

Vernieuwing Digitale Werkomgeving KB

Project-startarchitectuur

Versiehistorie

Versie	Auteur	Datum	
0.1	DO	05-12-2018	Eerste concept
0.2	DO	11-03-2019	
0.8	DO	20-06-2019	
0.9	DO	01-07-2019	
1.0	DO	03-10-2019	
1.1	DO	28-10-2019	

Generated on	Document file location

© 2018 Koninklijke Bibliotheek, Den Haag

Alle rechten voorbehouden.

Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de Koninklijke Bibliotheek.

INHOUDSOPAVE

1	Over deze PSA	3
2	Vernieuwing Digitale Werkomgeving KB	4
2.1	MANAGEMENT SAMENVATTING.....	4
2.2	PROJECT-AANLEIDING	4
2.2.1	Korte beschrijving.....	4
2.2.2	Business drijfveren	5
2.2.3	Architectuur drijfveren	5
2.3	BUSINESS-ARCHITECTUUR.....	6
2.3.1	Processen.....	6
2.3.2	Organisatie	7
2.3.3	Producten en diensten	7
2.4	INFORMATIE-ARCHITECTUUR.....	7
2.4.1	Functionele componenten (applicaties).....	7
2.4.2	Bedrijfsgegevens	16
2.4.3	Kwaliteitseisen en wensen	16
2.5	TECHNISCHE ARCHITECTUUR	17
2.5.1	Client hardware	17
2.5.2	Sourcing	18
2.5.3	Systeem configuratie	18
2.5.4	Systeem componenten.....	18
2.5.5	Ontwikkelaarchitectuur.....	20
2.6	BEVEILIGINGSARCHITECTUUR	20
2.6.1	Informatiebeveiliging	21
2.6.2	Beveiligingsbesturing.....	23
2.7	BEHEERARCHITECTUUR	24
2.7.1	Beheerketen	24
2.7.2	Componenten.....	Fout! Bladwijzer niet gedefinieerd.
2.8	ONTWERPBESLISSINGEN	25
2.8.1	Gemaakte keuzes	25
2.8.2	Nog te nemen besluiten	26
2.9	ARCHITECTUURISSUES.....	27
2.9.1	Openstaande issues.....	27
2.9.2	Afwijkingen van de architectuur	27
3	Termen en begrippen.....	Fout! Bladwijzer niet gedefinieerd.

1 Over deze PSA

In deze project-startarchitectuur (PSA) wordt de globale oplossingsrichting van het project ‘ Vernieuwing Digitale Werkomgeving KB’ vastgelegd. De PSA beschrijft in globale termen hoe de informatie- en technische architectuur eruit zien.

Deze versie van de PSA is bedoeld voor de aanbestedingsfase. In een later stadium, nadat de leverancier is gekozen, wordt de PSA uitgebreid met de kaders voor de implementatie.

Een PSA wordt samengesteld door een vertegenwoordiging van het architectenteam, en wordt opgeleverd voorafgaand aan het vaststellen van een door de projectleider opgesteld PID. Tezamen vormen deze documenten de startdocumentatie voor het project.

De PSA is de vertaling van de enterprise architectuur naar de specifieke situatie van het project. Het doel van de PSA is om een project een concrete, relevante en praktisch realiseerbare scope mee te geven zodat het projectresultaat past in het grotere geheel van de organisatie. De PSA zorgt er ook voor dat er wordt nagedacht over applicatie- en technische risico's en dat zo veel mogelijk de huidige kennis en componenten worden hergebruikt.

De verdere indeling van het document volgt zo veel mogelijk – en waar zinvol – de structuur van de PSA template zoals opgesteld door Sogeti als onderdeel van de architectuur methodiek DYA:

- Project aanleiding: beschrijft de context en redenen voor het project. Wat voor soort project is het, welke doelen, voor wie, etc.
- Businessarchitectuur: welke processen, organisatieonderdelen en producten/diensten worden geraakt door het project.
- Informatiearchitectuur: welke functionaliteiten zullen gerealiseerd worden en welke informatie en services worden hierdoor geraakt.
- Technische architectuur: beschrijft de technische architectuur voor dit project.
- Beveiligingsarchitectuur: beschrijft de bestaande beveiligingsarchitectuur en nieuwe beveiligingseisen.
- Beheerarchitectuur: beschrijft de componenten die in de operationele situatie beheerd gaan worden.
- Ontwerpbeslissingen: beschrijft de genomen en de nog te nemen ontwerpbeslissingen.
- Afwijkingen van de architectuur: beschrijft waar in het project wordt afgeweken van de architectuur. Voor elke afwijking wordt de reden, consequenties en risico's gegeven en welke maatregelen genomen moeten worden om deze risico's te controleren.

2 Vernieuwing Digitale Werkomgeving KB

2.1 MANAGEMENT SAMENVATTING

Het project vernieuwing digitale werkomgeving realiseert een nieuwe digitale werkplek voor KB-medewerkers met een optimale samenwerkingsondersteuning tussen KB-medewerkers onderling en tussen niet KB-relaties. De nieuwe digitale werkplek zal ook het nieuwe werken meer optimaal ondersteunen doordat functionaliteit (afhankelijk van de gekozen oplossing en te ondersteunen platformen) plaats-, tijd- en apparaat onafhankelijk beschikbaar wordt.

Naast het realiseren van een vernieuwde werkplek wordt met dit project ook een noodzakelijke technologische refresh gedaan om compliant te blijven op het gebied van veiligheid en ondersteuning van de gebruikte technologie.

Als belangrijk deel van de oplossing hiervoor is door het management al gekozen voor Microsoft Office 365. Dit platform is door zijn gangbaarheid door veel andere met KB vergelijkbare instellingen als kantoorautomatiseringsplatform gekozen en biedt bovendien een scala aan beveiligingsmaatregelen voor het beschermen van bedrijfsdata. Hiermee wordt een groot deel van de huidige on premise infrastructuur vervangen met Cloud technologie waarmee wordt voldaan aan het patroon om client-software (userinterfaces) in beginsel web-gebaseerd uit te voeren hierbij gebruik makend van het standaard http protocol.

