TNO

PSA Mobility

PSA LITE

Auteur : Willy Schutte
Versie : 1.0
Date : 28/02/2021
Project /
Change nr: 060.00980

1. Document Informatie

1.1 Historie

Datum	Versie	Auteur(s)	Wijziging
17/12/2021	0.1	Willy Schutte	Initiele draft versie
24/12/2021	1.0	Willy Schutte	Aanpassingen verwerkt. Definitieve versie

1.2 Recensenten

Versie	Datum	Naam	Functie	Rol
1.0	03-01-2022	Lex Beijk	Enterprise Architect	A
		Willy Schutte	Information Architect	C
0.1	20-12-2021	Karel van Houten	Security Officer	C
0.1	21-12-2021	Jan Haentjens	Solution Architect	C
0.1	20-12-2011	Ruud van Rijnsoever	Project Manager	C
01.	20-12-2021	Bart Lauret	Business Relation Manager	C

1.3 Document akkoord verklaringen

Versie	Datum	Naam	Functie	Verklaring

1.4 Distributie

Versie	Datum	Naam	Functie
		Lex Beijk	Enterprise Architect
		Willy Schutte	Information Architect
		Edsger Jager	Technisch Architect
		Ronald Mens	Technisch Architect
		Karel van Houten	Security, Risk en Compliance Manager
		Ruud van Rijnsoever	Project Manager
		Jan Haentjens	Solution Architect
		Bart Lauret	Business Relation Manager

1.5 Ingangsdocumenten

Versie	ID	Naam Document	Auteur
		PID	Ruud van Rijnsoever
		Presentatie Mobility beleid	
		Requirementsdocument Mobiliteitsprovider	Bart Lauret
		Requirementsdocument (lokaal)	Bart Lauret
		Security Requirement Mobility	Karel van Houten

Inhoudsopgave

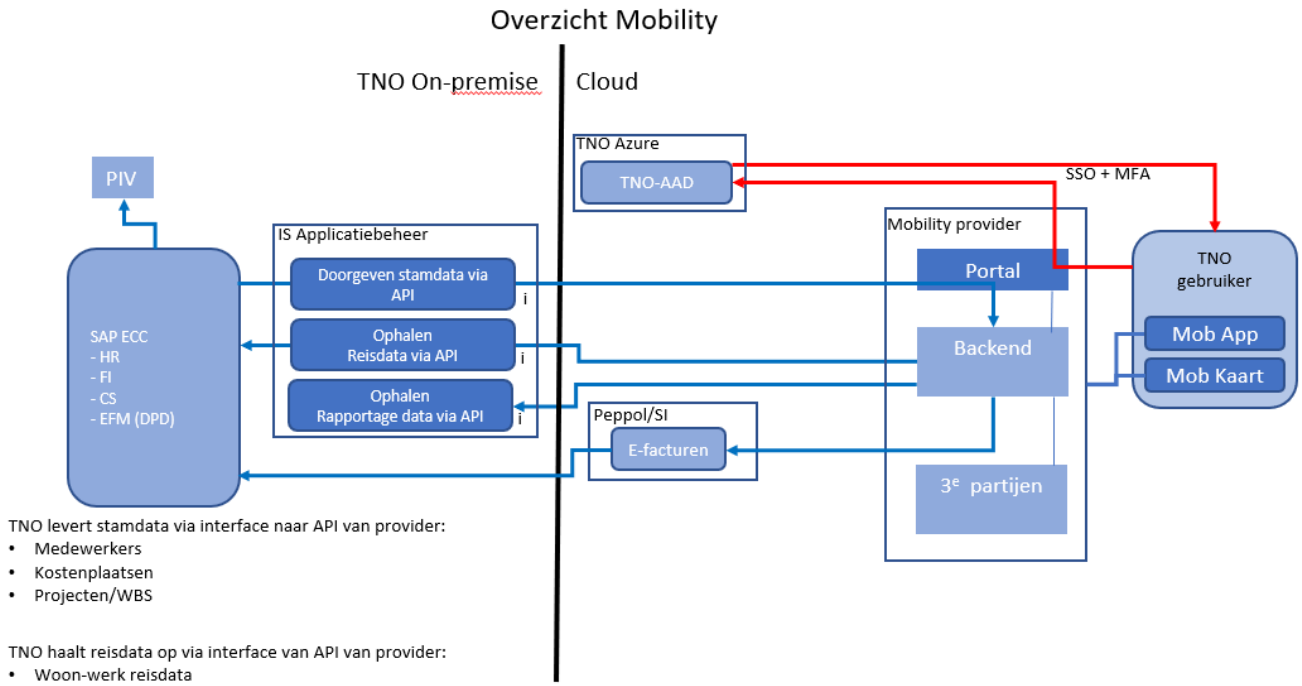
1. Document Informatie 2
1.1 Historie 2
1.2 Recensenten 2
1.3 Document akkoord verklaringen 2
1.4 Distributie 2
1.5 Ingangsdocumenten 2
Inhoudsopgave 3
2. Introductie 4
3. Architectuur Richtlijnen 5
4. Exceptions 6

