

Aansluitvoorwaarden ProRail WGID

o.b.v. Technology en LCM Roadmap I&O

Van Eigenaar	ProRail ICT Infrastructuur & Operatie (ICT I&O) Team platform diensten Windows
Bestand	Aansluitvoorwaarden ProRail 5.01.docx
Status	Goedgekeurd. Dit document heeft een beperkte houdbaarheid. De laatste goedgekeurde versie is te vinden op: https://prorailbv.sharepoint.com/teams/dc2015_0001/Documents/Forms/AllItems.aspx

Inhoudsopgave

1	Inleiding	3
1.1	Belangrijkste wijzigingen	3
2	Uitgangspunten	4
2.1	Organisatie en Proces	4
2.2	Principes & keuzes	4
2.3	Cloud	5
3	Actueel overzicht toegepaste technologie	6
3.1	Categorieën	6
3.2	Template beschrijving voorwaarden	6
4	Verkorte lijst van infrastructuur componenten	6
4.1	User Workspace	6
4.2	Auto update	8
4.3	Serverdiensten	9
4.4	Netwerk	11
4.5	Security t.a.v. accounts	11
4.6	Security gerelateerde producten	11
4.7	System Management	12
5	Applicatie Selectie Criteria	13

1 Inleiding

Dit document bevat de voorwaarden waaraan technische oplossingen moeten voldoen om te kunnen worden opgenomen in de Werkplek en Generieke IT Diensten (WGID) ICT-infrastructuur van ProRail. Dit omvat de Windows ICT-Infrastructuur en dus niet de Post21 Linux platformen.. Voor cloud en netwerk toepassingen zijn aparte aansluitvoorwaarden beschikbaar op IV-Plaza. ([Introductiepagina - IV Plaza \(sharepoint.com\)](#)). Het doel van dit document is om in een zo vroeg mogelijk stadium te waarborgen dat technische oplossingen (gebouwd of gekocht) binnen de ICT-infrastructuur van ProRail zullen functioneren en beheersbaar zijn. Dit document kan ter ondersteuning door een projectleider worden gebruikt om met leveranciers te inventariseren welke mogelijkheden er zijn om nieuwe applicaties in de WGID-infrastructuur van ProRail op te nemen.

Ten tijde van oplevering van een project is het verplicht om te voldoen aan de laatste versie van de aansluitvoorwaarden. Bij langlopende projecten is het beter om eerst af te stemmen met het Team platform diensten KA en/of de Technology Roadmap te raadplegen. De Aansluitvoorwaarden zijn bedoeld voor in- en externe communicatie, de Technology Roadmap is niet bedoeld voor externe communicatie.

Een oplevering van de “Technische oplossing” van een project is in dit verband het geheel aan applicaties en alle eventueel daarbij meegeleverde technologie (platformen, OS, hardware, etc.) dat als één geheel wordt geleverd en als één geheel in productie en onder beheer gebracht moet worden.

Het toevoegen van een product aan een applicatiegroep is niet alleen een kwestie van een woord toevoegen. Er moet ook bepaald worden wat de impact is t.a.v.:

- compatibiliteit
- roadmap
- opleidingen
- (externe) ondersteuning

Tijdens de oplevering moet er een aanspreekpunt en “productbeheerder” benoemd worden en de ondersteunende tooling moet zijn ingericht. Dit zijn voorwaarden waarmee ProRail ICT kan borgen dat het product procedureel en technisch beheerd kan worden.

Dit is een levend document en zal regelmatig geactualiseerd worden. Het bestaat uit twee delen:

- een actueel overzicht van de in de infrastructuur toegepaste technologie,
- een lijst van voorwaarden die aansluit op de acceptatiecriteria.

1.1 Belangrijkste wijzigingen

Ten opzichte van de vorige editie zijn de belangrijkste wijzigingen:

- Windows 10 versie naar 22versieH2 en Office365 naar 2311(Auto update)
- Update beleid voor Office invoegtoepassingen
- Gebruik van Oracle gelicenseerde producten verwijderd (Niet meer in te zetten voor nieuwe toepassingen).
- In lijn met Technology Roadmap 2024

2 Uitgangspunten

2.1 Organisatie en Proces

De ICT-infrastructuur wordt beheerd door ProRail I&O. Hierbinnen is de afdeling Platformdiensten Windows verantwoordelijk voor de Windows platformen in de ProRail ICT omgeving. Deze rol bestaat hoofdzakelijk uit het coördineren en regisseren van de operationele processen. De gecontracteerde partner (Conclusion) voert het dagelijks operationeel beheer uit en is verantwoordelijk voor installatie en continuïteit van de ICT-installaties.

