Annex 3.1: PROGRAMMA VAN EISEN

Generieke RAS (Remote Access Solution) Dienst

Versie:	1.0
Datum:	29-05-2026
Status:	Definitief
Classificatie:	Openbaar
Auteur:	ProRail ICT I&O

Inhoudsopgave

1. Inleiding

1.1. Doel van dit document

Dit Programma van Eisen (PvE) beschrijft de functionele, non-functionele security en organisatorische eisen voor de aanschaf van een Generieke RAS Dienst (Remote Access Service) voor ProRail. Het document dient als basis voor de aanbesteding en selectie van een leverancier die een oplossing kan bieden voor veilige externe en ProRail toegang tot OT- en IT-systemen binnen de ProRail infrastructuur.

De Generieke RAS Dienst wordt in het Programma van Eisen verder ‘de Dienst’ genoemd.

1.2. Scope en afbakening

De aanbesteding betreft de vervanging van verschillende digitale, verouderde en maatwerk, toegangsdiensten die in gebruik zijn bij ProRail. De Dienst moet veilige externe toegang bieden tot OT-systemen in de stations- en spoorinfrastructuur en tot centrale IT-systemen. Dit wordt verder toegelicht in hoofdstuk 2 Context.

Producten / Diensten	Toelichting
Levering van een Remote Access dienst	Remote Access dienst voor de test/acceptatie en productie omgevingen van ProRail
Implementatie van de dienst	Implementatie van de Dienst in de ProRail test/acceptatie en productie omgevingen
Migratie naar de Dienst	Migratie van maximaal vijf (5) standaard gebruikers van de test/acceptatie en productie omgevingen naar de Dienst
Beheer van de Dienst	Het beheer van de Dienst gericht op de operatie, techniek, life cycle management, security en functionaliteit en daarnaast het ondersteunen van veranderingen als gevolg van lifecycle management van ProRail systemen.
Integratie IAM	Integratie met bestaande en toekomstige identity- en accessmanagement-systemen (IAM) van ProRail
Rapportage en logging	Rapportage- en loggingfunctionaliteit voor toegangsverzoeken, authenticatiepogingen, afwijkende patronen en standaard gebruik van de Dienst op basis van OpenTelemetry en geïntegreerd met de observability-tool van ProRail.
Portal functie	Portal voor governance en beheer van gebruikers en beheerders per gebruikstoepassing en op meerdere administratieve niveaus
Toegangsbeheer	Governance op toegangsbeheer, ondersteund door gebruik van IAM.

Consultancy	Consultancy en training op verzoek van ProRail

Tabel 1 Scope van de aanbesteding

1.3. Buiten scope

De volgende onderdelen vallen expliciet buiten de scope van deze aanbesteding:

Producten / Diensten	Toelichting
ProRail IT infrastructuur	Installatie, beheer en onderhoud van ***onderliggende*** netwerkinfrastructuur en connectiviteit wat nodig is voor de Dienst (valt onder verantwoordelijkheid van ProRail ICT)
ProRail Asset infrastructuur	Software, hardware, infrastructuur wat benodigd is om de IT- en OT-assets te beheren (valt onder verantwoordelijkheid van ProRail of derden)

Tabel 2 Buiten scope van de aanbesteding

1.4. Leeswijzer

Dit document is als volgt opgebouwd:

Hoofdstuk	Inhoud
1. Inleiding	Doel, scope en leeswijzer
2. Context	Organisatie, huidige situatie, gewenste situatie, omvang
3. Eisen	Functionele en niet-functionele eisen en dienstverlening
4. Exit-strategie en Transitie	Exit en Transitie
5. Implementatie	Implementatie en migratie
6. **Fout! Verwijzingsbron niet gevonden.**	Afkortingen, definities, referentiedocumenten

2. Context

2.1. ProRail organisatie

ProRail is de beheerder van de Nederlandse spoorweginfrastructuur en is verantwoordelijk voor het beheer, onderhoud en de uitbreiding van het spoornetwerk. Als beheerder van deze kritieke nationale infrastructuur valt ProRail onder de NIS2-richtlijn (EU 2022/2555) als essentiële entiteit in de transportsector.

De stations- en spoorinfrastructuur omvat diverse operationele technologie (OT) systemen die 24/7 beschikbaar moeten zijn voor veilig en betrouwbaar treinverkeer. Remote toegang tot deze systemen is essentieel voor efficiënt beheer en snelle incidentrespons, maar stelt hoge eisen aan beveiliging gezien de kritieke aard van de infrastructuur. ProRail ICT heeft veel systemen om het treinverkeer veilig en betrouwbaar te laten verlopen en om (data-gedreven) onderhoud, planning en communicatie tussen alle betrokken partijen te ondersteunen. Daarnaast zijn er de ICT-systemen voor de bedrijfsvoering.

De belangrijkste afdelingen voor de Dienst zijn:

ICT I&O (Infrastructuur & Operatie)

De afdeling ICT I&O levert kwalitatieve, schaalbare en toekomstbestendige ICT Infrastructuur & Operations diensten die de continuïteit van de organisatie waarborgen en bijdragen aan een veilige, wendbare digitale werkomgeving. De dienstverlening omvat onder meer het beheer, de monitoring en het lifecycle management van systemen, netwerken, opslag en clouddiensten, evenals proactieve ondersteuning en incidentafhandeling. De leverancier werkt volgens best practices op het gebied van security, compliance en IT-servicemanagement, en zorgt voor transparante rapportage, meetbare prestaties en een hoge mate van beschikbaarheid.

CSD (Centrale Service Desk)

Binnen ICT I&O valt ook de CSD. De CSD is een centraal georganiseerde Service Desk die fungeert als hét single point of contact voor alle ICT gerelateerde vragen, verzoeken en incidentmeldingen. De CSD biedt toegankelijke, deskundige en klantgerichte ondersteuning, waarbij tickets efficiënt worden geregistreerd, geprioriteerd en afgehandeld conform overeengekomen servicelevels. Door gebruik te maken van gestandaardiseerde processen, actuele kennisdatabases en proactieve monitoring, draagt de CSD bij aan een hoge mate van continuïteit en gebruikerstevredenheid. De dienstverlening omvat zowel eerstelijns ondersteuning als de regie op escalaties naar tweede- en derdelijns teams.

Gebruikerskant

De afdelingen die gebruik gaan maken van de Generieke RAS dienst zijn:

Asset Management (AM) zorgt voor strategisch en integrale uitbesteding van beheeractiviteiten van alle Spoorse assets en gerelateerde bedrijfsvoeringsmiddelen gedurende hun volledige levenscyclus.

Stations organisatie beheert, ontwikkelt en exploiteert stationsgebieden en reizigersvoorzieningen, met focus op veiligheid, toegankelijkheid en een prettige klantbeleving.

