

[dubbelklik hier om een foto in te voegen]



Technisch Programma van Eisen Deel 1 (Unified Security Platform)

uitgave 02-02-2026

Technisch Programma van Eisen Deel 1 (Unified Security Platform)

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

Colofon

Technisch Programma van Eisen Deel 1 (Unified Security Platform)

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 Scope van Perceel 1	5
1.2 Leeswijzer	5
2 Uitgangspunten en normering	6
2.1 Algemene uitgangspunten	6
2.2 Veiligheidsdoelstellingen Eindhoven Airport	6
2.3 Wet- en regelgeving & normen	6
2.4 Luchthavenspecifieke normen	6
2.5 Installatieverantwoordelijkheid	7
3 Systeemarchitectuur	8
3.1 Unified Security Platform concept	8
3.2 Netwerkinfrastructuur en redundantie	8
3.3 Cyber security & hardening	8
3.4 Performance eisen en service levels	8
3.5 IT-infrastructuur en hosting	9
4 Zonering en classificatie	12
4.1 Risicoclassificatie ruimtes	12
4.2 Zone-overgangen en weerstandsklassen	12
5 Specificaties toegangscontrole	13
5.1 Veldapparatuur en hardware	13
5.2 Controllers en intelligentie	13
5.3 Kaarttechnologie en lezers	13
5.4 Biometrie en hoog-risico zones	14
5.5 Hardware componenten - indicatieve aantallen	14
5.6 Autonome werking bij netwerkuitval	14
6 Specificaties Video Management Systeem	15
6.1 Opslag en retentie	15
6.2 Integratie met TGC	15
6.3 Beeldkwaliteit en streams	15
6.4 VMS opslag – capaciteit en retentie	15
6.5 Video Content Analytics - basisvereisten	16
7 Specificaties Security Management Systeem	17
7.1 Operator interface en dashboarding	17
7.2 Alarmmanagement en workflows	17
7.3 Plattegronden en GIS-integratie	17
7.4 Visuele identiteitsverificatie	17
8 Migratie en implementatie	18
8.1 Fasering	18
8.2 Migratiestrategie en fallback	18
8.3 Oplevering en testen	19
9 Training en kennisoverdracht	21

1 Inleiding

Dit Technisch Programma van Eisen (TPvE) beschrijft de technische specificaties voor **Perceel 1: Unified Security Platform (USP)**. Het doel is de realisatie van een geïntegreerd, toekomstbestendig platform dat toegangscontrole (TGC), videomanagement (VMS) en security management (SMS) combineert.

1.1 Scope van Perceel 1

De scope omvat de levering, configuratie, installatie (behoudens specifieke afbakeningen, zie paragraaf Installatieverantwoordelijkheid) en inbedrijfstelling van:

- **Hardware:** Controllers, kaartlezers, I/O-modules, server-hardware (indien on-premise) en werkplekken.
- **Software:** Een Unified Security Platform voor TGC, VMS en SMS.
- **VMS:** Integratie van circa 360 bestaande en nieuwe camera's.
- **Migratie:** Vervanging van het huidige TCS in de bestaande terminalgebouw en implementatie in de nieuwbouw.
- **Passen:** Leveren 4000 stuks nieuwe MIFARE DESFire EV3

Expliciet **buiten** scope van dit perceel (maar wel onderdeel van integratie):

- Physical Identity & Access Management (PIAM) software (zie TPvE Deel 2).
- Levering van camera-hardware (reeds aanwezig of via separaat traject).
- Fysieke bekabeling en installatiewerkzaamheden van de hardware in zowel bestaande als nieuwbouw.

1.2 Leeswijzer

Dit document dient in samenhang gelezen te worden met:

- TPvE Deel 2 (PIAM)
- TPvE Deel 3 (Integratie-eisen)
- Het Interface Control Document (ICD)

2 Uitgangspunten en normering

2.1 Algemene uitgangspunten

De oplossing moet gebaseerd zijn op open standaarden of gangbare industrieprotocollen om vendor lock-in te voorkomen. Het systeem dient modulair en schaalbaar te zijn, voorbereid op een groei van minimaal 50% in veldcomponenten zonder verlies van performance.

2.2 Veiligheidsdoelstellingen Eindhoven Airport

Conform het *Handboek Safety & Security* en het *Toegangsbeleid* zijn de volgende doelen leidend:

- **Bescherming burgerluchtvaart:** Strikte scheiding tussen Landside Public Area (LPA), Security Restricted Area (SRA) en SRA-Critical Part (SRA-CP).
- **Continuïteit:** Het systeem is bedrijfskritisch. Uitval mag de operatie niet stilleggen (autonome werking controllers).
- **Functionele noodzakelijkheid:** Toegang wordt verleend op basis van “need to be”.