2. Introductie

Dit document beschrijft de Architectuur voor project Mobility van TNO.

Het TNO mobiliteitsbeleid is recent vastgesteld (Presentatie Mobility beleid en Requirementsdocument Mobiliteitsprovider). Hybride werkvormen brengen structurele veranderingen in reisbehoeften en -patronen met zich mee. Een moderne SAAS mobility tool is noodzakelijk om de uitgangspunten van het mobilteitsbeleid te realiseren, zoals flexibiliteit en gebruiksvriendelijkheid, met lage beheerlast. Onderdelen van de mobility tool zijn een mobiliteitsportaal, mobiliteitsapp en mobiliteitskaart. Daarmee wordt het reisgedrag dagelijks geregistreerd en automatisch verwerkt.

High level architectuuroverzicht:



TNO levert stamdata via interface naar API van provider:
- Medewerkers
- Kostenplaatsen
- Projecten/WBS

TNO haalt reisdata op via interface van API van provider:
- Woon-werk reisdata
- Zakelijke reisdata
- Thuiswerkvergoeding

TNO haalt rapportage data op via API van provider

Provider stuurt e-facturen via Peppol/SI

3. Architectuur Richtlijnen

1. Classificatie gegevens mobility tool rubricering TNO-V.
2. Authenticatie Portal:
    a. Uitsluitend toegang via SSO op basis van TNO account. Gebruik van Azure Active Directory als Identity provider voor SSO met Azure MFA obv SAML2, OAuth2.
    b. Gebruikers met een extra rol (bijvoorbeeld functioneel beheerders die ook een backoffice rol hebben) krijgen een 2e AD account (dlg account) voor hun functioneel beheer rol.
    c. Beheerders van de provider hebben geen accounts in de mobility portal.
3. Authenticatie App: Eenmalige authenticatie vindt plaats via authenticatie via mobility portal in combinatie met toegangscode voor de app op persoonlijke mobiele telefoon. Daarna is pincode, vingerafdruk of gezichtsherkenning voor de app op een privé mobiele telefoon verplicht. Bij een TNO managed device kan deze 2^{e} factor komen te vervallen. Een gebruiker moet alle mobility handelingen ook zonder de mobility app kunen doen (dus alleen gebruik maken via de mobility kaart en de mobility portal).
4. Authenticatie Kaart: bijvoorkeur gebruik van een kaart op de smartphone door middel van NFC met dezelfde authenticatie als voor de App beschreven. Een fysieke kaart wordt op naam gesteld en wordt persoonlijk verzonden met een initiele registratie via de portal of app.
5. Userbeheer in de mobility applicatie. Voor geauthentiseerde gebruikers is een persoonlijk gebruikersaccount noodzakelijk. Een gebruikersaccount wordt via het medewerker interface automatisch in de applicatie aangemaakt en verwijderd. Hiertoe wordt een einddatum in het medewerker interface mee gegeven, opdat het account bij uitdienst kan worden geblokkeerd. Zodra bewaartermijn verstreken is, worden het account en de medewerkersgegevens verwijderd.
6. Bij het verwijderen van een account worden de persoonlijke medewerkersgegevens verwijderd (in overeenstemming met AVG.
7. Rollentoewijzing in de applicatie verloopt via het medewerkers interface voor de gebruikersaccounts, en via TNO AD groepen voor de functioneel beheeraccounts.
8. Koppelingen voor gegevensoverdracht verlopen via REST API's met OAuth2.0 authenticatie en API key.
9. Interfaces uitgaand. Voor de gegevensoverdracht vanuit TNO naar de Mobility provider worden dagelijks de volgende stamdata doorgegeven naar een API van de provider:
    a) Medewerkersgegevens via API van provider.
    b) Kostenplaatsgegevens via API van provider.
    c) Projecten/WBS stamgegevens via API van provider.
10. Interfaces binnenkomend. Geadministreerde reisdata wordt door de Mobility provider voor TNO beschikbaar gesteld via API's van de provider:
    a) Woon-werk reisdata (op vastgestelde dagen).
    b) Thuiswerk vergoeding (op vastgestelde dagen).
    c) Zakelijke reisdata (dagelijks).
    d) Aanvullende data t.b.v. rapportages (tenminste maandelijks).
11. De veldenstructuur voor elk binnenkomend interface is zodanig opgesteld dat de gegevens in SAP automatisch kunnen worden verwerken (zie H5 Bijlage 1 van dit document voor details):
