

3e Nota van Inlichtingen

Behorende bij de Europese openbare aanbesteding 'Leveren, implementeren en onderhouden van een Identity and Access Management-systeem'

Gemeente Zaanstad

Kenmerk: 2026-198

CPV-code: 48000000-8 Software en informatiesystemen

Datum: 9-10-2026

Deze Nota van Inlichtingen maakt integraal onderdeel uit van de aanbestedingsstukken en prevaleert daarboven. De vragen zijn geanonimiseerd weergegeven en waar nodig geclusterd; bij gelijksoortige vragen wordt verwezen naar het antwoord waarin het onderwerp volledig is behandeld.

Gewijzigde en nieuwe aanbestedingsstukken

Naar aanleiding van deze Nota van Inlichtingen worden de volgende documenten in gewijzigde vorm gepubliceerd:

- Offerteleidraad IAM-systeem – aangepast nav 3e NvI: In de Offerteleidraad IAM-systeem – aangepast nav rectificatie is geconstateerd dat het beoordelingskader in paragraaf 5.3.1, G2.1 Wensen, beschrijvingen bevat die niet in eerdere versies van de offerteleidraad voorkwamen. Tevens was de benaming van W3 (Aanvragen, goedkeuren, toekennen en intrekken van Procesrollen en Autorisaties, en beheer van mandaten) niet consistent geschreven. Beide punten zijn hersteld in de Offerteleidraad IAM-systeem – aangepast nav 3e NvI. Verder is de beoordelingswijze voor G2.2 Plan van Aanpak verduidelijkt.
- Bijlage 5. IAM-systeem Zaanstad - Programma van Eisen en Wensen (On-Premise) - aangepast nav 3e NvI: Bijlage 5. IAM-systeem Zaanstad - Programma van Eisen en Wensen (On-Premise) - aangepast nav 3e NvI is naar aanleiding van de derde Nota van Inlichtingen aangepast. Hierin zijn enkele beschrijvingen gecorrigeerd en zijn verwijzingen naar eisen die niet correct waren, aangepast.
- Bijlage 12. IAM-systeem Zaanstad - Demonstratiescript - aangepast nav 3e NvI: In bijlage 12. IAM-systeem Zaanstad - Demonstratiescript - aangepast nav 3e NvI is op pagina 4 de vermelding van 100 minuten gewijzigd in 120 minuten. Deze tijdsduur is hiermee consistent met de overige plaatsen in de bijlage en de overige documenten van de aanbesteding waar deze termijn is vermeld.

