

BIJLAGE H – ARCHITECTUURKADERS

Europese aanbesteding voor Mobiliteitsoplossing



Niets uit dit document mag zonder schriftelijke toestemming vooraf van de Sociale Verzekeringsbank worden verveelvoudigd, openbaar gemaakt of voor andere doelstellingen gebruikt dan het indienen van een Inschrijving.

Inhoudsopgave

1.	ALGEMEEN	3
1.1.	INLEIDING	3
1.2.	KERNFUNCTIONALITEITEN	3
1.3.	APPLICATIES	3
1.4.	KOPPELINGEN	4
2.	KADERS	7
2.1.	TOE TE PASSEN STANDAARDEN	7
2.2.	TOE TE PASSEN PRINCIPES	8
2.3.	TOE TE PASSEN OVERIGE KADERS	10
2.4.	INTEGRATIES	10

1. Algemeen

1.1. Inleiding

Dit document bevat de kaders ten aanzien van de IT architectuur van de Mobiliteitsoplossing. Deze kaders zijn niet bedoeld als ontwerp, maar geven de contouren aan waarbinnen het ontwerp moet worden gerealiseerd.

1.2. Kernfunctionaliteiten

De Mobiliteitsoplossing biedt op hoofdlijnen de volgende kernfunctionaliteiten:

1. Mobiliteitskaart
2. Openbaar Vervoer
3. Elektrisch deelfervoer
4. Fietsenstalling
5. Mobiliteitsapp
6. Mobiliteitsportal

1.3. Applicaties

In de volgende tabel worden de huidige en toekomstige applicaties van de SVB toegelicht waarmee de Mobiliteitsoplossing moet integreren:

Applicatie	Toelichting
SAP Succesfactors	<u>Personeelsadministratiesysteem (PAS)</u>. Het personeelsadministratiesysteem is als bronsysteem verantwoordelijk voor de actuele en complete verzameling aan medewerker gegevens inclusief functie, organisatie en leidinggevende. PAS ondersteunt aanvragen voor HR diensten en producten door medewerkers, waaronder de aanvraag voor toegang tot de Mobiliteitsoplossing.
IBIS	<u>Centraal identiteiten en toegangsrechten beheersysteem (IRS)</u>. Met dit systeem worden de eindgebruiker accounts, rollen en rechten beheerd. Hiertoe ontvangt het systeem stamgegevens over de organisatie inclusief organisatiestructuur en de functies van Medewerkers. Sommige gegevens van een user account worden terug geleverd aan het personeelsadministratiesysteem, bijvoorbeeld het zakelijk emailadres van de Medewerker. IBIS levert gebruiker identiteiten (accountnamen), autorisaties en stamgegevens, zoals bijvoorbeeld functie, inclusief mutaties aan systemen met een eigen (decentrale) gebruikersadministratie, naast de levering hiervan aan de generieke Identity & Access Management (IAM) systemen Active Directory en Entra ID. Aanvullend levert het de organisatie- en organisatiestructuurgegevens door aan systemen die deze gegevens nodig hebben voor hun applicatiefuncties zoals Proactis en Unit4ERP, namens het personeelsadministratiesysteem dat de bron is. IBIS is hiervoor een 'verlengstuk' of 'doorgeefluik' van het personeelsadministratiesysteem.

Unit4 ERP	<u>Financieel administratiesysteem</u> inclusief aanverwante functionaliteiten voor bijvoorbeeld crediteuren- en debiteurenbeheer, project accounting en urenregistratie. De directe relatie met de personeel- en salarisadministratie is gelegen in de kostenplaatsen waarvoor het FA systeem verantwoordelijk is.
Proactis	<u>Bestel- en contractmanagementsysteem</u> . Via dit systeem wordt ook de verrekening van de ingehuurde arbeidskrachten via de inhuurbrokers uitgevoerd. Hiertoe ontvangt het de gegevens van de ingehuurde arbeidskrachten (externen en uitzendkrachten).
BI&DA	<u>Business Intelligence en Data Analytics systeem</u> . Via dit systeem worden ook de dashboards met PowerBI geleverd. Met dit systeem wordt onder andere management informatie gemaakt voor het sturen op en verantwoorden over de bedrijfsvoering van de SVB. Vanuit HR wordt hiervoor periodiek de HR brondata aangeleverd.
Entra ID	<u>Authenticatie en autorisatiesysteem inclusief single sign on (SSO) functie</u> . Systemen van de Mobiliteitsoplossing koppelen met dit systeem voor single sign on en autorisatie.
Topdesk	<u>Enterprise Service management systeem voor afhandeling van interne service verzoeken</u> . Met dit systeem worden onder andere de bedrijfsmiddelen beheerd en uitgegeven, zoals bijvoorbeeld een notebook, smartphone en (Arbo) werkplekmeubilair. Het huidige systeem wordt momenteel vervangen door Topdesk.