ERTMS programma (European Rail Traffic Management System) is het organisatieonderdeel dat het Europese treinbeveiligingssysteem ERTMS realiseert.

HFM (Human Facility Management) verzorgt de facilitaire dienstverlening, zoals huisvesting, services en werkplekomgevingen, zodat medewerkers optimaal kunnen werken.

ICT Logistiek, ICT A&B (Assets & Bedrijfsvoering) en ICT I&O leveren en beheren alle digitale systemen, applicaties, infrastructuur en beveiliging die nodig zijn om de bedrijfsvoering en operationele processen van ProRail te ondersteunen.

2.2. Huidige situatie (IST)

Op dit moment zijn er meerdere functioneel vergelijkbare digitale toegangsdiensten. Dit zijn toegangsdiensten zoals VPN verbindingen (Virtual Private Network), Fortinet toegangsmethoden en een tijdelijke RAS (Remote Access Service) waar enkele gebruikers binnen ProRail (Stations-, AM- en ERTMS afdelingen) gebruik van maken met kleine aantallen assets. ProRail wil deze type verbindingen vervangen voor een moderne en veilige Generieke RAS dienst. Zodra de Dienst actief is en de gebruikers gemigreerd zijn, ruimt ProRail de huidige toegangsdienst(en) op.

2.3. Gewenste situatie (SOLL)

De gewenste situatie na implementatie van de Dienst. Zie Figuur 1.

2.3.1. Functioneel

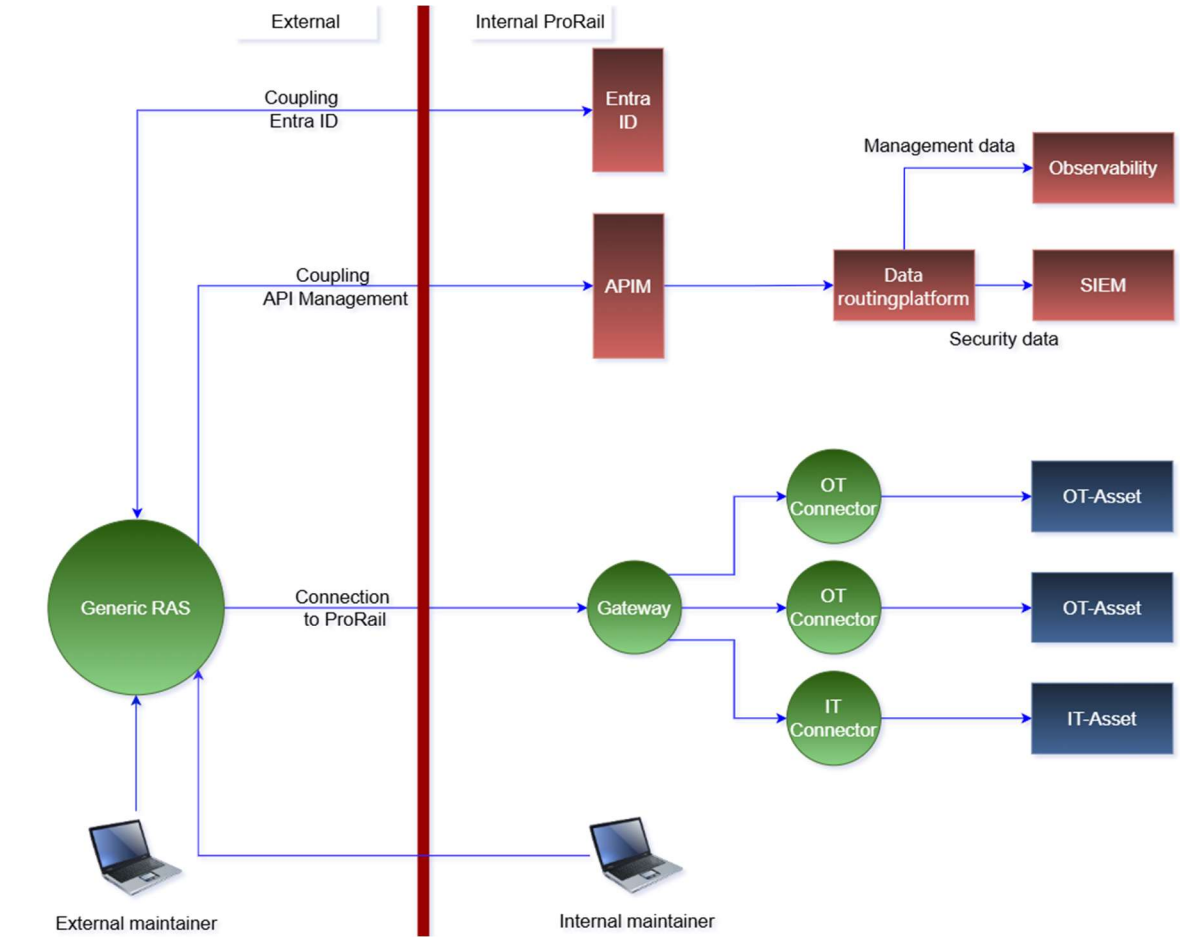
- Veilige, gecontroleerde toegang tot OT- en IT-systemen voor geautoriseerde beheerders en beheerpartijen van externe en ProRail gebruikers;
- Browser based toegang voor standaard protocollen;
- Gedelegeerd beheermodel voor toegang;
- Volledige audit trail op identificatie niveau voor alle toegangsactiviteiten;
- Session recording voor analyse achteraf.

2.3.2. Technisch

- Dienst in test/acceptatie omgeving en productie omgeving;
- Integratie met Microsoft Entra ID (SSO en MFA)
- Passend in het huidige ProRail netwerk;
- Voldoen aan Data residency en Cybersecurity regelement.

2.3.3. Organisatorisch

- Eenduidige beheerverantwoordelijkheid bij leverancier;
- 24/7 support dienstverlening;
- Duidelijke SLA met meetbare KPI's.



Figuur 1: Architectuur van de Dienst en ProRail omgeving

Legenda:

- Rood: componenten van ProRail
- Groen: componenten van de Dienst
- Blauw: OT/IT Assets
- Links van de rode streep = Extern
- Rechts van de rode streep = Intern

Figuur 1 geeft een beeld van hoe de Generieke RAS eruit kan komen te zien.

De rode componenten zijn ProRail-componenten waarop een leverancier van de Dienst aansluit.

De groene componenten zijn onderdelen van de Dienst. Deze componenten zijn deels binnen de ProRail-omgeving beschikbaar en deels bij de leverancier.

De blauwe componenten zijn bestaande assets die met de Dienst worden ontsloten. Dit zijn OT-componenten, maar ook IT- componenten. De OT- en IT-componenten moeten van elkaar gescheiden zijn om te voorkomen dat problemen met IT ook impact hebben op OT.

Met managed en unmanaged devices kan veilige toegang tot OT en IT worden verkregen door externe en interne beheerders. Een interne beheerder gebruikt daarbij hetzelfde veilige pad als een externe beheerder.

