ProRail

Informatiebeveiliging ProRail

Logisch identiteits- en toegangsbeleid

Eigenaar ICT – CIO Office
Auteur Thijs Wientjes

Kenmerk IBB-24
Versie 3.12
Datum November 2022
Bestand IBB-2.4 Logisch identiteits- en toegangsbeleid.docx

Status Publicatie 3.12
Informatieclassificatie Intern

Inhoudsopgave

1 Introductie

In de beleidsdocumenten (IBB-21 – IBB-23) is het risicomanagement aan de orde geweest. Met ProRail Risicobeheersing als basis geeft dit document de kaders voor de persoon- en groep gebonden aspecten van de logische toegang.

Het doel van dit document is de kaders uit zetten voor het gebruik van identiteiten, authenticatie (bewijs van identiteiten) en autorisatie (toekennen van rechten).

2 Logische toegangsarchitectuur

De informatievoorziening van ProRail kan niet functioneren op een eiland. Informatie van partners in de railsector is van belang voor het primaire proces van ProRail en omgekeerd is dat ook waar: partners zijn afhankelijk van informatie die ProRail levert.

ProRail gebruikt de informatievoorziening en de beveiliging hiervan om haar positie te versterken. Dat betekent dat de infrastructuur moet zijn ingericht op het faciliteren van toegang tot diensten voor medewerkers en externen op een veilige manier. Dit kan alleen door controle te houden op wie wat kan doen. Identiteits- en toegangsbeheer en compartimentering van de infrastructuur (door verschillende zones te creëren) zijn hiervoor geschikte maatregelen. Hiermee kunnen standaardoplossingen voor de beveiliging van de diversiteit aan systemen aangeboden worden die eenvoudig te beheren zijn.

2.1 Uitgangspunten

- Het beleid is uniform geldig voor alle systemen binnen de infrastructuur van ProRail binnen heel ProRail. Binnen domeinen met een hoger security-risico (zoals VL) dienen extra maatregelen geïmplementeerd te worden om het verhoogde risico te mitigeren en/of weg te nemen;
- Interactie en continuïteit zijn kenmerkende aspecten voor ProRail's ICT;
- Medewerkers dienen op kantoor toegang te hebben tot applicaties die door ProRail ter beschikking zijn gesteld, opslag, printers, e-business applicaties[1] en ProRail's publieke diensten;
- Medewerkers die niet op kantoor zijn hebben toch toegang nodig tot bedrijfsapplicaties, opslag, printers, e-business applicaties, ProRail's publieke diensten en externe diensten;
- Business partners hebben toegang nodig tot e-business applicaties en de publieke diensten van ProRail. Hierin dient alleen toegang gegeven te worden tot de informatie die voor de partner van belang is;
- Voor onderhoud aan systemen hebben derden toegang tot systemen en netwerkcomponenten nodig;
- De rest van de wereld heeft alleen toegang tot de publieke diensten van ProRail;
- Naast personen hebben ook andere actoren (zoals andere informatiesystemen) toegang nodig tot ProRail informatie en/of informatiesystemen;
- Voor alle typen van toegangsverlening tot informatie dient deze toegang altijd identificeerbaar te zijn naar de actor die deze toegang heeft opgevraagd;
- Het beheer van identiteiten en het bewijzen ervan is altijd strikt gescheiden van het toekennen van autorisaties aan die identiteiten.

[1] Bij ProRail wordt onder e-business applicaties verstaan: de groep applicaties die met business partners wordt gebruikt

2.1.1 Definities identiteit, authenticatie en autorisatie

Ten behoeve van dit beleid hanteren we de definities voor identiteit, authenticatie en autorisatie zoals samengevat in de volgende tabel:

Begrip	Defintiie	Kenmerk	Uniek?
Identiteit	Het feit wie een persoon of wat een entiteit/ding is. Beantwoordt de vraag: “Wie ben je?”	Publieke bewering, aangeboden door te autoriseren entiteit. Oftewel: degene die iets wil vertelt wie hij is.	Ja
Authenticatie	Het proces of de actie van bewijzen of aantonen dat de bewering waar, echt, of valide is. Beantwoordt de vraag: “Wat is je bewijs?”	Persoonlijk geheime reactie of persoonlijk bezit, aangeboden door te autoriseren entiteit.	Nee
Autorisatie	De daadwerkelijke actie van het autoriseren: Officiële toestemming of goedkeuring geven aan hetgeen de entiteit wil uitvoeren. Beantwoordt de vraag: “Mag je wat je wilt uitvoeren?”	Identiteitsbewijs nodig met daarin de gebruikte kenmerken voor toegangscontrole. De eigenaar van het object bepaalt volledig of hij het bewijs accepteert, en of hij de toestemming verleent.	n.v.t.

Met andere woorden, door:

1. de unieke, publieke identiteit
2. te verifiëren met een geheime/privé reactie op een opgave voor bewijsvoering, kan
3. op basis van de kenmerken van deze bewezen identiteit het juiste niveau van toegang verleend worden.

2.2 Identiteiten

De beleidsnormen binnen dit document gelden voor alle digitale identiteiten die binnen ProRail gebruikt worden. Bovenstaande uitgangspunten leiden tot onderstaande generieke eisen aan die identiteiten:

- Voor toegang tot publieke diensten is geen unieke identiteit benodigd;
- Voor toegang tot semi-publieke diensten (Vertrouwelijkheid=Laag) is een unieke identiteit benodigd in een door ProRail beheerde of vertrouwde identiteitendatabase;
- Voor alle andere ProRail diensten is een unieke identiteit benodigd in een door ProRail beheerde of vertrouwde identiteitendatabase;
    - Aan deze identiteit ligt altijd een formele overeenkomst (contract) ten grondslag dat de kaders schetst voor het uitvoeren van werkzaamheden in ProRail systemen;
- Het gebruik van een identiteit is alleen toegestaan voor of door de entiteit waaraan deze identiteit expliciet is toegewezen in overeenstemming met de accounttypen beschreven in hoofdstuk 3;
- Elke identiteit bevat alle kenmerken die nodig zijn om (1) de unieke actor te kunnen identificeren en (2) de toegangsverlening tot informatiesystemen expliciet te kunnen toepassen;
    - De identiteiten bevatten naast voornaam en achternaam geen privacygevoelige gegevens zolang deze niet expliciet benodigd zijn voor de direct bovenstaande punten (1) en (2).

