

[dubbelklik hier om een foto in te voegen]



Technisch Programma van Eisen Deel 3 (Integratie eisen)

uitgave 02-02-2026

Technisch Programma van Eisen Deel 3 (Integratie eisen)

Dit document is een bijlage van de Uitnodiging tot Inschrijving
van Eindhoven Airport N.V. inzake Aanbesteding
Toegangscontrolesysteem

Colofon

Technisch Programma van Eisen Deel 3 (Integratie eisen)

Uitgave 02-02-2026

Versie 1.0

Eindhoven Airport N.V.

Office Luchthavenweg 13

Telefoon +31 (0) 40 2919 9829

Terminal Luchthavenweg 25,
5657 EA Eindhoven

1 Inleiding	5
1.1 Interface Control Document (ICD)	5
2 Koppeling Perceel 1 (USP) & Perceel 2 (PIAM)	5
2.1 Minimale Data-elementen	5
2.2 Performance en Betrouwbaarheid	6
2.2.1 Latency	6
2.2.2 Consistentie	6
2.2.3 Beschikbaarheid	6
2.3 Faalveiligheid en Escalatiematrix	6
2.3.1 USP Autonomie	6
2.3.2 Automatisch Herstel	6
2.3.3 Logging	6
2.3.4 Escalatiematrix Interface-storingen	7
3 Interfaces met externe systemen	8
3.1 Brandmeldinstallatie (BMI) – Perceel 1 (USP)	8
3.1.1 Primaire Veiligheidsinterface	8
3.1.2 Informatieve Interface	8
3.1.3 Implementatie	8
3.2 Active Directory	8
3.2.1 Microsoft Entra ID (voorheen Active Directory)	8
3.2.2 Verantwoordelijkheid	8
4 Algemene Interface-eisen	9
4.1 Security en Encryptie	9
4.2 Logging en Monitoring	9
4.3 Naming conventions en Master data	9
4.3.1 Asset naamgeving	9
4.3.2 Master Data	10
4.3.3 Governance	10
5 Acceptance en Commissioning	11
5.1 Interface Validatie	11
5.1.1 Functionele Testen	11
5.1.2 Resilience Testen	11
5.1.3 Load Testen	11
5.1.4 Security Testen	11
5.2 Commissioning Verantwoordelijkheden	12
5.2.1 Perceel 1 & 2 Gezamenlijk	12
5.2.2 Commissioningplan	12
6 Documentatie	13
6.1 Technische Documentatie	13
6.1.1 Interface Control Document (ICD)(zie 1.1)	13
6.1.2 API-documentatie	13
6.1.3 Netwerk-diagrammen	13
6.1.4 Configuratiehandleiding	13
6.2 Operationele Documentatie	13
6.2.1 Troubleshooting guide	13

6.2.2	Escalatie procedures	14
6.2.3	Change management	14
6.2.4	Runbook	14
6.2.5	Kwaliteitseis documentatie	14
7	IT Infrastructuur Uitgangspunten EANV	15
7.1	Netwerkinfrastructuur	15
7.1.1	Netwerklevering door EANV	15
7.1.2	Netwerksegmentatie	15
7.1.3	802.1X-authenticatie	15
7.1.4	Netwerkdiensten door EANV	15
7.1.5	E-mail (SMTP)	15
7.2	Server en virtualisatie	15
7.2.1	Virtualisatieplatform	15
7.2.2	Levering door EANV	16
7.2.3	OS-patching	16
7.2.4	Anti-virus en anti-malware	16
7.3	Test- en acceptatieomgeving	16
7.4	Security en hardening	16
7.4.1	CIS Level 1 hardening	16
7.4.2	Security Annex IT	17
7.5	Backup en recovery	17
7.6	Monitoring en logging	17
7.6.1	Verantwoordelijkheidsverdeling	17
7.6.2	SIEM-integratie	17
7.7	Vulnerability scanning	17
7.8	Beheer	17
7.9	Database management	18
7.9.1	Verantwoordelijkheid leverancier	18
7.9.2	Data-extractie	18
7.10	Authenticatie	18
7.10.1	Single Sign-On (SSO)	18
7.10.2	Contractor management	18
7.11	Client software	18

1 Inleiding

Dit document beschrijft de eisen voor integratie tussen het Unified Security Platform (Perceel 1), het PIAM-systeem (Perceel 2) en bestaande externe systemen. Een naadloze werking tussen alle subsystemen is essentieel voor operationele veiligheid.