2.4. Omvang

Deze paragraaf beschrijft het aantal verwachte domeinen, beheerpartijen, gebruikers (Named user) en de mogelijke groei van het gebruik van de Dienst voor de productieomgeving. Het eerste gebruik zal voornamelijk in het OT domein zijn.
Op dit moment gebruiken meerdere afdelingen de tijdelijke RAS en deze gebruikers migreren zo snel mogelijk naar de Dienst. Dit is een onderdeel van het implementatie- en migratietraject van de Dienst.

Kenmerk	Initieel	Groeimodel (8 jaar)
Domeinen	2	8
Externe partijen	5	50
Named users	50	300

Tabel 3: Omvang van de Dienst (Schatting)

De genoemde gebruiks- en volumeschattingen dienen uitsluitend ter indicatie; hieraan kunnen door leverancier geen rechten of aanspraken worden ontleend.

3. Eisen

Dit hoofdstuk beschrijft de eisen die van toepassing zijn op de Dienst en de leverancier.

Op dit moment zijn er binnen ProRail veel verschillende systemen in gebruik om toegang te krijgen tot OT-systemen, en dit aantal neemt nog steeds toe. De oplossingen die hiervoor worden gebruikt zijn kwetsbaar op het gebied van cybersecurity, verouderd, vaak specifiek ontworpen voor één type asset en sluiten onvoldoende aan op de standaarden van ProRail. Dit leidt tot verhoogde cybersecurityrisico's, beperkte beheersbaarheid en een toenemende beheerlast.

Met de Dienst stellen we een dienst beschikbaar voor het verbinden van externe partijen en interne medewerkers met OT- en IT-systemen. Hiermee kunnen systemen in het veld worden beheerd en onderhouden zonder dat fysieke aanwezigheid op locatie noodzakelijk is. De Dienst is 24/7 beschikbaar, zodat onderhoud en beheer ook buiten kantooruren kan plaatsvinden.

De Dienst is een softwarematige, ZTNA-gebaseerde oplossing. IT- en OT-systemen zijn hierbij logisch van elkaar gescheiden, vanwege de grote verschillen in lifecyclemanagement (LCM) en de aanwezigheid van specifieke kwetsbaarheden binnen OT-omgevingen.

Met de Dienst creëren we een veilige, gecontroleerde en eenvoudige toegangspoort tot assets. Daarbij vervangen we zoveel mogelijk bestaande oplossingen. De Dienst wordt gekoppeld aan ProRail Entra ID, zodat gebruikers met een ProRail-account kunnen inloggen en de juiste autorisaties krijgen.

Het gebruik van de Dienst wordt gemonitord. Gegevens over het gebruik worden via een API aan ProRail beschikbaar gesteld, zodat onder andere het SOC hiervan gebruik kan maken. De leverancier stelt een platform beschikbaar waarin actuele informatie over het gebruik van de Dienst inzichtelijk is. Dit platform biedt tevens de mogelijkheid om gebruikers lokaal te registreren, indien dit noodzakelijk is.

Met de Dienst verbeteren we de cybersecurity en zetten we een belangrijke stap richting de doelstellingen van NIS2 en de CBW. De Dienst biedt uitgebreide mogelijkheden voor het monitoren van verbindingen en het controleren van gebruikers.

De leverancier levert de Dienst en installeert de benodigde componenten binnen het ProRail-netwerk en/of de Cloud omgeving. Na installatie is de leverancier verantwoordelijk voor de instandhouding en het beheer van de Dienst. Daarnaast verzorgt de leverancier het onboarden van systemen.

Voor gebruikers wordt een webportal beschikbaar gesteld waarmee toegang tot systemen kan worden verkregen. Het is hierbij niet nodig om een applicatie of tool te installeren op het device dat wordt gebruikt om in te loggen.

Indien onderhoud noodzakelijk is, stelt de leverancier ProRail hier tijdig van op de hoogte. Daarnaast wordt ProRail actief geïnformeerd over (potentiële) cybersecurityrisico's. De leverancier zorgt voor actuele en volledige documentatie van de Dienst, levert adequate ondersteuning en draagt zorg voor een goede migratie en eventuele re-transitie wanneer de dienstverlening tot een eind komt.

3.1. Functionele eisen

Dit hoofdstuk beschrijft de functionele eisen aan de Dienst.

3.1.1. Kernfunctionaliteit

De kernfunctionaliteit omvat de basiscapaciteiten om, met niet door ProRail beheerde devices, veilige externe en ProRail toegang te bieden tot ProRail-assets (OT- en IT-systemen). De Dienst bestaat uit een test/acceptatie omgeving en een productieomgeving. De ProRail test/acceptatie omgeving is opgebouwd in het ProRail Test Centrum in Amersfoort.

Eis 1. Productieomgeving
De leverancier moet een werkende Dienst leveren en onderhouden voor de productieomgeving van ProRail.

Eis 2. Test/acceptatie omgeving
De leverancier moet een functioneel identieke, werkende Dienst leveren en onderhouden voor de test/acceptatie omgeving.
In overleg met ProRail kan de test/acceptatie omgeving zo ingericht worden dat aan de doelstellingen van functioneel, identieke Dienst wordt voldaan.

Eis 3. Toegangsportal
De Dienst moet een secure toegangsportal bieden voor het aanmaken en beheren van assets en gebruikers.

3.1.2. Toegangsbeheer

Eis 4. Externe en ProRail gebruikers
Externe en ProRail gebruikers moeten via Entra ID op de RAS omgeving toegevoegd kunnen worden.

Eis 5. Asset owner finale beslissing
De Dienst moet waarborgen dat de asset owner te allen tijde de finale beslissing heeft over het verlenen van toegang tot een asset. Geen toegang kan worden verleend zonder expliciete goedkeuring van de asset owner.

Eis 6. Tijdgebonden toegang
De Dienst moet tijdgebonden toegang ondersteunen waarbij toegangsrechten automatisch verlopen na een geconfigureerde periode en op een specifiek tijdstip.

Eis 7. Verplichte MFA
De Dienst moet Multi-Factor Authenticatie (MFA) verplicht stellen voor alle gebruikers. Toegang zonder MFA is niet toegestaan.

Eis 8. MFA methodes
De Dienst moet minimaal de volgende MFA methodes ondersteunen: authenticator app (TOTP) en push notificatie. SMS als tweede factor is niet toegestaan.

Eis 9. Hardware token voor beheerders
De Dienst moet voor beheeraccounts met verhoogde rechten MFA via hardware token (FIDO2/PKI) ondersteunen als afdwingbare beleidsinstelling.

Eis 10. Generieke accounts
Gedeelde of generieke accounts zijn niet toegestaan.

Eis 11. Single Sign-On via Entra ID
De Dienst moet Single Sign-On (SSO) ondersteunen via Microsoft Entra ID (voorheen Azure AD) met SAML 2.0 of OpenID Connect.