Deze keuze ondersteunt ook de behoefte om het beheer van de werkplekomgeving binnen de huidige kantoorautomatisering terug te dringen.

2.2 PROJECT-AANLEIDING

2.2.1 Korte beschrijving

Het project realiseert een nieuwe (digitale) werkplekomgeving gebaseerd op cloud technologie van Microsoft, Office 365.

De directe aanleiding voor het project is een noodzakelijke technologische refresh vanwege het out of support raken van Windows 7 en Exchange 2010.

De doelen die met het project gerealiseerd worden zijn:

Plaats- en tijdonafhankelijk werken

Zoveel als mogelijk altijd overal kunnen werken ongeacht op welk apparaat. In de praktijk zal niet alle functionaliteit op alle mogelijk voorkomende apparaten beschikbaar zijn. De haalbaarheid hiervan is afhankelijk van de gekozen oplossing en het aantal te ondersteunen platformen. Dit is ook een kosten/baten afweging.

Bring your own device (BYOD)

Ondersteuning van het gebruik van eigen apparatuur.

Samenwerken

Optimale ondersteuning voor samenwerken met collega's en externen mbv document management functionaliteiten als tegelijkertijd aan een document kunnen werken, documenten delen en versiebeheer.

De werkplek heeft minimaal dezelfde applicatiefunctie als de bestaande werkplekomgeving, inclusief email, instant messaging en videoconferencing (ook met externen) en printen en scannen obv de bestaande follow me oplossing.

Doelen op technisch gebied:

Een nieuwe digitale werkplek gebaseerd op cloud technologie met als uitgangspunt dat de hosting en exploitatie ervan zoveel mogelijk wordt uitbesteed en er alleen minimaal (administratief) beheerwerk resteert.

2.2.2 Business drijfveren

De drijfveren vanuit de business voor dit project zijn:

- Het realiseren van een digitale werkplek voor KB-medewerkers waarmee plaats-, tijd- en apparaat onafhankelijk kan worden gewerkt. Apparaat onafhankelijkheid hangt, zoals eerder vermeld, af van de gekozen techniek en de hoeveelheid te ondersteunen platformen. Hier zal een kosten/baten overweging moeten worden gemaakt.
- Naast het realiseren van een vernieuwde werkplek dient ook een noodzakelijke technologische refresh te worden gedaan om compliant te blijven op het gebied van veiligheid en ondersteuning van de gebruikte onderliggende technologie.
- De digitale werkplek moet het samenwerken met collega's en externen waarmee wordt samengewerkt beter ondersteunen.
- Deze digitale werkplek dient toekomstvast te zijn. Dat wil zeggen dat de gebruikte technologie flexibel kan mee evolueren met de veranderende wensen en eisen van de organisatie.
- De uitvoering voor het faciliteren van de digitale werkplek (kantoorautomatisering) voor de KB medewerker is niet strategisch voor business en IT. Hierdoor is het verstandig dit uit te besteden en uit te voeren als SaaS of Clouddienst en de hiermee vrijkomende resources voor organisatie-strategische onderwerpen in te zetten.
- Deze vernieuwing zal er dus toe moeten leiden dat de hosting en exploitatie ervan zo veel mogelijk wordt uitbesteed. De verwachting is dat er een hybride omgeving zal ontstaan waarvan het beheer voor een groot deel uit het administreren van het cloud deel zal bestaan met een minimale werklast voor de (beheer)organisatie. Deze werkzaamheden vereisen een ander type functionaris; cloud-beheerder.

2.2.3 Architectuur drijfveren

De drijfveren vanuit de architectuur voor dit project zijn:

- Toekomstvastheid van de digitale werkplek. Dat wil zeggen dat de gebruikte technologie flexibel kan mee evolueren met de veranderende wensen en eisen van de organisatie. Dit vergt graduele omvorming naar een groep services van de technologische oplossing.
- Standaardisatie in de vorm van een generieke oplossing voor de digitale werkplek dat zorgt voor het drastisch terugdringen van beheer van de omgeving en flexibiliteit in outsourcing.
- Het toepassen van de strategie om zoveel mogelijk gebruik te maken van web gebaseerde software o.b.v. het standaard http-protocol t.b.v. standaardisatie en flexibiliteit.
- Goede afbakening van functionaliteit van de digitale werkplek waarmee functionaliteit die elders technologisch moet worden opgelost zichtbaar wordt. Een voorbeeld hiervan zijn oneigenlijke toegangen vanaf werkplekken van functioneel beheerders naar backend systemen vanwege het ontbreken van de benodigde functionaliteit op applicatieniveau. Dergelijke functionaliteit dient binnen de desbetreffende applicatie te worden opgelost.
- Client-applicaties die niet web-gebaseerd zijn kunnen alleen vanaf door KB verstrekte werkplekken worden gebruikt. Deze laatste categorie dient dus te worden afgebouwd en te worden omgezet naar web- of Cloud-native applicaties zodat het applicatie portfolio in de toekomst, afhankelijk van de aard van de te verwerken data, zo breed mogelijk voor elk type device toegankelijk wordt.

2.3 BUSINESS-ARCHITECTUUR

In dit hoofdstuk wordt de scope van het project aangegeven met betrekking tot de business architectuur. Deze business architectuur valt uiteen in drie delen:

- de bedrijfsprocessen
- de organisatie
- de producten en diensten

2.3.1 Processen

De nieuwe digitale werkplek zal, afhankelijk van de gekozen techniek en het aantal te ondersteunen platformen, de functies bieden die KB medewerkers ter ondersteuning van hun werk nodig hebben. Deze functies zullen, afhankelijk van type medewerker in relatie tot de aard van de functie en voor zover mogelijk, plaats-, tijd en apparaat-onafhankelijk beschikbaar worden gesteld.

Als onderdeel van de nieuwe digitale werkplek is er het fysieke deel waaronder een desktop, laptop of een eigen apparaat wordt verstaan, een browser, generieke- en specifieke bedrijfsapplicaties en de mogelijkheid tot printen en scannen. De desktop behoort tot de vaste digitale werkplek en de laptop of eigen device behoort tot de mobiele digitale werkplek. Uitgangspunt voor de digitale werkplek is alles mobiel tenzij.

