markt biedt verschillende beheer- en supportmodellen: co-sourcing met een gezamenlijk team, volledig managed services en meer traditionele 2e/3e-lijnsondersteuning. Belangrijke aandachtspunten zijn helder incident-, change- en releasemanagement, goede monitoring en realistische SLA s per component. Aanbevelingen Vraag leveranciers om meerdere beheer- en supportvarianten te beschrijven (co-sourcing en managed services), inclusief voor- en nadelen voor DUO. Neem eisen op voor integratie met het bestaande ITSM-proces (ticketing, prioritering, rapportages) en voor monitoring en updatebeleid. Laat leveranciers inzichtelijk maken welke interne capaciteit en rollen bij DUO nodig zijn voor stabiel beheer en onderhoud.

Vragen gericht op implementatie en migratie van de dienstverlening

Leveranciers benadrukken dat succes vooral afhangt van mensen, processen, datakwaliteit en governance; techniek is een randvoorwaarde maar niet doorslaggevend. Gefaseerde migratie via MVP s, co-existentie en stapsgewijze onboarding wordt breed geadviseerd boven een big-bang-benadering. Aanbevelingen Neem een verplichte discovery- en voorbereidingsfase op in de aanbesteding, inclusief datakwaliteitsanalyse, applicatie-inventarisatie en governance-inrichting. Eis een concrete migratiestrategie met fasering (MVP, co-existentie, migratie per subdomein), fallbackscenario s en duidelijke risicobeheersing. Vraag leveranciers om uitgewerkte opleidings-, adoptie- en veranderplannen met nadruk op betrokkenheid van business-eigenaren en key users.

3 Verdere verdieping

Na aanleiding van de mondelinge toelichting en presentaties van de marktconsultaties zijn onderstaande vervolgvragen gesteld

IGA specifiek:

1. Hoe ziet de communicatie tussen PAM (sec mon) en IGA er uit? Wat is de geadviseerde methode, gebaseerd op de door u aangeboden oplossingen.
2. DUO heeft het eigenaarschap van objecten zoals identiteiten, accounts en resources ingericht. Versneld dit de implementatie van IGA?
3. Als PAM eerst aangesloten wordt op de huidige IGA oplossing, welk soort communicatie tussen PAM en IGA wilt u voorstellen en waarom?
4. Indien u een API gebruiken wilt voor de communicatie, hoe lang zou het opzetten van die communicatie doorgaans duren en waaraan moet dat voldoen?
5. Welke attributen op een account zijn minimaal nodig om PAM succesvol in te richten?
6. Is de door u geboden oplossing in staat om AI agents te beheren en bewaken, zo nee welke tools zou DUO daarvoor moeten overwegen

PAM specifiek:

7. Wat is de impact op uw oplossing van het vereisen van een Radius rol voor de PAM-functionaliteit, zodat deze in een Cisco ISE opstelling valt te integreren (cascadering Radius)?

Deze zijn bij de geïnteresseerde partijen uitgezet en met Cronos besproken op 21-4-2024.

Bijlage A: Gecumuleerd overzicht van antwoorden op de marktconsultatie

Bijlage B: Verslag presentatie/toelichting

- Cronos
- Topicus
- IBM Nederland
- Xalient

4 Bijlage C: Aanvullende vragen

Beantwoording aanvullende vragen door Cronos, IBM en Xalient