    a. Woon-werk reisdata en thuiswerkvergoedingen kunnen direct in SAP HR wordt verwerkt. Naast deze data dient ook een PDF (met details over de kilometerbepaling inclusief de goedkeuring van de reisdata) in het interface worden opgenomen.
    b. Zakelijke reisdata kan direct in SAP FI worden geboekt. Naast deze data dient ook een PDF (met details over de kilometerbepaling inclusief de goedkeuring van de reisdata) in het interface worden opgenomen.
    c. Facturen (inclusief PDF bijlage) worden bijvoorkeur als e-facturen ontvangen (via Peppol/SI) en worden automatisch in SAP geboekt.
12. De mobility applicatie is voorbereid om huurauto's via de mobility portal te kunnen ontsluiten en gebruikt hiervoor een gestandariseerde interface met vervoerders (TOMP api).
13. De mobility applicatie gebruikt de dagelijks door TNO doorgegeven stamdata als basis voor het vastlegging van de reisdata.
14. Maatwerk wordt zoveel mogelijk ontweken. Maatwerk resulteert in meer beheer en complexiteit.
15. Voor de functionele beheerders van TNO dient naast de productieomgeving minimaal 2 niet-productieomgevingen beschikbaar te zijn die functioneel gelijk zijn aan (of vooruitlopen op) de productieomgeving: 1. Testomgeving met anonieme data en 2. een acceptatie omgeving met recente

productie data. De interfaces van deze omgevingen zijn aan de overeenkomende omgevingen van TNO gekoppeld.

16. De mobility applicatie wordt pas in productie genomen na doorlopen van een testproces in een acceptatieomgeving en na goedkeuring door TNO. In de acceptatieomgeving kunnen onder andere de genoemde interfaces worden getest.
17. De functionaliteit is testbaar met gangbare automatische test tools.
18. Er is een rollback mogelijkheid als een release teruggedraaid moet worden.
19. De mobility applicatie dient goed beheerbaar te zijn door TNO Functioneel Beheer. De beheeromgeving is gebruiksvriendelijk en goed en actueel gedocumenteerd.
20. Voor deze dienst is LCM op informatie geregeld. Er wordt alleen data vastgelegd die noodzakelijk is voor de dienst. Als data niet meer van belang is, dan wordt deze gearchiveerd (bijvoorbeeld data van medewerkers die langer dan x dagen uit dienst zijn). Reisgegevens worden bijvoorbeeld automatisch na een vastgestelde periode na doorsturen naar TNO uit de mobility applicatie verwijderd (zie ook 11a en 11b).
21. Borging van de implementatie wordt gedaan middels correcte en volledige documentatie. De documentatie beschrijft o.a. :
    1. de beschrijving van de aangeboden SAAS omgeving,
    2. de architectuurbeschrijving,
    3. hosting van de dienst (waar staat de data, hoe is backup en veiligstellen van data naar TNO geregeld, hoe is archivering geregeld, hoe is informatiebeveiliging geregeld, welke certificeringen zijn aanwezig, hoe is technisch beheer geregeld, wie kunnen bij het systeem en de data).
    4. Beschrijving van de interfaces die zijn ingeregeld en benoemd in de PSA (SSO, login, accounts, API koppelingen).
    5. Invulling van de gestelde Security Requirement Mobility en architectuurrichtlijnen. .
22. De mobility applicatie dient flexibel en dynamisch schaalbaar te zijn en kan aansluiten op een flexibele organisatie en kan de performance afspraken waarborgen.
23. De mobility applicatie heeft een Life Cycle roadmap en deze wordt gedeeld met TNO.
24. Groei en krimp in de workload zijn eenvoudig op te vangen.
25. De dienst is gebaseerd op (defacto) moderne standaard en proven technologie en standaard componenten.
26. De dienst dient goed te functioneren op gangbare besturingssystemen en browsers (minimaal: Edge Chromium, Chrome).
27. De dienst dient goed te functioneren op mobiele devices, zoals smartphones, tablets en dient een goed gebruikersgemak te hebben. De applicatie start vlot op, reageert snel, is intuitief en ondersteunt de gebruiker bij het vlot kunnen invullen (bijvoorbeeld door eerder ingevulde waarden voor te stellen).
28. Verzenden van mail. Vanwege compliancy en monitoring moet voor verzenden van mail vanuit een SAAS applicatie met verzendadres van het domein @tno.nl gebruik worden gemaakt van een door TNO beheerde dienst.