2.3 Authenticatie: bewijs van identiteiten

Voor authenticatie voor toegang tot informatiesystemen dient het bewijs van de identiteit voldoende kenmerken te hebben om aan te tonen dat het de betreffende identiteit is. Afhankelijk van het beveiligingsniveau van het te benaderen systeem of informatie bestaat dit uit 1 of meer kenmerken. Dit leidt globaal tot de volgende eisen:

- Publieke diensten zijn voor iedereen beschikbaar zonder authenticatie;
- Semi-publieke diensten (Vertrouwelijkheid=Laag): De informatie en diensten hebben weliswaar een lage vertrouwelijkheid maar om tactische reden dient te worden geauthentiseerd met een Gebruikersnaam/Wachtwoord;
- Om bij toegang vanaf het ProRail-netwerk geautoriseerd te kunnen worden voor applicaties die door ProRail ter beschikking zijn gesteld die zijn geclassificeerd met vertrouwelijkheid midden of hoog dient geauthentiseerd te worden met gebruikersnaam en wachtwoord;
- Om bij toegang vanaf niet-ProRail netwerken geautoriseerd te kunnen worden voor applicaties met een bedrijfsmatige toepassing die zijn geclassificeerd met vertrouwelijkheid midden of hoog dient geauthentiseerd te worden met een multi-factor authenticatiemethode, bijvoorbeeld een persoonlijk bezit (token, ProRail device-certificaat);
- Reguliere gebruikers op werkstations binnen de ProRail Netwerken (KA, VL, OCCR, Donna enz.) authentiseren met gebruikersnaam en wachtwoord voor toegang tot de applicaties;
- High-privileged gebruikers (zie hoofdstuk 3 voor details) op werkstations binnen de ProRail Netwerken (KA, VL, OCCR, Donna enz.) authentiseren met multi-factor authenticatie voor toegang tot beheerfuncties van de IT-services;
- Tokens ten behoeve van bewijs van identiteit voor ProRail systemen worden altijd een op een gekoppeld aan een entiteit uitgegeven. Gedeelde tokens zijn hiervoor dus niet toegestaan.

2.3.1 Authenticatiedirectory / Single Sign-on

Voor een beheersbare en daardoor beveiligde authenticatie van entiteiten moet deze taak gedelegeerd worden aan een centrale, beveiligde authenticatiedienst (bijvoorbeeld Active Directory of PKI).

Deze authenticatiedirectory wordt primair gevoed vanuit de identiteitendatabase (op dit moment het identity manager systeem IDM). Additionele kenmerken voor identiteiten die nodig zijn om de toegangsverlening tot informatiesystemen expliciet te kunnen toepassen (bijvoorbeeld additionele business rollen) die niet in de identiteitendatabase aanwezig zijn kunnen vanuit andere brongegevens worden gevoed.

Nieuwe systemen dienen tijdens implementatie (en dus voor vrijgave naar productie) gekoppeld te worden, bestaande systemen op basis van het verhoogde risico dat niet-gekoppeld zijn betekent, maar minimaal bij revisie.

In de KA omgeving is een standaard authenticatieprovider (de KA Active Directory) aanwezig waarvan gebruik gemaakt dient te worden. In andere ProRail netwerkdomeinen die van de KA omgeving gescheiden zijn, dient een eigen centrale authenticatieprovider aanwezig te zijn.

Externe identiteiten/accounts zijn of opgenomen in de centrale authenticatiedirectory of worden geauthentiseerd op basis van een vertrouwde externe authenticatiedirectory (bijvoorbeeld via federatie / OAuth, etc.)

In de bedrijfsdirectory dient het onderscheid tussen interne medewerkers, ingehuurd personeel en extern personeel (partners) te allen tijde direct en eenduidig te zijn vast te stellen.

2.3.2 Vereist minimaal authenticatieniveau in relatie tot locatie

Het niveau van gevraagd identiteitsbewijs is afhankelijk van de locatie waar de gebruiker zich bevindt. Kort samengevat gelden hierbij de regels zoals gegeven in onderstaande tabel:

Toegang	Medewerker	Partner
Vanaf netwerk ProRail	Gebruikersnaam / wachtwoord	
Vanaf besloten externe netwerken	Afhankelijk van classificatie applicatie: (Federatie, Sterke authenticatie of Gebruikersnaam / wachtwoord).	
Vanaf andere netwerken	Multi-Factor authenticatie	

Dit betreft het minimale niveau. Afhankelijk van de classificatie van het doelsysteem en het type account kunnen extra maatregelen van toepassing zijn.

2.3.3 Multi-factor Authenticatie

Multi-factor authenticatie kent een aantal gradaties. Binnen ProRail dienen de volgende standaardcombinaties van apparaat en authenticatiemethode ingezet te worden bij toegang vanaf externe netwerken:

Apparaat	Toegang tot	Authenticatiefactoren:
ProRail laptop	KA	1. Directe VPN met versleuteling en Certificaat 2. KA uid/Wachtwoord
ProRail Mobiele device	KA	1. ProRail Mobiel device management 2. KA uid/Wachtwoord
Any	Browser-gebaseerde applicaties die door ProRail ter beschikking zijn gesteld (https)	1. Persoonlijke token 2. Wachtwoord
Mobiele device (niet ProRail)	Outlook App	1. Beveiliging device met pincode (ProRail activesync policies) 2. Wachtwoord
Any	KA	1. Persoonlijke token 2. Wachtwoord
VL werkplek	VL applicaties	1. Wachtwoord voor aan werkplek gebonden operator account 2. Persoonsgebonden registratie van toegang tot de ruimte waar de VL werkplek zich bevindt (dit kan fysiek of digitaal zijn).
ProRail laptop	VL applicaties	1. Geen directe toegang, maar alleen toegang tot VL werkplek 2. Via KA en beveiligde publicatieservice voor de werkplek 3. Wachtwoord en Persoonlijke fysieke token
ProRail laptop	Beheer DMZ GROEN / VL / M&S	1. Via KA en beheerproxy 2. Persoonlijke fysieke token 3. Wachtwoord
Any	Beheer Niet-KA	1. Via beheerproxy. Nooit direct. 2. Ontkoppeld via remote toegangssysteem met eigen authenticatiedirectory.

2.4 Autorisatie: Toegangscontrole voor personen tot informatiesystemen

Voor toegangsverlening (autorisatie) gelden globaal de volgende eisen:

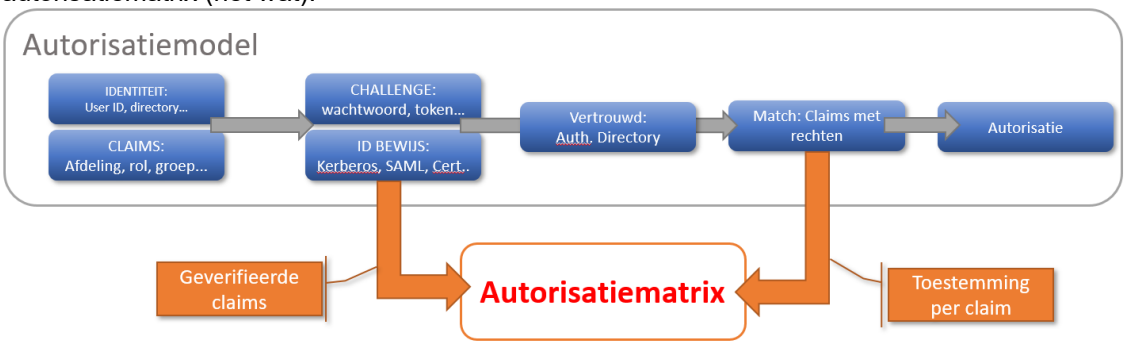
- Autorisaties zijn primair gekoppeld aan de rol van een persoon in de organisatie (business rol) en worden gegeven op basis van 'need-to-know';
- Naast de kenmerken van de identiteit zelf, dienen ook andere kenmerken te worden geëvalueerd voordat toegang wordt geautoriseerd, bijvoorbeeld:
  - De locatie waar de identiteit zich bevindt (zie sectie 2.4.2)
  - Het apparaat dat de identiteit gebruikt om toegang te verkrijgen
  - Het tijdstip waarop de identiteit gebruikt wordt om toegang te krijgen
- Gebruikers krijgen geen lokale administrator autorisaties op hun werkplek;
- Hoger geclassificeerde sub-netwerken als VL zijn nooit rechtstreeks van buiten ProRail te benaderen en deze toegang is vanuit andere ProRail netwerken per definitie sterk gelimiteerd en gebonden aan specifieke rollen (niet aan generieke businessrollen).