De mobiele digitale werkplek is op iedere locatie te gebruiken. Hierbij wordt geen onderscheid gemaakt tussen het KB-gebouw, thuis, onderweg of in het buitenland. Er is wel variatie van de beschikbaarheid van functionaliteit op verschillende locaties. Beschikbaarheid van connectivity is hierin de bepalende factor: bij beperkte connectivity is beperkte beschikbaarheid, al zal er maximaal ingezet worden op (veilige) offline beschikbaarheid van gegevens. Concrete invulling is afhankelijk van het gebruiksprofiel van de medewerker. Deze gebruikersprofielen, de zogenaamde persona's, zijn als actoren weergegeven in het contextdiagram van het hoofdstuk Informatie-architectuur.

2.3.2 Organisatie

Het resultaat van het project is een nieuwe digitale werkplek voor alle KB medewerkers. Samenwerkingsfuncties welke het project beschikbaar zal maken kunnen, wanneer van toepassing, ook door externen worden gebruikt. Denk hierbij aan communicatiemiddelen als video conferencing of het delen van documenten.

Adoptie van de nieuwe digitale werkplek is een belangrijk onderdeel om het project te laten slagen. Dit kan grote negatieve impact hebben op de organisatie wanneer dit onderdeel onvoldoende aandacht krijgt binnen het project. Het is aan de stuurgroep om dit in het project te laten borgen.

2.3.3 Producten en diensten

De digitale werkplek KB (DWK) zal de bestaande KB werkplek vervangen. Omdat de digitale werkplek plaats-, tijd- en apparaat onafhankelijk werken mogelijk maakt zal de eindgebruiker dit anders ervaren (veel hogere flexibiliteit) in het uitvoeren van zijn- of haar werk.

2.4 INFORMATIE-ARCHITECTUUR

In dit hoofdstuk wordt de scope van het project aangegeven met betrekking tot de informatiearchitectuur.

2.4.1 Functionele componenten (applicaties)

2.4.1.1 Contextdiagram

In onderstaand contextdiagram is de SOLL situatie van de digitale werkplek weergegeven. Bovenaan zijn de verschillende typen afnemers van de digitale werkplek afgebeeld, de zogenaamde persona's. Deze zijn gekoppeld aan de voor het type persona opgeld doende bedrijfsservices welke weer verbonden zijn met de onderliggende bedrijfsfuncties.

De bedrijfsfuncties zijn weer gekoppeld aan het type apparaat waarmee deze beschikbaar worden gesteld.



Binnen de contexten "Hybrid Identity platform", "On-premise applicatie deployment", "Endpoint protectie" en "Microsoft 365" zijn de benodigde applicaties gerubriceerd weergegeven die de bedrijfsfuncties op de verschillende typen apparaten beschikbaar maken.

Binnen het project zal aan de hand van een representatieve gebruikersgroep moeten worden getoetst of de uitgewerkte persona's, zoveel als mogelijk, kloppend zijn met de typen voorkomende KB medewerkers. Ook zal het percentage van iedere persona moeten worden bepaald.

Vervolgens kan worden getoetst of de verwachte functionaliteit van deze gebruikersgroep overeenkomt met de bedrijfsservices uit het contextdiagram.



Figure 1 : Functies Digitale Werkplek KB

2.4.1.2 Bestaande componenten

ArchiMate_BusinessFunction	Details	Dependency: Activity
Printen en scannen		Afdrukken, scannen informatie

ArchiMate_SystemSoftware	Details	Usage: Component
SCCM	SCCM is de bestaande software deployment management omgeving. Deze zal worden heringezet voor de nieuwe digitale werkomgeving tbv OS en softwaredeployment. De ontwikkelingen op het gebied van mobile device management platformen voorspellen dat er op termijn steeds meer functionaliteit van SCCM zal worden overgenomen. Op dit moment is dat nog onvoldoende waardoor vooralsnog in dit project wordt gekozen voor een hybride inzet van beide middelen voor een optimale dekking van functionaliteit waardoor de lagere beheersinspanning voor het beschikbaarstellen van applicaties pas op termijn gerealiseerd zal worden.	(none)

ArchiMate_ApplicationComponent	Details	Dependency: Component
AD	Active Directory Bestaande on premise directory service Active Directory. Voorziet in authenticatie en autorisatie tbv het kantoorautomatiseringsdomein. De bestaande identiteiten zullen dmv het koppelvlak AD-connect synchroniseren naar de IDaaS directory service Azure Active Directory om plaatsonafhankelijk alle op het Office 365 platform aangesloten resources te kunnen ontsluiten naar digitale werkplek gebruikers.	(none)
Kantoor automatisering applicaties	Kantoorautomatiseringapplicaties, die bestaande functionaliteit dekken, welke zoveel als mogelijk geschikt gemaakt moeten worden voor plaats-, tijd- en apparaatonafhankelijk gebruik. De haalbaarheid hiervan hangt voor een groot deel af van het type huidige applicaties. Legacy applicaties zullen lastig plaats en apparaatonafhankelijk beschikbaar	(none)

ArchiMate_ApplicationComponent	Details	Dependency: Component
	gemaakt kunnen worden omdat deze veelal lokaal geïnstalleerd moeten worden waardoor ze apparaatafhankelijk zijn. Het inzetten van technologie om deze wel plaatsafhankelijk beschikbaar te kunnen maken is kostbaar en beheerlastverhogend. Beter zou zijn om legacy applicaties te vervangen door web- of native applicaties.	

2.4.1.3 Nieuwe componenten

ArchiMate_BusinessFunction	Details	Dependency: Activity
Generieke applicaties		Generieke toepassingen
Email		(none)
Instant messaging		(none)
Agenda		(none)
Document management		(none)
Directory services		(none)
Video conferencing		(none)
Rolspecifieke applicaties		Rolspecifieke toepassingen
Opslaan en delen van bestanden		(none)
Samenwerken in documenten		(none)

ArchiMate_BusinessService	Details	Association: Class
Generieke toepassingen		Taakwerker Kenniswaerker Kantoorwerker
Afdrukken, scannen informatie		Taakwerker Kenniswaerker Externen Kantoorwerker
Rolspecifieke toepassingen		Taakwerker Kenniswaerker Kantoorwerker

ArchiMate_BusinessActor	Details
Taakwerker	Medewerkers die dagelijkse standaard taken uitvoeren op een vaste werkplek op nagenoeg dezelfde locatie en een aantal stabiliteit en performance vereisende toepassingen gebruiken.