Eis 12. Entra ID groepen synchronisatie
De Dienst moet Entra ID groepen kunnen synchroniseren en gebruiken voor het toekennen van toegangsrechten, zodat wijzigingen in groepslidmaatschap automatisch worden doorgevoerd.

Eis 13. Role-Based Access Control
De Dienst moet Role-Based Access Control (RBAC) ondersteunen, waarbij gebruikersrechten worden bepaald door toegewezen rollen in plaats van individuele permissies.

Eis 14. Conditional Access ondersteuning
De Dienst moet Entra ID Conditional Access policies respecteren en ondersteunen, zodat bestaande ProRail security policies kunnen worden toegepast.

Eis 15. Gedelegeerd beheermodel
De Dienst moet een gedelegeerd beheermodel ondersteunen waarbij meerdere beheerders met verschillende bevoegdheden kunnen worden aangewezen per Domein of Asset groep.

Eis 16. Delegatie authenticatiebevoegdheid
De Dienst moet het delegeren van authenticatiebevoegdheid aan vertrouwde externe partijen ondersteunen, zodat externe beheerpartijen hun eigen gebruikers kunnen authenticeren via hun eigen Identity Provider.

Eis 17. User Interface
De Dienst moet een gebruikersinterface aanbieden die volledig voldoet aan WCAG 2.1 niveau AA conform EN 301 549 of vergelijkbaar.

Eis 18. Configureerbare time-out
De Dienst moet een configureerbare sessie time-out ondersteunen per Asset, Asset groep of Domein. Bij inactiviteit wordt de sessie automatisch beëindigd.

Eis 19. Sessie herstel
De Dienst moet automatisch sessieherstel ondersteunen bij een onderbreking van maximaal vijf minuten van de netwerkverbinding, zonder dat de gebruiker opnieuw moet authenticeren.

Eis 20. Actieve sessie beëindiging
De Dienst moet beheerders de mogelijkheid bieden om actieve sessies van gebruikers direct te beëindigen in geval van een beveiligingsincident of operationele noodzaak.

Eis 21. Gelijktijdige sessies
De Dienst moet het maximum aantal gelijktijdige sessies per gebruiker kunnen limiteren tot één (1) sessie per gebruiker om misbruik van accounts te voorkomen.

3.1.3. Asset onboarding

Eis 22. Asset groepering
De Dienst moet het groeperen van assets ondersteunen in logische domeinen en subdomeinen, waarbij toegangsbeleid kan worden toegepast op groepsniveau.

Eis 23. Onboarding zonder impact bestaande operatie
De Dienst moet het toevoegen van nieuwe assets, asset owners en beheerpartijen ondersteunen zonder impact op de bestaande operationele verbindingen.

Eis 24. Geen netwerkwijzigingen bij onboarding
De Dienst moet wijzigingen in de gebruikers- en assetkant uitvoeren zonder configuratiewijzigingen aan het ProRail netwerk.

Eis 25. Bulk onboarding via een API
De Dienst moet bulk onboarding van assets ondersteunen via een API (aansluitend op de APIM van ProRail, zie Eis 45, zodat grote aantallen assets geautomatiseerd kunnen worden toegevoegd, geconfigureerd of aangepast..

3.1.4. Protocollen

De Dienst moet diverse protocollen ondersteunen voor toegang. Onderscheid wordt gemaakt tussen standaard protocollen (browser based) en niet standaard, applicatiespecifieke protocollen.

Eis 26. Browser based
De Dienst moet via een browser based interface minimaal de volgende protocollen ondersteunen: RDP, VNC, SSH, HTTPS en HTTP.

Eis 27. Agentless voor standaard protocollen
De Dienst moet voor de standaard protocollen (RDP, SSH, VNC, HTTPS, HTTP) agentless werken, waarbij geen software-installatie op de doelsystemen (assets) vereist is.

Eis 28. Aanvullende protocollen
De Dienst moet uitbreidbaar zijn met aanvullende protocollen noodzakelijk voor OT applicaties.

Eis 29. Ondersteuning niet standaard protocollen
De Dienst moet een secure, centraal beheerde jump-server als fallback ondersteunen.

3.1.5. Session management

Sessie management is essentieel voor zowel de gebruikerservaring als voor audit en compliance doeleinden.

Eis 30. Sessie opname
De Dienst moet alle sessies kunnen opnemen (session recording) voor analyse achteraf. De opname omvat minimaal: scherminhoud, toetsaanslagen en muisacties.

Eis 31. Sessie recording
De Dienst moet session recording kunnen configureren per asset, asset groep en domein, zodat opname kan worden in- of uitgeschakeld op basis van risicoprofiel.

Eis 32. Opslag sessie-opnames
De Dienst moet sessie-opnames ondersteunen. De retentieperiode moet configureerbaar zijn per domein of asset groep.

Eis 33. Back-up sessie-opnames
De Dienst moet minimaal wekelijks een back-up maken van sessie-opnames en autorisatiematrix.

Eis 34. Doorzoekbare opnames
De Dienst moet sessie-opnames doorzoekbaar maken op basis van metadata (gebruiker,, asset, tijdstip) en indien mogelijk op basis van inhoud (uitgevoerde commando's).

Eis 35. Volledige audit trail
De Dienst moet een volledige audit trail bijhouden van alle toegangsactiviteiten, waarbij minimaal wordt geregistreerd: wie (gebruiker), wanneer (timestamp), welke asset, welk protocol, succesvolle authenticatie, sessieduur en bron-IP. Gebruikersacties moeten traceerbaar zijn naar een individuele gebruiker.

Eis 36. Audit trail gegevens
De leverancier moet de gegevens van de audit trial beschikbaar stellen aan ProRail.

Eis 37. Onveranderbare logs
De Dienst moet waarborgen dat audit logs niet kunnen worden gewijzigd of verwijderd.

Eis 38. Log export naar SIEM
De Dienst moet audit logs kunnen exporteren naar ProRail SIEM (Security Information and Event Management).

Eis 39. Real-time dashboard
De Dienst moet een real-time dashboard bieden met minimaal: aantal actieve sessies, aantal geregistreerde gebruikers, aantal aangesloten assets, en recente toegangsactiviteiten.

Eis 40. Toegangsrapportage
De Dienst moet rapportages kunnen genereren van alle toegangsactiviteiten over een configureerbare periode, met filters op gebruiker, asset en tijdsperiode.

Eis 41. Export functionaliteit
De Dienst moet rapportages kunnen exporteren in gangbare formaten (minimaal CSV en PDF) voor verdere verwerking of archivering.

3.1.6. API en integraties

De Dienst moet via API's integreren met bestaande ProRail systemen voor automatisering en centrale monitoring.