2.4.1 Vastlegging van autorisaties

Voor elk informatiesysteem dienen de afgesproken autorisatieniveaus, de toekenningen van businessrollen en/of specifieke rollen aan deze autorisatieniveaus, en de rechten behorende bij deze autorisatieniveaus te zijn vastgelegd in een administratie die zich buiten dat informatiesysteem bevindt (specifiek: vastgelegd in een autorisatiematrix).

Op basis van deze administratie dienen de toegekende rechten binnen een informatiesysteem periodiek door een ProRail interne audit-afdeling te worden getoetst aan de gemaakte afspraken (auditeerbaarheid).

Deze administratie dient onderscheid te maken tussen het autorisatiemodel (het hoe), en de autorisatiematrix (het wat):



Het autorisatiemodel beschrijft:

- Welke kenmerken moet de identiteit bevatten om deze te kunnen autoriseren (rol, afdeling, wijze van aanstelling, etc.);
- Welke digitale identiteitsgegevens daarvoor gebruikt worden;
- Hoe die kenmerken uit de digitale identiteit worden afgeleid en aangeboden aan het informatiesysteem (attributen als groepslidmaatschap, personeelsnummer of andere attributen die in het identiteitsbewijs aanwezig zijn).

De autorisatiematrix beschrijft:

- Welke rechtenniveaus (technische systeemrollen) het informatiesysteem bevat;
- Aan welke businessrollen / attributen deze autorisatieniveaus worden toegekend;
- Welke rechten met deze rechtenniveaus worden verkregen.

2.4.2 Toegangseisen voor Gegevensverzamelingen.

Gegevensverzamelingen met een hoger vertrouwelijkheidsniveau dan "Laag" hebben een gelimiteerde toegang. (bv. HR-data, financiële gegevens, aanbestedingsinfo., enz).

Toegangsaanvragen tot dit soort gegevens dienen altijd door de data-eigenaar (of diens gedelegeerde) gefiatteerd te worden. *De goedkeuring van een lijnmanager van de aanvrager is in deze onvoldoende.*

2.4.3 Toegangseisen met betrekking tot locatie

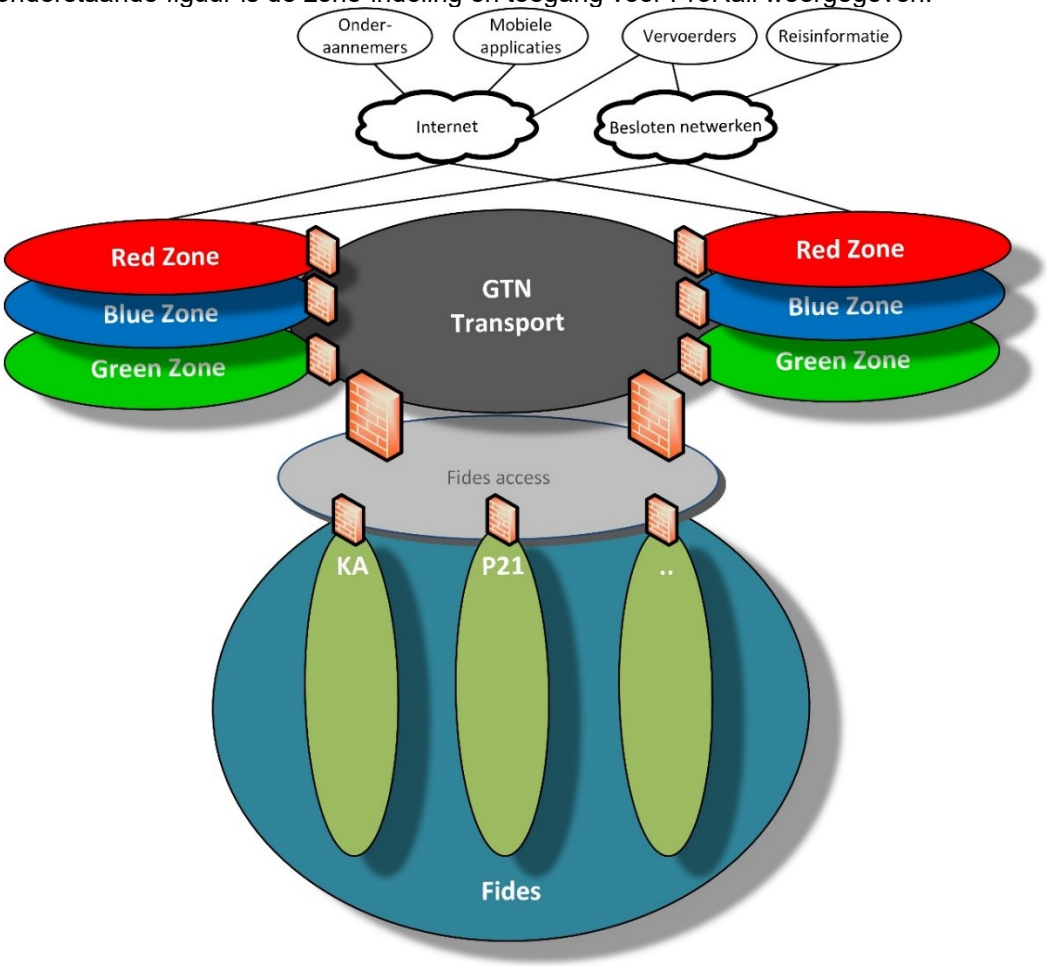
Ter ondersteuning van een veilige toegang van entiteiten die zich buiten het vertrouwde netwerkdomein bevinden (externe systemen) is de interne infrastructuur gezoneerd. Per zone kunnen specifieke toegangseisen gelden.

Deze zonering is vergelijkbaar met de fysieke beveiliging van gebouwen: voor de receptie is een publieke ruimte, erachter de kantoren en apart hiervan zijn er apparatuur- of computerruimten. Dit maakt het mogelijk om hanteerbare oplossingen te implementeren voor aansluiting van verschillende partners.

Uitgangspunten van de compartimentering zijn:

- Vanwege de verschillende beschikbaarheid-eisen die aan onze systemen worden gesteld, wordt onderscheid gemaakt tussen meerdere gebruikersnetwerken. (VL/P21, KA, Infoplus/reisinformatie, Donna, OCCR, meten& sturen enz.);
- De domeinen Donna, OCCR en Reisinformatie hebben vanwege de aanwezigheid van verschillende organisaties in het domein, aparte authenticatiedirectories;
- Voor de interne domeinen is een basis BIV classificatie vastgesteld die minimaal gehanteerd moet worden voor toegang tot een systeem in die domeinen. Deze classificaties zijn uitgewerkt in hoofdstuk 5;
- ProRail-medewerkers die vanaf externe locaties via de beveiligde toegang verbonden zijn hebben dezelfde mogelijkheden als de medewerkers op het kantoornetwerk (Citrix, DA-Laptop);
- De extern gepubliceerde applicaties die interne data publiceren (e-businessapplicaties) worden geplaatst in de extranets. Extranets zijn beveiligde netwerkzones waar geautoriseerde externen toegang krijgen. Publieke diensten worden aangeboden vanuit een aparte beveiligde netwerkzone.