1.1 Interface Control Document (ICD)

De winnende inschrijvers van Perceel 1 en Perceel 2 zijn verplicht gezamenlijk een Interface Control Document (ICD) op te stellen binnen 4 weken na gunning. Eindhoven Airport committeert zich eraan hier een coördinerende en faciliterende rol in te spelen. Een eenmalige verlenging van 4 weken is mogelijk na akkoord van opdrachtgever. Dit document specificeert:

- Welke data wordt uitgewisseld (data dictionary)
- Technische protocollen en beveiliging
- Frequentie van synchronisatie
- Foutafhandeling en escalatie procedures
- Verantwoordelijkheden bij interface-storingen

Het ICD moet worden goedgekeurd door Eindhoven Airport voordat implementatie start.

2 Koppeling Perceel 1 (USP) & Perceel 2 (PIAM)

Het Unified Security Platform (USP) en het Physical Identity and Access Management systeem (PIAM) vormen samen de kern van de beveiligingsinfrastructuur van Eindhoven Airport. Het USP (Perceel 1) omvat de technische beveiligingslaag: toegangscontrolesysteem (TGC), videomanagementsysteem (VMS) en Security Management Systeem (SMS). Het PIAM (Perceel 2) beheert de identiteiten, autorisaties en credentials van alle personen die toegang nodig hebben tot de luchthaven.

Een betrouwbare en performante koppeling tussen beide systemen is essentieel voor de operationele veiligheid. Dit hoofdstuk beschrijft de eisen voor deze integratie.

PIAM is de Single Source of Truth voor identiteiten en autorisaties:

- PIAM → USP (in het bijzonder toegangscontrole): Provisioning van identiteiten, credentials en toegangsrechten
- USP → PIAM: Feedback over toegangsgebeurtenissen en credential-status voor audit/rapportage

Inschrijvers moeten in hun offerte beschrijven:

- Welke technische protocollen zij voorstellen (REST API, SOAP of gelijkwaardig)
- Hoe data-integriteit wordt gewaarborgd
- Hoe synchronisatie wordt beheerd (real-time vs. batch)

2.1 Minimale data-elementen

De interface moet minimaal de volgende objecten kunnen uitwisselen:

- Personen: Unieke ID, naam, functie, afdeling, foto, geldigheidsperiode
- Credentials: Kaartnummer, biometrische templates (toekomst), PIN-codes (encrypted)
- Autorisaties: Toewijzing aan toegangsgroepen, zones, tijdvensters
- Events: Access granted/denied, antipassback violations, credential status changes

2.2 Performance en betrouwbaarheid

2.2.1 Latency

- Provisioning individueel: Maximaal 60 seconden tussen actie in PIAM en activatie op fysiek toegangspunt
- Provisioning batch (>10 identiteiten): Maximaal 5 minuten
- Event feedback: Maximaal 3 minuten tussen gebeurtenis op deur en zichtbaarheid in PIAM audit-log

2.2.2 Consistentie

- Er moet een dagelijks automatisch reconciliation proces draaien dat verschillen tussen PIAM en USP detecteert, rapporteert en zoveel mogelijk automatisch oplost
- Bij gedetecteerde inconsistenties: automatische alarmering naar functioneel beheerders met overzicht van discrepanties

2.2.3 Beschikbaarheid

- Interface beschikbaarheid: 99,5% (kritiek pad)
- Bij interface-storing: automatische alarmering binnen 5 minuten