4. Exceptions

5. Bijlage 1 Datauitwisseling

Onderstaande beschrijving geeft slchts op hoofdlijnen de datastromen weer.

1. Datastroom medewerker (TNO naar mobility provider)

Frequentie: dagelijks

Veld	Omschrijving	Voorbeeld
Personeelsnummer		00012345
Naam		Peter Janssen
E-mailadres	T.b.v. notificaties	peter.janssen@tno.nl
Kostenplaats	Wordt gebruikt als standaard kostenplaats bij zoekhulp	0002190612
Mobiliteitsprofiel	Categorisering van leaserijders, niet-leaserijders, trainees (nieuw in te richten in SAP)	
Leidinggevende	Mailadres van leidinggevende? In overleg met leverancier	
Standplaats	Adres standplaats	Delft, Stieltjesweg 1
Datum einde dienstverband		

2. Datastroom Kostenplaatsen (TNO naar mobility provider)

Frequentie: dagelijks

Veld	Omschrijving	Voorbeeld
Nummer	Kostenplaatsnummer	
Titel (korte tekst)	Beschrijving van kostenplaats	
Kostenplaatsverantwoordelijke	Naam kpl-verantwoordelijke	
Status boekbaar	Is kostenplaats boekbaar (peildatum vandaag)	

3. Datastroom Projectcodes (TNO naar mobility provider)

Frequentie: dagelijks

Veld	Omschrijving	Voorbeeld
Nummer project	Projectnummer (niet uniek)	060.01234
Omschrijving project		
Nummer wbs		060.01234/01.24.01
Omschrijving wbs		
Verantwoordelijke	Naam wbs-elementverantwoordelijke	
Status boekbaar	Is wbs-element boekbaar (peildatum vandaag)	

4. Datastroom Reisbewegingen en deelfaciliteiten (Mobility provider naar TNO)

Frequentie: dagelijks (vergoeding/kosten over goedgekeurde reisbewegingen van periode vorige maand(en)) in een vast en eenduidig format

Veld	Omschrijving	Voorbeeld
Unieke identifier reisbeweging	Ten behoeve van matching met reiskostenfactuur	

Personeelsnummer of e-mailadres	Ten behoeve van identificatie van medewerker	00012345 of bert.janssen@tno.nl
Classificatie	T.b.v. onderscheid woon-werk/zakelijk/ prive	" Zakelijk"
Type	Fiets/auto/OV 1e klas/OV 2e klas/OV-fiets/deelscooter/…	" Auto"
Datum reisbeweging		15.10.2021
Traject	Begin- en eindpunt van reisbeweging	
Omschrijving	T.b.v. onderbouwing zakelijke reis	"Congres"
Aantal km bij eigen vervoer		25
Kosten geen eigen vervoer	Bijv. OV-kosten	18,92
Vergoeding of tegmoetkoming voor eigen vervoer	Bijv tegemoetkoming voor reis met fiets	15,12
Looncomponent	Code voor verwerking in TNO-salarisadministratie	5012