Eis 42. REST API
De Dienst moet een REST API bieden die compatible is met de ProRail APIM, voor alle functionele onderdelen, inclusief gebruikersbeheer, asset management, toegangsbeheer en rapportage.

Eis 43. Integratie (1)
De Dienst moet kunnen integreren met ProRail's monitoring en logging API's door middel van Open Telemetry.

Eis 44. Integratie (2)
De Dienst moet kunnen integreren met ProRail's service management systeem (OTSM – OpenText Service Management).

Eis 45. REST API Management
De REST API, van de leverancier, moet aansluiten bij API Management van ProRail. Het APIM is gebaseerd op onderstaande Design Rules:

- NLGov REST API Design Rules: NLGov REST API Design Rules 2.1.0
- Forum Standaardisatie - REST-API Design Rules: REST-API Design Rules | Forum Standaardisatie

Eis 46. API documentatie
De Dienst moet volledige API documentatie, in OpenAPI formaat, bieden die te allen tijde actueel en beschikbaar is, inclusief voorbeelden en foutafhandeling.

Eis 47. API Bulk operaties
Bulk operaties moeten door de Dienst worden geaccepteerd als asynchrone taken en de Dienst moet via de API inzicht geven in de voortgang en voltooiing van deze taken (minimaal: gestart, in uitvoering, voltooid, mislukt).

3.2. Non-functionele eisen

Dit hoofdstuk beschrijft de non-functionele eisen aan de Dienst. Deze eisen specificeren de kwaliteitsattributen van de Dienst, waaronder performance, beschikbaarheid, beveiliging en schaalbaarheid.

3.2.1. Performance

De performance van de Dienst is zeer belangrijk voor een goede gebruikerservaring bij de toegang tot de OT- en IT-systemen.

Eis 48. UI response tijd
De gebruikersinterface van de Dienst moet een response tijd hebben van maximaal één (1) seconde voor alle standaard gebruikersacties, gemeten vanaf het ProRail netwerk.

Eis 49. Sessie opbouwtijd
De Dienst moet een remote sessie kunnen opbouwen binnen vijf (5) seconden na succesvolle authenticatie, exclusief netwerk latency naar de doelasset. We meten dit met een standaard ProRail laptop en een OT-systeem in een domein, via het internet, waarbij bandbreedte naar de dienst geen limiterende factor is.

Eis 50. Sessie latency
De Dienst moet de toegevoegde latency beperken tot maximaal 250 milliseconden van gebruikersconnecties, bovenop de inherente netwerk latency tussen gebruiker en doelsysteem.

Eis 51. Grafische sessie kwaliteit
De Dienst moet voor grafische sessies (RDP, VNC) een vloeiende weergave bieden met minimaal tien (10) frames per seconde bij standaard beheernetwerk connectiviteit (>10 Mbps).

Eis 52. Gelijktijdige sessies
De Dienst moet minimaal voor 10% van het aantal geregistreerde gebruikers een gelijktijdige actieve sessies ondersteunen zonder merkbare degradatie van performance.

3.2.2. Security

De beveiligingseisen waarborgen dat de Dienst voldoet aan de hoge security standaarden die gelden voor kritieke infrastructuur.

Eis 53. Zero Trust architectuur
De Dienst moet gebaseerd zijn op een Zero Trust Network Access (ZTNA) architectuur.

Eis 54. Purdue Model
De RAS-oplossing van de leverancier moet een Purdue-gebaseerde zoneringsarchitectuur ondersteunen (waaronder een OT-DMZ).

Eis 55. Gescheiden opslag
De leverancier moet ProRail data logisch gescheiden opslaan van data van andere klanten. Er mag geen mogelijkheid bestaan voor andere klanten om toegang te krijgen tot ProRail data.

Eis 56. Security advisories
De leverancier moet ProRail proactief informeren over security vulnerabilities die de Dienst raken, inclusief CVE-nummers, impact assessment en mitigatiemaatregelen.

Eis 57. Geen offensief cyberprogramma landen
De leverancier mag niet gevestigd zijn in, of beheer uitvoeren vanuit, een land met een offensief cyberprogramma gericht tegen Nederlandse belangen conform de actuele AIVD dreigingsanalyse.

Eis 58. Transport encryptie
De Dienst moet alle communicatie end-to-end beveiligen met de geldende TLS standaard van de Internet Engineering Task Force (IETF).

Eis 59. End-to-end encryptie
De Dienst moet end-to-end encryptie bieden op verbindingsniveau tussen de gebruiker tot en met de connector.

Eis 60. Cipher suites
De Dienst moet uitsluitend cipher suites gebruiken die door het NCSC als "Goed" zijn gekwalificeerd.

Eis 61. Brute force bescherming
De Dienst moet bescherming bieden tegen brute force aanvallen door middel van account lockout na maximaal vijf (5) mislukte inlogpogingen en progressieve vertraging.

Patching:
Uitgangspunt voor ProRail is dat kwetsbare software tijdig dient te worden voorzien van security patches. Leveranciers moeten voldoen aan de ProRail voorwaarden.

Eis 62. Laatste patches
De Dienst moet voorzien zijn van de laatste security patches.

Eis 63. Kwetsbaarheden
Leverancier moet bij het bekend worden van security kwetsbaarheden direct bij de CSD een security incident aan laten maken en conform het security incidentbeheer proces dit op te pakken. Indien van toepassing op ProRail leidt dit tot het aanbrengen van mitigerende beveiligingsmaatregelen, zo mogelijk installatie van security patches.

Eis 64. CVE's
Op basis van urgentie moet de leverancier een CVE binnen 72 uur (critical) oplossen. Niet critical CVE's moeten binnen één maand opgelost zijn.

Eis 65. Fasering
Het installeren van (security) patches/updates dient gefaseerd doorgevoerd te worden in eerst de test/acceptatie en productieomgeving.

3.2.3. Certificaten

Eis 66. TLS richtlijn
De leverancier conformeert zich aan het vigerend TLS-richtlijn van het Nationaal CyberSecurity Center (NCSC), NCSC - Transport Layer Security (TLS) richtlijnen 2025-05, waarbij de protocollen en instellingen van het beveiligingsniveau GOED of VOLDOENDE moeten zijn.

Eis 67. Maximale geldigheidsduur certificaat
De maximale geldigheidsduur van de certificaten moet voldoen aan de richtlijnen van CA/Browser forum (CA/Browser Forum - Certificate Issuers, Certificate Consumers, and Interested Parties Working to Secure the Web). De geldigheidsduur wordt de komende jaar afgebouwd volgend onderstaande planning:
- 398 dagen tot 15 maart 2026
- 200 dagen tot 15 maart 2027
- 100 dagen tot 15 maart 2029
- Vanaf 15 maart 2029: 47 dagen

Eis 68. Browser root stores
De certificaten moeten opgenomen zijn in de gangbare browser root stores. Om ongewenste foutmeldingen te voorkomen dienen de certificaten inclusief de chain of trust opgenomen te zijn in de root stores van de gangbare browsers.