Om nieuwe componenten in de ICT-infrastructuur onder te brengen is het noodzakelijk om dit in een vroegtijdig stadium af te stemmen en in overeenstemming met de beherende partij uit te voeren. Dit zodat de stabiliteit, veiligheid en capaciteit gewaarborgd blijft. Projecten dienen hiervoor contact op te nemen met de ProRail Service Manager van het Team platform diensten Windows. Deze begeleidt de inhoudelijke afstemming tussen project en beheerder en besluit over het al dan niet toelaten van de implementatie en de geldende voorwaarden voor beheer.

2.2 Principes & keuzes

De volgende architectuurprincipes zijn relevant voor de ICT-infrastructuur in de context van de aansluitvoorwaarden.

1. De (overeengekomen) kwaliteit en beschikbaarheid van de generieke informatiedienstverlening moet gehandhaafd blijven.
2. Op elk moment wordt de generieke informatiedienstverlening, waaronder WGID, verzorgd door één volledig bekende en stabiele configuratie van infrastructuur, systemen, platformen, databases, standaard KA applicaties en overige applicaties.
3. Elke wijziging aan deze configuratie moet, indien mogelijk geautomatiseerd, maar altijd gecontroleerd uitgevoerd worden en moet weer één bekende en stabiele configuratie opleveren.
4. De frequentie van handmatige wijzigingen moet zo laag mogelijk zijn voor de generieke infrastructuur. Handmatige wijzigingen worden zoveel mogelijk doorgevoerd op enkele, vooraf vastgestelde momenten in de jaarkalender.
5. Wijzigingen aan de configuratie moeten steeds zo beperkt mogelijk zijn.
6. Minimaliseer het aantal vendors en de hardware- en softwareproducten
7. ProRail gebruikt proven technology, en hanteert daarvoor de volgende aanpak: *Een product moet zich in de praktijk bij andere afnemers voldoende hebben bewezen, en de ondersteuning door de leverancier moet bewezen afdoende zijn gebleken.*
8. Stem de veranderingen in de generieke ICT-infrastructuur af met de ondersteuning geleverd door de leveranciers.
9. Gebruik Open standaarden
10. Volg beleidsuitgangspunt: Microsoft tenzij, SAP tenzij.
11. Implementeer conform het informatiebeveiligingsbeleid¹
12. Volg de ProRail standaarden en de "Best Practises" uit de makrt.

¹ Zie [pagina voor informatiebeveiligingsbeleid \(alleen intern ProRail\)](#)

2.3 Cloud

Voor het afnemen van cloud diensten zijn afwijkende voorwaarden van toepassing. Zie hiervoor de aansluitvoorwaarden “ProRail Cloud Landing Zone”. De genoemde producten in hoofdstukken 4.3 en 4.7 zijn niet van toepassing bij het leveren van SaaS-diensten. Van de aansluitvoorwaarden die in dit document zijn weergegeven zijn de criteria zoals opgenomen in hoofdstuk 5 die op lokale installaties slaan niet van toepassing. Hier zijn vooral de algemene eisen en meer specifiek de koppelingen en authenticatie eisen (S5, S6, S7 en S9) relevant.

De eventuele beperkingen in producten die gelden voor het leveren van een dienst vanuit de cloud zijn in het “Richtlijnen en voorwaarden cloud” weergegeven.

Een actuele verwijzing naar het cloudbeleid is te vinden in het document “Cloudbeleid introductie”. Concrete aansluitvoorwaarden zijn te vinden in de Aansluitvoorwaarden “ProRail Cloud Landing Zone

De hierboven genoemde documenten zijn te vinden in het documentencentrum van IV Plaza:
https://prorailbv.sharepoint.com/teams/dc2015_0001/Documents/Forms/Geldige%20documenten.aspx

3 Actueel overzicht toegepaste technologie

Om de voorwaarden overzichtelijker te maken is een aantal specifieke gebieden (categorieën) te onderscheiden waarbinnen deze gelden. Bijvoorbeeld: hardware, beveiliging, netwerk.