2.3 Wet- en regelgeving & normen

Opdrachtnemer dient te voldoen aan onder meer:

- **NEN-EN 50133 of gelijkwaardig:** Alarmsystemen en toegangscontrole.
- **NEN-EN 60839 of gelijkwaardig:** Elektronische toegangscontrolesystemen.
- **NEN-EN 50132 / IEC 62676 of gelijkwaardig:** Cameratoezichtsystemen.
- **IEC 62443 of gelijkwaardig:** Cybersecurity voor industriële automatiseringssystemen (minimaal SL2-niveau)
- **ISO 27001 of gelijkwaardig:** Informatiebeveiliging.
- **ISO 27701 of gelijkwaardig:** Bescherming van persoonsgegevens conform AVG, met o.a. borging van Privacy by design & default.
- **EANV specifiek:** Bijlage P.7 - Handboek Safety en Security.
- **EANV specifiek:** Bijlage J - Security Annex IT en Informatiebeveiliging.
- **NEN 2654 of gelijkwaardig:** Beheer, controle en onderhoud (voor zover van toepassing op geïntegreerde systemen).
- **Open protocollen:** De oplossing ondersteunt ONVIF, OSDP en PSIA protocollen voor interoperabiliteit met apparatuur van derden.

2.4 Luchthavenspecifieke normen

Het systeem dient te voldoen aan de volgende luchthavenspecifieke wet- en regelgeving:

- **ICAO 9303:** Machine Readable Travel Documents — het systeem ondersteunt verificatie van machineleesbare reisdocumenten conform ICAO 9303.
- **ACI Security Guidelines:** het systeem voldoet aan de ACI Security Guidelines voor toegangscontrole op luchthavens.
- **ECAC Doc 30:** Part II — Security. Het systeem voldoet aan de beveiligingseisen uit ECAC Doc 30.
- **EU-verordening 2015/1998:** het systeem voldoet aan de eisen voor luchthavenbeveiliging uit EU-verordening 2015/1998.

- **Regeling beveiliging burgerluchtvaart:** het systeem voldoet aan de Regeling beveiliging burgerluchtvaart.
- **Eisen ILT:** het systeem voldoet aan de eisen van de Inspectie Leefomgeving en Transport (ILT) ten aanzien van toegangscontrolesystemen op luchthavens.

2.5 Installatieverantwoordelijkheid

Cruciaal voor de uitvoering is de strikte scheiding in installatieverantwoordelijkheid:

- **Nieuwbouw (westzijde):** Installatiewerkzaamheden (bekabeling, fysieke montage) worden uitgevoerd door **Heijmans**. Opdrachtnemer Perceel 1 levert hardware aan, verzorgt engineering, toezicht en inbedrijfstelling.
- **Bestaande bouw (oostzijde):** Installatiewerkzaamheden worden uitgevoerd door **SPIE**. Opdrachtnemer Perceel 1 levert hardware aan, verzorgt engineering, toezicht en inbedrijfstelling.
- Opdrachtnemer Perceel 1 blijft **eindverantwoordelijk** voor de werking van het totale systeem en coördineert werkzaamheden met Heijmans en SPIE. Zie hiervoor tevens de coördinatieovereenkomst, bijlage O.3, die onderling overeen dient te worden gekomen.

3 Systeemarchitectuur

3.1 Unified Security Platform concept

De gevraagde oplossing betreft een 'Unified' of naadloos geïntegreerd platform. Dit houdt in dat TGC, VMS en SMS in één native omgeving draaien of volledig geïntegreerd zijn, waarbij:

- **Voorkeur:** Native unified platform (1 database, 1 user interface, 1 leverancier)
- **Acceptabel:** Best-of-breed integratie mits:
 - Single Sign-On (1 login voor alle modules)
 - Unified operator interface (1 scherm voor alle alarmen en events)
 - Shared database of real-time synchronisatie (<1 sec latency)
 - 1 vendor eindverantwoordelijk voor total solution (prime contractor model)

Gunning: Native unified oplossingen scoren hoger op GC2 (Kwaliteit oplossing) vanwege eenvoudiger beheer en betere performance.