ArchiMate_BusinessActor	Details
	Rollen die hiertoe behoren bevinden zich bij: Digitalisering & Documentverwerking, Publieksdiensten, Serviceteam, Supportdesk en (directie)secretaresses.
Kenniswerker	De mobiele en self supporting werker die vaak flexwerkt en reist naar verschillende locaties en op elk gewenst moment informatie co-creëert en deelt binnen communities met grote behoefte aan remote toegang tot bedrijfs(project)gegevens. Rollen die hiertoe behoren zijn: Informatiemanagers, Researchers, Architecten en management.
Kantoorwerker	Medewerkers met directe bedrijfsondersteunende functies die doorgaans op kantoor werken en remote toegang gebruiken vanaf thuis. Rollen die hiertoe behoren bevinden zich bij: Bedrijfsvoering (G&F, HR, Inkoop, Financien) en Corporate Communicatie.
Externen	Medewerkers veelal ingehuurd door KB en/of participierend in een project voor een afgebakende taak, gebruik makend van eigen apparatuur (BYOD). Dit kunnen ook relaties in het erfgoed en OB veld zijn. Mogelijkheid bestaat dat dit type persona altijd elders werkt. Rollen die hiertoe behoren bevinden zich in de categorie: Inhuur tbv consultancy.

ArchiMate_Device	Details	Usage: Component
Smartphone	Een mobiele telefoon die uitgebreidere computermogelijkheden biedt. In tegenstelling tot de huidige situatie zal dit type apparaat na uitvoering van het project onderhevig zijn aan beleid tbv het beschermen van bedrijfsdata. Dit kunnen bestanden zijn of email. Dit gebeurt dmv het installeren van software op het apparaat waarmee een bedrijfscontainer op het apparaat kan worden gevoerd en beheerd.	(none)
Laptop	Laptop computer ontworpen om eenvoudig mee te kunnen nemen naar verschillende locaties fungerend als digitale werkplek.	(none)
BYOD	BYOD staat voor "bring your own device". BYOD kan werknemers toestaan om (onder condities) met persoonlijke apparaten (laptops, tablets en smartphones) te werken. BYOD apparaten kunnen alleen worden gebruikt onder de voorwaarde dat een corporate container door de eigenaar op het apparaat wordt toegestaan	(none)

ArchiMate_Device	Details	Usage: Component
	waarover beheer tbv databescherming, encryptie en remote wipe wordt gevoerd.	
Desktop	Desktop computer ontworpen om op een bureau te plaatsen fungerend als digitale werkplek. De desktop computer heeft een vaste plek als onderdeel van een fysieke werkplek binnen de KB.	(none)

ArchiMate_SystemSoftware	Details	Usage: Component
Samenwerken	Nieuw te realiseren cloud samenwerkingsomgeving tbv instant messaging en videoconferencing, onderdeel van Office 365. Vervangt de on premise Lync server.	(none)
Persoonlijke opslag	Nieuw te realiseren cloud opslag voor persoonlijke zakelijke bestanden, onderdeel van Office 365. Vervangt de F-schijf binnen de huidige kantoorautomatisering.	(none)
Mail en Calendar	Nieuw te realiseren mailomgeving op basis van Exchange Online, onderdeel van Office 365. Vervangt de on premise Exchange mailserver.	(none)
Windows 10	Nieuw te realiseren client besturingssysteem component op basis van Windows 10 enterprise edition tbv "company owned" beheerde apparaten. Dit besturingssysteem dient geautomatiseerd uitrolbaar te zijn dmv de beschikbare tools SCCM en MDM.	(none)
Document management systeem	Nieuw te realiseren cloud opslag voor bedrijfsdocumenten en bestanden, onderdeel van Office 365. Vervangt zoveel als mogelijk de on premise fileserver (G:\- en M:\-schijf). De mate hierin wordt bepaald door de BIV-dataclassificatie.	(none)

ArchiMate_ApplicationComponent	Details	Dependency: Component
MFA	Multi factor authenticatie Voor toegang tot de nieuwe digitale werkplek zal naast een gebruikersaccount met bijbehorend wachtwoord een tweede factor vereist zijn welke dmv een authenticatie app op een persoonlijk	(none)

ArchiMate_ApplicationComponent	Details	Dependency: Component
	mobiel apparaat kan worden bediend. Hiervoor dient binnen de (cloud) omgeving een applicatie te worden geïmplementeerd.	
MDM/MAM	Mobile device management/mobile application management Omdat de nieuwe kantoorautomatisering omgeving voornamelijk uit mobiele apparaten zal bestaan (voor vaste werkplekken met randapparatuur kunnen nog steeds desktops worden ingezet) en het ook mogelijk moet zijn om op een veilige manier eigen apparaten (BYOD) voor het werk te kunnen gebruiken, is mobile device management (MDM)/mobile application management (MAM) een vereiste. Met MDM kunnen alle zogenaamde company owned en BYOD apparaten worden beheerd. Hiermee moet het mogelijk zijn dat mobiele apparaten (zakelijke) data versleuteld opslaan. Ook moet het mogelijk zijn de (zakelijke) data op het apparaat op afstand te wissen bij verlies of diefstal. Een MAM-oplossing is een vereiste voor het kunnen aanbieden van zakelijke mobiele apps op een BYOD. MAM moet een portal kunnen aanbieden waar vandaan (op basis van de functionele behoefte) zakelijke apps kunnen worden gedownload en de app en daaraan gerelateerde data kan worden beheerd. Het moet ook de mogelijkheid bieden om zakelijke apps met daaraan gerelateerde data en zakelijke email gescheiden te houden van persoonlijke apps en email (sandbox/container).	(none)
PTA & password hashing	Nieuw te realiseren component welke voorziet in het authenticeren van gebruikers bij Active Directory voor het toegang geven tot cloud resources waaronder ook extern gekoppelde bedrijfsapplicaties zoals Topdesk en Plein.	(none)