2.3 Faalveiligheid en Escalatiematrix

2.3.1 USP Autonomie

- Bij verlies van verbinding met PIAM moet het USP blijven functioneren met de laatst bekende configuratie
- Bij verlies van verbinding dient er automatische alarmering plaats te vinden, ten minste via e-mail.
- Minimale autonome werking: 72 uur

2.3.2 Automatisch Herstel

- Bij herstelde verbinding moet het systeem automatisch synchroniseren zonder handmatige interventie
- Pending wijzigingen tijdens storing moeten binnen 30 minuten na herstel worden doorgevoerd

2.3.3 Logging

- Alle interface-transacties moeten worden gelogd met timestamp, gebruiker, actie en resultaat
- Logs moeten minimaal 12 maanden bewaard blijven voor audit-doeleinden

2.3.4 Escalatiematrix Interface-storings

Bij interface-storingsen tussen Perceel 1 en Perceel 2 geldt een gelaagde escalatieprocedure waarbij EANV de eerstelijnsanalyse uitvoert voordat leveranciers worden ingeschakeld.

Eerstelijnsanalyse (EANV, binnen 15 minuten)

Symptoom	Eerste analyse	Verantwoordelijk
PIAM → USP: data arriveert niet	Controle PIAM-applicatie, netwerkconnectiviteit en basislogging	EANV Security
USP → PIAM: events komen niet terug	Controle USP-applicatie, netwerkconnectiviteit en basislogging	EANV Security
Netwerkonderbreking	Controle switches, firewalls en VLAN-configuratie	EANV IT
Data-inconsistentie (reconciliation)	Vaststellen welk systeem afwijkt en sinds wanneer	EANV Security
Provisioning latency overschreden	Controle queue depth en systeembelasting	EANV Security

Escalatie naar leveranciers

Situatie	Escalatie	Doorlooptijd
Oorzaak ligt bij PIAM-zijde of onduidelijk	Perceel 2 analyseert; Perceel 1 stand-by	Start binnen 1 uur na melding EANV
Oorzaak ligt bij USP-zijde	Perceel 1 analyseert; Perceel 2 stand-by	Start binnen 1 uur na melding EANV
Oorzaak onduidelijk na 2 uur	Gezamenlijke troubleshooting Perceel 1 + 2	Sessie binnen 4 uur
Infrastructuur-gerelateerd	EANV IT lost op; leveranciers stand-by voor hertest	Conform EANV IT SLA

Algemene principes

EANV fungeert als single point of contact voor storingsmeldingen en coördineert de escalatie. Tijdens het onderhoudscontract werken Perceel 1 en Perceel 2 gezamenlijk aan interface-issues wanneer de oorzaak niet eenduidig is vast te stellen.

Kosten worden verdeeld conform vastgestelde oorzaak (Perceel 1, Perceel 2, of EANV-infrastructuur).

Bovenstaande doorlooptijden gelden tijdens overeengekomen servicevensters. Buiten servicevensters gelden de responstijden uit de onderhoudsovereenkomst.

3 Interfaces met externe systemen

3.1 Brandmeldinstallatie (BMI) – Perceel 1 (USP)

3.1.1 Primaire Veiligheidsinterface

- Type: Hardwired relais-contacten voor fail-safe ontgrendeling bij brandalarm
 - Zie bijlage I voor aantallen en locaties. (scope perceel 1).
- Responstijd: Maximaal 2 seconden tussen alarm en deur-ontgrendeling
- Scope: Alle deuren in evacuatieroutes van zowel bestaande als nieuwbouw
- Implementatie: Fail-safe circuit (normally closed) - bij stroomuitval of kabelbreuk worden deuren automatisch ontgrendeld

3.1.2 Informatieve Interface

- Type: Protocol-gebaseerde koppeling (bijv. ESPA 4.4.4, BACnet, Modbus TCP, of gelijkwaardig) voor tekstmeldingen naar SMS
- Functie: Visualisatie brandmelders en ontgrendelde deuren op floorplan in meldkamer
- Responstijd: Maximaal 10 seconden (informatief, niet safety-kritiek)