3.2 Netwerkinfrastructuur en redundantie

- **High Availability:** De centrale software servers dienen redundant uitgevoerd te zijn (hot-standby, actief-actief cluster, of gelijkwaardig). Uitzondering hierop zijn de video recorders.
- **Offline continuïteit:** Bij netwerkuitval moeten deurcontrollers volledig autonoom functioneren (beslissingsbevoegdheid lokaal), inclusief buffering van events (minimaal 50.000 events per controller).

3.3 Cyber security & hardening

- Communicatie tussen server en controllers moet versleuteld zijn (conform moderne standaarden).
- Communicatie tussen controller en lezer moet versleuteld zijn (OSDP v2 met Secure Channel of gelijkwaardige beveiliging).
- Ondersteuning voor 802.1X authenticatie op netwerkpoorten of gelijkwaardige netwerk access control.

3.4 Performance eisen en service levels

Het USP moet voldoen aan de volgende performance-eisen:

Responstijden:

- Maximum deur-response tijd: < 2 seconden (van pas-presentatie tot slot-aanslag)
- SMS client schermverversing bij alarm: < 3 seconden
- VMS camera call-up bij toegangsgebeurtenis: < 2 seconden

Systeemcapaciteit:

- Event processing capacity: continue minimaal 100 events/seconde simultaan
- Database capaciteit: ondersteuning voor minimaal 100.000 historische events per dag met doorzoekbaarheid binnen 5 seconden

Beschikbaarheid:

- Uptime requirement totaalsysteem: 99.9% (exclusief geplande onderhoudsvensters)
- Maximum geplande downtime: 4 uur per kwartaal (tijdens baansluiting of nacht)
- Bij voorkeur is onderhoud mogelijk zonder (systeem-brede) downtime
- Recovery Time Objective (RTO) na calamiteit: < 4 uur
- Recovery Point Objective (RPO): < 15 minuten (data-verlies maximaal 15 min)
- Servicewindow 24/7

MTBF:

- Inschrijver specificeert de Mean Time Between Failure (MTBF) per componenttype (controllers, kaartlezers, servers, I/O-modules).

Schaalbaarheid:

- Het systeem moet zonder performance-degradatie kunnen schalen naar 500 kaartlezers (circa 67% groei t.o.v. huidig)
- Performance moet gelijk blijven aan bovenstaande eisen

3.5 IT-infrastructuur en hosting

Virtualisatie platform:

Eindhoven Airport levert virtuele machines op basis van VMware vSphere of gelijkwaardige virtualisatie-technologie. Opdrachtnemer dient de benodigde specificaties voor VM's aan te leveren.

Inschrijver specificeert per benodigde VM:

- Aantal CPU cores (vCPU) - minimum benodigd
- Hoeveelheid werkgeheugen (RAM in GB) - minimum benodigd
- Opslagcapaciteit (GB/TB) en type (SSD/HDD) - minimum benodigd
- Netwerk-interfaces en bandbreedte-behoefte
- Operating System (Windows Server / Linux distributie + versie)
- Rationale voor gekozen specificaties

IT-diensten door EANV:

Eindhoven Airport levert de volgende infrastructurele diensten die door het USP gebruikt mogen/moeten worden:

- Netwerkinfrastructuur (Layer 2 + 3 switching)
- 802.1X netwerkauthenticatie (uitrol Q1 2026) of gelijkwaardige network access control
- Basisdiensten: DHCP, DNS, NTP
- VM hosting inclusief geografische redundantie (on-site maar gescheiden locaties)
- Backup (snapshots + full VM backups) met rollback-mogelijkheid
- Monitoring en logging op OS- en server hardware-niveau
- Vulnerability scanning op VM-niveau
- SIEM (dient geïntegreerd te worden in de applicatie)
- SOC

- Rackspace in meerdere datacenters op locatie. Alle ruimtes zijn voorzien van dubbele koelingen, dubbele stroom feeds, UPS en noodstroom (aggregaat) en zijn onderling verbonden op een 10Gbit backbone.

IT-verantwoordelijkheden opdrachtnemer:

- Applicatie software (TGC/VMS/SMS) inclusief configuratie
- Database management inclusief database-backups op applicatie-niveau
- Functionele monitoring en logging (events, alarmen, audits)
- Het opstellen van een OS patchplan in samenspraak met opdrachtgever.