Nr.	Onderwerp	Vraag	Antwoord
220	Programma van Eisen - W6D Beschikbaarheid On-premise-oplossing bij uitval Microsoft Entra ID	Voldoet een Inschrijver aan de uitvraag indien, naast de gevraagde break-glass-functionaliteit, geen aanvullende lokale fallback-authenticatie wordt toegepast bij tijdelijke onbeschikbaarheid van Microsoft Entra ID?	Deze wens betreft het waarborgen van de beschikbaarheid van de On-premise Oplossing bij (tijdelijke) onbeschikbaarheid van Microsoft Entra ID. Dit is een wens, geen eis. Uw voorstel voldoet eraan indien u het minimaal adresseert. De uitwerking van deze wens wordt beoordeeld aan de hand van het beoordelingskader in paragraaf 5.3.1 G2.1 Wensen. De mate van invulling bepaalt uw score op deze wens.
221	Programma van Eisen - W5 Bundeltickets TOPdesk	Voldoet een Inschrijver aan wens W5 indien gebruik wordt gemaakt van de standaard presentatie van bundeltickets vanuit de aangeboden oplossing, mits zowel de aangevraagde wijziging als de resulterende autorisatiesituatie voor de beoordelaar duidelijk inzichtelijk zijn?	Deze wens heeft betrekking op het bundelticketmechanisme voor ticket-based doelsystemen, waarbij geautomatiseerde provisioning (ticket-based) centraal de inzichtelijkheid van wijzigingen en autorisaties waarborgt. Dit is een wens, geen eis. Uw voorstel voldoet eraan indien u het minimaal adresseert. De uitwerking van deze wens wordt beoordeeld aan de hand van het beoordelingskader in paragraaf 5.3.1 G2.1 Wensen. De mate van invulling bepaalt uw score op deze wens.
222	Programma van Eisen - E55 Documentatie en ondersteuning	Voldoet een Inschrijver aan eis E55 indien klantspecifieke gebruikers- en beheerdocumentatie in het Nederlands wordt geleverd, terwijl de standaard technische productdocumentatie en gespecialiseerde technische ondersteuning voor de aangewezen technisch beheerders van Opdrachtgever in het Engels beschikbaar zijn?	E55 is bij de rectificatie reeds versoepeld. Voor specialistische ondersteuning in de 3e lijn en ondersteuning door onderliggende partijen mag Engels worden gebruikt, mits de communicatie voor de aangewezen medewerkers van Opdrachtgever goed begrijpelijk is. Klantspecifieke gebruikers- en beheerdocumentatie dient in het Nederlands beschikbaar te zijn. Voor standaard technische productdocumentatie die uitsluitend is gericht op specialistische technische beheerders, kan Engels worden gebruikt, mits deze documentatie voor de aangewezen technisch beheerders goed begrijpelijk is. De overige in E55 genoemde onderdelen blijven ongewijzigd van toepassing.
223	Programma van Eisen - E51 Conversiedata G4Gem	In welk technisch formaat worden de bestaande autorisatiegegevens uit G4Gem beschikbaar gesteld aan de Opdrachtnemer? Kan Opdrachtgever tevens aangeven: - welke gegevens minimaal onderdeel uitmaken van de conversiedataset; - wat de indicatieve omvang van deze dataset is; - of de gegevens vooraf door Opdrachtgever worden opgeschoond; - welke partij verantwoordelijk is voor de datakwaliteit voorafgaand aan de migratie.	Voor de initiële conversie worden de bestaande autorisatiegegevens uit G4Gem eenmalig als CSV-bestand beschikbaar gesteld. De verdere technische invulling van de conversie wordt in onderling overleg afgestemd. Opdrachtgever is hierin flexibel ten aanzien van het technische formaat en de datastructuur van de aan te leveren bestanden. Opdrachtgever kan de gegevens, waar nodig, zodanig structureren dat deze aansluiten op de door Opdrachtnemer gehanteerde structuur. Dit wordt bij voorkeur gezamenlijk afgestemd, mede omdat bepaalde gegevens voor meerdere interpretaties vatbaar zijn en een zorgvuldige afstemming het risico op interpretatie- en conversiefouten beperkt.

Nr.	Onderwerp	Vraag	Antwoord
			Ten aanzien van de overige vragen geldt: - Conversiedataset: de minimaal benodigde gegevens zijn opgenomen in Bijlage 15. - Omvang: de dataset zal vergelijkbaar zijn qua omvang met Bijlage 15 en zal een omvang hebben van ca. 600-800 KB. - Datakwaliteit: Opdrachtgever levert de gegevens voorafgaand aan de migratie gecontroleerd en intern consistent aan. De dataset bevat geen onbedoelde dubbelingen en bevat consistente benamingen en verwijzingen, waaronder procesrolbenamingen. De gegevens worden aangeleverd in een vorm die geschikt is voor een correcte verwerking binnen de Oplossing. - Verantwoordelijkheid datakwaliteit: Opdrachtgever is verantwoordelijk voor de datakwaliteit van de aangeleverde brongegevens. Opdrachtnemer is verantwoordelijk voor een correcte verwerking en conversie van de aangeleverde gegevens binnen de Oplossing.
224	Programma van Eisen - E42 Supervised connection	Voldoet een Inschrijver aan eis E42 indien beheerwerkzaamheden plaatsvinden via een gecontroleerde en gemonitorde beheerverbinding die voldoet aan de beveiligingseisen van Opdrachtgever, zonder dat permanente lokale beheerrechten noodzakelijk zijn?	Nee. Voor de On-Premise Oplossing geldt dat voor de normale werking, het beheer, de monitoring, het autorisatiebeheer, de logging, het uitvoeren van updates, het herstellen van de Oplossing en het gebruik van de overeengekomen functionaliteit geen noodzakelijke afhankelijkheid mag bestaan van door Opdrachtnemer of derden geëxploiteerde cloud-, SaaS- of beheerdiensten. Dit is onderdeel van de definitie van de On-Premise Oplossing binnen deze aanbesteding. Opdrachtgever moet de Oplossing zelfstandig kunnen beheren en gebruiken, zoals ook is vastgelegd in E46. Een structurele beheerverbinding met Opdrachtnemer is daarom niet toegestaan. Indien voor technische ondersteuning incidenteel toegang door Opdrachtnemer noodzakelijk is, stelt Opdrachtgever hiervoor een gecontroleerde break-glass-account beschikbaar. Deze toegang wordt uitsluitend tijdelijk en voor de betreffende ondersteuningswerkzaamheden verleend en wordt conform de daarvoor geldende beveiligingsmaatregelen beheerd, gelogd en gemonitord.