In onderstaande figuur is de zone-indeling en toegang voor ProRail weergegeven.



De interne koppelingen zijn nader uitgewerkt in: ***IBB-26 Interne connectie standaarden***
De externe koppelingen zijn nader uitgewerkt in: ***IBB-25 Externe connectie standaarden***

2.5 Overig, referenties

- **Maatregelen per beveiligingsniveau**
  De minimale maatregelen voor Beschikbaarheid, Integriteit en Vertrouwelijkheid zijn beschreven in:
  IBB-23 Risicobeheersing en classificatie bij Informatievoorziening ProRail

- **Externe Connecties**
  De mogelijkheden en maatregelen voor externe toegang zijn beschreven in:
  IBB-25 Externe connectie standaarden

- **Interne Connecties**
  De mogelijkheden en maatregelen voor interne verbindingen en toegang zijn beschreven in:
  IBB-26 Interne connectie standaarden

- **Operationeel wachtwoordbeleid ICT**
  Praktische uitwerking van het wachtwoordbeleid:
  IBB-1.2 Handboek informatie beveiliging ProRail: *Hoofdstuk: Wachtwoordbeleid*

- **Baseline Informatiebeveiliging Overheid**
  Vanuit CIO-Office is besloten dat ProRail zich conformeert aan de BIO (Baseline Informatiebeveiliging Overheid, https://bio-overheid.nl/). De BIO is de overheidsuitwerking van de ISO 27001. Binnen deze BIO is ook het thema toegangsbeveiliging uitgewerkt: https://www.cip-overheid.nl/media/1553/202010-bio-thema-uitwerking-toegangsbeveiliging-v20-def.pdf

- **Definitiedocument: Identiteit, Authenticatie en Autorisatie (en hoe we dit helpen implementeren)**
  Document ter verduidelijking van het onderscheid tussen identiteit, authenticatie en autorisatie, dat is opgesteld om de lezer van dit beleid van de voorkennis te voorzien om dit beleid beter te kunnen implementeren.

3 Soorten accounts

Principieel is dat iedereen op persoonlijke titel en met een persoonlijk account aanmeldt en authentiseert op de ProRail infrastructuur. Er zijn echter situaties waarbij een persoonlijk account een niet werkbare situatie oplevert of zelfs technisch niet mogelijk is.

Om voor alle situaties een beveiligde situatie te handhaven gaat dit hoofdstuk in op de verschillende typen accounts die we binnen ProRail hanteren. Samengevat maken we onderscheid tussen:

1. Persoonlijke accounts
   Dit zijn accounts die 1 op 1 aan een persoon zijn gekoppeld, en door die persoon gebruikt worden om zich te authentiseren en de acties uit te voeren waarvoor die persoon via de kenmerken van deze account is geautoriseerd. Van dit type account bestaan 2 verschijningsvormen:
   a. Regulier account
      Dit is het primaire account waarmee de persoon de standaardwerkzaamheden binnen ProRail uitvoert;
   b. High-privileged account
      Hieronder vallen alle accounts waaraan additionele rechten zijn toegekend die gebruikt worden voor het wijzigen van de technische configuratie van de technische ICT-of OT-services en systemen.

2. Niet-persoonlijke accounts
   Dit zijn accounts die niet zijn gekoppeld aan een persoon, maar aan een andere entiteit, bijvoorbeeld een device of een applicatie-service. Van dit type bestaan 3 verschijningsvormen:
   a. Serviceaccounts:
      Accounts ten behoeve van het uitvoeren van taken door een device of een applicatie-service;
   b. Resourceaccounts
      Accounts ten behoeve van het uitvoeren van taken door meerdere personen op een gedeelde resource, waarbij het gebruik van persoonlijke accounts aantoonbaar tot een onwerkbare en/of onveilige situatie leidt of technisch niet te realiseren is.
   c. Robotaccounts
      Accounts ten behoeve van het geautomatiseerd nabootsen van menselijk gedrag in en zo representatief mogelijke menselijke context

3.1 Persoonlijk Account: Regulier Account

Een persoonlijk regulier account vertegenwoordigt één persoonlijke identiteit binnen ProRail. Dit accounttype kent een aantal categorieën:

Categorie	Bron:	Opmerking:
Eigen personeel	SAP-HR	
Inhuur personeel “op naam”	SAP-HR + Inhuurdesk	
Inhuur personeel “op capaciteit”	IdM (door lijnmanager)	(=projectaccount)
Extern Account *)	IDM (door externe partij)	Format: EX_bedrijf_naam
Persoonlijk account via Federatie	Gefedereerde partij	

*) Een extern Account krijgt toegang tot een specifieke applicatie of zone.

- Een specifieke directory in SharePoint (Ook online) voor samenwerking
- Een specifieke applicatie, zoals SAP.

Externe accounts dienen elk jaar verlengd te worden door de beheerder. Wanneer de verlenging niet wordt toegepast, verloopt de geldigheid va het account.
Accounts bij Inhuur op capaciteit hebben een looptijd van maximaal 1 jaar en kunnen verlengd worden, als dat gewenst is, met max. 1 jaar, tot einde contract.
Bij einde dienstverband of einde registratietermijn worden de accounts geblokkeerd en zijn niet overdraagbaar aan anderen. Ter volledigheid: Aanmelden met een andermans account geldt volgens de AVG als identiteitsfraude en is daarmee expliciet verboden !

3.2 Persoonlijk account: High-privileged account

3.2.1 Definitie

De definitie van een high-privileged account in het kader van Identiteit- en Toegangsbeheer binnen ProRail luidt:

Alle accounts waaraan additionele rechten toegekend zijn die gebruikt worden voor het wijzigen van de technische configuratie van de ICT services en systemen.

3.2.2 Voorbeelden

Ter verduidelijking bevat onderstaande tabel enkele voorbeelden van ICT accounts, met een beschrijving of en waarom de wel of niet binnen de bovenstaande definitie vallen.

Voorbeeld	High privilege account?	Uitleg
Windows/Linux/netwerk beheerder VL	JA	Deze accounts zijn specifiek bedoeld om de technische configuratie van netwerk en/of platformen aan te passen, met potentieel grote (onbedoelde) invloed op de treinenloop.
Technisch applicatiebeheerder	JA	Deze accounts zijn specifiek bedoeld om de technische configuratie van toepassingen aan te passen, met potentieel grote (onbedoelde) invloed op de treinenloop.
Functioneel applicatiebeheerder	NEE	Deze account passen alleen de interne administratie van een toepassing aan en niet de technische werking.
SharePoint poweruser	NEE	Dit is een verbijzondering van een functioneel applicatiebeheerder.
Operationeel account VL applicatie	NEE	De VL medewerker kan met dit account wel de treinenloop beïnvloeden, maar dat is de kernfunctie van de toepassing die de VL medewerker gebruikt. Dit account kan echter NIET worde gebruikt om de technische configuratie van de toepassing aan te passen.
Beheeraccount KA	JA	Deze accounts zijn specifiek bedoeld om de technische configuratie van toepassingen en IT services aan te passen, met potentieel grote invloed op toegankelijkheid van informatie en/of functies met grote invloed op de ProRail bedrijfsprocessen, inclusief (indirect) de treinenloop.