Operating system en patching:

- EANV levert VM inclusief OS en voert OS-patching uit (geautomatiseerd)
- Opdrachtnemer ondersteunt: 1x per kwartaal verificatie dat applicatie nog correct functioneert na patches
- Minimale patch-frequentie OS: maandelijks security updates, kwartaal overige updates
- Opdrachtnemer levert anti-malware (Microsoft Defender for Endpoint of gelijkwaardig)

Hardening:

- Opdrachtnemer is verantwoordelijk voor hardening van servers conform CIS Benchmark Level 1 of gelijkwaardige security baseline
- EANV kan hardening OS-niveau uitvoeren indien dit geen applicatieproblemen oplevert (afstemming vooraf vereist)
- Opdrachtnemer verzorgt in samenwerking met opdrachtgever voor de hardening.
- De applicatie dient secure-by-design te zijn (least-privilege principe)

Netwerk segmentatie:

- Server-segment gescheiden van randapparatuur (controllers, lezers, camera's)
- Segmentatie op basis van logische zones (binnen/buiten, layered security model)
- Firewalling tussen segmenten (geen layer-3 routing zonder firewall)
- Opdrachtnemer is in de lead voor de detailengineering (low-level design) van de netwerksegmentatie en legt dit voor akkoord voor bij opdrachtgever.

4 Zoning en classificatie

4.1 Risicoclassificatie ruimtes

Eindhoven Airport hanteert de volgende risicoklassen (conform *Toegangsbeleid INTERN*):

Classificatie	Omschrijving	Voorbeelden	Beveiligingseis
Hoog	Kritische infrastructuur	Serverruimtes, HVK, SRA-CP toegangen	2-factor authenticatie (Biometrie/Pin), Video-verificatie, Anti-passback
Midden	Operationele techniek	Technische ruimtes, Ops ruimtes airside	Kaartlezer, Deurstandsignalering
Laag	Algemene toegang	Kantoorruimtes, Facilitaire kasten, Landside	Kaartlezer of gecontroleerde sleutel

4.2 Zone-overgangen en weerstandsklassen

- **SRA-grens:** Overgangen van LPA/LRA naar SRA vereisen fysieke barrières (draaideuren, sluizen, of gelijkwaardige anti-tailgating oplossingen) die tailgating voorkomen.
- **Serverruimtes:** Deuren naar 'Hoog' geclassificeerde ruimtes moeten voldoen aan weerstandsklasse RC3 of gelijkwaardig.

5 Specificaties toegangscontrole

5.1 Veldapparatuur en hardware

- Opdrachtnemer levert alle controllers, voedingen, I/O-modules en daarbij behorende componenten (behuizing, etc.).
- Behuizingen: Controllers in technische ruimtes dienen in afsluitbare stalen kasten of gelijkwaardige beschermde behuizingen geplaatst te worden, voorzien van sabotagedetectie.
- Voeding: PoE+ (Power over Ethernet Type 2, 802.3at) heeft de voorkeur voor deurcontrollers, mits ondersteund door de switch-infrastructuur van EANV. Mocht PoE++ noodzakelijk zijn gaan opdrachtnemer en opdrachtgever hierover in gesprek. Anders lokale 12/24V voeding met accu-backup (autonomie > 4 uur).

5.2 Controllers en intelligentie

- Volledige IP-native controllers.
- Ondersteuning voor OSDP of gelijkwaardig protocol.
- Capaciteit voor minimaal 100.000 kaarthouders lokaal in het geheugen.

5.3 Kaarttechnologie en lezers

- **Technologie:** Compatibiliteit met de laatste stand van MIFARE DESFire (EV2 of EV3) technologie is **vereist**.
- **Migratie:** Gefaseerde overgang naar nieuwe credentials is mogelijk maar niet verplicht binnen projectscope. De migratiestrategie wordt na gunning in detail afgestemd.
- Vandalbestendigheid: Minimaal IK08 of gelijkwaardig voor lezers in publiek gebied.
- **Toekomstbestendigheid:** Lezers moeten hardwarematig voorbereid zijn op mobiele toegang (Bluetooth Low Energy / NFC) voor toekomstige implementatie.

Indicatief aantal lezers:

- Circa 300 kaartlezers verdeeld over beide terminals
- 50-100 extra lezers als reserve/uitbreiding mogelijk

5.4 Biometrie en hoog-risico zones

- **Toekomstige integratie:** Het systeem moet voorbereid zijn op integratie van biometrische verificatie (vinger, gezicht, iris, of gelijkwaardig). Biometrie is **geen onderdeel van deze aanbesteding** maar moet technisch mogelijk zijn zonder systeemwijzigingen. Biometrie wordt waarschijnlijk op korte termijn geïmplementeerd, maar niet tijdens dit project.
- **Hardware readiness:** Controllers en software-architectuur moeten biometrische terminals kunnen ondersteunen (multi-factor authentication).
- **Privacy:** Bij toekomstige implementatie dienen biometrische templates op de kaart te worden opgeslagen (Template-on-Card) of in een beveiligde, encrypted database conform AVG. Het is inschrijvers toegestaan hun visie op dit onderwerp toe te lichten en een alternatief te bieden.