De beschrijving van elke voorwaarde wordt op een uniforme wijze uitgevoerd zie 3.2.

3.1 Categorieën

Applicaties hebben te maken met de volgende categorieën ICT-componenten:

1. User Workspace (Werkplek diensten)
2. Generieke IT Diensten: Servers (Hardware, OS), Directory, Web, Distributie, Database, E-mail
3. Netwerk
4. Security
5. Systems Management

3.2 Template beschrijving voorwaarden

Om alle voorwaarden op een eenduidige manier te beschrijven is het volgende template ontworpen:

<Subcategorie>			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen

De omschrijving geeft het product weer. De kolom "Minimaal vereist" geeft de actuele versie weer die nu in gebruik is, de kolom "Maximaal toegestaan" geeft weer welke versie bij uitzondering en/of op relatief korte termijn gepland staat om in gebruik te worden genomen. Indien de kolom "Maximaal toegestaan" leeg is, is "Maximaal toegestaan" gelijk aan "Minimaal vereist".

4 Verkorte lijst van infrastructuur componenten

Hieronder is een niet uitputtende lijst van de belangrijkste generieke infrastructuur componenten opgenomen. Indien u componenten mist of vragen heeft over de inhoud, dan kunt u contact opnemen met de afdeling Systeeminfra & Basisinfra voorzieningen.

4.1 User Workspace

OS – werkstations			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Microsoft Windows	Windows 10 x64 22H2	Windows 10 x64 22H2	Semi-Annual Channel release
Microsoft Defender for Endpoint	Always Green		Elke applicatie dient binnen dit Framework te functioneren.

OS – draagbaar			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Windows tablet	10	11	versie in lijn met workstation
Android	13	14	
iPad iOS	16	17	

Client applicaties en platforms			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Office applicaties	Microsoft Office 365 ProPlus versie 2311 (O365)	Microsoft Office 365 ProPlus versie: Actueel via Auto update	Compatibiliteit met Office 365 is vereist
Microsoft Edge	Microsoft Edge Chromium for business (Auto update)	Microsoft Edge Chromium for business (Auto update)	De serverzijde dient aan te geven in welke compatibiliteitsmodus de browser dient te Werken. CIS security adviezen zijn van toepassing
Chrome	Volgt strikt het release beleid van Google	Volgt strikt het release beleid van Google	CIS security adviezen zijn van toepassing. Applicaties dienen altijd de laatste versie van Chrome te ondersteunen. Geen uitzondering mogelijk.
.pdf reader	Adobe Acrobat Reader Continuous release versie 23.006.20380	Adobe Acrobat Reader Continuous Release	Actueel via Auto update
Java	Ondersteunde, compatibele en gelicenseerde Java versie meegeleverd als onderdeel van de applicatie	Ondersteunde, compatibele en gelicenseerde Java versie meegeleverd als onderdeel van de applicatie	Oracle Java mag niet apart worden gebruikt en gelicenseerd. Overleg altijd met de ProRail SAM specialist.
Media Player	Windows Media Player behorend bij Windows release	Windows Media Player behorend bij Windows release	
Terminal Services	Windows remote desktop	Windows remote desktop	²
SBC Client	Citrix Workspace 2309	Citrix Workspace 2309	Actueel via auto update
.NET	.Net Framework 4.8	.Net Framework 4.8	

ProRail

Opmerking: Mogelijke invoegtoepassingen die voor Office applicaties zijn bedoeld kunnen niet worden geïnstalleerd. Deze maatregel voorkomt dat er voor elke wijziging, van zowel de betrokken Office invoegcomponent, als vanuit Office365 een recursieve test met alle betrokken componenten moet worden uitgevoerd.

Dit geldt voor elk type VBA, COM en/of VSTO invoegtoepassing.

Er kan een uitzondering gemaakt worden voor de zogenoemde Office Add-ins, als deze essentieel zijn voor de ondersteuning van een ProRail bedrijfsproces.