3.2.3 Extra eisen t.a.v. high-privileged accounts[2]

- De privileged accounts kunnen op 2 manieren worden gerealiseerd: door de rechten op het primaire account tijdelijk te verhogen, of door een secundair account ter beschikking te stellen;
    - De eerstgenoemde optie heeft daarbij de voorkeur;
- In alle gevallen dienen extra maatregelen actief te zijn om deze verhoogde rechten, ongeacht type implementatie, veilig en gecontroleerd aan de medewerker ter beschikking te stellen. Deze uitgifte vindt plaats onder verantwoordelijkheid van een business rol/functie van die los staat van de business rol/functie die verantwoordelijk is voor de uitgifte van identiteiten;
    - Multi-factor authenticatie kan hiervoor als maatregel worden ingezet, wanneer deze wordt vereist door de te benaderen ICT service;
- Administratie en opslag van deze beheertoegangsgegevens dient altijd uitgevoerd te worden conform de BIV classificatie met integriteit en vertrouwelijkheid HOOG;
- De secundaire accounts zijn herkenbaar als beheeraccount (voorvoegsel _beh) en zijn altijd persoonlijk;
- Alle activiteiten uitgevoerd met dit account dienen te worden gelogd;

[2] De toewijzing van verhoogde rechte in Azure en Azure DevOps zoals die nu door ProRail gehanteerd wordt is een voorbeeld van een implementatie die aan de extra eisen voor high-privileged accounts voldoet.

- Een secundair account mag niet voor standaard gebruikersacties (zoals standaard KA taken) gebruikt worden, dus naast dit account heeft een gebruiker ook een normaal account;
- Het is niet toegestaan met dit account een permanente interactieve inlogsessie te hebben op een werkplek, ongeacht de verschijningsvorm van die werkplek;
- Het is niet toegestaan high-privileged accounts direct te gebruiken voor authenticatie op een ProRail remote access service.

3.3 Niet persoonlijk accounts: Service-/machineaccount

3.3.1 **Definitie**

De definitie van een serviceaccount in het kader van Identiteit- en Toegangsbeheer binnen ProRail luidt:

Accounts ten behoeve van het uitvoeren van taken door een device of een applicatie-service

Een machine-account is hiermee dus een specifieke vorm van een serviceaccount. Hierna zal alleen de term serviceaccount gebruikt worden.

3.3.2 **Voorbeelden**

Voorbeelden voor het gebruik van een serviceaccount zijn:

- Een toepassing heeft toegang nodig tot een gegevensbron, bijvoorbeeld een database;
- Een toepassing heeft lokaal extra rechten nodig om een proces uit te kunnen voeren, bijvoorbeeld een lokale registeraanpassing;
- Op een server dient op afroep of periodiek automatisch een taak of script uitgevoerd te worden, bijvoorbeeld een automatische installatie of een gegevensback-up;
- Een toepassing wil functionaliteit aanroepen, die zich buiten die toepassing bevindt, bijvoorbeeld het aanroepen van een API van een externe applicatie;
- Een device authentiseert zich op een netwerkservice om toegang te krijgen tot services op dat netwerk.

3.3.3 **Extra eisen t.a.v. serviceaccounts**

- Gelijk aan een persoonlijk account, dienen serviceaccounts altijd 1 op 1 gekoppeld te zijn aan de device of applicatieservice die deze account gebruikt;
- Applicaties kunnen meerdere services bevatten. Indien per service verschillende risicoprofielen bestaan, dient per service binnen de applicatie gebruik gemaakt te worden van gescheiden serviceaccounts (bijvoorbeeld 1 voor het uitvoeren van de applicatie zelf, en een apart account voor het extern (cloud) ophalen van gegevens);
- Serviceaccounts mogen niet gebruikt worden voor interactieve logons/gebruikerssessies;
- Het serviceaccount krijgt expliciet alleen die autorisaties toegewezen die voor het functioneren van de betreffende toepassing noodzakelijk zijn;
    - Het wijzigen van rechten voor groepen gebruikers mag geen wijziging in rechten voor het service-account tot gevolg hebben tenzij dit mechanisme aantoonbaar noodzakelijk is voor het functioneren van de toepassing;
    - Generieke rechten die voor alle ProRailers gelden, zoals Office, intranet- en internettoegang mogen NIET standaard worden toegewezen aan een service-account. Deze worden alleen minimaal en expliciet toegekend wanneer dit voor de functionaliteit van het serviceaccount noodzakelijk is
- Serviceaccounts zijn herkenbaar door gebruik van een voorvoegsel in de authenticatiedirectory (bijvoorbeeld _SVC);
- Voor elk serviceaccount dient in de beheerdocumentatie van de betreffende toepassing een werkinstructie aanwezig te zijn die in detail beschrijft hoe een wachtwoordwijziging voor het serviceaccount moet worden uitgevoerd;
    - Deze documentatie dient te zijn opgeslagen op een veilige locatie;
- Het serviceaccount dient administratief te worden opgeslagen als onderdeel (configuratie-item) van de toepassing waaraan het serviceaccount is toegewezen;
    - Deze administratie bevat geen wachtwoordgegevens
    - De verantwoordelijkheid van deze administratie is persoonlijk (op naam) toegewezen aan de eigenaar van het systeem
- Het beheer en de uitgifte van serviceaccounts en wachtwoorden vindt plaats onder verantwoordelijkheid van een business rol/functie van die los staat van de business rol/functie die verantwoordelijk is voor het beheer van de betreffende toepassing;

- Administratie en opslag van deze beheertoegangsgegevens dient altijd uitgevoerd te worden conform de BIV classificatie met integriteit en vertrouwelijkheid HOOG;
- Alle activiteiten uitgevoerd met serviceaccounts dienen te worden gelogd.

3.4 Niet persoonlijk accounts: Shared-Resourceaccount

3.4.1 Definitie

De definitie van een resourceaccount in het kader van Identiteit- en Toegangsbeheer binnen ProRail luidt:

Accounts ten behoeve van het uitvoeren van taken door meerdere personen op een gedeelde resource, waarbij het gebruik van persoonlijke accounts aantoonbaar tot een onwerkbare en/of onveilige situatie leidt

3.4.2 Voorbeelden

Voorbeelden voor het gebruik van een resource account zijn:

Type	Voorbeeld	Kenmerken
Placeholder	Gedeelde Outlook mailbox	- Een op een gekoppeld aan de mailbox - Account is uitgeschakeld - Account wordt nooit gebruikt voor login
Shift operator	- Receptie - Operationele werkplek - OT operator station - OCCR werkplek	- T.b.v. speciale functies die op capaciteit gecontracteerd zijn. - Resource wordt per dagdeel door een andere medewerker gebruikt maar de inhoud is gericht op de functie. - Logon vereist op de resource
Single purpose werkplek	- Kiosk - Monitorwerkplek	- Bedoeld om specifieke informatie permanent te tonen (zonder stand-by / schermbeveiliging), bijvoorbeeld via een webbrowser, of monitoringapplicatie.
Built-in accounts	- root - administrator	- Standaard aanwezige gebruikers in resources na installatie - Standaard niet gebruikt - Beheer en uitgifte valt onder beleid high-privileged accounts
Installatie-account		- Bedoeld om bepaalde applicaties die dit vereisen periodiek te upgraden via een interactieve loginsessie - Standaard uitgeschakeld, en alleen ad-hoc geactiveerd t.b.v. geplande installatiewerkzaamheden.