Inschrijver beschrijft in offerte:

- Hoe het systeem voorbereid is op toekomstige biometrie-integratie
- Welke biometrische technologieën ondersteund worden
- Impact op architectuur en kosten bij latere toevoeging

5.5 Hardware componenten - indicatieve aantallen

Bijlage I - Locatie- en Assetlijst beschrijft de aantallen en opbouw van het systeem.

Aanvullende hardware:

- UPS-voorzieningen per controllerlocatie (>4 uur autonomie)
- Netwerk (incl. Switching): door EANV geleverd
- Bekabeling nieuwbouw: door Heijmans (Cat6A of gelijkwaardig naar controllers)
- Bekabeling bestaand: hergebruik waar mogelijk, anders door SPIE

5.6 Autonome werking bij netwerkuitval

Het toegangscontrolesysteem is bedrijfskritisch en mag niet uitvallen bij netwerk- of serverstoringen.

Eisen autonome werking per controller:

- **Autonomietijd:** Minimaal 72 uur volledig functioneel zonder netwerkverbinding
- **Lokale autorisaties:** Alle autorisaties lokaal beschikbaar (laatste synchronisatie met server)
- **Lokale besluitvorming:** Controller beslist zelfstandig over toegangsverlening (geen “fail-open”)
- **Event buffering:** Minimaal 50.000 events lokaal opslaan tijdens netwerkuitval
- **Automatisch herstel:** Bij terugkeer netwerkverbinding automatische synchronisatie binnen 5 minuten

Redundantie centrale servers:

- Hot-standby, actief-actief cluster, of gelijkwaardige redundantie-configuratie
- Automatische failover binnen 30 seconden bij server-uitval
- Geen data-verlies bij failover (synchrone replicatie of gelijkwaardig mechanisme)

Monitoring netwerk- en serverstatus:

- Dashboard in SMS toont real-time status van elke controller (online/offline/autonoom)
- Automatische alarmering bij > 5% van controllers offline
- Heartbeat monitoring: elke 30 seconden of sneller

6 Specificaties Video Management Systeem

6.1 Opslag en retentie

- Opname op basis van bewegingsdetectie, continue opname of event-gestuurd.
- Retentie: Minimaal 48 uur, voorkeur 7 dagen, voor alle camera's, tenzij anders gespecificeerd.
- Failover: N+1 redundantie voor opnameservers of gelijkwaardige redundantie-oplossing.

6.2 Integratie met TGC

- "Camera call-up": Bij een geforceerde deur of 'access denied' moet direct het relevante camerabeeld op de operator-scherm verschijnen.
- Bookmarks: TGC-events moeten als bookmarks in de videotijdlijn worden gemarkeerd voor snel terugzoeken.

6.3 Beeldkwaliteit en streams

- Ondersteuning voor H.264 en H.265 compressie of gelijkwaardige moderne codecs.
- Multistreaming (live view op lagere resolutie, opname op hoge resolutie).
- Ondersteuning voor ONVIF Profile S en T of gelijkwaardige open camera-standaarden.

6.4 VMS opslag – capaciteit en retentie

Retentie-eisen:

- Minimaal: 48 uur (wettelijke verplichting)
- Voorkeur: 7 dagen voor operationele doeleinden

Bestaande opname-infrastructuur

Eindhoven Airport beschikt over 10 NVR's met totaal 110 TB bruto opslagcapaciteit. Deze recorders zijn recent vervangen en functioneren naar behoren. Onderstaand een overzicht van de specificaties. Alle servers zijn van AsusTek in ieder geval voorzien van: Windows Server 2019 Standard, 4x1GbE poorten en een Avago MegaRAID 9361-8i controller. In onderstaande tabel staat tevens de installatiedatum per server aangegeven.