Aan het gebruik van een Office Add-in zijn de volgende voorwaarden verbonden:

- Indien de Office Add-in de werking van de huidige of een toekomstige Office versie nadelig beïnvloedt, wordt deze Add-in uitgeschakeld.
- Indien de Office Add-in niet goed meer functioneert na een Office update of patch, dient de applicatie eigenaar maatregelen te nemen om dit te herstellen, de invoering van een nieuwe update of patch zal niet uitgesteld worden.
- De Office Add-in bewaart en verwerkt data op een door ProRail goedgekeurde locatie (Zie cloudbeleid).
- ProRail heeft een samenwerking relatie met de leverancier van de Office Add-in. (De Add-in is een onderdeel van andere applicatie die ProRail afneemt).
- Er wordt een beschrijving van de leverancier over de werking en veiligheid van de Office Add-in aangeleverd.
- De Office Add-ins worden bewaakt via de Microsoft beveiligingsomgeving CASB.

Indien een applicatie eigenaar een Office Add-in onder bovengenoemde condities wil invoeren, dient deze een schriftelijk verzoek bij de manager van de afdeling Windowsplatform diensten in, waarin expliciet vermeld is dat bovengenoemde consequenties aanvaard worden.

Na akkoord kan er een wijzigingsverzoek (Change) worden ingediend, onderdeel van het Changeproces is een Risico en Impact Analyse (IRA) waar naast de juiste werking ook de veiligheid wordt getoetst.

Wijzigingen voor Office365 worden vanuit Microsoft Office365 doorgevoerd. De wijzigingen, met uitzondering van kritische patches, worden bij ProRail op de werkplek ter beschikking gesteld middels het LCM proces in de cyclus van het Windows Semi-Annual Channel en Office updateproces.

In de groep optionele applicaties is het mogelijk om beperkt Microsoft Access ter beschikking te stellen als persoonlijk database programma. Vanwege beheer, netwerk technische en performance redenen mag de database niet in multi usermode worden gebruikt. Voor multi usermode databasesystemen dient SQL Server gebruikt te worden.

Het installeren van extensies in browsers is niet mogelijk op de werkplek. Indien een applicatie een browser extensie vereist wordt die extensie als onderdeel van het applicatiepackage opgenomen. Bij incompatibiliteit tussen een browserversie en een extensie heeft de browserversie prioriteit. Dit betekent dat een extensie uitgeschakeld kan worden na een browserupdate bij gebleken incompatibiliteit.

4.2 Auto update

Voor een aantal applicaties is het wenselijk dat nieuwe functionaliteit vaker dan 1 x per jaar beschikbaar komt. Voor andere applicaties geldt dat beveiligingsaanpassingen vaker dan 1 x per jaar moeten worden doorgevoerd. Applicaties worden nu per werkplek release geüpdatet.

Indien een applicatie de mogelijkheid biedt voor auto updates heeft deze functie de voorkeur onder de volgende voorwaarden:

- Een applicatie mag een auto update uitvoeren zo lang de impact van de wijziging zich beperkt tot de applicatie zelf.
- Er geen componenten geüpgraded worden afkomstig uit andere packages, zoals bijvoorbeeld Office componenten die door Microsoft geplaatst worden.
- De eigenschappen van de werkplek moeten ongewijzigd blijven met uitzondering van de applicatie zelf.
- De functioneel beheerder van de applicatie stemt met zijn collega's van de applicatieketen af of de auto update functie geactiveerd wordt.

Het besluit wordt aangegeven op het AIF. Bij de omschrijving van de applicatie in de store wordt aangegeven dat de applicatie zichzelf update.