Eis 69. ProRail certificaten gebruik
De Dienst moet gebruik maken van de interne ProRail Public Key Infrastructure(PKI) voor interne ProRail endpoints.

Eis 70. Cryptografische sleutels
Leverancier hanteert voor het beheer van cryptografische sleutels, waaronder certificaten, de standaard ISO 11770 Framework (ISO/IEC 11770-1) en andere relevantie gedeelten of een gelijkwaardige internationale standaard voor key management (sleutelbeheer) in informatiebeveiliging.

3.2.4. Schaalbaarheid

De Dienst moet kunnen meegroeien met de toenemende behoefte aan remote access binnen ProRail.

Eis 71. Schaalbaarheid
De Dienst dient mee te groeien in het aantal assets, gebruikers en domeinen zoals uitgevraagd in de Annex 5.1 Aanbiedingsbegroting.

3.2.5. Implementatie en onderhoudbaarheid

De Dienst moet goed implementeerbaar, onderhoudbaar en inpasbaar zijn met minimale impact op de ProRail organisatie en operatie.

Eis 72. Generieke Dienst
De Dienst moet functioneren zonder vereiste aanschaf, installatie of gebruik van vendor specifieke netwerkapparatuur of diensten van derden.

Eis 73. ProRail infrastructuur
Componenten van de Dienst, die noodzakelijk op ProRail infrastructuur moeten landen, moeten geïmplementeerd worden op de generieke Cloud infrastructuur (Azure Kubernetes Service – AKS) van ProRail, zonder vereiste wijzigingen in of vervanging van netwerkapparatuur. Hiervoor gelden de BCP Aansluitvoorwaarden.

Eis 74. Beheer van Dienst
Leverancier is verantwoordelijk voor het beheer van de Dienst. Beheer van componenten in het ProRail netwerk moet met ProRail tijdig afgestemd worden. De procesafspraken moeten in het SLA en DAP opgenomen worden.

Eis 75. CMDB
Bij implementatie en bij wijzigingen van de Dienst moet leverancier CMDB wijzigingen (automatisch) doorgeven aan ProRail binnen drie werkdagen.

Eis 76. Gebruik van DNS en dynamische adressering
De Dienst moet gebruikmaken van DNS namen en dynamische adressering, zodat wijzigingen in IP adressen of netwerksegmentatie binnen ProRail GEEN wijzigingen bij de leverancier vereisen.

3.2.6. Informatiebeveiliging

Voor de Dienst zijn informatiebeveiligingseisen van toepassing, passend bij de risico’s van toegang op afstand. De Dienst en alle data moet binnen de Europese Economische Ruimte blijven conform wettelijke vereisten en ProRail beleid.

De scope en inrichting van het ISMS (Information Security Management System) en BCMS (Business Continuity Management System) worden door ProRail getoetst op relevantie en effectiviteit. Back-up en Data Recovery moeten meegenomen worden in de BCM. Uit de

toets kan volgen dat de leverancier haar ISMS en BCMS moet verbeteren om aan de uitgangspunten van de scope en inrichting te voldoen.

Eis 77. Informatiebeveiliging awareness
De leverancier moet ervoor zorgen dat gedurende de levering van de Dienst zijn medewerkers eens per jaar en aantoonbaar op het belang van informatiebeveiliging en hun rol daarin worden gewezen (security awareness).

Eis 78. Business Continuity Management (BCM)
Leverancier moet ISO22301 gecertificeerd zijn (of gelijkwaardig) en de dienstverlening aan ProRail moet voldoen aan de normen van ISO22301. De kwaliteit van uitvoering hiervan mag gedurende de overeenkomst door ProRail op verzoek getoetst worden.

Eis 79. BCM en ISM Certificaten
Leverancier moet de gevraagde certificaten voor BCM en ISM (Information Security Management) ter beschikking stellen aan ProRail.

Eis 80. Contactpersoon Informatiebeveiliging
De leverancier wijst één vaste contactpersoon voor informatiebeveiliging aan. Deze contactpersoon wordt vóór de start van de dienstverlening vastgelegd in de SLA. De contactpersoon beschikt aantoonbaar over relevante kennis van informatiebeveiliging (minimaal: bekend met ISO 27001-principes en risicomanagement) en heeft mandaat om beveiligingsafspraken te beoordelen, te adviseren en escalaties te initiëren. Afstemming over informatiebeveiligingsonderwerpen vindt altijd plaats onder regie van de contractmanager van ProRail.

Eis 81. Gegevensuitwisselingen
Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier. Verbindingen zijn ingericht en worden onderhouden conform de standaarden van ProRail.

Eis 82. Beveiligingsniveau Data
Opgeslagen data binnen de Dienst van de leverancier, dient beveiligd te worden conform het beveiligingsniveau dat bij deze data is overeengekomen. Persoonsgegevens moeten minimaal Vertrouwelijk geclassificeerd zijn.

Eis 83. Locatie Dienst
De Dienst bevindt zich fysiek binnen de Europese Economische Ruimte (EER) en is alleen vanuit een locatie buiten de EER toegankelijk en/of bewerkbaar vanaf een beveiligd werkstation waarbij lokale opslag niet mogelijk is en een beveiligde verbinding en multi-factor authenticatie gebruikt wordt.

Eis 84. Data
De data mogen de EER niet verlaten.

Eis 85. Data registratie
Leverancier registreert de data en de data staat op een centrale plaats. De registratie van de data is up to date en bevat altijd de eigenaar.

Eis 86. Gegevensdragers
Gegevensdragers die vertrouwelijke data bevatten zijn voorzien van encryptie, en We opgeslagen op een plek die niet toegankelijk is voor onbevoegden.

Eis 87. Beveiligingsincidenten
Er wordt een vaste procedure voor het melden van (IT en OT) beveiligingsincidenten en kwetsbaarheden afgesproken tussen ProRail en de leverancier.

Eis 88. Melding Beveiligingsincidenten
De leverancier meldt (beveiligings-)incidenten en kwetsbaarheden direct aan ProRail, en als dat wettelijk noodzakelijk is, ook aan de Autoriteit Persoonsgegevens. Bij niet-gemelde incidenten waar persoonsgegevens bij betrokken zijn, kan ProRail de leverancier in gebreke stellen. De Leverancier geeft (beveiligings-)incidenten volgens gemaakte afspraken opvolging en rapporteert daarover aan ProRail.

Eis 89. Risicomanagement
Leverancier vult direct na contractering een self-assessment in waaruit de mate van beveiliging blijkt, met als kader het beveiligingsbeleid van ProRail. Het self-assment moet aan ProRail ter beschikking gesteld te worden.

Eis 90. Risicoanalyse
Leverancier moet gedurende de looptijd van het contract te beschikken over een actuele, gedocumenteerde en door zijn management geaccordeerde classificatie en risicoanalyse, van de Dienst.