3.1.3 Implementatie

- Inschrijver Perceel 1 specificeert welke hardwired contacten nodig zijn (aantal, type, specificaties)
- Coördinatie met Heijmans (nieuwbouw) en SPIE (bestaande bouw) voor fysieke aansluitingen
- Inschrijver beschrijft in offerte hoe fail-safe werking wordt gewaarborgd en hoe dit wordt getest

3.2 Active Directory

3.2.1 Microsoft Entra ID (voorheen Active Directory)

- Functie: Single Sign-On (SSO) voor beheerders en eindgebruikers van PIAM-portaal (perceel 2) en Security management clients (perceel 1)
- Authenticatie: SAML 2.0, OAuth 2.0, of gelijkwaardig modern protocol
- Multi-Factor Authentication (MFA): Moet ondersteund worden voor beheerdersaccounts

3.2.2 Verantwoordelijkheid

- Inschrijver Perceel 2 (PIAM) beschrijft hoe SSO met Microsoft Entra ID wordt geïmplementeerd
- Inschrijver Perceel 1 (SMS-clients) beschrijft hoe SSO met Microsoft Entra ID wordt geïmplementeerd
- Moet rekening houden met bestaande IT-security policies van Eindhoven Airport

4 Algemene Interface-eisen

4.1 Security en Encryptie

- Primair voldoen alle software, hardware en interfaces aan de eisen in Bijlage J - Security Annex IT en Informatiebeveiliging.
- Alle interfaces over IP moeten gebruik maken van TLS 1.2 of hoger
- Authenticatie via certificaten (PKI) of API-keys met rotatie (minimaal elke 90 dagen)
- Geen plain-text wachtwoorden of credentials in logs of configuraties

4.2 Logging en Monitoring

Alle interface-transacties moeten worden gelogd met:

- Timestamp (met milliseconde precisie, UTC timezone)
- Bron en bestemming systeem (hostname/IP)
- Actie en resultaat (succes/failure met foutcode indien van toepassing)
- Gebruiker of service-account
- Bericht-grootte en verwerkingstijd

Logs minimaal 12 maanden bewaren, met mogelijkheid om te archiveren voor externe opslag.

Real-time monitoring dashboard met minimaal:

- Interface beschikbaarheid (up/down status)
- Provisioning latency (gemiddeld en 95th percentile laatste 24u)
- Error rate (aantal fouten per uur)
- Queue depth (aantal pending synchronisaties)

4.3 Naming conventions en Master data

4.3.1 Asset naamgeving

Er moet een consistente naamgevingsconventie worden gehanteerd voor alle assets (deuren, readers, camera's, controllers) in PIAM, USP en CAD-tekeningen.

Minimale (mogelijke) structuur:

- Gebouw-identificatie (TRM-EAST / TRM-WEST)
- Verdieping (L00 = begane grond, L01 = eerste verdieping, etc.)
- Zone (LPA / SRA / SRA-CP)
- Ruimtenummer of -naam
- Asset-type (DOOR, READER, CAMERA, CTRL)
- Volgnummer (indien meerdere van zelfde type in ruimte)

Voorbeeld: TRM-EAST_L01_SRA_TECH-105_DOOR-01

4.3.2 Master Data

- Eindhoven Airport levert uiterlijk 4 weken na gunning het master data-bestand met alle asset-namen
- Formaat: Excel met kolommen:
 - Asset ID (uniek, primary key)
 - Asset naam (conform naming convention)
 - Type (deur/reader/camera/controller/zone)
 - Locatie (gebouw, verdieping, ruimtenummer)
 - Zone-classificatie (LPA/SRA/SRA-CP)
 - Coördinaten X,Y (voor GIS/plattegrond-weergave)
 - Opmerkingen (bijzonderheden, bijv. “nooduitgang”, “24/7 toegang”)
- Verantwoordelijkheid inschrijver: Begroot (in ieder geval) 40 uur voor ondersteuning om de data geschikt te maken voor import, validatie en kwaliteitscontrole van master data.
- Inschrijver neemt daarnaast uren op voor de daadwerkelijke implementatie van deze data.
- Afwijkingen: Indien tijdens implementatie blijkt dat asset-namen in werkelijkheid afwijken van master data, dan rapporteert inschrijver dit binnen 1 week aan Eindhoven Airport voor correctie in master data-bestand