4.3 Serverdiensten

De Generieke IT diensten worden vanuit een hybride infrastructuur aangeboden. Applicaties kunnen zowel in de ProRail Azure tenant worden gehost als in de ProRail datacenters. Hiervoor geldt het "Cloud first" beleid. Er dient wel altijd een afweging gemaakt te worden in de vorm van een business case. De ProRail Generieke Infrastructuur is redundant opgebouwd en voorziet in het serviceniveau Brons, Brons+ en Zilver. Afhankelijk van de BIVP-classificatie van een toepassing wordt hierin een keuze gemaakt. Business applicaties kunnen van deze diensten gebruik maken. Dit moet in het architectuurontwerp worden meegenomen, standaard is verbeterde beschikbaarheid binnen één rekencentrum. *Vanuit de infrastructuur wordt voor de backup-systemen een replicatiedienst over beide datacentra geleverd.* In Azure dient dit in het architectuurontwerp opgenomen te worden

OS - servers			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Windows	MS Windows 2022	MS Windows 2022	Alle nieuw te plaatsen servers moeten dit server OS gebruiken
Linux/Unix	Red hat RHEL8	Red hat RHEL8	Linux servers worden momenteel nog niet geleverd binnen WGID.
Virtualisatie	VMware vSphere V7.x	VMware vSphere V8.x	

Directory			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Microsoft AD	AD Windows 2022 (domain functional level: Windows Server 2012R2)	AD Windows 2022 (domain functional level: Windows Server 2016)	

ProRail

Microsoft Entra ID	Microsoft Entra ID (Cloud, always up to date)		
--------------------	---	--	--

Server appl. platform en middleware			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Deployment voor Java	Wildfly,		Meestal als onderdeel van een solution. Alleen n en n-1 toegestaan. Dmv LCM dient dit actueel gehouden te worden.
SAP Cloud Platform (mob apps)	Volgens dienst		Toepassing bij ontsluiten app diensten tbv mobile devices en applicatie ontwikkeling. Dienst wordt afgenomen in cloud.
Terminal services	Browser based	Browser based	Als uitzonderling kan in overleg Azure Virtual Desktop worden toegepast.
Tibco ESB	Current-1	Zie minimum	Bij integratie svp benodigde component en versie opvragen
Web server	MS IIS 10	MS IIS 10	Meegeleverd met Windows OS

Software distributie			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Microsoft Intune	Always Green	Always Green	Migreert mee met Azure releases
MS Microsoft Updates	Via Microsoft Intune	Via Microsoft Intune	

Database (server)			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Windows	MS SQL2022	MS SQL2022	Zowel Standard als Enterprise Editie

E-Mail			
--------	--	--	--

ProRail

Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Server	Microsoft 365	Microsoft 365	Onderdeel van Office 365
Client	Outlook Office 365 ProPlus	Volgt Office updates	
MailRelay	Gebruik Flow mailer	Gebruik Flow mailer	Voor Cloud toepassingen.

4.4 Netwerk

Hardware - netwerk			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Fabrikant routers, switches	Cisco		
Netwerk Protocollen	TCP/IP V4 (S)FTP, (S)RCP, RDP, NTP, HTTP(S), ICA, 802.1X	TCP/IP V4	IP V6 voorbereid
Services: DHCP, WINS, DNS, DFS	Windows 2022	Windows 2022	
Load Balancers	Citrix NetScaler VPX	Citrix NetScaler VPX	Versie 12

4.5 Security t.a.v. accounts

Naast technische maatregelen zoals genoemd in de tabel hieronder geldt er vanuit security de eis op traceerbaarheid. Dit betekent dat alle niet publiek toegankelijk informatie of handelingen voor het aanmaken en muteren van informatie herleidbaar moet zijn naar een natuurlijke persoon. Om deze reden zijn functionele accounts niet toegestaan. In het Logisch identiteits- en toegangsbeleid ([ISP-O.06](#)) wordt dit verder verduidelijkt.

4.6 Security gerelateerde producten

preventie			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Virusscan server	Microsoft defender for Cloud (servers)	Microsoft defender for Cloud (servers)	Voor de Windows systemen binnen Post21 wordt TRelix gebruikt.
Client	Microsoft Defender for Endpoint		
Server	Microsoft Defender for Cloud		
Exchange	Microsoft Exchange Online protection		

ProRail

Office	Micosoft Defender for Office	Cloud component	
Identity	Microsoft Defender for Identity	Cloud component	
Encryptie client (inclusief USB storage)	BitLocker		
Reverse proxy / Proxy	NetScaler/ Cisco WSA		
SSL / TLS	Minimaal TLS 1.2		SSL3 en lager is niet toegestaan.
SMB	v2 bij voorkeur v3		
Apparaat netwerktoegangsbeveiliging (van toepassing op apparatuur die in een kantoor omgeving op het netwerk wordt aangesloten)	802.1X		Authenticatie voor device middels PEAP / EAP-TLS / PEAP-MSChapv2

