Rijksinkoopsamenwerking
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Marktconsultatie ICT-oplossing
Identity and Access Management (IAM)
ten behoeve van
het ministerie van Binnenlandse Zaken, SSC-ICT

Contactpersoon	Jeroen Kuijsten
Datum	8-4-2026
Kenmerk	201865002.030.012
Versie	1.0
Status	Definitief

Inleiding
Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), SSC-ICT, heeft in samenwerking met de Rijksinkoopsamenwerking in de maanden februari en maart 2026 een Marktconsultatie uitgevoerd, ten behoeve van een ICT-oplossing voor Identity and Access Management (IAM).

Doel van de marktconsultatie
Het doel van deze Marktconsultatie was om te verkennen in hoeverre de gestelde ambities realiseerbaar zijn met beschikbare oplossingen in de markt. Daarnaast werden ook niet-functionele eisen zoals privacy, security, compliance, implementatie, beheer en toekomstvastheid onderzocht, omdat deze randvoorwaarden bepalend zijn voor een succesvolle implementatie en het goed functioneren van de toekomstige gedeelde identiteits- en toegangsbeheer oplossing.

Verloop van de Marktconsultatie
Voor de Marktconsultatie hebben 41 marktpartijen interesse getoond. Er was 1 vragenronde (NvI). In de Marktconsultatiedocument zijn vooraf 31 vragen gesteld. De Aanbestedende Dienst heeft van 25 marktpartijen op deze vragen naar tevredenheid schriftelijk antwoord gekregen. Aanbestedende Dienst heeft daarom besloten om geen aanvullende individuele online gesprekken met marktpartijen meer te houden.

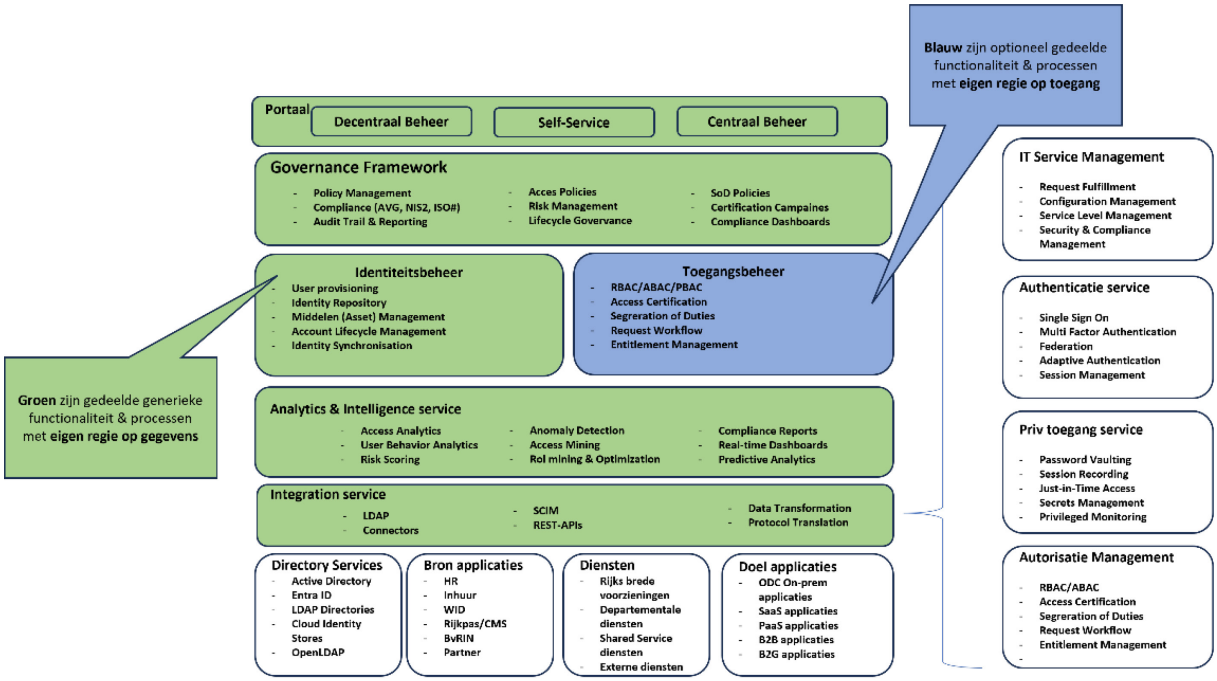
Vervolg marktconsultatie
Óf de Aanbestedende Dienst daadwerkelijk overgaat tot een (Europese) aanbesteding of een functionele uitvraag via de mantelpartijen binnen huidige Raamovereenkomsten uitzetten en zo ja, op welke manier of in welke vorm de Aanbestedende Dienst dit doet, is nu nog niet bekend. Zodra hier meer over bekend is zal de Aanbestedende Dienst dit aan Marktpartijen via de hiervoor bestaande informatiekanalen kenbaar maken. Zoals u weet kunt aan informatie uit deze Marktconsultatie geen rechten ontlenen. Ook kan de uiteindelijke een functionele uitvraag binnen huidige Raamovereenkomsten of een (Europese) Aanbesteding, als die plaatsvindt, afwijken van hetgeen tijdens de marktconsultatie wordt geschetst.