Bij deze risicoanalyse moeten de bedreigingen voor de bedrijfsmiddelen, kwetsbaarheden en de invloeden op de continuïteit van de bedrijfsprocessen van ProRail zijn vastgesteld en het bijbehorende risiconiveau te zijn bepaald. Beheersmaatregelen die voortkomen uit de risicoanalyse en waar ProRail een aandeel in de implementatie heeft, worden afgestemd met ProRail en uitgevoerd.

Eis 91. Beheersmaatregelen
De leverancier moet ProRail (op verzoek) informeren over de getroffen beheersmaatregelen die relevant zijn binnen het kader van de Dienst.

Eis 92. Toegangsverlening Dienst
Er wordt een gedocumenteerde formele en actuele procedure afgesproken voor het registreren, verlenen, wijzigen en intrekken van de toegang tot de Dienst. Deze procedure wordt periodiek (minimaal eens per jaar) beoordeeld en geactualiseerd.

Eis 93. Need to know
De toegang van medewerkers van de leverancier is beperkt tot systemen bij ProRail, de leverancier en afgenomen diensten bij derden, die benodigd zijn voor het leveren van de Dienst (need to know principe).

Eis 94. Wachtwoorden
Toegang tot de systemen van de Dienst is beperkt met wachtwoorden volgens de wachtwoordeisen zoals opgenomen in het informatiebeveiligingsbeleid van ProRail.

3.3. Dienstverlening & Service-eisen

Dit hoofdstuk beschrijft de eisen aan de dienstverlening door de Leverancier. De eisen omvatten service levels, support, monitoring, rapportage, change management en de overlegstructuur tussen ProRail en de leverancier.

3.3.1. Service Level Agreement

De Service Level Agreement (SLA) definieert de afspraken over de kwaliteit en beschikbaarheid van de Dienst en dienstverlening. Zie Annex 3.2 Service Level Agreement voor de eisen aan de beschikbaarheid, wijzigingen, functieherstelttijden en support.

Eis 95. Service Level Agreement
De leverancier moet voldoen aan het Service Level Agreement: Annex 3.2 Service Level Agreement.

Eis 96. Service Level Productieomgeving
De Dienst op de Productieomgeving moet voldoen aan de service levels zoals uitgewerkt in de Annex 3.2 Service Level Agreement.

Eis 97. Service Level Test/Acceptatieomgeving
De Dienst op de Acceptatie/Test omgeving moet voldoen aan de service levels zoals uitgewerkt in de Annex 3.2 Service Level Agreement.

Eis 98. Goedkeuring Service Level Agreement
De leverancier moet binnen vier (4) weken na gunning het Service Level Agreement definitief maken in overleg met ProRail en laten goedkeuren door ProRail.

Eis 99. DAP (Dossier Afspraken en Procedures)
De leverancier moet binnen vier (4) weken na gunning het DAP opstellen in overleg met ProRail en laten goedkeuren door ProRail.

3.3.2. Escalatieprocedures

Eis 100. Escalatiematrix
De leverancier moet in de DAP een escalatiematrix opstellen en onderhouden met contactpersonen en escalatiepaden voor verschillende incidentniveaus, inclusief management escalatie bij P1 incidenten.

3.3.3. Support

Eis 101. Communicatiekanalen
De leverancier moet minimaal de volgende communicatiekanalen bieden voor support: telefoon (Nederlands en/of Engelstalig sprekend), e-mail en een ticketsysteem met webportaal.

Eis 102. Known issues en workarounds
De leverancier moet een overzicht leveren van alle bekende issues, workarounds, en specifieke configuratie-eigenaardigheden die relevant zijn voor het beheer van de Dienst.

Eis 103. Technische documentatie
De leverancier moet technische documentatie leveren inclusief: architectuurbeschrijving, installatie- en configuratiehandleiding, API documentatie en troubleshooting guide (in het Nederlands of Engels).

Eis 104. Documentatie-updates
De leverancier moet alle documentatie up-to-date houden en binnen tien (10) werkdagen na wijzigingen aan de dienst de relevante documentatie bijwerken.

3.3.4. Monitoring

De leverancier moet proactieve monitoring uitvoeren om incidenten te voorkomen en snel te kunnen reageren.

Eis 105. Inzicht monitoring data
De leverancier moet ProRail inzicht geven in de monitoring data, inclusief uptime statistieken, performance metrics en incident overzichten.

Eis 106. Proactieve monitoring
De leverancier moet proactieve 24/7 monitoring uitvoeren op alle componenten van de Dienst, inclusief beschikbaarheid, performance en security events en ProRail direct over onregelmatigheden informeren conform de afspraken in de Overeenkomst.

Eis 107. Security monitoring
De leverancier moet security monitoring via een beveiligde API beschikbaar stellen aan het ProRail SOC voor integratie in SOC /SIEM processen.

De opvolging van de verdachte activiteiten wordt besproken met ProRail bij de implementatie.

3.3.5. Rapportage

De Leverancier moet periodieke rapportages leveren over de dienstverlening. Zie Annex 3.2 Service Level Agreement voor de rapportage eisen.

3.3.6. Overlegstructuur

Een effectieve overlegstructuur is essentieel voor de samenwerking tussen ProRail en de Leverancier. Zie Annex 3.2 Service Level Agreement voor de eisen aan de overlegstructuur.

3.3.7. Change Management

Wijzigingen aan de Dienst moeten gecontroleerd worden doorgevoerd om de stabiliteit te waarborgen.

Eis 108. Service management processen
Leverancier moet voor het service management aansluiten bij de ITILv4 processen van ProRail.

Eis 109. Vooraankondiging onderhoud
De leverancier moet gepland onderhoud aan de Dienst minimaal twintig (20) werkdagen vooraf aankondigen aan ProRail, inclusief datum, tijdstip, verwachte duur en mogelijke impact. Voor kritische security wijzigingen geldt deze aankondigingstijd niet.

4. Exit-strategie en Transitie

ProRail hecht grote waarde aan continuïteit van dienstverlening en een soepele transitie bij beëindiging van de overeenkomst. De leverancier moet een exitplan opstellen en onderhouden dat de basis vormt voor een gecontroleerde transitie. In de overeenkomst zijn de eisen aan de transitie (exit) bij beëindiging van de overeenkomst opgenomen. De leverancier moet een soepele overgang waarborgen naar een opvolgende leverancier of naar ProRail zelf, zonder onderbreking van de dienstverlening.

5. Implementatie

Dit hoofdstuk beschrijft de eisen aan de implementatie van de Dienst. De implementatie moet volgens een gestructureerde projectaanpak worden uitgevoerd. De migratie van de bestaande gebruikers van een toegangsdienst naar de dienst moet zorgvuldig worden uitgevoerd om continuïteit te waarborgen.