3.4.3 Extra eisen t.a.v. resourceaccounts

- Gelijk aan een persoonlijk account, dienen resourceaccounts altijd een op een gekoppeld te zijn aan de resource waarvoor deze account gebruikt wordt;
    - De verantwoordelijkheid voor het account is daarbij persoonlijk (op naam) toegewezen aan de eigenaar van de betreffende resource
- Deze resource bestaat uit ofwel één device, ofwel enkele devices gegroepeerd op één beperkte locatie (bijvoorbeeld een receptie);
- Resourceaccounts mogen niet gebruikt worden voor interactieve logons/gebruikerssessies op andere resources dan waar de account expliciet aan is toegewezen;
- Het resourceaccount krijgt expliciet alleen die autorisaties toegewezen die voor het uitvoeren van de specifieke functie noodzakelijk zijn;
- Resourceaccounts zijn herkenbaar door gebruik van een voorvoegsel in de authenticatiedirectory (bijvoorbeeld RSC_);
- Voor elk resourceaccount dient in de beheerdocumentatie van de betreffende resource een werkinstructie aanwezig te zijn die in detail beschrijft hoe een wachtwoordwijziging voor het resourceaccount moet worden uitgevoerd;
- Het resourceaccount dient administratief te worden opgeslagen als onderdeel (configuratie-item) van de resource waaraan het resourceaccount is toegewezen;
    - Deze administratie bevat geen wachtwoordgegevens

- Alle activiteiten uitgevoerd met resourceaccounts dienen te worden gelogd;
    - Deze logging moet met extra informatie te combineren zijn zodat de onder dat account uitgevoerde acties herleidbaar zijn naar een persoon;
- Voor elke nieuwe resourcetype dient eerst een detailontwerp ter goedkeuring te worden voorgelegd, waaruit duidelijk blijkt:
    - Dat de beoogde functionaliteit niet werkbaar en veilig realiseerbaar is via gebruik van standaard persoonlijke accounts;
    - Welke extra toegangsbeperkingen aan het resourceaccount en/of de resource zijn opgelegd om misbruik te voorkomen.

3.4.4 **Voorbeelden van extra maatregelen**

- De resource bevindt zich op een locatie met extra maatregelen voor fysieke toegangsbeveiliging, bijvoorbeeld een afgesloten ruimte of direct persoonlijk toezicht;
- De resourceaccountgegevens zijn bij niemand bekend doordat automatisch wordt ingelogd;
- Inlogrestrictie op basis van Tijd/ locatie;
- Expliciete denies op resources;
- Herleidbaarheid van gebruik naar persoon via cameratoezicht.

3.5 Niet-persoonlijke accounts: Robotaccount

3.5.1 **Definitie**

De definitie van een robotaccount in het kader van Identiteit- en Toegangsbeheer binnen ProRail luidt:

Een account specifiek voor het nabootsen van een fysieke persoon die als eindgebruiker de standaard functionaliteit van een of meer toepassingen aanroept via dezelfde gebruikersinterface(s) die de fysieke persoon hiervoor zou gebruiken

Deze account houdt hiermee het midden tussen een shared resource account en een serviceaccount, maar kan niet aan alle voorwaarden voor een serviceaccount voldoen, en dient tegelijkertijd strikter beveiligd en beheerd te worden dan een shared resource account.

3.5.2 **Voorbeelden**

Voorbeelden voor het gebruik van een robotaccount zijn:

- Het geautomatiseerd vaststellen van de beschikbaarheid van specifieke applicatiefuncties voor eindgebruikers, zowel in test als in productie;
- Het geautomatiseerd uitvoeren van testscenario's, inclusief testflows die zich over een keten van meerdere applicaties afspelen;
- Het geautomatiseerd uitlezen van dashboards t.b.v. projectie op een groot scherm voor een hele afdeling;
- Het geautomatiseerd uitvoeren van repeterende werkzaamheden die uit stappen bestaan die normaal gesproken handmatige handelingen door een persoon betreffen in die betreffende toepassing(en).

3.5.3 **Extra en/of specifieke eisen t.a.v. robotaccounts**

Eisen aan de account zelf en het beheer en de inzet ervan:

- Robotaccounts moeten herkenbaar zijn door gebruik van een voorvoegsel in de authenticatiedirectory (bijvoorbeeld _RBT);
- Toepassingsgebied van robotaccounts moet herkenbaar zijn door gebruik van een achtervoegsel in de authenticatiedirectory (test, acc, prod e.d.)
- Voor een robotaccount dient een interactieve gebruikersomgeving (op een client-omgeving) geconfigureerd te zijn die 1 op 1 aan dat account is gebonden;
- De robotaccount mag op enig moment slechts 1 specifieke werkplek/ gebruikerssessie ingelogd zijn (1 account, 1 werkplek, 1 werk-set);
- De aanmeldgegevens van de robotaccount dienen te voldoen aan de wachtwoordeisen zoals die ook gelden voor serviceaccounts;

- Het beheer en de uitgifte van robotaccounts en wachtwoorden vindt plaats onder verantwoordelijkheid van een business rol/functie van die los staat van de business rol/functie die verantwoordelijk is voor het beheer van de betreffende toepassing[3];
- Administratie en opslag van deze beheertoegangsgegevens dient altijd uitgevoerd te worden conform de BIV classificatie met vertrouwelijkheid HOOG;
- Alle activiteiten uitgevoerd met robotaccounts dienen te worden gelogd;
- De robotaccount mag alleen worden geautoriseerd voor rechten die ook aan normale eindgebruikers mogen worden uitgegeven;
- De robotaccount mag niet worden ingezet voor enig ander andere type interactie met ICT services, zoals beheerwerkzaamheden, batchverwerkingen of A2A/API-toegang;
- De autorisaties aan het robotaccount dienen op exact dezelfde wijze te worden toegewezen als aan een fysieke persoon (de robot krijgt bijvoorbeeld dezelfde business rollen toegewezen);
    - Uitzondering hierop zijn de generieke rechten die voor alle ProRailers gelden, zoals Office, intranet- en internettoegang. Deze worden alleen minimaal en expliciet toegekend wanneer dit voor de werkset van de robotaccount noodzakelijk is.
- Voor elk robotaccount is actuele beheer documentatie aanwezig waaruit duidelijk blijkt aan welke test-sets en aan welke testwerkplek/ gebruikersomgeving de robotaccount is gebonden, welke rollen/rechten hiervoor aan het robotaccount zijn toegewezen, en welke beheerders via welke beheerrollen geautoriseerd zijn om de robotaccount en -gebruikersomgeving te benaderen, gebruiken en beheren;
    - Deze documentatie dient te zijn opgeslagen op een veilige locatie;
    - Deze documentatie mag geen wachtwoordgegevens bevatten;
    - Deze documentatie is onderdeel van de beheerdocumentatie van de software/ werkplek die van deze robotaccounts gebruik maakt, en valt daarmee onder verantwoordelijkheid van de eigenaar van de software/ werkplek;
- Wanneer een robotaccount aan een andere test- en/of applicatie-set wordt toegewezen, dienen eerst alle bestaande autorisaties en applicatietoewijzingen te worden verwijderd, waarna de account opnieuw geconfigureerd wordt met de nieuwe rollen, autorisaties en applicaties. Dit in lijn met het proces voor fysieke personen die een andere rol binnen ProRail gaan vervullen.