Neem gerust contact met ons op wanneer u vragen heeft over dit eindverslag van de Marktconsultatie. U kunt de betrokken inkoopadviseur (Jeroen Kuijsten) te bereiken via TenderNed.

Eindverslag marktconsultatie

Onderstaand treft u de geanonimiseerde set aan vragen en antwoorden aan van totaal 25 leveranciers, exclusief de commercieel vertrouwelijke informatie. De antwoorden zijn per vraag samengevat van alle partijen.

Algemene vragen



VRAAG 1.	Kunt u een algemeen beeld geven van de beschreven opzet en kansen/aandachtspunten?
Antwoord	De voorgestelde IAM-opzet wordt breed herkend als een moderne architectuur waarbij centrale identity lifecycle processen worden gecombineerd met decentrale regie op toegangsbeheer. Leveranciers zien dit als een bewezen multi-tenant model dat aansluit op rijksbrede samenwerking. Kansen liggen in standaardisatie, schaalbaarheid, kostenreductie en betere governance en compliance. Ook worden versnelling van onboarding, integraties en ondersteuning van Zero Trust genoemd. Aandachtspunten zijn governance, duidelijke rolverdeling en change management. Daarnaast zijn datakwaliteit, rolmodellering en harmonisatie cruciaal. Migratie en integratie vragen om een gefaseerde aanpak.

VRAAG 2.	Hoe ondersteunt uw ICT-oplossing de scheiding van gegevens en aangeboden functionaliteit tussen ministeries? En op welke wijze borgt u dat verschillende afnemers regie behouden op hun eigen data waarbij toegang van derden tot de data geminimaliseerd wordt?
Antwoord	Scheiding van gegevens en functionaliteit wordt gerealiseerd via multi-tenant architectuur met logisch gescheiden domeinen per ministerie. Dit wordt geborgd via tenant-isolatie, RBAC/ABAC, datasegmentatie en auditlogging. Ministeries behouden regie via gedelegeerd beheer. Centrale onderdelen richten zich op governance en standaarden. Toegang wordt beperkt via least privilege, encryptie en auditing.

VRAAG 3.	Hoe kijkt u aan tegen de gewenste oplossing waarbij het identiteitsbeheer voor iedereen van toepassing is en ministeries daarnaast desgewenst aanvullend het

	toegangsbeheer met eigen regie kunnen afnemen?
Antwoord	Leveranciers geven aan dat hun oplossing het mogelijk maakt om IDM centraal af te nemen en het AM deel optioneel per ministerie in te zetten met een eigen regie.

VRAAG 4.	Kan elk ministerie beschikken over een eigen logisch deel, tenant (eventueel met sub-tenants) of vergelijkbare structuur met eigen gegevens? In het geval dat één medewerker van ministerie A ook werkt voor ministerie B: wanneer ministerie B gebruik wil maken van de identiteitsgegevens (zoals de gegevens van de natuurlijke persoon en het unieke Rijks identificerend nummer) die initieel zijn geregistreerd in de tenant bij ministerie A, hoe zou dit in uw oplossing(en) werken?
Antwoord	Meerdere tenants zijn over het algemeen mogelijk en er zijn mogelijkheden om medewerkers ministerie/tenant overstijgend te kunnen laten werken