ArchiMate_ApplicationComponent	Details	Dependency: Component
NAC	Network access control Om op het KB-netwerk aangesloten BYOD apparaten te kunnen vertrouwen is een toegangscontrolesysteem op netwerkniveau (NAC) een vereiste. Dit systeem werkt samen met een Endpoint protectie systeem en kan BYOD apparaten scannen op een van te voren bepaalde baseline aan vereisten zoals (vertrouwd) besturingssysteemtype, patchlevel en aanwezigheid van anti-virus software met laatste virusdefinities.	(none)
AAD	Azure Active Directory De keuze voor het gebruik van Office 365 voor de vernieuwing van de kantoorautomatisering omgeving impliceert de introductie van Azure Active Directory (AAD) binnen de omgeving. AAD is de cloud directory service voor de Microsoft cloud waar Office 365 een onderdeel van uitmaakt. KB medewerkers zullen straks een AD account in deze directory hebben tbv authenticatie en autorisatie welke gesynchroniseerd wordt vanuit de bestaande on premise Active Directory (AD).	(none)
Endpoint protectie	Om KB-medewerkers van eigen apparatuur gebruik te kunnen laten maken (BYOD) is Endpoint security management een vereiste. Hiermee kan van client apparaten zoals PC's, laptops, tablets en smartphones worden afgedwongen dat deze aan bepaalde beveiligingseisen voldoen (oa een vertrouwd besturingssysteem met bepaald patchlevel, up-to-date anti-virus software) alvorens deze verbinding kunnen maken met bedrijfsystemen en bedrijfsapplicaties. Wanneer niet aan de gestelde voorwaarde wordt voldaan dan is toegang niet mogelijk of alleen beperkt tot een afgescheiden netwerk met alleen een verbinding naar het Internet.	(none)

ArchiMate_ApplicationComponent	Details	Dependency: Component
Azure AD Connect	Nieuw te realiseren component voor het synchroniseren van AD identiteiten naar AAD waarmee Office 365 functionaliteit toegankelijk wordt. Afhankelijkheid AAD met AD binnen het KB-bedrijfsnetwerk	(none)

2.4.2 Bedrijfsgegevens

2.4.2.1 Gegevensmodel

Extractie uit de bestaande bedrijfsservices van de relevante infra-services/functions binnen de digitale werkomgeving.

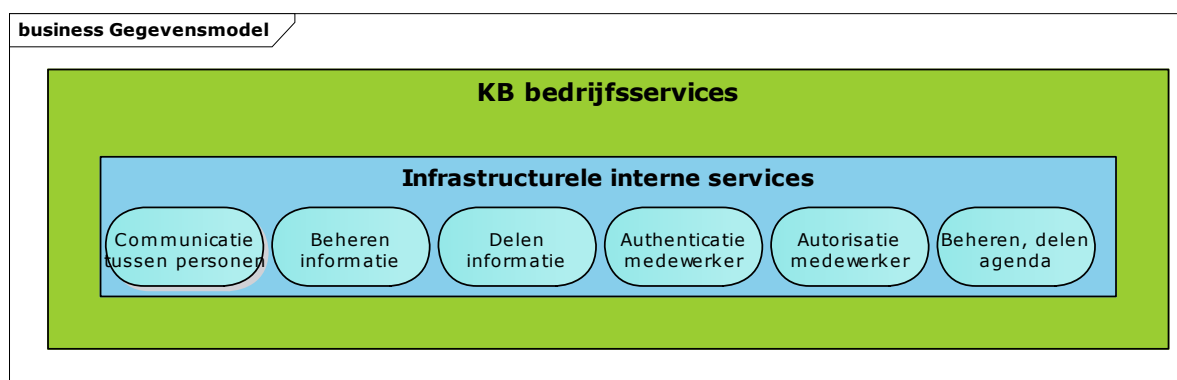


Figure 2 : Gegevensmodel

ArchiMate_BusinessService	Details	Association: Class
Delen informatie		(none)
Communicatie tussen personen		(none)
Autorisatie medewerker		(none)
Authenticatie medewerker		(none)
Beheren, delen agenda		(none)
Beheren informatie		(none)

2.4.3 Kwaliteitseisen en wensen

De nieuwe digitale werkomgeving dient minimaal dezelfde functionaliteit te bieden als de huidige werkplekomgeving waarbij het streven is dat deze functionaliteit zoveel mogelijk plaats-, tijd-, en apparaat onafhankelijk beschikbaar zal zijn. De haalbaarheid hiervan hangt

voor een groot deel af van het type huidige applicaties. Legacy applicaties zullen lastig plaats en apparaat onafhankelijk beschikbaar gemaakt kunnen worden omdat deze veelal lokaal geïnstalleerd moeten worden waardoor ze apparaat afhankelijk zijn. Het inzetten van technologie om deze wel plaats onafhankelijk beschikbaar te kunnen maken is kostbaar en beheerlastverhogend. Beter zou zijn om legacy applicaties te vervangen door web- of native applicaties.

Applicaties specifiek voor de behoefte van functioneel beheerders worden niet per definitie binnen de vernieuwing van de digitale werkomgeving aangepakt. Clientapplicaties ter ondersteuning van functioneel beheer die op de standaard manier uitrolbaar zijn worden wel in de vernieuwing meegenomen. De functionaliteit welke naast deze clientapplicaties door oneigenlijke toegangen tot backend systemen wordt geboden dienen te worden opgelost door interfaces binnen de desbetreffende applicatie.

Inloggen op de digitale werkplek dient eenmalig te gebeuren en eenmaal ingelogd toegang te bieden tot alle functionaliteit waar de gebruiker toe geautoriseerd is, ook al wordt dit geserviced vanaf verschillende achterliggende systemen (single sign-on).

Bestaande functionaliteit dient zo mogelijk te worden hergebruikt. Overlappende of dubbele functionaliteit dient geconsolideerd te worden. Specifieke functionaliteit dient maar een keer voor te komen.