4.3.3 Governance

- Wijzigingen in asset-namen gaan via formeel Change Management proces
- Inschrijvers committeren zich aan het gebruik van EANV-naming conventions zonder eigen afwijkingen

5 Acceptance en Commissioning

5.1 Interface Validatie

5.1.1 Functionele Testen

Tijdens commissioning moet worden aangetoond dat:

- PIAM → USP provisioning werkt: Identiteit aanmaken in PIAM resulteert in werkende pas op deur binnen 60 seconden (individueel) of 5 minuten (batch >10)
- USP → PIAM feedback werkt: Toegangsgebeurtenis op deur is zichtbaar in PIAM audit-log binnen 5 minuten
- Uitdiensttreding werkt: Handmatige markering “Uitdiensttreding” in PIAM resulteert in geblokkeerde pas binnen 15 minuten
- BMI-interface werkt: Brandalarm resulteert in deur-ontgrendeling binnen 2 seconden (fail-safe test)
- Azure AD SSO werkt: Inloggen in PIAM en SMS-clients met Azure AD credentials succesvol

5.1.2 Resilience Testen

Simuleer interface-storing PIAM ↔ USP en valideer dat:

- USP blijft functioneren met laatst bekende configuratie (72 uur autonomie test)
- Automatische alarmering binnen 5 minuten wordt gegenereerd

Herstel interface en valideer dat:

- Automatische synchronisatie binnen 30 minuten plaatsvindt
- Alle pending wijzigingen correct worden doorgevoerd

Simuleer netwerk-storing en valideer escalatiematrix conform sectie Escalatiematrix Interface-storingen

5.1.3 Load Testen

Tijdens commissioning wordt de interface tussen PIAM en USP getest onder realistische belasting:

- Batch provisioning: 1.000 identiteiten in één batch moeten succesvol worden gesynchroniseerd tussen PIAM en USP, zonder fouten en binnen 90 minuten.
- Piek-provisioning: 50 individuele provisioning-acties binnen 5 minuten mogen niet leiden tot queue-overloop of verlies van transacties.
- Event-feedback onder belasting: bij 100 gelijktijdige toegangsgebeurtenissen per minuut moet de USP → PIAM event-feedback binnen de gestelde latency (5 minuten) blijven.

Inschrijvers beschrijven in hun offerte hoe zij deze load testen uitvoeren en welke tooling zij hiervoor inzetten.

5.1.4 Security Testen

- Penetration test van alle interfaces door externe security auditor (door EANV aangesteld)
- Validatie dat TLS 1.2+ wordt gebruikt en geen zwakke ciphers
- Test API-key rotatie mechanisme

- Validatie dat geen credentials in plain-text worden gelogd

5.2 Commissioning Verantwoordelijkheden

5.2.1 Perceel 1 & 2 Gezamenlijk

- Opstellen Interface Control Document (ICD)(zie 1.1) en een daarop aansluitend integraal commissioningplan.
- Uitvoeren interface-testen volgens commissioning plan
- Demonstreren end-to-end functionaliteit (identiteit aanmaken t/m fysieke toegang)
- Gezamenlijk troubleshooten bij interface-issues tijdens commissioning

5.2.2 Commissioningplan

Winnende inschrijvers leveren gezamenlijk een gedetailleerd commissioningplan binnen 4 weken na afronding Interface Control Document (ICD)(zie 1.1).

Dit plan beschrijft:

- Alle testscenario's met verwachte resultaten
- Acceptatiecriteria per interface
- Betrokken partijen en verantwoordelijkheden
- Planning met mijlpalen
- Risico's en mitigatie
- Rollback-procedures bij falen

Commissioningplan moet worden goedgekeurd door Eindhoven Airport vóór inbedrijfstelling.