VRAAG 5.	Bij een eventuele verwerving van een oplossing geldt binnen de overheid de voorkeur voor open source oplossingen bij gelijke geschiktheid. Daarnaast komt er meer nadruk op soevereiniteit en autonomie, beperking van afhankelijkheid van niet Europese partijen en voorkomen van vendor lock-in. Kunt u aangeven hoe uw oplossing(en) hieraan tegemoetkomt/-komen?
Antwoord	Zowel Open Source als Closed Source aanbieders voorzien in de mogelijkheid onafhankelijk te zijn van niet-Europese aanbieders. Vendor lock-in wordt voorkomen door het gebruik van open standaarden.

VRAAG 6.	Uitganspunt is één nieuwe dienst op basis van één product'. Als deze beperking er niet is, zou u dan met een voorstel komen voor een andere oplossing die in uw ogen gelijkwaardig of beter scoort op samenhang, ondersteuning, toekomstvastheid?
Antwoord	Alle aanbieders geven aan dat de gevraagde functionaliteit uit één product geleverd kunnen worden.

Functionele vragen

De voorgestelde gedeelde identiteits- en toegangsbeheeroplossing heeft een aantal gewenste capabilities (zie bovenstaande figuur). In principe alleen configureerbare (no-code) capabilities is hierbij het uitgangspunt. Hierover hebben we de volgende vragen.

VRAAG 7.	Kunt u aangeven of de genoemde capabilities (Portaal, Governance framework, Identiteitsbeheer, Toegangsbeheer, Analytics & Intelligence service en Integration service) beschikbaar zijn binnen de door u aangeboden oplossing(en)?
Antwoord	Alle gevraagde capabilities zijn standaard beschikbaar binnen moderne IAM-oplossingen, geïntegreerd of modulair. Vaak no-code configureerbaar. Geïntegreerde oplossingen bieden een uniform datamodel. Aandachtspunten zijn afhankelijkheden en vendor lock-in.

VRAAG 8.	Kunt u voor elke beschikbare capability kort beschrijven en aangeven hoe deze beschikbaar wordt gesteld? a) Portaal b) Governance framework c) Identiteitsbeheer d) Toegangsbeheer e) Analytics & Intelligence service

	f) Integration service
Antwoord	Capabilities worden geleverd via een geïntegreerd platform: portaal (selfservice), governance (beleid/SoD), identiteitsbeheer (lifecycle), toegangsbeheer (RBAC/ABAC), analytics (monitoring) en integraties (API's). Functionaliteiten zijn role-based en tenant-specifiek.

VRAAG 9.	Kunt u aangeven hoe uw oplossing(en) in-, door- en uitstroomprocessen voor entiteiten ondersteunt met Identiteits- en Toegangsbeheer processen? En kunnen deze Identiteits- en Toegangsbeheer processen per tenant gedefinieerd worden?
Antwoord	Lifecycle-processen (JML) worden ondersteund via workflows en regels vanuit bronsystemen zoals HR. Automatische provisioning en deprovisioning zijn standaard. Ook tijdelijke situaties worden ondersteund. Logging en audit trails zijn essentieel. Deze kunnen per tenant gedefinieerd worden.

Scenario

In het vervolg van dit hoofdstuk wordt een aantal vragen gesteld over het volgende scenario.

- Een gedeelde voorziening identiteits- en toegangsbeheer volgens beschreven capabilities.
- TAP en opleidingsomgeving waarvan P redundant is uitgevoerd
- Respectievelijk 5.000, 6.000, 10.000, 17.000 en 20.000 te beheren (menselijke) identiteiten.
- Vijf deelnemende departementen, dus vijf transformaties vanuit vijf bestaande IdM-systemen naar één gedeelde oplossing met vijf logische tenants voor identiteitsbeheer met de volgende naar RESTfull-API te rationaliserende koppelvlakken:
    - WIDSCAN (nu inkomend XML-berichtenverkeer)
    - BVRIN (nu uitgaand XML berichtenverkeer)
    - P-Direkt (nu inkomende en uitgaande bestanden in XML- berichtenverkeer)
    - GCMS (nu inkomend en uitgaand XML berichtenverkeer)
    - Facilitor t.b.v. facilitaire zaken (nu uitgaand XML berichtenverkeer)
    - TOPdesk SSC-ICT (nu voornamelijk SQL-koppeling)
    - Follow-Me-Printen (nu voornamelijk SQL-koppeling)
    - Rijksdirectory (nu uitgaand LDIF-bestand)
    - Digitale Werkomgeving Active Directory (inkomende en uitgaande LDAP-koppelingen)
- Initieel onboarding van één ministerie met 10.000 identiteiten op de toegangsbeheeroplossing op basis van een combinatie van RBAC/ABAC gebaseerde autorisaties.