Eisen aan de gebruikersomgeving waarin de robotaccount functioneert:

- De interactieve gebruikersomgeving voor de robotaccount bevat alleen die toepassingen die voor de testdoeleinden benodigd zijn, indien noodzakelijk aangevuld met additionele toepassingen om de werking van de robotaccount mogelijk te maken en de gebruikersomgeving afdoende te beveiligen;
- Deze interactieve gebruikersomgeving dient te allen tijde voorzien te zijn van alle beveiligingsmaatregelen die voor gebruikersomgevingen/ -werkplekken van toepassing zijn binnen het ICT domein waarin zich deze interactieve gebruikersomgeving bevindt;
- Alle te testen/ gebruiken toepassingen op deze interactieve gebruikersomgeving dienen te worden geïnstalleerd op exact dezelfde wijze als dat ze voor een fysieke gebruiker zouden worden geïnstalleerd (bijvoorbeeld via Software center);
- Deze interactieve gebruikersomgeving mag door een fysieke persoon worden benaderd om de omgeving te configureren voor uitvoer van de (test)scenario's of om eventuele problemen met deze scenario's te analyseren en op te lossen;
- Toegang tot de interactieve gebruikersomgeving van de robotaccount is afgeschermd, en voor fysieke personen alleen toegankelijk na een persoonlijke autorisatie;
    - Toegang tot de beeldscherminformatie van de interactieve gebruikersomgeving mag permanent worden vrijgegeven binnen ProRail locaties, zolang de vertrouwelijkheid lager is dan HOOG.
- Toegang tot de interactieve gebruikersomgeving van de robotaccount via elke andere weg is niet toegestaan, tenzij deze standaard onderdeel is van de op die gebruikersomgeving geïnstalleerde en te testen applicaties.

[3] De huidige afspraak is dat deze gegevens voor KA in beheer zijn bij Conclusion.

3.6 Groepsaccount / Functioneel account

Groepsaccounts vallen onder geen van de bovengenoemde definities, en zijn binnen ProRail om die reden NIET toegestaan. Bovendien is voor groepsaccounts geen naar persoon herleidbare audit mogelijk voor uitgevoerde acties, waar dit voor de shared-resource accounts wel te realiseren is.

ProRail volgt hiermee ook de eisen zoals opgelegd in de BIO (zie referenties).

3.7 Overige Accounts

Er zijn speciale systemen, zoals b.v. de INTTEL, waar geen specifieke policy op te implementeren is. Voor deze systemen geldt een risico-afweging en een set van maatregelen “op maat”.

Het Cybersecurity Team onderhoudt een overzicht van dergelijke uitzonderingen. Deze uitzonderingen worden periodiek hernieuwd beoordeeld.

4 Wachtwoordbeleid

In de werkinstructies op uitvoerend niveau is het beleid verder uitgewerkt.
Voor bepaalde domeinen kunnen aangepaste regels gelden.

4.1 Aandachtspunt: Wachtwoorden vs. Andere geheime toegangsinformatie

Een wachtwoord is bij het schrijven van dit beleid nog steeds de meest gangbare vorm van geheime informatie die wordt aangeboden om de gepresenteerde identiteit te bewijzen (al dan niet vergezeld van extra authenticatiefactoren). Naast wachtwoorden wordt in veel gevallen ook gebruik gemaakt van andere vormen van geheime toegangsinformatie, zoals bijvoorbeeld (maar niet beperkt tot) shared secrets of SSH sleutels.

Waar in dit beleid gesproken wordt over wachtwoorden, geldt dit beleid onverminderd ook voor alle andere vormen van geheime toegangsinformatie, tenzij dit beleid voor een specifieke verschijningsvorm specifieke uitzonderingen beschrijft.

4.2 **Algemene policies** (Minimum voor alle zones en applicaties)**:**

Type wachtwoord-eis	Algemene-invulling	Beheer
Wachtwoord lengte	Minimaal 12 Karakters/tekens	Minimaal **20** Karakters/tekens
Password geldigheid	180 dagen	**90** dagen
Wachtwoord historie	24	
Wachtwoord verloopt	1 dag (mogelijkheid om na expiratie te wijzigen)	
Herinnering Wachtwoord verloopt	Dag 166 en 178	dag 76 en 88
Wachtwoord complexiteit	• Mag geen gebruikersnaam zijn, of delen (3 of meer opeenvolgende karakters) van de volledige naam. • Bevat karakters/tekens uit 3 van de 4 onderstaande categorieën: ➢ Hoofdletters (A…Z) ➢ Kleine letters (a … z) ➢ Cijfers (0 … 9 ➢ Vreemde tekens (bijv. !,$,#,% ë, ó, Ω)	
Repeterend patroon	Restrictie aanbrengen vwb tegen gaan logische opvolging is vereist als dat in het systeem te implementeren is.	
Account lockout	• Na 5 maal fout inloggen (verkeerd wachtwoord) wordt het desbetreffende account (tijdelijk voor 10 minuten) geblokkeerd. • Na 50 dagen inactief wordt het account geblokkeerd, tenzij de account onder de in 4.1.1. beschreven uitzondering valt.	

4.2.1 **Uitzondering op account lockout**

Binnen ProRail zijn enkele specifieke accounts aanwezig die vanwege hun specifieke functie met een zeer lage frequentie gebruikt worden, bijvoorbeeld 1 keer per kwartaal. Om te voorkomen dat deze telkens na 50 dagen geblokkeerd worden geldt voor deze specifieke accounts afwijkend beleid:

- De automatische blokkade gaat in na een periode gelijk aan het aantal dagen tussen het reguliere gebruik van deze accounts plus 2 dagen;
- Op de account zijn restricties ingesteld zodat deze alleen voor deze specifieke functies gebruikt kunnen worden;
- De restricties en geldigheidsduur worden per account samen met security vastgesteld;
- De configuratie van de betreffende account wordt opgenomen in de beheerdocumentatie van de toepassing waar deze account voor wordt gebruikt;
- Elke uitzondering dient geadministreerd te worden (bijvoorbeeld een problem of risico-acceptatie formulier).

4.3 Wachtwoordentropie

Het kan voorkomen dat een toepassing niet in staat is om complexe karakters in wachtwoorden te gebruiken en/of af te dwingen. Om het kraken van dit wachtwoord net zo strek te bemoeilijken als bovenstaande policy voorschrijft, dient in dat geval de wachtwoordlengte te worden aangepast totdat minimaal hetzelfde niveau van entropie is bereikt. Advies bij alleen letters voor normale gebruikersaccounts: Lengte 20 karakters.

4.4 Afwijking per accountsoort

4.4.1 Persoonlijk Account: Normaal Account

- Geen afwijkingen

4.4.2 Persoonlijk account: High-privileged Account

- Minimale lengte: 20 karakters;
- Het wachtwoord mag niet gelijk zijn aan het wachtwoord van enig ander persoonlijk account dat de persoon in gebruik heeft.