Het commissioningplan valt onder de eis uit TPvE Deel 1 (Implementatie- & commissioningplan) en Deel 2. Deel 3 specificeert alleen de minimum interface-validaties die onderdeel moeten zijn van dat plan.

6 Documentatie

6.1 Technische Documentatie

Inschrijvers leveren na oplevering documentatie van professionele kwaliteit:

6.1.1 Interface Control Document (ICD)(zie 1.1)

- Taal: Nederlands
- Formaat: PDF + bewerkbare bron (Microsoft Word of Markdown)
- Minimale inhoud:
 - Interface architectuur diagram (high-level en gedetailleerd)
 - Data dictionary: alle velden met datatype, lengte, constraints, voorbeeldwaarden
 - Protocol specificatie inclusief voorbeeld-berichten (request/response)
 - Foutcodes en afhandelingsprocedures (wat te doen bij elke error)
 - Sequence diagrams voor kritieke flows (bijv. provisioning, uitdiensttreding)
 - Security specificaties: certificaten, encryptie-algoritmes, key-management
 - Performance baseline: verwachte latency en throughput onder normale condities
- Versie beheer:
 - Major update (1.0 → 2.0) bij breaking changes die incompatibiliteit veroorzaken
 - Minor update (1.0 → 1.1) bij toevoegingen zonder breaking changes
 - Patch update (1.0.0 → 1.0.1) bij correcties van fouten in documentatie
- Review cyclus: EANV beoordeelt binnen 2 weken na indiening en geeft feedback

6.1.2 API-documentatie

- Indien REST/SOAP API's worden gebruikt: volledige OpenAPI 3.0 / WSDL specificaties
- Interactive documentation (bijv. Swagger UI) voor testen van endpoints
- Code-voorbeelden in minimaal Python en C# voor veelgebruikte operaties

6.1.3 Netwerk-diagrammen

Overzicht van alle verbindingen tussen systemen met:

- IP-adressen (of IP-ranges indien DHCP)
- Poorten en protocollen
- Firewall-regels die nodig zijn
- VLAN-segmentatie

Fysieke netwerktopologie (switches, routers, kabelroutes)

6.1.4 Configuratiehandleiding

- Stapsgewijze instructies voor wijzigen van interface-instellingen
- Screenshots van relevante configuratieschermen
- Backup en restore procedures voor configuraties

6.2 Operationele Documentatie

6.2.1 Troubleshooting guide

- Top 20 veel voorkomende interface-storingen met oorzaak en oplossing

- Diagnostische commando's en interpretatie van output
- Flowcharts voor systematische probleemoplossing

6.2.2 Escalatie procedures

- Wie te benaderen bij welke type storing (conform escalatiematrix)
- Contactgegevens 24/7 support met telefoonnummers en email
- SLA's per priority-level

6.2.3 Change management

- Procedure voor wijzigingen aan interfaces die impact hebben op andere systemen
- Template voor Change Request Document
- Approval workflow en communicatieplan

6.2.4 Runbook

- Dagelijkse, wekelijkse en maandelijkse onderhoudstaken
- Health check procedures
- Monitoring dashboards en interpretatie van alerts

6.2.5 Kwaliteitseis documentatie

- Alle documentatie moet professioneel opgemaakt zijn (huisstijl of neutrale template)
- Consistent taalgebruik (geen mix van Nederlands en Engels binnen één document tenzij technische termen)
- Inhoudsopgave, paginanummering, versie-informatie en wijzigingsgeschiedenis
- Digitaal doorzoekbaar (geïndexeerde PDF's, geen gescande documenten)
- Tevens online beschikbaar in kennisbank met bruikbare index en zoekfunctie
- Referentie kwaliteit: Vergelijkbaar met documentatie van enterprise software-leveranciers zoals Microsoft, Cisco of SAP

7 IT Infrastructuur Uitgangspunten EANV

Dit hoofdstuk beschrijft de IT-infrastructuur die Eindhoven Airport (EANV) beschikbaar stelt en de uitgangspunten waarmee inschrijvers rekening moeten houden bij het ontwerp van hun oplossing.