1.4. Koppelingen

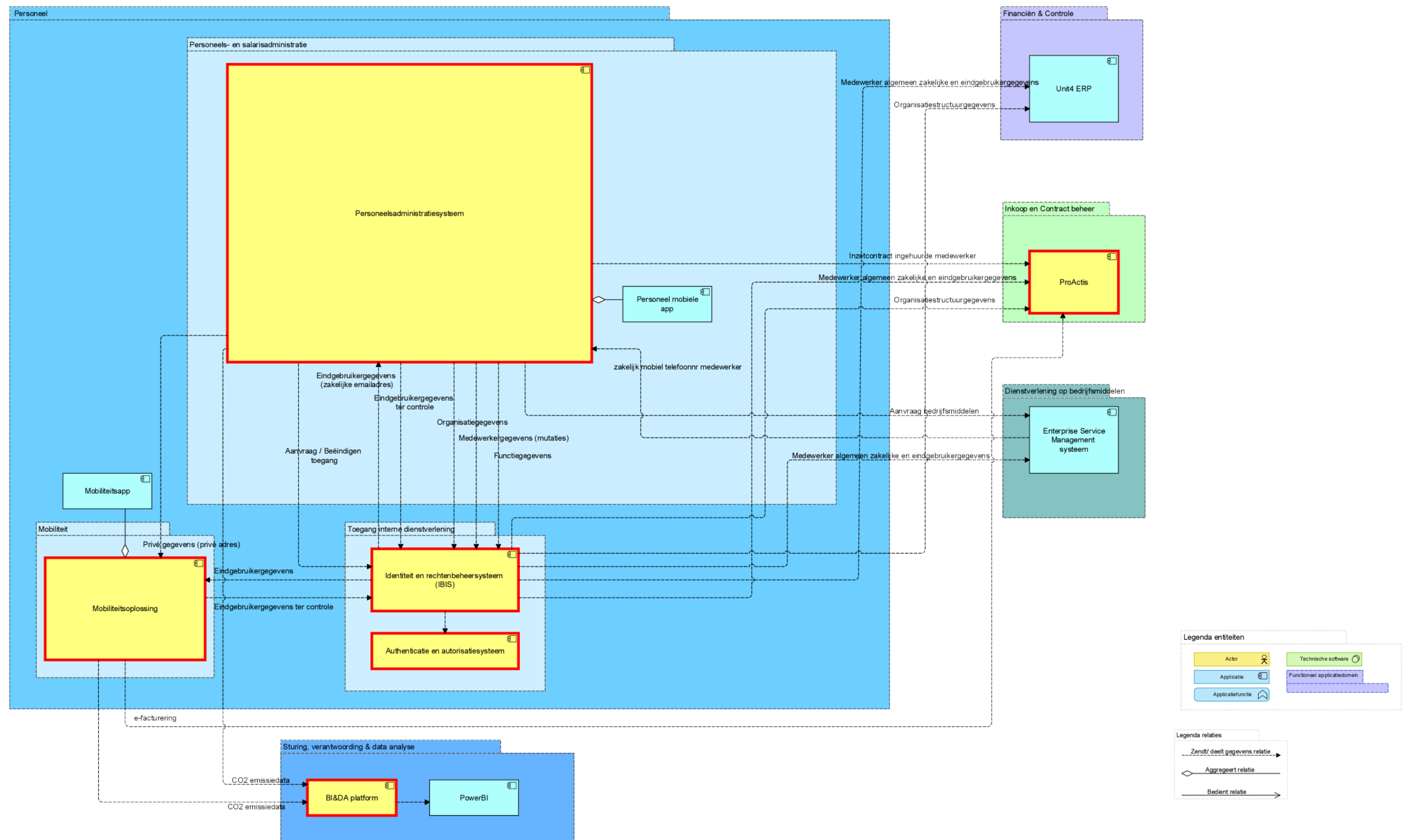
In deze paragraaf wordt een overzicht geboden van de vereiste Koppelingen tussen de Mobiliteitsoplossing en SVB systemen en met externe partijen voor het ontsluiten van informatie en functionaliteit.