Hosting vragen

Uitgangspunt is dat de gedeelde identiteits- en toegangsbeheeroplossing gehost gaat worden in een overheidsdatacenter (ODC). Hierover hebben we de volgende vragen.

VRAAG 10.	Kunt u aangeven of de door u aangeboden oplossing volledig realiseerbaar is in ons eigen datacenter? Is dit onder andere mogelijk op basis van containerization?
Antwoord	Containerization wordt breed ondersteund (Docker/Kubernetes) en maakt schaalbare deployment mogelijk. On-premise biedt maximale controle. SaaS is minder geschikt voor lokale hosting. Aandachtspunten zijn beheer en infrastructuurkosten.

VRAAG 11.	Kunt u aangeven of (delen van) de aangeboden oplossing een backend applicatie connectie nodig heeft naar een cloud backend en/of een andere voorziening op internet?
Antwoord	Uit de leveranciersreacties blijkt dat de meeste IAM-oplossingen volledig on-premise kunnen functioneren zonder verplichte backendconnectie naar cloud-

	of internetvoorzieningen. De kernfunctionaliteiten zoals identity governance, provisioning en logging draaien autonoom binnen het overheidsdatacenter. Externe connectiviteit is in de meeste gevallen optioneel en alleen nodig bij specifieke scenario's zoals koppelingen met SaaS-applicaties, federatieve authenticatie of aanvullende diensten. Sommige oplossingen vereisen beperkte uitgaande verbindingen voor updates, licentievalidatie of optionele functionaliteiten zoals threat intelligence. Cloud-native oplossingen vormen hierop een uitzondering en vereisen structureel internetconnectiviteit. Over het algemeen geldt dat organisaties volledige regie houden over eventuele externe verbindingen. Beveiligingsmaatregelen zoals whitelisting en proxy's worden aanbevolen. Het ontbreken van verplichte externe afhankelijkheden wordt gezien als positief voor soevereiniteit en compliance.

VRAAG 12.	Kunt u een inschatting geven van de benodigde infrastructuur voor bovenstaande scenario?
Antwoord	De benodigde infrastructuur is afhankelijk van de gekozen architectuur (on-premise, containerized of SaaS), maar leveranciers schetsen een consistent beeld van een schaalbare, hoog beschikbare omgeving. Voor on-premise implementaties wordt doorgaans gewerkt met meerdere applicatieservers, databaseclusters en connectorservers. Containerplatformen zoals Kubernetes worden vaak genoemd als basis voor schaalbaarheid en beheer. Productieomgevingen worden redundant ingericht (HA), aangevuld met test-, acceptatie- en opleidingsomgevingen. Capaciteit varieert, maar omvat doorgaans meerdere VM's of nodes met voldoende CPU, RAM en snelle opslag (SSD/NVMe). Database- en auditopslag vormen een belangrijk deel van de footprint. Integraties en piekbelasting (bijv. migraties) vragen om extra capaciteit. Definitieve sizing wordt meestal bepaald in een latere ontwerpfase.

Koppelvlak vragen

SSC-ICT en haar afnemers wensen te standaardiseren volgens Forum Standaardisatie op ingezette koppelvlakmethoden en -technieken, en eventueel gebruik of hergebruik te maken van door u ter beschikking te stellen applicatiespecifieke koppelvlakken in een volledig toegankelijke software *library*. Hierbij is het uitgangspunt om in principe alleen configureerbare (no-code) koppelvlakken voor het beheerteam te hanteren. Hierover hebben we de volgende vragen.