Intel Xeon E-2336 CPU @ 2.90 GHz, 6 Cores, 12 Logical Processors	2x8GB 2667 MHz (2 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	11/08/2023
Intel Xeon E-2336 CPU @ 2.90 GHz, 6 Cores, 12 Logical Processors	2x8GB 2667 MHz (2 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	18/06/2025
Intel Xeon E-2336 CPU @ 2.90 GHz, 6 Cores, 12 Logical Processors	2x8GB 2667 MHz (2 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	11/08/2023
Intel Xeon E-2336 CPU @ 2.90 GHz, 6 Cores, 12 Logical Processors	2x8GB 2667 MHz (2 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	18/06/2025
Intel Xeon E-2336 CPU @ 2.90 GHz, 6 Cores, 12 Logical Processors	2x8GB 2667 MHz (2 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	16/08/2023
Intel Xeon E-2336 CPU @ 2.90 GHz, 6 Cores, 12 Logical Processors	2x8GB 2667 MHz (2 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	14/08/2023
Intel Xeon E-2336 CPU @ 2.90 GHz, 6 Cores, 12 Logical Processors	2x8GB 2667 MHz (2 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	11/08/2023
Intel Xeon E-2336 CPU @ 2.90 GHz, 6 Cores, 12 Logical Processors	2x8GB 2667 MHz (2 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	11/08/2023
Intel Xeon E-2336 CPU @ 3.40 GHz, 6 Cores, 12 Logical Processors	2x8GB 2667 MHz (2 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	22/09/2023
Intel Xeon E-2336 CPU @ 2.90 GHz, 6 Cores, 12 Logical Processors	1x8GB 2666 MHz (3 slots empty)	4x4TB = 12 TB (RAID5) + 128GB SSD (OS) (4x 3.5" slots empty)	18/06/2025

Capaciteitsberekening (indicatief):

Resolutie	Aantal	Bitrate (H.265)
2MP (1080p)	150	2 Mbps
4MP (1440p)	150	4 Mbps
8MP (4K)	60	8 Mbps
Totaal	360	1.380 Mbps

Bij motion-based recording (reductiefactor 0,4) en 7 dagen retentie: circa 40 TB netto. De bestaande 110 TB capaciteit is hiervoor voldoende.

Hergebruik bestaande recorders

Hergebruik van de bestaande NVR's is niet verplicht, maar wordt aangemoedigd indien compatibel met het aangeboden VMS. Inschrijver specificeert:

- Compatibiliteit met bestaande recorders (ja/nee, met onderbouwing)
- Eventuele aanpassingen voor integratie
- Alternatief: specificatie nieuwe opslag indien hergebruik niet haalbaar

Opslagarchitectuur

Inschrijver specificeert de gekozen architectuur (centraal/gedistribueerd/hybride). Opdrachtgever heeft voorkeur voor spreiding over minimaal twee serverruimtes (room-redundantie).

6.5 Video Content Analytics - basisvereisten

Het VMS moet minimaal de volgende Video Content Analytics functionaliteiten ondersteunen:

Verplicht voor alle camera's:

- **Motion detection:** Configureerbare detectiezones en gevoeligheid
- **Camera tampering:** Alarm bij afdekking, rotatie of defocussing camera
- **Video loss detection:** Alarm bij uitval videosignaal

Verplicht voor minimaal 50 camera's configureerbaar:

- **Line crossing:** Detectie van personen/voertuigen die een virtuele lijn overschrijden
- **Intrusion detection:** Alarm bij ongeautoriseerde aanwezigheid in gedefinieerde zone
- **Loitering detection:** Alarm bij te lang verblijven in specifiek gebied (configureerbare tijd)

Optioneel (meerwaarde bij gunning op GC2 - Kwaliteit oplossing):

- People counting voor capaciteitsmanagement openbare ruimtes
- License Plate Recognition (ANPR) voor parkeergarage-integratie toekomst
- Facial recognition voor toegangsverificatie toekomst
- Onbeheerde bagage
- People tracking (het volgen van een of meerdere personen door het gebouw op verschillende camera's)
- Andere geavanceerde analytics die operationele waarde bieden

Performance VCA:

- VCA-processing mag maximaal 10% extra bandbreedte/opslag toevoegen
- False positive rate: < 5% (na initiële tuning-periode van maximaal 1 maand)

7 Specificaties Security Management Systeem

7.1 Operator interface en dashboarding

- Intuïtieve GUI voor de meldkamer (Airport Operations).
- Ondersteuning voor meerdere monitoren.
- Dashboard met real-time status van controllers, lezers en deuren (online/offline/storing).

7.2 Alarmmanagement en workflows

- Prioritering van alarmen (bijv. SOS-drukker > Deur te lang open > Technische storing).
- Configureerbare instructie-popups (SOPs) voor operators bij specifieke alarmen.