De volgende tabel geeft de koppelingen weer tussen de systemen in scope:

Nr.	Van IT service aanbiedend systeem	Omschrijving koppeling	Frequentie	Naar aanroepend (afnemend) systeem
1	Personeels-administratie (PAS)	Doorgifte uit PAS aan IRS van algemeen zakelijke medewerker gegevens om het beheer te kunnen voeren over gebruikers van applicaties.	Periodiek en bij mutaties Mutaties betreft indiensttreding, personeelsmutatie (andere functie en/of andere organisatie-eenheid) en uitdiensttreding	Identiteiten en toegangsrechten beheersysteem – IRS (IBIS)
2	Personeels-administratie (PAS)	Automatisch toekennen of intrekken van een autorisatie rol in IRS naar aanleiding van een goedgekeurde aanvraag toegang Mobiliteitsoplossing binnen PAS. Indien deze koppeling leidt tot ongewenst maatwerk, kan alternatief de autorisatie rol door ESMA of handmatig worden toegekend of ingetrokken.	Periodiek en bij mutaties	Identiteiten en toegangsrechten beheersysteem – IRS (IBIS)

3	Identiteiten en toegangsrechten beheersysteem	Beheren toegang: Aanmaken / muteren account + rol. Doorgifte uit IRS aan Authenticatie en autorisatiesysteem van een beperkte set persoonlijke gegevens en de rechten van een medewerker .		Authenticatie en autorisatiesysteem
4	Identiteiten en toegangsrechten beheersysteem	Beheren toegang: Aanmaken / muteren account + rol. Doorgifte uit IRS aan Mobiliteitsoplossing van eindgebruiker gegevens en algemeen zakelijke medewerker gegevens, organisatiegegevens . Betreft de gegevens die van belang zijn voor de interne gebruikersadministratie van de mobiliteitsoplossing.	Periodiek en direct voor mutaties	Mobiliteitsoplossing
5	Mobiliteitsoplossing	Doorgifte uit Mobiliteitsoplossing aan IRS van de eindgebruiker gegevens (account, rollen en toegangsrechten) inclusief decentrale mutaties. Deze service maakt controle (attestatie/reconciliatie) en vervolgacties mogelijk ingeval van verschillen tussen de centrale en decentrale gebruikersadministraties.	Periodiek	Identiteiten en toegangsrechten beheersysteem
6	Mobiliteitsoplossing	E-facturering op basis van de open standaard PEPPOL. Wanneer het versturen van een XML factuur via peppol niet mogelijk is, dan kan ook een pdf-factuur verwerkt worden (per mail aanleveren).	Maandelijks	Proactis

In de figuur op de volgende pagina zijn deze in geel – rood omkaderd weergegeven. De pijlen geven de datastromen, inhoud en richting, tussen systemen weer.



2. Kaders

2.1. Toe te passen standaarden

Onderstaand wordt aangegeven welke open standaarden van toepassing zijn op basis van de verplichte (Pas-toe-of-leg-uit) en aanbevolen open standaarden op de lijst van het Forum Standaardisatie voor Nederlandse overheidsorganisaties.