VRAAG 13.	Kunt u aangeven of de capability Integration service standaard out-of-the-box gebruikmaakt van de volgende standaarden: RESTfull-API, SCIM 2.0 en LDAP?
Antwoord	Leveranciers geven vrijwel unaniem aan dat moderne IAM-oplossingen standaard ondersteuning bieden voor RESTful API's, SCIM 2.0 en LDAP. Deze standaarden vormen de basis voor integraties met zowel bron- als doelsystemen en sluiten aan bij gangbare overheidsstandaarden. REST en SCIM worden voornamelijk gebruikt voor lifecycle-processen en provisioning, terwijl LDAP wordt ingezet voor directory-integraties. De ondersteuning is doorgaans out-of-the-box beschikbaar via connectorframeworks en vereist geen maatwerkontwikkeling. Integraties kunnen veelal no-code of low-code worden ingericht. Voor legacy-systemen kunnen aanvullende methoden nodig zijn. De brede ondersteuning draagt bij aan interoperabiliteit en toekomstvastheid.

VRAAG 14.	Kunt u aangeven op welke wijze specifieke koppelvlakken per tenant of subtenant ingezet kunnen worden?
Antwoord	Koppelvlakken kunnen volgens leveranciers flexibel per tenant of subtenant worden ingericht via configureerbare connectoren en API-gateways.

	Elke tenant kan eigen endpoints, credentials en mappings beheren binnen een logisch gescheiden omgeving. Dit maakt het mogelijk om maatwerk per ministerie toe te passen zonder impact op andere tenants. Integraties worden vaak gemodelleerd als afzonderlijke applicaties of connectorconfiguraties. Centrale koppelingen kunnen gedeeld worden met tenant-specifieke filters. Authenticatie en autorisatie worden per tenant ingericht. De configuratie is doorgaans no-code en beheerbaar via een portaal. Aandachtspunten zijn governance, consistentie en beheercomplexiteit.

VRAAG 15.	Kunt u aangeven of de capability Integration service standaard beschikt over een software library met meerdere applicatiespecifieke koppelvlakken, zodat het beheerteam zelfstandig zonder softwarecode (no-code) koppelvlakken kan realiseren?
Antwoord	De meeste leveranciers bieden out of the box connectoren aan die hooguit geconfigureerd hoeven te worden. Daarnaast worden intuïtieve interfaces geboden waarmee low-code connectoren kunnen worden gebouwd of geconfigureerd.

Realisatie en transformatie

Momenteel hebben de zeven deelnemende departementen ieder hun eigen departementale identiteitsbeheer voorziening met (beperkte) toegangsbeheer-functionaliteit. Het streven is op termijn volledige rationalisatie en inzet van de beschreven shared identiteits- en toegangsbeheer oplossing. Hierover hebben we de volgende vragen:

VRAAG 16.	Hoe zou uw transformatiestrategie eruitzien om meerdere bestaande IdM-systemen op termijn uit te faseren en over te gaan naar een door u aangeboden oplossing?
Antwoord	Leveranciers geven vrijwel unaniem aan te kiezen voor een gefaseerde transformatie met oog voor datakwaliteit, risicobeheersing en continuïteit.

VRAAG 17.	Hoe zou continuïteit bij organisaties en eindgebruikers gewaarborgd kunnen worden?
Antwoord	Leveranciers geven aan dat continuïteit gewaarborgd wordt door een gefaseerde migratie met fall back scenario's, strakke regie en schaduw draaien.

VRAAG 18.	Hoe zou de datamigratie tussen IST en SOLL eruitzien?
Antwoord	Leveranciers geven aan een gefaseerde aanpak te prefereren waarbij eerst de Ist situatie in kaart wordt gebracht waar vanuit de mapping naar de Soll wordt gemaakt. Koppelingen worden gedefinieerd. Er wordt een gefaseerde aanpak met roll-back scenario's voorgesteld en functionaliteiten worden in fases geactiveerd.

VRAAG 19.	Hoe zou uw gewenste realisatie- en transformatieteam eruitzien? En hoe zijn de belangrijkste verantwoordelijkheden binnen dat team verdeeld?
Antwoord	Uit de ontvangen antwoorden blijkt dat leveranciers kiezen voor de inzet van een multidisciplinair team samengesteld rondom IAM kennis en expertise. Deze teams combineren verschillende rollen om zowel de implementatie als de organisatorische verandering te ondersteunen.