Nr.	Onderwerp	Vraag	Antwoord
225	Programma van Eisen - E45 Authenticatie beheerderstoegang	Voldoet een Inschrijver aan eis E45 indien beheerderstoegang wordt beveiligd met multifactorauthenticatie die een gelijkwaardig beveiligingsniveau biedt, zonder dat daarbij een specifieke fysieke authenticatiemethode wordt toegepast?	Nee. Opdrachtgever vraagt niet om een afzonderlijke multifactorauthenticatieoplossing voor beheerderstoegang. E45 schrijft voor dat de Oplossing een gecontroleerde noodtoegangsvoorziening (break-glass) ondersteunt. Opdrachtgever levert en beheert hiervoor de break-glass-account(s) en het bijbehorende fysieke authenticatiemiddel. De Oplossing dient deze break-glass-functionaliteit conform de voorwaarden van E45 te ondersteunen.
226	Programma van Eisen - E44 Technische installatie en lifecyclebeheer	Voldoet een Inschrijver aan eis E44 indien de technische installatie, versie-upgrades en overige technische lifecycle-activiteiten door Opdrachtnemer worden uitgevoerd, waarbij beheerders van Opdrachtgever aanwezig zijn ten behoeve van kennisoverdracht en overdracht naar beheer? Kan Opdrachtgever tevens bevestigen dat de garantie- en SLA-verplichtingen geen betrekking hebben op installaties of wijzigingen die niet overeenkomstig de door Opdrachtnemer voorgeschreven procedures zijn uitgevoerd?	Ja. E44 vereist dat Opdrachtgever de Oplossing op basis van de door Opdrachtnemer geleverde software en documentatie zelfstandig kan installeren en herstellen. Het is niet vereist dat iedere installatie, update of andere technische lifecycle-activiteit door Opdrachtgever zelf wordt uitgevoerd. Het is toegestaan dat Opdrachtnemer deze werkzaamheden uitvoert, waarbij de beheerders van Opdrachtgever bijvoorbeeld aanwezig zijn ten behoeve van kennisoverdracht en overdracht naar beheer. De zelfstandige installatie- en herstelmogelijkheid van Opdrachtgever, zoals beschreven in E44, blijft daarbij onverkort van toepassing. Ten aanzien van de tweede vraag geldt dat garantie- en SLA-verplichtingen worden bepaald door de overige aanbestedings- en contractstukken. E44 bevat geen algemene bepaling dat deze verplichtingen vervallen indien werkzaamheden niet overeenkomstig door Opdrachtnemer voorgeschreven procedures zijn uitgevoerd.
227	Programma van Eisen - E28 YouForce integratie	Voldoet een Inschrijver aan eis E28 indien de aangeboden oplossing zowel de huidige BINT XML-bestandsuitwisseling als de toekomstige YouForce IAM REST API ondersteunt, waarbij tijdens de implementatie gebruik wordt gemaakt van de door Opdrachtgever beschikbare integratievariant? Indien bij aanvang van de implementatie gebruik wordt gemaakt van BINT XML-bestanden, verzoeken wij Opdrachtgever tevens aan te geven: - via welk transportmechanisme deze bestanden beschikbaar worden gesteld; - met welke frequentie deze worden aangeleverd; - welke partij verantwoordelijk is voor de benodigde inrichting en licenties van de YouForce-koppeling.	Ja. De Oplossing mag zowel de huidige BINT XML-bestandsuitwisseling als de toekomstige YouForce IAM REST API ondersteunen. Bij de implementatie wordt gebruikgemaakt van de integratievariant die op dat moment door Opdrachtgever beschikbaar wordt gesteld. Voor de huidige situatie geldt dat de BINT XML-bestandsuitwisseling de beschikbare integratievariant is. Indien tijdens de looptijd de YouForce IAM REST API beschikbaar komt en door Opdrachtgever wordt gekozen als integratievariant, kan deze voor de koppeling worden gebruikt. Voor de huidige BINT XML-bestandsuitwisseling geldt het volgende: - De XML-bestanden worden op een fileshare van Opdrachtgever geplaatst. De Oplossing leest de bestanden vanaf deze fileshare in. Zie ook Bijlage 17 voor een voorbeeld van de BINT-bestanden. - De bestanden worden tweemaal per dag beschikbaar gesteld. - Opdrachtgever is verantwoordelijk voor het beschikbaar stellen van de XML-

