

2^e Nota van Inlichtingen: Toegangsservice Gezamenlijke Voorzieningen (systemen en websites) voor de veiligheidsregio's, keten- en crisispartners

Betreft: 2^e Nota van Inlichtingen Europese aanbesteding: Toegangsservice Gezamenlijke Voorzieningen (systemen en websites) voor de veiligheidsregio's, keten- en crisispartners
Kenmerk: NIPV-EA-00117
Datum: 4 augustus 2023
Status: Definitief

Geachte lezer,

Voor u ligt de 2^e Nota van Inlichtingen (hierna te noemen: NvI) van de Europese aanbesteding: Toegangsservice Gezamenlijke Voorzieningen (systemen en websites) voor de veiligheidsregio's, keten- en crisispartners.

De NvI maakt integraal onderdeel uit van het Beschrijvend Document d.d. 4 mei 2023.

Met vriendelijke groet,

Giang Phan
Inkoopadviseur

Vragen en Antwoorden

Hieronder vindt u de vragen die zijn gesteld door marktpartijen met daarbij het antwoord van Opdrachtgever. De vragen en antwoorden zijn door Opdrachtgever ingedeeld per bijlage.

BD TGV v2.0

Vraagnr.	Document	Paragraaf, artikelnaam of tekeningnaam	Pagina	Vraag	Antwoord
1.	Algemeen			Er wordt in verschillende documenten gesproken of systemen en websites. Opdrachtnemer gaat er van uit de de systemen wel gebaseerd zijn op webtechnologie en gekoppeld kunnen worden via SAML of OIDC. Is dit een correcte aanname?	In eis 4.2 van het PvE is gesteld: De TGV kan koppelen met systemen en websites die voldoen aan de volgende open standaarden: • LDAP v2 • OAuth2 • NL GOV Assurance profile for OAuth 2.0 • OpenIDConnect • API (om beheer activiteiten uit te kunnen voeren en data uit TGV te kunnen halen) • SCIM2.0 De te koppelen systemen en websites zullen moeten voldoen aan één van bovenstaande standaarden. Daarnaast moet ook SAML aan dit rijtje worden toegevoegd.

Bijlage 07. Programma van Eisen TGV v2.0 (NDA)

Vraagnr.	Document	Paragraaf, artikelnaam of tekeningnaam	Pagina	Vraag	Antwoord
2.	Bijlage 7, PvE	Eis 3.6	4	Hoe voorziet NIPV dat verkeersplein signalen ontvangt van trusted Identity Providers (federatie) voor het verwijderen van accounts in TGV?	De koppeling met het verkeersplein is een tweede routing van data/netwerkverkeer. Indien de Partners zijn gefedereerd dan worden er geen accountgegevens in TGV opgeslagen. Voor het beheer van de TGV omgeving zelf wordt dit handmatig uitgevoerd door landelijk functioneel beheer.
3.	Bijlage 7, PvE	Eis 3.7	4	Hoe voorziet NIPV dat geaggregeerde accounts verwijderd moeten worden uit TGV? Wie zou eigenaar moeten zijn van deze aggregatie?	Indien er al gebruik gemaakt gaat worden van aggregatie, dan is het decentraal functioneel beheer van het account waar de persoon primair in dienst is (hierover zijn afspraken gemaakt tussen de regio's) verantwoordelijk voor dat account en dus eigenaar van de aggregatie.
4.	Bijlage 7, PvE	Eis 3.7	4	Hoe voorziet NIPV gedelegeerd gebruikersbeheer (m.b.t. eigenaarschap) in het geval van aggregatie?	Zie het antwoord op vraag 3.
5.	Bijlage 7, PvE	Eis 3.7	4	Is het opdrachtnemer toegestaan om geen aggregatie binnen TGV toe te passen, maar in plaats daarvan te zorgen voor het hergebruik van identificerende sleutels, zodat de geleverde diensten dit zien als hetzelfde account? En dat op deze manier het beoogde doel (niet apart inloggen met verschillende accounts) gerealiseerd kan worden?	Dit is toegestaan indien er dan nog onderscheid gemaakt kan worden tussen de verschillende systemen, dus dat bijvoorbeeld voor systeem a wel aggregatie wordt toegepast en voor systeem b niet. Opdrachtgever verwacht dat Inschrijver in gunningscriterium 2 Volledigheid van de TGV, onder b aangeeft in de kwalitatieve beantwoording hoe dit dan wordt opgelost, inclusief wat dit betekent voor de beheerlasten (zie onderdeel e van gunningscriterium 2).