VRAAG 20.	Welke licentiemodellen voor entiteiten (zoals natuurlijke personen, niet-natuurlijke personen en middelen) zijn beschikbaar op basis van uw

	oplossing(en)?
Antwoord	De gehanteerde licentiemodellen variëren van enterprise subscription tot licenties per type gebruiker, connector of resource.

VRAAG 21.	Hoe zou het licentiemodel voor uw beschikbare oplossing eruitzien voor de gewenste gedeelde identiteits- en toegangsbeheeroplossing?
Antwoord	Leveranciers geven aan dat het licentiemodel in de meeste gevallen gebaseerd is op het aantal identiteiten binnen de oplossing, vaak in combinatie met het aantal koppelingen of modules. Veel modellen zijn subscription-gebaseerd en schaalbaar, waarbij kosten meegroeien met het aantal actieve gebruikers. Er wordt vaak gewerkt met enterprise-licenties of rijksbrede bundels om dubbele kosten te voorkomen. In multi-tenant omgevingen wordt doorgaans één identiteit slechts één keer gelicenseerd. Sommige leveranciers hanteren aanvullende kosten voor specifieke connectoren of modules. Open-source varianten kennen vaak geen licentiekosten maar wel supportcontracten. Er is vaak flexibiliteit in looptijd en schaalbaarheid. Aandachtspunten zijn transparantie, voorspelbaarheid en voorkomen van verborgen kosten.

VRAAG 22.	Potentieel gaan we aangeboden oplossing in verband met beveiligingsniveaus meervoudig op verschillende klantdomeinen implementeren. Zijn hiervoor separate licenties nodig?
Antwoord	De meeste leveranciers geven aan dat geen separate licenties nodig zijn bij implementatie over meerdere klantdomeinen of beveiligingsniveaus. Licenties zijn doorgaans gebaseerd op het totaal aantal identiteiten en niet op het aantal omgevingen of tenants. Dit voorkomt dubbele kosten bij multi-tenant gebruik. Uitzonderingen bestaan wanneer sprake is van volledig gescheiden fysieke omgevingen of extra identiteiten. In sommige gevallen kan architectuurkeuze invloed hebben op kosten. Over het algemeen blijft het uitgangspunt dat één identiteit één keer wordt gelicenseerd. Dit ondersteunt schaalbaarheid en flexibiliteit. Governance en architectuurkeuzes blijven wel bepalend.

VRAAG 23.	Zijn naast de standaard koppelvlakken op basis van RESTfull-API, SCIM 2.0 en LDAP, alle applicatiespecifieke beschikbare koppelvlakken in uw library in de licentie inbegrepen?
Antwoord	Leveranciers geven aan dat standaard koppelvlakken (REST, SCIM, LDAP) vrijwel altijd inbegrepen zijn in de basislicentie. Voor applicatiespecifieke connectoren geldt dat deze meestal grotendeels inbegrepen zijn, maar dat uitzonderingen bestaan. Sommige 'premium' of diepgaande integraties (bijv. SAP, Oracle) kunnen additionele kosten met zich meebrengen. Open-source oplossingen bieden vaak volledige toegang tot connectorlibraries. Maatwerkconnectoren vallen doorgaans buiten de standaardlicentie. Aandachtspunt is het voorkomen van verborgen kosten bij uitbreiding. Transparantie over connectorlicenties is essentieel.

VRAAG 24.	Op welk moment gaan de eventuele vaste en variabele licentiekosten gelden? a) Is dit op het moment van aanschaf of het moment van in productie name? b) Hoe zou dit gaan als de transformatie van IST naar SOLL 2 jaar duurt? c) Of nog langer als departementen pas (veel) later aansluiten? d) Of als er departementen bijkomen in het verzorgingsgebied?

Antwoord	Leveranciers hanteren verschillende modellen voor het moment waarop licentiekosten ingaan. Vaak starten vaste kosten bij contractondertekening of aanschaf, terwijl variabele kosten gekoppeld zijn aan productiegebruik. In gefaseerde migraties groeien kosten mee met het aantal actieve identiteiten. Ramp-up modellen worden vaak toegepast om dubbele kosten te voorkomen tijdens transitie. Bij latere aansluiting van departementen worden kosten pas actief bij onboarding. Uitbreidingen worden doorgaans verwerkt via schaal- of true-up mechanismen. Flexibiliteit en voorspelbaarheid zijn belangrijke aandachtspunten.