De digitale werkplek dient minimaal de functionele behoeften van de in de KB-organisatie voorkomende persona's te kunnen bedienen: Gebruik gecentreerd ontwerp. Het ontwerp van functionaliteit is gericht op de taken die gebruikers moeten uitvoeren en niet op de functies die systemen kunnen leveren. Binnen het project zal getoetst moeten worden of de uitgewerkte persona's alle benodigde functionaliteit dekken. Deze functionaliteit dient te worden geleverd door diensten (services). Het concept van een dienst (een service) staat centraal in de structurering van functionaliteit. De functionaliteit van een service correspondeert zo veel mogelijk met de bedrijfsactiviteiten.

Uitgangspunt hierbij is dat de oplossing flexibel is en makkelijk kan worden aangepast aan de veranderende behoeften.

Applicatie overstijgende rapportages voor sturing en verantwoording dienen te worden ondersteund vanuit een centrale rapportagevoorziening.

Data zal volgens de door de veiligheidscoördinator en CIO vastgestelde BIV-classificatie geclassificeerd zijn alvorens de data naar opslaglocaties binnen de digitale werkplek zal worden verplaatst.

2.5 TECHNISCHE ARCHITECTUUR

2.5.1 Client hardware

De door de KB verstrekte computerwerkplekken zijn in principe laptops om hiermee het tijd- en plaats onafhankelijk werken te faciliteren. Alleen wanneer dat door de aard van het werk of andere omstandigheden niet kan wordt een desktopcomputer verstrekt.

2.5.2 Sourcing

De digitale werkplek (kantoorautomatisering) is niet strategisch voor business en IT en komt hiermee in aanmerking voor uitbesteden en uitvoeren als SaaS of Cloud-dienst. De hiermee vrijkomende resources kunnen voor organisatie-strategische onderwerpen worden ingezet.

Deze vernieuwing van de digitale werkplek zal er dus toe moeten leiden dat de hosting en exploitatie ervan zo veel mogelijk wordt uitbesteed. De verwachting is dat er een hybride omgeving zal ontstaan waarvan het beheer voor een groot deel uit het administreren van het clouddeel zal bestaan met een minimale werklast voor de (beheer)organisatie.

2.5.3 Systeem configuratie

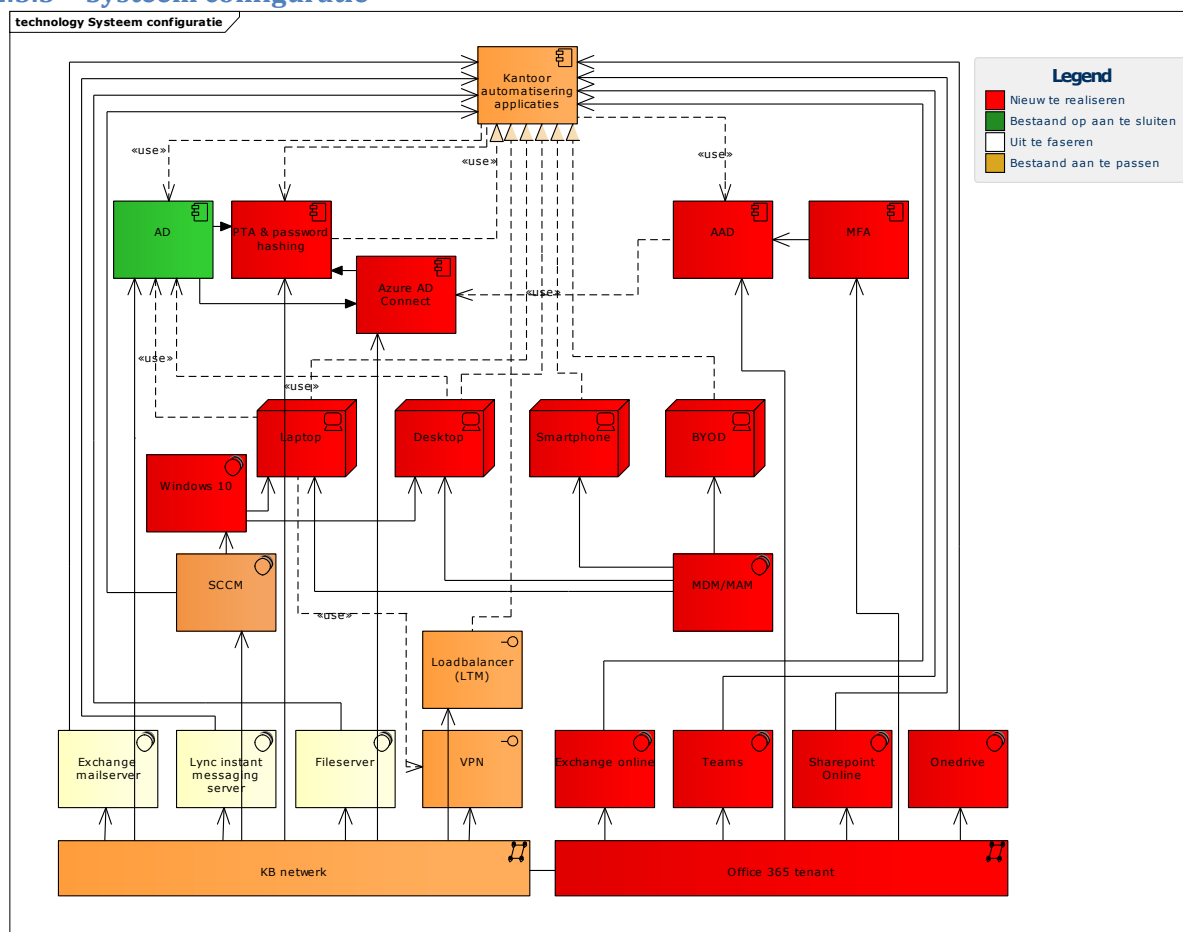


Figure 3 : Systeem configuratie

2.5.4 Systeem componenten

ArchiMate_CommunicationNetwork	Details	Association: Component
KB netwerk	Er dient op zowel het bedrade als het draadloze netwerk in het KB-gebouw voldoende bandbreedte te zijn ivm het permanente gebruik van Cloud storage en toepassingen	AD PTA & password hashing Azure AD Connect