Standaard	Omschrijving	Impact
REST API	Voorkeurs methode voor ontsluiting van data en/of functies aan andere applicaties.	Applicatie services, voor ontsluiting van data en/of functies aan andere applicaties, worden bij voorkeur geleverd via REST API's.
SOAP, XML	SOAP (Simple Object Access Protocol) is de aanbevolen open standaard voor webservices met XML (aanbevolen open standaard) als standaardformaat voor de berichtdefinities van webservices. Deze zijn een alternatieve tweede keuze mocht REST-API niet direct haalbaar zijn of beperkingen geven op basis van het pas toe of leg uit principe.	Alternatief voor interface gebaseerde gegevensuitwisseling met Restful API's.
FTP	Aanbevolen open standaard voor de uitwisseling van grote bestanden tussen informatiesystemen.	Van toepassing indien sprake is van uitwisseling via export en transport van data in bestandsformaat naar het dataplatform van de SVB voor management informatie en data-analyse. Geldende open standaard hiervoor is FTP over TLS of alternatief SFTP.
OpenAPI Specification	Verplichte open standaard voor het specificeren van een REST API op het vlak van de geaccepteerde input en de teruggeven output, zodat hergebruik van API's makkelijker wordt.	Versie 3.0 van deze standaard moet gebruikt worden voor het beschrijven/specificeren van de REST API gebaseerde koppelvlakken van de Mobiliteitsoplossing.
JSON	Aanbevolen open standaard voor de datastructuur van uit te wisselen berichten	Eis voor berichtuitwisseling met REST API's
CSV	Aanbevolen open standaard voor het bestandsformaat van bestanden met geëxporteerde of uit te wisselen gestructureerde gegevens.	Van toepassing voor bestand-gebaseerde exports van data en metadata.
CSS	Aanbevolen open standaard voor opmaak van websites.	Van toepassing op geboden portalen.
HTML	Aanbevolen open standaard voor de opmaak van webpagina's.	Van toepassing op geboden portalen.
Datum en Tijd	Aanbevolen open standaard voor het vastleggen van datum en tijd, zodat betekenis transparant is bij uitwisseling van dit type gegevens.	Van toepassing op alle data records opgeslagen in de oplossing en bij uitwisseling van deze data.
PDF	Verplichte open standaard voor een apparaat onafhankelijk documentformaat voor niet- of beperkt reviseerbare documenten.	Minimaal moeten de PDF 1.X versies ondersteund worden voor bestaande documenten. Nieuw gecreëerde PDF documenten moeten minimaal voldoen aan PDF 1.7. Duurzaam toegankelijke documenten moeten voldoen aan de PDF standaard PDF/A-1 of PDF/A-2.
EPUB	Aanbevolen open standaard e-book formaat voor het publiceren van geoptimaliseerde documenten voor lezen op een mobiel apparaat	Van toepassing voor documenten gepubliceerd via een mobiele app. Alternatief hiervoor is het PDF formaat.

AES	Aanbevolen open standaard Advanced Encryption Standard (AES) voor versleuteling van opgeslagen en verzonden data.	Bedrijfsgegevens worden versleuteld opgeslagen en verzonden.
TLS	Verplichte open standaard voor beveiligd dataverkeer over het internet.	De koppelingen met andere internetsystemen en/of met websites zijn tijdens transport minimaal beveiligd volgens de verplichte open standaard TLS 1.2 of hoger met certificaten voor versleuteld dataverkeer. De voorkeur gaat uit naar TLS 1.3.
HTTPS en HSTS	Verplichte open standaard voor beveiligd dataverkeer over het internet tussen client en server. In deze standaards wordt TLS toegepast, bijvoorbeeld als uitbreiding op HTTP. HSTS zorgt ervoor dat een beveiligde verbinding niet vervangen kan worden door een onbeveiligde verbinding.	Gebruik aanvullend voor beveiligd dataverkeer over het internet tussen client (internetbrowser) en server (website) de verplichte open standaards HTTPS en HSTS.
OpenID.NLGov of SAML	Verplichte authenticatie standaarden voor eindgebruiker-toegang tot cloud diensten.	Toepassing van 1 van deze standaarden is verplicht voor de aansluiting op het SVB Authenticatie en autorisatiesysteem: 'SVB eenmalig aanloggen'. Nu gerealiseerd door EntraID met SSO en Multi-factor authenticatie. Voorkeur voor SAML 2.0 of OpenID.NLGov. Alternatief (niet de voorkeur!): WS-Federation v1.2
SCIM	Aanbevolen open standaard voor de uitwisseling van identiteitsinformatie voor de gebruikersadministratie van een cloud applicatie.	Van toepassing voor de geautomatiseerde user provisioning zodat door SVB geautoriseerde gebruikers via een koppeling met het identity management systeem van de SVB (Entra ID) geautomatiseerd kunnen worden aangemaakt, geautoriseerd, gemuteerd en verwijderd/gearchiverd kunnen worden. Voor de koppeling met Entra ID ondersteunt de oplossing bij voorkeur SCIM. Alternatieven zijn één van de volgende protocollen: SAML JIT en/of OIDC.
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Verplichte open standaard voor het digitaal toegankelijk maken van web diensten voor mensen met een beperking, zoals bijvoorbeeld voor slechtziendheid en slechthorendheid. Deze moet toegepast worden op het aanbieden van web gebaseerde informatie-, interactie-, transactie- en participatiediensten. Per 1 juli 2018 is deze wettelijk verplicht volgens het besluit toegankelijkheid digitale overheid .	Deze standaard is verplicht voor alle web gebaseerde onderdelen van de oplossing van websites, webapplicaties t/m ontsloten documenten. Betrokken standaards zijn HTML , PDF (NEN-ISO) en PDF/UA .