Financiele vragen, bemensing en planning

VRAAG 25.	Wat zouden de geschatte structurele en incidentele kostenposten en de TCO voor 8 jaar zijn voor het beschreven scenario? In de uitwerking graag minimaal de volgende onderverdeling: • (Licentie)kosten identiteits- en toegangsbeheer software, vast en variabel; • (Licentie)kosten voor koppelvlakken; • Onderhoudskosten en supportkosten; • Eenmalige realisatie- en transformatiekosten.
Antwoord	Leveranciers geven aan dat de Total Cost of Ownership bestaat uit licentiekosten, beheer- en supportkosten en eenmalige implementatiekosten. Voor Open Source geldt kosten voor subscription en een onderhoudscontract. Licentiekosten vormen een structurele component en zijn vaak gebaseerd op aantal identiteiten. Beheer- en supportkosten betreffen operationele kosten na livegang. Implementatiekosten omvatten analyse, ontwerp, migratie en training. De totale kosten worden sterk beïnvloed door scope, aantal systemen en mate van standaardisatie. Sommige leveranciers geven indicatieve bedragen, maar benadrukken dat definitieve kosten afhankelijk zijn van aanbesteding en detailuitwerking. Gefaseerde implementatie kan kosten spreiden. Transparantie in TCO-opbouw is essentieel.

VRAAG 26.	Uitgaande van het beschreven scenario, wat is het verwachte aantal FTE voor het centrale technisch, applicatief en functioneel beheer?
Antwoord	Op basis van de verzamelde input varieert het benodigde aantal FTE sterk afhankelijk van standaardisatiegraad, automatisering, aantal koppelingen en governance-eisen. Voor een sterk gestandaardiseerde en geautomatiseerde omgeving ligt de centrale beheerinspanning doorgaans tussen circa 3 en 8 FTE. In scenario's met meer maatwerk, hogere complexiteit en uitgebreide compliance-eisen loopt dit op naar circa 8 tot 17 FTE. In meer uitgebreide 'full-control' modellen met veel integraties en governance-activiteiten kan dit oplopen tot circa 15 tot 35 FTE centraal. De verdeling bestaat doorgaans uit technisch beheer (circa 1–5 FTE), applicatief beheer (circa 2–8 FTE) en functioneel beheer/governance (circa 2–11 FTE). Daarnaast is er vaak aanvullende decentrale capaciteit per ministerie nodig (circa 0,5–3 FTE-equivalent per organisatie). Tijdens de transitieperiode is extra tijdelijke capaciteit nodig (circa 10–25 FTE) voor migratie, testen en adoptie. De belangrijkste beïnvloedende factoren zijn het aantal applicatiekoppelingen, datakwaliteit, mate van procesharmonisatie en gekozen sourcingmodel (intern vs. leverancier). Een centrale, multi-tenant architectuur met hoge automatisering leidt structureel tot lagere beheerlast en schaalvoordelen. Een duidelijke afbakening van rollen tussen SSC-ICT, departementen en leveranciers is essentieel voor een realistische FTE-inschatting. Samengevat: een bandbreedtebenadering is noodzakelijk, waarbij circa 5–10 FTE realistisch is voor een efficiënt ingericht basis scenario.