ArchiMate_CommunicationNetwork	Details	Association: Component
	die QoS vereisen. Hier zijn aanpassingen voor nodig.	
Office 365 tenant	Nieuw te realiseren platform dat als basis dient voor de digitale werkplek.	AAD MFA

ArchiMate_SystemSoftware	Details	Usage: Component
Sharepoint Online	Nieuw te realiseren cloud opslag voor bedrijfsdocumenten en bestanden, onderdeel van Office 365. Vervangt zoveel als mogelijk de on premise fileserver (G:\- en M:\-schijf). De mate hierin wordt bepaald door de BIV-dataclassificatie.	AAD
Teams	Nieuw te realiseren cloud samenwerkingsomgeving tbv instant messaging en videoconferencing, onderdeel van Office 365. Vervangt de on premise Lync server.	AAD
Exchange online	Nieuw te realiseren mailomgeving op basis van Exchange Online, onderdeel van Office 365. Vervangt de on premise Exchange mailserver.	AAD
Fileserver	On premise fileservers dienen zoveel als mogelijk te worden uitgefaseerd en vervangen door cloud opslag. BIV-dataclassificatie en het beleid hierin zal de mate waarin dit mogelijk is bepalen.	AD
Exchange mailserver	On premise mailserver op basis van Microsoft Exchange dient gemigreerd te worden naar cloud oplossing binnen Office 365, Exchange Online.	AD
Onedrive	Nieuw te realiseren cloud opslag voor persoonlijke zakelijke bestanden, onderdeel van Office 365. Vervangt de F-schijf binnen de huidige kantoorautomatisering.	AAD

ArchiMate_TechnologyInterface	Details	Usage: Component
Loadbalancer (LTM)	De huidige loadbalancer biedt functionaliteit voor het publiceren van	(none)

ArchiMate_TechnologyInterface	Details	Usage: Component
	webapplicaties. De webapplicaties Exact en Interflex worden al op deze manier plaats-, tijd- en apparaatonaafhankelijk ontsloten. Deze functionaliteit kan ook voor andere webapplicaties worden ingezet. Een alternatief is webapplicaties aanbieden via een Web Application Proxy. Dit component is al aanwezig voor het ontsluiten van ADFS. Welke oplossing zal worden ingezet is nog nader te bepalen. Dit staat ook vermeld onder het hoofdstuk ontwerpbeslissingen.	
VPN	Bestaande VPN oplossing voor veilige toegang tot de vertrouwde netwerkkzone (KB kantoorautomatiseringsnetwerk) waarbinnen zich bedrijfsdata bevindt. Omdat bedrijfsdata wordt gemigreerd naar cloud opslag zal de inzetbaarheid van de VPN functie voor dit aspect veranderen. Alle andere functionaliteit dat door VPN wordt ontsloten zoals bedrijfsapplicaties en toegang tot back-end systemen tbv (functioneel(beheer) blijven vooralsnog ongewijzigd.	AD

2.5.5 Ontwikkelarchitectuur

Niet relevant omdat de gekozen oplossing een SaaS oplossing betreft en de ontwikkeling hiervan door Microsoft wordt gedaan.

2.6 BEVEILIGINGSARCHITECTUUR

In dit hoofdstuk wordt op hoofdlijnen vastgelegd wat de architectuurimpact van het project vernieuwing digitale werkplek is op het gebied van beveiliging en privacy.

De oplossing zal vertrouwelijke informatie gaan verwerken waardoor informatiebeveiliging bijzondere aandacht nodig heeft. De oplossing dient dan ook aan het KB Informatiebeveiligingsbeleid te voldoen.



2.6.1 Informatiebeveiliging

Systemen en software tbv de digitale werkplek zijn veilig en betrouwbaar. Systemen bieden adequate voorzieningen voor (multi-factor) authenticatie, autorisatie, RBAC, versleuteling, data labeling en andere beveiliging.

2.6.1.1 Authenticatie en autorisatie

Single Sign On

Vanuit de werkplek wordt een Single Sign On ervaring aangeboden (één keer inloggen) zover de vertrouwelijkheid van de te benaderen gegevens dit toelaat.

Schaalbaar

Wanneer er extra beveiliging van gegevens of systemen nodig is, kunnen additionele beveiligings-lagen modulair worden toegevoegd.

Tweede factor authenticatie

Standaard dient een gebruiker zich met een voor een bepaalde duur geldig gebruikersnaam en wachtwoord aan te melden op de digitale werkomgeving. Wachtwoorden dienen aan eisen van complexiteit te voldoen, deze worden afgedwongen door het systeem. Toegang tot de digitale werkplek en resources behorende bij de digitale werkomgeving vanaf niet vertrouwde netwerkzones (buiten het kantoorautomatisering netwerk van de KB) dient met een tweede factor te gebeuren in de vorm van een authenticatie-app op een mobiel device.

Toegang tot clouddiensten

Publieke beschikbare inlogschermen vanaf het Internet dient het transport beveiligd te zijn met officiële SSL certificaten. De SSL/TLS configuratie dient van courante en adequate hardening te worden voorzien (zie KB hardeningsbeleid)

Rol gebaseerd

Autorisatie is zoveel mogelijk rol gebaseerd. Autorisaties worden toegekend via functie(s) en organisatie onderdelen.

2.6.1.2 Data

Dataclassificatie



Data dient geclassificeerd te zijn (door data-eigenaren) alvorens deze, afhankelijk van de classificatie en maatregel, gemigreerd worden naar cloud opslag.

Opslag van data

Alle in de cloud opgeslagen data dient adequaat versleuteld te zijn volgens de norm aangegeven opgesteld in het informatiebeveiligingsbeleid (zie...). De encryptiesleutel dient in het bezit te zijn van KB en op een speciaal hiervoor ingerichte beveiligde locatie te worden bewaard.

KB moet van de cloudleverancier de garantie hebben dat de gegevens alleen in geografische locaties worden opgeslagen zoals bepaald in het contract.