7.1 Netwerkinfrastructuur

7.1.1 Netwerklevering door EANV

EANV levert de volledige netwerkinfrastructuur op basis van HP Enterprise (HPE). De volgende functionaliteit is beschikbaar:

- Layer 2 switching (beheer door EANV)
- Layer 3 routing (beheer door EANV)

7.1.2 Netwerksegmentatie

Inschrijvers dienen een segmentatievoorstel in te dienen op basis van de Purdue-referentiearchitectuur. Het voorstel moet minimaal het volgende adresseren:

- Servers gesegmenteerd van alle randapparatuur
- Verdere segmentatie op basis van logische zones (bijvoorbeeld binnen/buiten of layered security)

7.1.3 802.1X-authenticatie

EANV rolt in Q1 2026 802.1X-authenticatie uit op basis van HPE. Inschrijvers moeten in hun oplossing beschrijven hoe zij 802.1X ondersteunen voor alle netwerkcomponenten.

7.1.4 Netwerkdiensten door EANV

De volgende netwerkdiensten worden door EANV geleverd en beheerd. Inschrijvers nemen deze diensten af van EANV en begroten deze niet separaat:

- RADIUS
- DHCP
- DNS
- NTP

7.1.5 E-mail (SMTP)

EANV heeft geen standaard SMTP-dienst beschikbaar. Indien e-mailnotificaties noodzakelijk zijn voor de oplossing, beschrijft de inschrijver in de offerte hoe dit wordt gerealiseerd en welke afhankelijkheden dit creëert.

7.2 Server en virtualisatie

7.2.1 Virtualisatieplatform

EANV biedt virtuele machines (VM's) aan op basis van VMware met de volgende eigenschappen:

- Voldoende capaciteit beschikbaar
- Geografisch gescheiden infrastructuur (on-site)
- Proportioneel gebruik: één server per discipline (TGC, SMS/PSIM, PIAM)

7.2.2 Levering door EANV

EANV levert virtuele machines inclusief besturingssysteem (Windows Server of Linux, afhankelijk van applicatievereisten).

EANV is verantwoordelijk voor:

- Installatie en initiële configuratie van het besturingssysteem
- Geautomatiseerde OS-patching (minimaal eens per kwartaal)

Inschrijver is verantwoordelijk voor:

- Specificatie van OS-vereisten (type, versie, configuratie) voorafgaand aan levering
- Hardening conform §7.4
- Kwartaalondersteuning bij patching: validatie van applicatiewerking na toepassing van patches
- Tijdige melding van incompatibiliteiten met geplande patches (minimaal 10 werkdagen voorafgaand aan geplande patchwindow)
- Applicatielaag en middleware beheer.

7.2.3 OS-patching

Vanwege de high-risk classificatie van de beveiligingssystemen is directe internettoegang niet beschikbaar. Uitzondering hierop zijn de systemen voor contractor- en visitormanagement, die van (gecontroleerde) internettoegang worden voorzien.

Inschrijvers beschrijven in hun offerte hoe veilige OS-patching wordt gerealiseerd zonder directe internettoegang (bijvoorbeeld via data diode of patching server in DMZ).

7.2.4 Anti-virus en anti-malware

Inschrijver beschrijft in de offerte welke anti-virus en anti-malware oplossing wordt toegepast. Uitgangspunt is dat gangbare enterprise-oplossingen zoals Microsoft Defender worden ondersteund.

7.3 Test- en acceptatieomgeving

Een separate test- en acceptatieomgeving is niet verplicht. Inschrijver beslist zelf of een dergelijke omgeving wordt aangeboden en onderbouwt deze keuze in de offerte. Indien geen separate omgeving wordt aangeboden, beschrijft inschrijver hoe testen en acceptatie op de productieomgeving wordt uitgevoerd zonder operationele risico's.