4.4.3 Non-personal account: Serviceaccounts en robotaccounts

- Minimale lengte: 32 karakters;
- Het wachtwoord mag niet gelijk zijn aan het wachtwoord van enig ander service-/robotaccount dat binnen ProRail in gebruik is.

4.4.4 Non-personal account: Resourceaccounts

- Standaard geen afwijkingen

Op basis van het te maken ontwerp voor de betreffende resource kunnen door de security manager, na risicoanalyse, uitzonderingen op de policy worden gegeven, of extra eisen aan het wachtwoord worden gesteld.

4.4.5 Local-Admin/ Root-account

➢ De security policy voor wat betreft de built-in locale admin/root-wachtwoorden heeft wat afwijkingen:

Alle ProRail domeinen			
Servers	***Alle platformen***	***Clients***	***Alle platformen***
Installatie (inrichting-basis)		Installatie (inrichting-basis)	
Uniek t.o.v. vergelijkbare accounts?	**Ja**	Uniek t.o.v. vergelijkbare accounts?	**Ja**
Sterk wachtwoord?	Ja	Sterk wachtwoord?	Ja
Password never expires	**Ja**	Password never expires	**Ja**
Implementatie (uitrol)		Implementatie (uitrol)	
Gedeeld alg. wachtwoord?	Nee	Uniek t.o.v. vergelijkbare accounts?	**Ja**
Sterk wachtwoord?	Ja	Sterk wachtwoord?	Ja
Password never expires	**Ja**	Password never expires	**Ja**

Daarnaast dienen built-in admin accounts standaard te zijn uitgeschakeld.

4.4.6 Emergency accounts

Voor enkele applicaties is een nood-account beschikbaar (als high-privileged beheeraccount), dat via een hard copy en een zgn. “rode envelop procedure” in noodgevallen ter beschikking wordt gesteld.

Om praktische redenen gelden voor deze accounts enkele aanpassingen op het beleid voor high-privileged accounts:

- Minimale lengte: 40 karakters;
- Het wachtwoord mag niet gelijk zijn aan het wachtwoord van enig ander emergency account dat binnen ProRail in gebruik is;
- Na elk gebruik van een emergency account dient het wachtwoord direct gewijzigd te worden;
- Wachtwoord geldigheid: 13 maanden (wachtwoord dient elk jaar vernieuwd te worden).

4.4.7 Overige accounts

- Invulling a.d.h.v. risico’s en mogelijkheden “op maat” in lijn met het risiconiveau.

4.5 Opslag van wachtwoorden

Principieel dienen wachtwoorden niet geregistreerd te zijn buiten een specifiek voor dat doel ingezette kluis. Een wachtwoord is iets persoonlijks dat iedereen, net als de pincode, dient te onthouden.

4.5.1 Uitzonderingen

Op de bovenstaande regel zijn een aantal, vrijwel onvermijdbare, uitzonderingen te bedenken. Te denken valt dan aan:

- Wachtwoorden binnen een testomgeving;
- Wachtwoorden van databases;
- Wachtwoorden van systeemaccounts;
- Veelvoud aan beheeraccounts;
- Hardcopy van een specifiek account voor “rode envelop” procedures.

Voor deze typen kan een veilige, beperkt toegankelijke opslagomgeving gemaakt worden. (Fysieke kluis of digitale Password Vault met geautoriseerd aanvraag en uitgifteproces).

Deze opslag is in voorkomende gevallen ook noodzakelijk vanwege de eisen aan beheer en uitgifte van bijvoorbeeld high-privileged account en serviceaccounts, zie ook hoofdstuk 3.

4.5.2 Eisen aan de opslag

- Toegang is gebonden aan gebruikersgroepen waarbij alleen de rechthebbenden op basis van persoonlijke Identiteit, gelogd, toegang hebben tot de eigen set van wachtwoorden;
- De opslag is beveiligd met een veilige encryptie (AES 256 of gelijkwaardig);
- Opslagmechanisme is universeel toepasbaar binnen ProRail en wordt dus als standaard pakket aangeboden;
- De opslag dient volledig on-premises te kunnen functioneren zonder dat daarvoor een verbinding met het internet benodigd is.

4.6 Pincode

Een aantal toepassingen wordt beschermd door een pincode. Denk aan de Win10 werkplek en de telefoons die een policyset via de aangewezen beheersoftware krijgen. De lengte hiervan is minimaal 8 posities, numeriek of beter. Deze pincode dient aan de persoonlijke device van de gebruiker verbonden te zijn.

5 Verschillen in classificatie per zone / Domein

Door hun gevoeligheid kennen de verschillende zones, verschillende eisen van toegang.

5.1 Generieke zone / KA

Deze zone kent de standaard toegangsregels gebaseerd op de Classificatie van de onderliggende systemen.

5.2 Spoorse zone / VL, M&S, TCS enz…

Oorspronkelijk had dit domein geen enkele connectie buiten het domein, op de aangesloten terminals / terminal-emulators na en stond voor het domein de classificatie op basis van intern gebruik.

- **Opm**: Vertrouwelijkheid tussen de VL applicaties, dus *binnen* dit domein werd, vanwege het gesloten karakter doorgaans laag geacht waardoor er in het verleden te laag geclassificeerd is. Die classificaties zijn, voor zover ze nog voorkomen in documentatie, ongeldig en gesteld op minimaal **Middel.**
- Read-only koppelingen tot dit domein zijn beperkt en worden gemonitord.
- Overige koppelingen met dit domein zijn, vanwege het gevoelige karakter van de spoorbesturing, minimaal geclassificeerd op:
    - Beschikbaarheid: **Hoog** (3)
    - Integriteit: **Middel** (2) tot Hoog (3)
    - Vertrouwelijkheid: **Middel** (2) tot Hoog (3)

5.3 Operationeel Controle Centrum Rail (OCCR)

OCCR heeft hetzelfde gevoelige karakter als VL wat betreft de spoorbesturing en dus:

- Integriteit: **Middel** (2) tot Hoog (3)
- Vertrouwelijkheid: **Middel** (2) tot Hoog (3)

5.4 Donna

De risicoanalyse op dit systeem is door NS en ProRail gezamenlijk gedaan.
Alle maatregelen zijn gebaseerd op de classificatie van het zwaarste onderdeel.

- Beschikbaarheid: **Middel** (2)
- Integriteit: **Middel** (2)
- Vertrouwelijkheid: **Middel** (2)

5.5 Reisinformatie

Het domein is onderdeel van het ProRail netwerk. De systemen zijn formeel van de NS.. Het draait in een grote verwevenheid met de spoorse zone. De ontvlechting gaat de komende tijd gerealiseerd worden..
De risicoanalyse op dit systeem is door NS en ProRail gezamenlijk gedaan.
Alle maatregelen zijn gebaseerd op de classificatie van het zwaarste onderdeel.

- Beschikbaarheid: **Middel** (2)
- Integriteit: **Middel** (2)
- Vertrouwelijkheid: **Middel** (2)

5.6 GSM / Rail

Is (nu nog) gekoppeld aan het VL netwerk.
Vanwege het dragerschap van Communicatie, Reisinformatie en Treinbeveiliging (ERTMS) is de classificatie:

- Beschikbaarheid: **Hoog** (3)
- Integriteit: **Middel** (2) tot Hoog (3)
  Vertrouwelijkheid: **Middel** (2) tot Hoog (3)