Aanvullend voor zakelijke reis en afgenomen deelfaciliteit:

Veld	Omschrijving	Voorbeeld
Kostenplaats		
Wbs-element		
Goedgekeurd door		

Aanvullend voor woon-werkreis:

Veld	Omschrijving	Voorbeeld
Bewijs voor kilometer-bepaling	Conform fiscale regels (artikel 23.1.5 van het handboek loonheffingen)	

5. Datastroom OV-klassewissel (mobility provider naar TNO)

De volgende informatie heeft TNO minimaal nodig om inhouding op de payroll te doen voor een medewerker bij een upgrade naar 1e klas voor woon-werkverkeer:

- Meerkosten 1e klas t.o.v. 2e klas
- Datum en tijdstip van klasse-up- of downgrade
- Type van klasse-up- of downgrade
- Op deze datum heeft een zakeljke reis plaatsgevonden (J/N)

6. Datastroom Thuiswerkdagen (mobility provider naar TNO)

Frequentie: minimaal maandelijks (vergoeding over goedgekeurde thuiswerkdagen van periode vorige maand(en))

Veld	Omschrijving	Voorbeeld
Personeelsnummer		
Datum		
Looncomponent	Code voor verwerking in TNO-salarisadministratie	

7. Datastroom Fiscale ruimte (mobility provider naar TNO)

In de Mobiliteitstooling zal worden bepaald wat de fiscale ruimte voor uitruil is die is ontstaan door woon-werkverkeer.

N.B. Voor de medewerker is op elk gewenst moment het bedrag aan uitruil inzichtelijk in de app/portaal.

De fiscale uitruilbedragen dienen doorgegeven te worden conform onderstaande frequentie.

Maandelijks dienen de (voor dat jaar gecumuleerde) uitruilbedragen aan TNO worden doorgegeven om deze te kunnen verwerken bij uitdiensttreding. De uitruilbedragen dienen in eerste week van de maand beschikbaar worden gesteld.

Bovenstaande impliceert dat in de eerste week van januari van enig jaar de ruimte die is opgebouwd in het voorgaande jaar doorgegeven dient te worden, met uitzondering voor medewerkers die uit dienst zijn getreden voor 1 december van het voorafgaande jaar.

Voorzien wordt dat deze bedragen zullen worden ingelezen in SAP HR als looncomponent (IT0015)

Eventueel zou het nog mogelijk moeten zijn om de daadwerkelijk uitgevoerde uitruil door te geven aan de provider zodat dat verrekend kan worden met de fiscale ruimte.

Frequentie: maandelijkse doorgifte t.b.v. uitruil

Veld	Omschrijving	Voorbeeld
Personeelsnummer		
Fiscale ruimte in EUR		
Looncomponent	Code voor verwerking in TNO-salarisadministratie	

8. Datastroom Factuur (mobility provider naar TNO)

Maandelijks ontvangt TNO één verzamelfactuur met de doorbelasting van alle gemaakte OV reizen incl. overige deelfaciliteiten. De factuur voldoet minimaal aan de minimale factuurvereisten zoals deze gesteld zijn door de Belastingdienst.

De factuur wordt in PDF geleverd en in een digitaal format wat gebruikt kan worden voor het boeken van de details van de factuur.

Frequentie: Maandelijks

Veld	Omschrijving	Voorbeeld
Unieke identifier reisbeweging		
Kosten		
Btw code		
Kostenplaats		
WBS-element (projectcode)		
Classificatie		

9. Datastroom Rapportage (mobility provider naar TNO)

De onderstaande data dient te kunnen worden onttrokken aan de mobiliteitstooling. Let op, er is met sommige gegevens een overlap met de overige datastromen

Frequentie: op verzoek, minimaal wekelijks

Veld	Omschrijving	Voorbeeld
Personeelsnummer		
Reistype	Fiets/auto/OV	
Aantal kilometers		
CO2-uitstoot		

Classificatie	T.b.v. onderscheid woon-werk/zakelijk	
Datum reisbeweging		