6.	Bijlage 7, PvE	Eis 3.6	4	Kan opdrachtnemer uitgaan van standaard interfaces for het deprovisionen van accounts in dienstleveranciers? Denk hierbij aan SCIM. Of zal er spake zijn van andere mechanismen, zoals custom API's of handmatige opschoning?	Er wordt uitgegaan van SCIM, wetende dat niet alle diensten dit reeds ondersteunen, maar ook custom API's zijn niet uit te sluiten. Belangrijkste aan deze eis is dat TGV het deprovisionen van accounts in diensten moet kunnen bieden, ook al is besloten om deze functionaliteit niet direct bij start van de Overeenkomst te gaan gebruiken.
7.	Bijlage 7, PvE	Eis 5.3	5	Is het voor decentraal functioneel beheerders ook toegestaan om met (eigen) account van de organisatie (Partner) in te loggen? Waarbij de MFA van die organisatie wordt gebruikt?	Decentraal functioneel beheerders mogen met hun Partner account in de TGV oplossing inloggen. Ook al hebben ze voor een eerste inlog bij dat partneraccount een multifactor authenticatie gebruikt, bij het inloggen op de TGV beheeromgeving wordt altijd een extra/aanvullend multifactor authenticatie gevraagd.
8.	Bijlage 7, PvE	Eis 8.14	11	Onduidelijk is wie er verantwoordelijk is voor de uitvoering en rapportage. Moet opdrachtnemer ermee akkoord gaan dat dit gebeurt of moet opdrachtnemer dit ook uitvoeren/begeleiden?	De Opdrachtnemer moet medewerking verlenen met het uitvoeren van deze audit. Op het moment dat dit relevant is zal de Opdrachtgever opdracht geven voor deze audit aan een derde partij.
9.	Bijlage 7, PvE	Eis 3.5	3	Geldt dit ook of juist voor gebruikers die in AD worden beheerd (en dus via Federatie inloggen)? Is het in dat geval acceptabel dat alleen accounts die al geprovisioned zijn (via JIT-provisioning) van rollen te kunnen voorzien?	In de basis kan op 3 plaatsen rolkoppeling plaatsvinden: 1. AD 2. Applicatie 3. TGV Indien eerste 2 niet kunnen, dan moet het mogelijk zijn om dit binnen TGV te organiseren. Wel is het zo dat als optie 1 en 2 altijd gebruikt kunnen worden het niet toegestaan is om gegevens over gefedereerde accounts binnen TGV op te slaan. Optie 3 wordt bij voorkeur alleen gebruikt voor niet geaccrediteerde partners waarvoor het gebruikersaccount binnen TGV wordt aangemaakt.
10.	Bijlage 7, PvE	8.15	11	Onduidelijk is voor welke systemen en processen deze quickscan uitgevoerd moet worden. Betreft	Dit betreft TGV en de beheerprocessen voor TGV die de Opdrachtnemer hanteert.

				het TGV zelf of betreft het de processen bij opdrachtnemer? Of wordt er nog iets anders bedoeld?	
11.	Bijlage 7, PvE	8.12	11	Wat is de scope van deze penetratietesten en hoe wordt eventuele goedkeuring van aangesloten Partners georganiseerd?	De scope van de penetratietesten is TGV, dit betreft grey box en black box testing op basis van de OWASP top 10. De Opdrachtgever zorgt voor toestemming van de aangesloten Partners door dit op te nemen in de gebruikersovereenkomsten met de Partners.
12.	Bijlage 7, PvE	6.20	8	Kan NIPV uitleggen waarom dit 12 maanden voor de definitieve beëindiging moet worden opgesteld?	De 12 maanden geven de Opdrachtgever de tijd om een nieuwe aanbesteding uit te voeren én het re-transitieplan uit te voeren binnen de Overeenkomst met de Opdrachtnemer.
13.	Bijlage 7, PvE	6.19/6.20	8	Kan NIPV beargumenteren waarom dit kosteloos zou moeten gebeuren en niet op basis van (naar alle redelijkheid) bestede consultancy uren?	De Opdrachtgever gaat ervanuit dat de Opdrachtnemer ervaren is met re-transitieplannen en de uitvoering daarvan en derhalve de kosten hiervan voldoende kan inschatten. Deze kosten dienen door de Opdrachtnemer vooraf te worden opgenomen in de aanbieding en mogen niet achteraf in rekening worden gebracht. Zo kan de Opdrachtgever de TCO (fictieve totaalprijzen) van de verschillende inschrijvingen goed met elkaar vergelijken.

Einde.