VRAAG 27.	Zou u voor het beschreven scenario een planning op hoofdlijnen kunnen uitwerken?
Antwoord	De verwachte doorlooptijd varieert afhankelijk van complexiteit, migratiestrategie en besluitvorming, maar ligt in de praktijk meestal tussen de 12 en 60 maanden. Een minimale doorlooptijd van circa 12–24 maanden is haalbaar bij beperkte complexiteit en sterke standaardisatie, maar wordt vaak als ambitieus beschouwd voor rijksbrede trajecten. Een meer realistische planning voor grootschalige consolidaties ligt tussen de 24 en 48 maanden, terwijl complexe scenario's kunnen oplopen tot circa 60 maanden. De aanpak bestaat doorgaans uit meerdere fasen: initiatie en analyse, ontwerp en harmonisatie, technische inrichting, pilot en eerste implementaties, gefaseerde uitrol per ministerie en uiteindelijk decommissioning van legacy-systemen. Gefaseerde migratie met parallelle werking is essentieel om continuïteit te borgen. Versnelling is mogelijk door parallelle implementaties ('waves'), maar verhoogt risico's en vraagt extra capaciteit. Kritische succesfactoren zijn datakwaliteit, standaardisatie van processen, beschikbaarheid van stakeholders en duidelijke governance. Ook het applicatielandschap en bestaande maatwerkoplossingen hebben grote invloed op de doorlooptijd. Een realistische planning houdt rekening met nazorg, optimalisatie en doorontwikkeling na livegang. Samengevat: een gefaseerde aanpak met een totale doorlooptijd van circa 2 tot 4 jaar is voor dit type traject het meest realistisch.

Overige vragen

VRAAG 28.	Welke vragen zijn, of informatie is, volgens u essentieel of van (groot) belang en is niet opgenomen in deze vragenlijst? Kunt u deze benoemen?
Antwoord	Leveranciers geven aan dat risico's en afhankelijkheden in kostenmodel een belangrijk onderdeel vormt van het totale kostenmodel. Kostenstructuren zijn vaak flexibel ingericht om mee te bewegen met groei en gebruik. Er wordt gebruikgemaakt van mechanismen zoals schaalmodellen, staffels en contractuele afspraken. Belangrijk is dat kosten voorspelbaar en transparant blijven gedurende de looptijd. Aandachtspunten zijn afhankelijkheid van volumes, gekozen architectuur en aanvullende modules. Daarnaast spelen indexatie en marktontwikkelingen een rol. Een duidelijke contractstructuur helpt om financiële risico's te beheersen. Optimalisatie is mogelijk door standaardisatie en centrale governance.

VRAAG 29.	Wat is in uw beleving de grootste uitdaging in een soortgelijk traject?
Antwoord	Als grootste uitdagingen worden de synergie in de processen benoemd, samen met de scope bewaking. Ook overtuigen en betrokkenheid van de ministeries en voldoende draagvlak wordt als een uitdaging gezien. Ook de kwaliteit van de legacy behoort tot de grotere uitdagingen. Standaardisatie van rolmodellen, identiteiten en data over ministeries heen is een uitdaging.

VRAAG 30.	Bent u bereid met Aanbestedende Dienst (optioneel) individueel een

	onlinegesprek te voeren naar aanleiding van uw gegeven antwoorden?
Antwoord	Ja, de meeste leveranciers waren bereid om een individueel online gesprek te voeren. De gegeveven schriftelijke informatie van de marktpartijen was echter voor de Aanbestedende Dienst voldoende om geen aanvullende online individuele gesprekken te houden.

VRAAG 31.	Wat vindt u van deze Marktconsultatie? Wat kunnen wij in het vervolg beter doen?
Antwoord	De marktconsultatie wordt over het algemeen als duidelijk en gestructureerd ervaren, met een goede basis om inhoudelijk te reageren op de beoogde IAM-oplossing. Het gebruik van een concreet scenario wordt positief beoordeeld, omdat dit leveranciers in staat stelt om realistische en toepasbare antwoorden te geven. Tegelijkertijd wordt aangegeven, dat aanvullende context en verdieping bij specifieke vragen nog meer kan bijdragen aan nog gerichtere en beter vergelijkbare antwoorden. Met name bij technische en architectuurvragen kan extra toelichting helpen om interpretatieverschillen te beperken. Daarnaast wordt geadviseerd om in een vervolgtraject meer aandacht te besteden aan risico's, afhankelijkheden en randvoorwaarden, zoals datakwaliteit, governance en organisatiegereedheid. Ook wordt het belang benadrukt van duidelijke kaders rondom standaardisatie, interoperabiliteit en vendor lock-in. Verder wordt aanbevolen om in de aanbestedingsfase concrete eisen op te nemen ten aanzien van migratiestrategie, beheerorganisatie en kostenstructuur. Tot slot wordt aangegeven dat de consultatie een waardevolle stap is richting een toekomstbestendige IAM-oplossing, mits de opgehaalde inzichten worden vertaald naar heldere en toetsbare eisen in het vervolgproces.