2.2. Toe te passen principes

De oplossing moet voldoen aan de volgende SVB principes die afgeleid zijn van de NORA.

Architectuurprincipe	Impact
Nauwkeurige dienstbeschrijving (AP05)	Toelichting over en instructies voor de dienst zijn beschikbaar voor de medewerker toegankelijk gemaakt in de Mobiliteitsoplossing zelf of te benaderen via de Mobiliteitsoplossing.
Gebruik standaard oplossingen (AP06)	De oplossing bestaat uit één integrale Mobiliteitsoplossing uit de markt.
Gebruik standaard oplossingen (AP06)	De oplossing wordt as-is geïmplementeerd voor de SVB. Processen, functionaliteit en data worden ingericht volgens de standaard mogelijkheden en best practices van de

	oplossing. Procesintegratie en koppelingen met andere SVB systemen worden beperkt tot het noodzakelijke, voor zover de gewenste functionaliteit niet geboden wordt binnen de standaard mogelijkheden van de oplossing. Maatwerk functionaliteit wordt vermeden. Wel wordt er aangesloten op standaard verplichtte SVB processen en systemen zoals voor aanvragen en beheren van toegang en doorgifte van medewerker gegevens.
Gebruik standaard oplossingen (AP06)	De oplossing moet volledig web gebaseerd zijn voor alle type gebruikers; niet alleen voor eindgebruikers maar ook voor beheerders.
Gebruik standaard oplossingen (AP06)	De oplossing biedt standaard, veilige koppelvlakken voor de ontsluiting van informatie in en/of functionaliteit van de oplossing aan SVB systemen.
Gebruik standaard oplossingen (AP06)	Applicaties uit verschillende domeinen dienen zoveel mogelijk ontkoppeld te blijven waardoor geen maatwerk in deze applicaties gebouwd hoeft te worden zodat ze standaard blijven en makkelijker te vervangen zijn door een andere oplossing. Koppelvlakken met andere IT oplossingen die standaard worden geboden door de mobiliteitsoplossing en/of de te koppelen IT oplossing, en die voldoen aan alle gestelde eisen, kunnen rechtstreeks worden gelegd. Wanneer geen standaard koppelvlak beschikbaar is die voldoet aan alle eisen, kan – na afstemming – het SVB integratieplatform gebruikt worden.
Gebruik beschikbare bouwstenen (AP07)	Autorisatiebeheer wordt bij de SVB uitgevoerd middels het Identiteiten- en rechtensysteem (IRS) waarin identiteiten rechten en accounts op doelsystemen toegekend krijgen én het Enterprise Service Management Applicatie (ESMA) systeem dat een rol speelt bij het aanvragen en goedkeuren van rechten. Rapportages en management informatie die niet standaard door de Mobiliteitsoplossing geleverd worden, moeten door het Dataplatform van de SVB gerealiseerd worden. Daarnaast moet tactische en strategische managementinformatie op het Dataplatform gegenereerd worden als centrale bron voor dit type informatie.
Gebruik open standaarden (AP08)	De diensten maken gebruik van toepasselijke open standaarden ter bevordering van interoperabiliteit. Zie paragraaf 'Toe te passen standaarden'.
Eénmalige uitvraag (AP12)	Medewerker gegevens worden éénmalig ingevoerd en als bron in de personeelsadministratie beheerd en ontsloten. Dit zelfde geldt voor andere HR gegevens zoals organisatie en functie en privé gegevens waaronder het privé adres.
Gegevens (blijven) bij de bron, Bronregistraties zijn leidend (AP13)	HR informatie en gegevens over de medewerker, de organisatie en functies, worden op één plek beheerd, namelijk in de personeelsadministratie. Ook bepaalde privé gegevens waaronder het privé adres worden in de personeelsadministratie beheerd. Identiteit en zakelijk e-mailadres worden als bron beheerd door het identiteiten- en toegangsrechtenbeheersysteem.
Perspectief gebruiker (AP19)	De medewerker kan zelfstandig Mobiliteitsdiensten regelen dan wel aanvragen ('self-service').
Transparante dienstverlening (AP25)	De medewerker wordt geïnformeerd over de status van ingediende aanvragen.
Verantwoording dienstverlening mogelijk (AP30)	Er vindt dossiervorming in de oplossing plaats inclusief bijhouden van de bewaartermijn en uitvoeren van acties voor de vernietiging of permanente bewaring van gegevens.
Veilig en betrouwbaar (BP07)	De diensten voldoen aan het SVB Security & Privacy beleid. Hieronder valt bijvoorbeeld toegang alleen voor bevoegden middels identificatie, authenticatie en autorisatie, bescherming tegen cybercriminaliteit, in het ontwerp van de diensten zijn security en privacybescherming expliciet meegenomen, beschikbaarheid van de dienst, juistheid en compleetheid van gegevens, controlemogelijkheden middels logging en audittrail; leverancier en zijn diensten zijn ISO gecertificeerd ten aanzien van beveiliging.