4.7 System Management

Monitoring			
Omschrijving	Minimaal vereist	Maximaal toegestaan	Opmerkingen
Monitoring (System/Events)	Micro Focus OBM - laagst ondersteunde versie	Micro Focus OBM - hoogst ondersteunde versie	In beheer bij IT4IT, Windows Server VM's hebben de zgn. OBM agent.
Remote Management diversen systemen	Als protocol: RDP, SSH, HTTPS	Als protocol: RDP, SSH, HTTPS, BLAST	Voor het beheer van zowel storage systemen als server systemen.
RSAT (Remote Server Administration Tools)	Minimaal ondersteunde versie door Microsoft Windows Server OS	Maximaal ondersteunde versie door Microsoft Windows Server OS	Wordt gebruikt om Windows Servers (incl. rollen) te beheren.
File Services (waaronder VSS)	SMB 3.0, NFS4.0	SMB 3.0, NFS4.2	-

5 Applicatie Selectie Criteria

De navolgende tabel bevat de criteria die gehanteerd worden bij de selectie en/of acceptatie van applicaties. Bij elke applicatieselectie worden deze criteria meegenomen in het selectieproces, uiteraard aangevuld met de functionele criteria en toepassing specifieke criteria.

De (architectuur van de) oplossing moet vooraf worden getoetst door ProRail ICT Services aan kwaliteitseisen en de inpasbaarheid binnen de bestaande architectuur.

Er is een opdeling gemaakt in standaard applicaties (niet specifiek voor ProRail ontwikkeld) en maatwerk applicaties (wel specifiek voor ProRail ontwikkeld). Voor de laatste categorie gelden enkele additionele voorwaarden. "Knock-out" geeft aan of onverkort aan het criterium moet worden voldaan.

APPLICATIE SELECTIE CRITERIUM			
OK	Nr	Knock out	Algemeen (standaard en maatwerk applicaties)
	S1	Ja	Het platform voor servers is MS Windows 2022.
	S2	Ja	Het platform voor werkstations is MS Windows 10 Current -1 (22H2)
	S3	Nee	De gebruikersinterface is bij voorkeur WebBased.
	S4	Nee	Omgevingsinstellingen worden bij voorkeur opgeslagen in een aan het OS toegekende repository. Gebruikersinstellingen moeten centraal via een Group Policy (GPO) of Intune te beheren zijn.
	S5	Ja	Authenticatie (voorzover nodig) verloopt middels Microsoft Entra.. Zie S9
	S6	Ja	Authenticatie is gebaseerd op Modern Authentication (Tokens en claims).
	S7	Ja	Nieuwe applicaties moeten gebruik maken van Single Sign On functionaliteit o.b.v. Microsoft Entra Zie S9.
	S8	Ja	De applicatie gaat efficiënt om met de systeembronnen en is geschikt voor gevirtualiseerde hosts die gedeeld worden.
	S9	Ja	Voor applicaties wordt modern authenticatie geëist. Voorbeelden van compatibiliteit zijn OAuth, SAML of WS-Fed. (ref. IBB 24) Authenticatie via Microsoft Entra .
	S9-1	Nee	Waar mogelijk worden beschrijvende eigenschappen van userobjecten als onderdeel van het JWT-token doorgegeven aan de applicatie.
	S9-2	Ja	GraphAPI-toegang van het type "Delegated" zijn toelaatbaar. GraphAPI permissies van het type "Application permissions" zijn niet toegestaan.
	S9-3	Ja	Geautomatiseerd Inlezen/ophalen van userobjecten uit EntraID geschied middels SCIM-versie 2 met de meest restrictieve selectiecriteria mogelijk. Afkadering gebeurt a.d.h.v. ActiveDirectory/EntraID groepen.
	S10	Ja ²	De applicatie mag geen eisen stellen aan de omgeving, die conflicteren met andere applicaties, bijv. DLL's, registry-inhoud, java-versies, etc.
	S11	Ja ⁵	WebBased applicaties moeten op gedeelde applicatieservers kunnen werken. Hierbij is de voorkeur: MS Internet Information Server.