7.3 Plattegronden en GIS-integratie

- Interactieve plattegronden (import van CAD/GIS formaten zoals DWG, DXF, of gelijkwaardig) waarop iconen van camera's en deuren zijn geplaatst.
- Mogelijkheid om deuren te openen/sluiten en camera's te selecteren direct vanaf de plattegrond.

7.4 Visuele identiteitsverificatie

Het SMS dient een real-time weergave te ondersteunen waarin bij pasaanbieding op een configureerbare lezer automatisch de bijbehorende pasfoto wordt getoond. Eisen:

- Responstijd: pasfoto zichtbaar binnen 2 seconden na pasaanbieding
- Per lezer configureerbaar (in-/uitschakelbaar)
- Beschikbaar op mobiel device (tablet/iPad) voor gebruik door security officers op locatie
- Weergave minimaal: pasfoto, naam, autorisatiestatus, eventuele bijzonderheden

8 Migratie en implementatie

8.1 Fasering

- **Fase 1 (nieuwbouw):** Oplevering Q4 2026.
- **Fase 2 (bestaand):** Baansluiting (februari-juni 2027). Ombouw bestaande lezers en deuren naar het nieuwe systeem.

Mitigatie risico's baansluiting:

1. **Pre-staging:** Controllers voor bestaande terminal worden vooraf geconfigureerd en getest (Factory Acceptance Test) voordat fysieke installatie plaatsvindt tijdens baansluiting.
2. **SPIE beschikbaarheid:** SPIE garandeert volledige bemensing gedurende installatieperiode zonder vakantie-afwezigheid van sleutelpersoneel.
3. **Contingency:** Inschrijver plant minimaal 2 weken buffer binnen baansluiting voor onvoorziene omstandigheden.

8.2 Migratiestrategie en fallback

Kritieke uitgangspunten:

- Er mag **geen operationele downtime** zijn van beveiligingsfunctionaliteit in operationele gebieden tijdens migratie.

Inschrijver beschrijft in implementatieplan:

4. **Transitiescenario:**
 - Hoe wordt overgegaan van oud naar nieuw systeem per gebied/fase?
 - Is tijdelijke parallelle werking oud en nieuw systeem nodig? Zo ja, hoe wordt dit gerealiseerd?
 - Worden er tijdelijk dual-tech lezers ingezet of andere oplossingen?
5. **Data migratie:**
 - Overdracht van minimaal 12 maanden historische events en audit trails van oud naar nieuw systeem. Indien niet mogelijk: wat is de alternatieve strategie?
 - Behoud van volledige audit trail-integriteit (bewijslast wet- en regelgeving)
6. **Fallback procedure:**
 - Gedurende eerste 48 uur na go-live: mogelijkheid tot rollback naar oud systeem indien kritieke issues
 - Procedure voor terugschakelen inclusief data-synchronisatie
 - Testprocedure voor validatie fallback-functionaliteit vóór daadwerkelijke go-live
7. **Training operators:**
 - Indien parallelle werking: training voor beide systemen
 - Duidelijke communicatie over overgangsmomenten per gebied

Hergebruik bekabeling en hardware:

Hergebruik van bekabeling tussen deuren en controllers, tussen controllers (busbekabeling), en elektrische sloten/cilinders is het uitgangspunt in bestaande bouw, mits technisch verantwoord.

Keuringsprotocol hergebruik:

8. Opdrachtnemer voert steekproef uit (minimaal 20% van alle aansluitingen) in samenwerking met SPIE
9. Objectieve afkeurcriteria:
 - Bekabeling: isolatieweerstand < 50 MOhm, geen Cat5e/6 kwaliteit, zichtbare beschadiging
 - Sloten: mechanische slijtage, veroudering >15 jaar, niet-functionerend
10. Afwijkingen >20%: volledige vervanging categorie via SPIE (kosten EANV)
11. Afwijkingen <20%: gerichte vervanging (kosten Opdrachtnemer)
12. Eindverantwoordelijkheid werking systeem: altijd Opdrachtnemer Perceel 1

8.3 Oplevering en testen

Commissioningplan (verplichte deliverable):

Opdrachtnemer dient binnen 4 weken na gunning een gedetailleerd Commissioningplan ter goedkeuring aan Opdrachtgever voor te leggen, in samenwerking met Opdrachtnemer Perceel 2 voor interface-testen. Dit plan moet minimaal bevatten:

FAT-procedures (Factory Acceptance Test):