Nr.	Onderwerp	Vraag	Antwoord
			bestanden op de fileshare. Opdrachtnemer is verantwoordelijk voor het inlezen en verwerken van de bestanden binnen de Oplossing.
228	E34 - Beveiligingsonderzoek / Pentest	Kwalificeert een gecertificeerde partij als onafhankelijk in de zin van E34 als die niet betrokken is bij de ontwikkeling of het onderhoud van de Oplossing, maar wel tot hetzelfde concern behoort als Opdrachtnemer? Wat verstaat Opdrachtgever onder een "passende termijn" voor het oplossen van kritieke en hoog-risico kwetsbaarheden?	Nee. Onder een onafhankelijke partij als bedoeld in eis E34 verstaat de aanbestedende dienst een partij die juridisch, organisatorisch en financieel onafhankelijk is van Opdrachtnemer en van de softwareleverancier. Een certificering laat deze eis onverlet; certificering ziet (doorgaans) op de kwaliteit van het proces, niet op onafhankelijkheid. De aanbestedende dienst sluit hiermee aan bij BIO2-maatregel 5.20.03 (aantonen op basis van onderzoeken van onafhankelijke derden) en bij de NCSC-whitepaper "Pentesten doe je zo", die een financiële relatie tussen de pentester en de maker van het te testen product aanmerkt als risico voor de betrouwbaarheid van de resultaten. Onderzoek door een groepsmaatschappij zou onderdeel moeten zijn van het eigen secure-developmentproces (E32), maar geldt niet als invulling van E34. Een "passende termijn" hangt af van de aard, ernst, exploitatiemogelijkheid en impact van de kwetsbaarheid. Hoe kritieker en hoe hoger het risico, hoe sneller en met hogere prioriteit de kwetsbaarheid moet worden opgelost. Van Opdrachtnemer wordt verwacht dat hierop wordt geanticipeerd.
229	Overeenkomst art. 5.3 - Fatale implementatietermijn	De implementatie is mede afhankelijk van Opdrachtgever (installatie op eigen infrastructuur, YouForce, TOPdesk en conversiedata). Is Opdrachtgever bereid te bevestigen dat de fatale einddatum opschuift indien vertraging wordt veroorzaakt door Opdrachtgever of door door Opdrachtgever ingeschakelde derden?	Zie het antwoord op vraag 9.