² Afwijken hiervan is mogelijk in zeer speciale gevallen, waar het gerechtvaardigd is om een serverapplicatie op (een) eigen server te installeren

	S12	Ja	De applicatie moet worden opgeleverd met een installatie programma (msi) en systeemdokumentatie (release documentatie, installatiedokumentatie, userdocumentatie), waaruit duidelijk blijkt wat de randvoorwaarden zijn, de systeem vereisten en afhankelijkheden.
	S13	Ja	De applicatie moet flexibel configureerbaar zijn. Er mogen in de uit te voeren code geen harde verwijzingen zijn naar IP-adressen, driveletters, paden (incl. UNC) en temp bestandslocaties.
	S14	Nee	De applicatie maakt voor data uitwisseling met de omgeving gebruik van open standaarden (XML, ODF etc.).
	S14-2	Ja	De applicatie- en gebruikersdata wordt opgeslagen in de ProRail cloudopslag (Azure storage). In uitzonderingsgevallen kan data op de generieke centrale opslagvoorziening (SAN) worden opgeslagen (vooraf goedkeuring vereist).

APPLICATIE SELECTIE CRITERIUM			
OK	Nr	Knock out	Algemeen (standaard en maatwerk applicaties)
	S15	Ja	De (server)applicatie kan via een script afgesloten worden zodat een consistente back-up gemaakt kan worden.
	S16	Ja	De data kan, online (terwijl de applicatie actief is) in de back-up meegenomen worden. De applicatie is verantwoordelijk voor het integer houden van de DB tijdens de backup.
	S17	Ja	Het functionele beheer kan worden uitgevoerd door gebruikers met aanvullende specifieke rechten (zonder administrator rechten). In de documentatie worden de rechten en de objecten/componenten waarop de rechten betrekking hebben beschreven.
	S18	Ja	De applicatie maakt geen gebruik van specifieke hardware (dongles) voor licentiebeheer.
	S19	Ja	De applicatie maakt gebruik van netwerkprinters.
	S20	Ja	De applicatie maakt gebruik van de standaard logging faciliteiten van het operating systeem.
	S21	Ja	De applicatie voldoet aan de eisen die de Nederlandse wet stelt ten aanzien van bijvoorbeeld archivering en bescherming van persoonsgegevens.
	S22	Ja	De applicatie wordt geleverd met een volledig ingevuld Applicatie Intake formulier. (AIF) Hierbij wordt gebruik gemaakt van het Intakeproces zoals dit binnen ProRail geldt.
	S23	Nee	Van een applicatie moet bekend zijn hoe de monitoring kan constateren dat de applicatie goed werkt op basis van het mee te leveren SCOM Management Pack.
	S24	Ja	Er moet een overzicht zijn van de eisen die de applicatie aan de infrastructuur stelt. Daarbij geldt de eis dat er gebruik wordt gemaakt van de standaard ProRail infrastructuur bouwblokken op gebied van server en storage.
	S25 ³	Ja	Het moet altijd mogelijk zijn de serverhardware te upgraden naar hardware met meer capaciteit, waarbij de wijzigingen in de applicatie/licensering vooraf duidelijk moet zijn.

³ Bijvoorbeeld logische opvolgers van toegepaste serversystemen met state of the art CPU's/cores