- Testopstelling bij Opdrachtnemer (laboratorium of testomgeving)
- Per subsysteem (TGC/VMS/SMS) alle functionele eisen testen
- Performance test: simulatie van 1000 simultane toegangen
- Integratie test: PIAM → USP provisioning en event feedback (zie TPvE Deel 3)
- Acceptatiecriteria: 0 critical defects, maximaal 5 major defects
- Aftekenformulieren per testonderdeel

SAT-procedures (Site Acceptance Test):

- Testmethode per deur: open/close cyclus, alarm-test, video call-up, status feedback
- Steekproef: minimaal 20% van alle deuren (minimum 50 deuren)
- Voor SRA-deuren: 100% individuele test verplicht
- Camera-test: beeldkwaliteit, opname, archivering, terugzoeken
- Acceptatiecriteria: >95% geslaagd, 100% voor SRA-deuren
- Non-conformance register en herstel-procedure

SIT-procedures (Site Integration Test):

- End-to-end scenario's conform TPvE Deel 3, paragraaf 5.1
- Minimaal 10 concrete user stories die operationele realiteit weerspiegelen, bijvoorbeeld:
 - "Catering truck arriveert 04:00 zonder vooraanmelding, chauffeur heeft geldige pas SRA, toegangspoort moet binnen 2 seconden openen"
 - "Operator markeert deur als 'defect' in SMS, automatische alarmering naar onderhoud binnen 30 seconden, status zichtbaar op dashboard"
 - "Bezoeker presenteert pas bij SRA-overgang zonder geldige autorisatie, access denied + automatische camera call-up + logging binnen 3 seconden"
- Aanvullende scenario's:
 - BMI failsafe test (zonder echte brand, via testsignaal)
 - PIAM offboarding test: persoon verwijderen in PIAM, pas geblokkeerd binnen 60 seconden op fysieke deur
 - PIAM-USP reconciliation test: kunstmatige discrepantie creëren, detectie en rapportage binnen dagelijkse batch
 - Performance test: 100 simultane deuropeningen binnen 30 seconden zonder vertragingen
- Acceptatiecriteria: alle scenario's succesvol, maximaal 2 minor defects

Testrapportage:

- Per testonderdeel: testdatum, testers, resultaten, gedetecteerde defects en resoluties
- Fotodocumentatie installatie (before/after)
- As-built tekeningen en documentatie

Afkeur en hertest:

- Bij afkeuring van een testonderdeel: herstelperiode maximaal 2 weken
- Hertest op kosten Opdrachtnemer
- Na 2x afkeuring: escalatie naar projectmanagement voor aanpassing planning

Definitieve oplevering:

- Pas na goedkeuring van alle testresultaten door Opdrachtgever
- Inclusief ondertekening opleverprotocol
- Start garantieperiode en SLA-verplichtingen

9 Training en kennisoverdracht

Opdrachtnemer verzorgt de volgende trainingen als onderdeel van de implementatie:

- **Training beheerders:** minimaal 3 dagen — configuratie, beheer en troubleshooting van het Unified Security Platform.
- **Training operators:** minimaal 2 dagen — bediening van het SMS/PSIM, inclusief alarmafhandeling en monitoring.
- **Training eindgebruikers:** minimaal 1 dag — gebruik van het badge center en self-service functies.
- **Training SPIE-medewerkers:** eerstelijns onderhoud en storingdiagnose. De duur wordt in overleg met Opdrachtgever vastgesteld.

10 Duurzaamheidseisen

Conform de Handleiding Duurzaamheid van Eindhoven Airport en de Maatschappelijk Verantwoord Inkopen-criteria (MVI) van de Rijksoverheid, gelden de volgende eisen:

- **E1. Energieverbruik controllers:** Controllers verbruiken in operationele stand maximaal 15W per unit.
- **E2. Levensduur kaartlezers:** Kaartlezers hebben een gegarandeerde levensduur van minimaal 10 jaar bij normaal gebruik, ondersteund door een vervangingsgarantie van de fabrikant.
- **E3. Recyclebaarheid hardware:** Minimaal 85% van het gewicht van de aangeboden hardware (controllers, lezers, bekabeling) is recyclebaar conform de WEEE-richtlijn.
- **E4. Verpakkingsmateriaal:** Verpakkingsmateriaal is 100% recyclebaar of biologisch afbreekbaar. Piepschuim (EPS) is niet toegestaan.
- **E5. Herkomst en transport:** Inschrijver geeft in de Compliance Matrix (Bijlage M) aan wat de productieland(en) van de kerncomponenten zijn en welke maatregelen zijn genomen om de CO₂-voetafdruk van transport te beperken.