2.3. Toe te passen overige kaders

In deze alinea wordt beschreven welke andere kaders gelden dan de eerder genoemde eisen.

Nr.	Onderwerp	Kader en impact
1	Gegevensuitwisseling via een API (Application Programming Interface)	Applicatie services, voor ontsluiting van data en/of functies aan andere applicaties, worden geleverd via REST API's.
2	Afspraken over datalevering tussen domeinen	Aanlevering aan het Dataplatform op basis van Gegevensleveringsovereenkomst (GLO)
3	Wijze van datalevering aan het dataplatform	De oplossing exporteert data en metadata via een PowerBI-connector die zij beschikbaar stelt of minimaal in CSV formaat die via bestandsuitwisseling beschikbaar gesteld wordt.
4	User interface	De user interface van een applicatie is web gebaseerd of als webapplicatie via de browser te bereiken. Minimaal moeten de laatste 2 versies van de standaard browsers Google Chrome en Microsoft Edge ondersteund worden.
5	Mobiele app	Mobiele apps behorende tot de Mobiliteitsoplossing moeten via een corporate app store van de SVB op het (privé) mobiele apparaat van de Medewerker geïnstalleerd worden. Daarmee wordt voldaan aan de beveiligingseisen.
6	Generatieve AI	Voorlopig gebruikt SVB geen generatieve artificiële intelligentie voor de uitoefening van haar taken.

2.4. Integraties

Idealiter maakt de Oplossing gebruik van bestaande en bewezen Koppelingen voor de data-uitwisseling tussen de Oplossing en de systemen van de SVB.

De opdrachtnemer biedt voor deze Koppelingen:

1. standaard connectoren met andere systemen en/of
2. generieke API's voor ontsluiting van functies en data van de Oplossing en/of
3. bestandsuitwisseling als alternatief voor specifieke Koppelingen zoals bijvoorbeeld integratie met het dataplatform van de SVB ten behoeve van management informatie en data-analyse.

Zie 'Toe te passen standaarden' en 'Toe te passen overige kaders' voor meer informatie hierover.

Deelnemers worden gevraagd om in hun uitwerking van SGC-K1 (Dienstverlening) aan te geven welke connectoren en welke API's voor de systemen van de SVB beschikbaar zijn op het moment van inschrijven. Opdrachtnemer is verantwoordelijk voor de werking en het onderhoud van deze connectoren en API's.

In het geval van een standaard connector hoeft deze alleen geactiveerd en geconfigureerd te worden op basis van de handleiding en documentatie van de Opdrachtnemer. In geval van een koppeling via een API, zal een Koppeling door Opdrachtnemer en SVB gezamenlijk gerealiseerd worden, waarbij elke partij verantwoordelijk is voor werking en onderhoud van het eigen deel.