	S26	Ja	Server based applicaties en applicatiecomponenten moeten in een VMware ESX Enterprise gebaseerde virtuele omgeving kunnen draaien, inclusief continuïteit oplossingen zoals DRS en HA. Of als containers in een Azure Kubernetes omgeving.
	S27	Ja	Applicaties waarvan failover tussen rekencentra gepland is, dienen zelf te voorzien in integere datarelicatie op basis van bijvoorbeeld MS SQL Always on.
APPLICATIE SELECTIE CRITERIUM			
OK	Nr	Knock out	Algemeen (standaard en maatwerk applicaties)
	S28	Nee	Applicaties voor interactie met gebruikers moeten in een gedeelde 'server based computing' omgeving op basis van Citrix kunnen draaien.
	S29	Ja	Applicaties die een serverlicentie gebruiken, dienen de partitionering van VMware te erkennen als licentie-eenheid van de aantallen beschikbaar te stellen resources ⁴ .
	S30	Nee	Voor algemeen ter beschikking gestelde applicaties geldt dat de licentie uitgifte plaatsvindt op basis van (virtuele) werkplekken en niet op basis van accounts. De overige, individueel beschikbaar gestelde applicaties moeten op basis van de gebruiker doorbelast kunnen worden.
	S31	Ja	Voor naam resolutie wordt gebruik gemaakt van DNS. Statische tabellen/bestanden zijn niet toegestaan. Configuratie voor applicaties en applicatiekoppelingen op basis van ip-adressen is niet toegestaan.
	S32	Ja	De clientapplicatie moet geschikt zijn om middels MSI beschikbaar gesteld te worden.
	S33	Ja	De clientapplicatie moet geschikt zijn voor werkplekken (hardware en software, inclusief gesloten desktop) zoals door ProRail uitgeleverd ten tijde van acceptatie.
	S34	Ja	Indien een applicatie voor zijn functionaliteit afhankelijk is van door derden gedistribueerde software, dan dient de leverancier een actief geformuleerd beleid te hebben om de door haar geleverde software geschikt te maken voor de defacto standaardversies van de door derden geleverde software componenten die in de markt gebruikt worden, waarvan de aan ProRail geleverde applicatie afhankelijk is.
	S35	Nee	De applicatie biedt de mogelijkheid om het niveau van logging te specificeren (bv: information, warning, error, security). Hiervoor wordt een Management Pack (MP) voor Microsoft System Center Operation Manager meegeleverd. Indien er geen MP wordt meegeleverd kan er geen pro-actieve monitoring op het systeem plaatsvinden. Het toepassen van meegeleverde alternatieve monitorsystemen is niet toegestaan.
	S36	Ja	Een app voor mobiel dient data op te halen via geauthentiseerde webservices.
	S37	Ja	Een apparaat dat in het WGID kantoor netwerk wordt aangesloten, dient 802.1x te ondersteunen. Dit geldt zowel voor bedraad netwerk als Wifi. Voor datacenter apparatuur geldt deze eis niet. Het is niet toegestaan om met niet datacenter gekwalificeerde apparatuur deze eis te omzeilen door plaatsing in een datacenter. De datacenter apparatuur is weergegeven in de Technology Roadmap. In geval van twijfel beslissen de ProRail WGID - en ProRail netwerk ontwerper op basis van consensus.
Extra (maatwerk applicaties)			

⁴ Resources, definieerbare systeembronnen zoals sockets, cores en memory

ProRail

	E1	Ja	Indien de applicatie is gebaseerd op MS .Net of Java, dan dient de applicatie niet Java versie afhankelijk zijn. Ingeval van .Net moet de applicatie gebruik maken van een actief door Microsoft ondersteunde versie van het .Net framework conform de ProRail Technology Roadmap.
	E2	Ja	Als een informatie systeem een database gebruikt, dan is dit MS SQL, versies zoals bovenstaand
	E3	Ja	Er moet een duidelijke indicatie worden gegeven voor de grootte van de vereiste opslag/database en de te verwachten groei in de eerste twee jaar. Bij de te reserveren ruimte op het systeem moet ook rekening worden gehouden met schijfcapaciteit voor de online backup naar disk;
	E4	Ja	Er moet een duidelijke indicatie worden gegeven voor het te verwachten beslag dat de applicatie legt op systeemresources: geheugengebruik, CPU belasting, netwerkbelasting.
	E5	Ja	Er moet worden aangegeven welke vanuit de applicatie wenselijke/noodzakelijke specifieke parameters en/of opties moeten worden geconfigureerd

Colofon

Titel	Aansluitvoorwaarden ProRail ICT WGID
Versie/Datum	November 2024
Geldigheid	max 1 jaar na verschijning of een volgende versie van de Technology roadmap release.
Status	Goedgekeurd
Documentnummer	B105661 (GEKKO)
Van	Prorail ICT
Eigenaar	Service management
Distributie	Intern en externe leveranciers
Document	Aansluitvoorwaarden ProRail 5.01.docx