7.4 Security en hardening

7.4.1 CIS Level 1 hardening

Alle servers moeten worden gehardend conform CIS Level 1 benchmark met een minimale score van 90%. De inschrijver is verantwoordelijk voor het uitvoeren van de hardening. EANV ondersteunt op verzoek.

Inschrijver neemt een Proof of Concept voor hardening op in het commissioningplan en toont aan dat de applicatie correct functioneert na hardening.

7.4.2 Security Annex IT

De Security Annex IT is standaard onderdeel van deze aanbesteding. Inschrijvers verklaren in hun offerte compliant te zijn met alle eisen uit de Security Annex. Penetratietesten worden uitgevoerd om conformiteit te valideren.

7.5 Backup en recovery

EANV verzorgt alle backups van de geleverde virtuele machines:

- Snapshots
- Full-VM backups
- Rollback-mogelijkheid naar eerdere staat

De volgende parameters zijn van toepassing:

Parameter	Waarde
Recovery Time Objective (RTO)	Maximaal 4 uur
Recovery Point Objective (RPO)	Maximaal 24 uur
Retentietijd backups	Minimaal 30 dagen

Recovery is een gezamenlijke verantwoordelijkheid van EANV IT (infrastructuur) en de leverancier (applicatie). Inschrijver beschrijft in de offerte welke acties aan leverancierszijde nodig zijn bij een recovery-scenario.

7.6 Monitoring en logging

7.6.1 Verantwoordelijkheidsverdeling

Verantwoordelijke	Scope
EANV IT	Monitoring en logging op OS- en hardware-niveau
Leverancier	Functionele monitoring en logging van de applicatie

7.6.2 SIEM-integratie

EANV beschikt over een SIEM-platform. Integratie met dit platform is verplicht. Inschrijver beschrijft in de offerte:

- Welke logs en events naar het SIEM worden gestuurd
- In welk formaat (syslog, CEF, of vergelijkbaar)
- Hoe de integratie technisch wordt gerealiseerd

7.7 Vulnerability scanning

EANV IT voert periodiek vulnerability scans uit op alle servers, inclusief OT-systemen. De eisen voor vulnerability management en remediation zijn opgenomen in de Security Annex IT.

7.8 Beheer

De leverancier is verantwoordelijk voor het volledige functionele beheer van de geleverde oplossing gedurende de looptijd van het onderhoudscontract.

7.9 Database management

7.9.1 Verantwoordelijkheid leverancier

De database is onderdeel van de applicatie. De leverancier is verantwoordelijk voor installatie, configuratie, onderhoud en optimalisatie van de database.

7.9.2 Data-extractie

EANV vereist toegang tot de database voor analytics en rapportage. Inschrijver beschrijft in de offerte hoe deze toegang wordt gerealiseerd (bijvoorbeeld read-only database user, API, of data-export functionaliteit).

7.10 Authenticatie

7.10.1 Single Sign-On (SSO)

SSO moet worden geïmplementeerd via Microsoft Entra ID (voorheen Azure AD) met OpenID Connect. Inschrijver beschrijft in de offerte hoe SSO wordt gerealiseerd voor:

- PIAM-beheerinterface (Perceel 2)
- SMS-clients (Perceel 1)
- Overige beheerinterfaces

7.10.2 Contractor management

Voor het beheer van contractor-toegang biedt de inschrijver een oplossing die voldoet aan de volgende eisen:

- Contractor-bedrijven kunnen eigen gebruikers beheren (self-service)
- Twee-factor-authenticatie (2FA) is verplicht, bij voorkeur via e-mail of authenticator-app
- Integratie met Microsoft Entra ID voor EANV-medewerkers die contractors beheren

Inschrijver beschrijft de voorgestelde oplossing in de offerte.

7.11 Client software

EANV heeft een voorkeur voor web-based client software. Indien thick-client software noodzakelijk is, onderbouwt de inschrijver waarom dit nodig is en beschrijft:

- Op welke werkplekken de client moet worden geïnstalleerd
- Welke systeemeisen gelden
- Hoe updates en patches worden gedistribueerd