De acceptatie van de Dienst moet formeel door ProRail worden vastgesteld voordat de productieomgeving in gebruik wordt genomen.

Eis 110. Implementatieplan
De leverancier moet binnen twee weken na gunning het implementatieplan in detail uitgewerkt hebben en door ProRail laten goedkeuren voordat met de implementatie begonnen kan worden

Eis 111. Implementatieduur
De leverancier moet de implementatie van de Dienst voltooien binnen drie maanden na gunning. De exacte planning wordt in overleg met ProRail vastgesteld.

Eis 112. Voortgangsrapportage
De leverancier moet wekelijks een voortgangsrapportage leveren tijdens de implementatiefase, met status van activiteiten, issues, risico's en planning.

Eis 113. Migratieplan
De leverancier moet, binnen vier weken na het verzoek van ProRail, het migratieplan in detail uitwerken in afstemming met ProRail. Het migratieplan beschrijft hoe de opgegeven gebruikers en assets, policies en configuraties worden gemigreerd en/of geïmplementeerd in de Dienst.

Eis 114. Acceptatietestplan
De leverancier moet een acceptatietestplan opstellen in samenwerking met ProRail, waarin alle testscenario's, acceptatiecriteria, verwachte resultaten vanuit de testscenario's en go/no-go criteria zijn vastgelegd.

Eis 115. Formele acceptatie
De leverancier moet de formele acceptatieprocedure van ProRail doorlopen waarbij ProRail schriftelijk akkoord geeft voordat de Dienst in productie gaat.

Eis 116. Beheerderstraining
De leverancier moet training verzorgen voor ProRail beheerders die verantwoordelijk zijn voor het dagelijks beheer van de Dienst. De training omvat minimaal: configuratie, gebruikersbeheer, troubleshooting en rapportage.

Eis 117. Eindgebruikersinstructie
De leverancier moet instructiemateriaal leveren voor eindgebruikers (beheerders van OT- en IT-systemen) zodat eindgebruikers met beperkte inspanning van de dienst gebruik kunnen maken.

Eis 118. Training in het Nederlands of Engels
De leverancier moet trainingen aanbieden in het Nederlands en/of Engels. Trainingsmateriaal mag in het Engels zijn indien Nederlandstalig materiaal niet beschikbaar is.

ProRail vraag ook uren ‘consultancy’ uit. In de Aanbiedingsbegroting en de toelichting op de aanbiedingsbegroting staat beschreven wat onder consultancy wordt verstaan. Consultancy kan gebruikt worden voor ondersteuning bij de implementatie, uitbreiding of aanpassing van de omgeving, migratie of onboarding van nieuwe gebruikers (niet limitatief).

Eis 119. Consultancy
De leverancier moet consultancy leveren conform de beschrijving en conform het aantal uren zoals gevraagd in de Aanbiedingsbegroting.

6. Afkortingen, definities en referentiedocumenten

Dit hoofdstuk bevat de afkortingen, definities en referentiedocumenten.

6.1. Afkortingenlijst

Afkorting	Betekenis
API	Application Programming Interface
AVG	Algemene Verordening Gegevensbescherming (GDPR)
BCP	Business Critical Platform
CA	Certificate Authority
CMDB	Configuration Management DataBase
CISO	Chief Information Security Officer
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
DAP	Dossier Afspraken en Procedures
DR	Disaster Recovery
EER	Europese Economische Ruimte
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	Informatietechnologie
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
KPI	Key Performance Indicator
MFA	Multi-Factor Authentication
NIS2	Network and Information Security Directive 2
OAuth	Open Authorisation
OT	Operationele Technologie
OTSM	OpenText Service Management
PKI	Public Key Infrastructure
PvE	Programma van Eisen
RAS	Remote Access Solution
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center
SSH	Secure Shell
SSO	Single Sign-On
TLS	Transport Layer Security
TOTP	Time-based One-Time Password
VNC	Virtual Network Computing
ZTNA	Zero Trust Network Access

6.2. Definities

Term	Definitie
Asset	Een OT-systeem, IT-systeem, applicatie of apparaat dat via de Dienst wordt ontsloten voor beheer op afstand.
Asset Owner	De functioneel verantwoordelijke binnen ProRail voor een specifiek Asset.
Beheerpartij	Door ProRail gecontracteerde partij of ProRail zelf die Assets beheren
(OT/IT) Connector	Interne proxy benodigd om een domein te ontsluiten.
Datalek	Een inbreuk op de beveiliging die leidt tot ongeoorloofde toegang tot, vernietiging, wijziging of openbaarmaking van persoonsgegevens.
Dienst	De definitie van de 'Generieke RAS Dienst' is beschreven in de Overeenkomst
(Asset) Domein	Een logische of netwerktechnische groepering van OT-assets (of IT-assets).
Exitplan	Een plan dat beschrijft hoe de dienstverlening kan worden overgedragen bij beëindiging van de overeenkomst.
Functionaliteit	Functionaliteit is het geheel aan beschikbare, correct werkende functies van de Dienst, waaronder (niet limitatief) de actuele autorisatiematrix, toegangsrechten, procesondersteunende functies, gegevensverwerking en alle overige onderdelen die nodig zijn om de Dienst conform het Overeengekomen gebruik te laten functioneren.
Functiehersteltijd	De tijd tussen het melden van een incident en het herstel van de Functionaliteit.
Gebruiker	Medewerker van de beheerpartij of van ProRail
Hypercare	Een periode direct na ingebruikname met verhoogde support en monitoring.
Incident	Een ongeplande onderbreking of vermindering van de kwaliteit van de dienstverlening.
Major Change	Een wijziging met potentiële impact op de beschikbaarheid, security of functionaliteit van de dienst.
Named user	Medewerker van de beheerpartij of ProRail en gebruiker van de Dienst
Leverancier	De leverancier die de Dienst levert aan ProRail
OT (Operationele Technologie)	Hardware en software die fysieke processen monitort en bestuurt, in dit geval de spoorinfrastructuur.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
ProRail	De Opdrachtgever, beheerder van de Nederlandse spoorinfrastructuur.
Transitie	Het proces van overdracht van de dienstverlening naar een opvolgende leverancier of naar ProRail.
Session Recording	Het opnemen van alle handelingen tijdens een remote access sessie voor audit doeleinden.
Verwerker	De partij die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke (ProRail).

6.3. Referentiedocumenten

De volgende documenten zijn gebruikt als referentiedocumenten.

Nr	Document	Referentie
R1	NIS2-richtlijn Cyberbeveiligingswet | Rijksinspectie Digitale Infrastructuur (RDI)	EU 2022/2555
R2	Algemene Verordening Gegevensbescherming (AVG) Home | Autoriteit Persoonsgegevens	EU 2016/679
R3	Baseline Informatiebeveiliging Overheid (BIO) Baseline Informatiebeveiliging Overheid 2 (BIO2) - bio-overheid	BIO2