Data op mobiele apparatuur

Voor mobiele apparaten die door KB zijn uitgegeven moet Mobile Device Management geregeld zijn voor databescherming, encryptie en remote wipe. BYOD apparaten kunnen alleen worden gebruikt onder de voorwaarde dat een corporate container door de eigenaar op het apparaat wordt toegestaan waarover beheer tbv databescherming, encryptie en remote wipe wordt gevoerd.

(Disaster)Recovery

Data in de cloud dient in een dagelijkse backup routine te worden meegenomen en in geval van dataverlies bruikbaar te zijn voor het terughalen van data. Bij ketensystemen dient het back-up mechanisme de data-integriteit van de informatieketen te waarborgen. Deze backup dient op een adequate manier beveiligd (versleuteld) te worden opgeslagen op een redundante omgeving waar alleen geautoriseerden (beheerverantwoordelijken) toegang toe hebben.

2.6.1.3 Logging en controle

Het gebruik van informatiesystemen binnen de digitale werkomgeving, alsmede informatiebeveiligingsincidenten worden vastgelegd in logbestanden. Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Er moeten maatregelen worden getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden door een gebruiker of systeembeheerder. In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen.

Logging moet in een feed naar de centrale logserver van de KB worden gestuurd en later ook naar een derde partij SIEM (security information and event management) oplossing.

2.6.1.4 Verbindingen

Alle verbindingen van en naar cloud resources dienen via de door de cloudleverancier standaard beschikbaar gestelde interfaces te lopen en uit open standaarden te bestaan. Deze verbindingen dienen over HTTPS te verlopen en adequaat versleuteld en gehardend te zijn volgens de hiervoor aangegeven richtlijnen in het KB hardeningsbeleid. Beveiligingscertificaten worden centraal beheerd door KB.

2.6.2 Beveiligingsbesturing

2.6.2.1 Active Directory

Autorisatie van KB medewerkers dient centraal geregeld te worden vanuit de directory service Active Directory.

2.6.2.2 Adoptie digitale werkomgeving en beveiliging

Beveiliging dient onderdeel te zijn van de adoptie van de digitale werkomgeving.

2.6.2.3 BYOD beleid

Er dient een BYOD beleid te worden opgesteld. Dit is aan (strategisch) management. Aansluitend dient het KB beveiligingsbeleid dan BYOD te dekken. Dit beleid moet er zijn voordat BYOD vanuit het project DWK binnen de KB kan worden toegepast.

2.6.2.4 Informatiebeleid

Er dient een classificatie-methodiek te worden opgesteld t.a.v. classificatie waarlangs data geclassificeerd en behandeld kan worden. Ook dient beleid te worden bepaald t.a.v. conditionele toegang tot informatie. Dit zal door individuele business owners moeten worden opgesteld. Dit traject loopt parallel aan het project.

2.6.2.5 Mobile Device Management

MDM/MAM dient vroegtijdig geïmplementeerd te zijn alvorens men kan aansluiten en aanmelden met (eigen) apparatuur.

2.6.2.6 Office 365 subscriptie

Om adequate beveiligingsmaatregelen te kunnen treffen binnen de digitale werkomgeving is het van belang de subscriptie van het cloud platform Office 365 af te nemen waarin o.a. AIP (Advanced Information Protection) zit vervat welke o.a. DRM op bestanden (Azure RMS) mogelijk maakt.

2.6.2.7 Patch management beleid

De binnen de digitale werkomgeving toegepaste werkplekken dienen van de laatste versie besturingssoftware en endpoint protectie software te zijn voorzien. (zie KB technische IT Security richtlijnen ad14). De endpoint protectie software is een vereiste voor Network Access Control (NAC) tbv BYOD.

2.6.2.8 Toegang tot applicaties

Toegang tot applicaties zal worden bepaald door het risicoprofiel van de applicatie en van waar vandaan deze wordt benaderd.

Webapplicaties zijn doorgaans toegankelijk vanaf BYOD en door KB verstrekte werkplekken.

Webapplicaties waarin gevoelig geclassificeerde informatie wordt verwerkt dienen met een tweede factor te worden ontsloten waarmee het principe separation of privilege wordt ondersteund.

Client-applicaties die niet web-gebaseerd zijn kunnen alleen vanaf door KB verstrekte werkplekken worden gebruikt. Deze laatste categorie dient dus te worden afgebouwd en te worden omgezet naar web- of Cloud-native applicaties zodat het applicatie portfolio in de toekomst, afhankelijk van de aard van de te verwerken data, zo breed mogelijk voor elk type device toegankelijk wordt.

Toegang tot applicaties en cloud resources voor gebruikers van de digitale werkomgeving dient op basis van rol of functie te worden ingeregeld (roll based access control) en ondersteunt het principe least privilege waarmee alleen de minimale reeks privileges zijn toegekend om de taken behorende bij een medewerker uit te kunnen voeren.

2.7 BEHEERARCHITECTUUR

Dit hoofdstuk beschrijft de beheerketen, en de componenten waaruit deze is opgebouwd.

2.7.1 Beheerketen

In onderstaande afbeelding zijn de te onderscheiden deelgebieden met bijbehorende componenten weergegeven welke beheerd moeten worden.



Figure 4 : Beheerketen

2.8 ONTWERPBESLISSINGEN

Dit hoofdstuk beschrijft de ontwerpbeslissingen die nog te nemen of al genomen zijn.

2.8.1 Gemaakte keuzes

2.8.1.1 Office 365

Als onderdeel van de solutionarchitectuur dient de digitale werkplek gebaseerd te zijn op Office 365. Deze oplossing is op management niveau al gekozen.



2.8.1.2 Mobiele werkplekken

Werkplekken zullen zoveel mogelijk worden vervangen door mobiele werkplekken tenzij de werkplek dit niet toelaat door de aard van de werkplek (balie) of aanwezige randapparatuur zoals lokale printers en scanners.

2.8.1.3 Windows 10

Het besturingssysteem waarmee de mobiele- en vaste werkplekken worden uitgerold is Windows 10 enterprise edition.

2.8.1.4 Azure Active Directory

Azure Active Directory (AAD) als IDaaS voorziening voor authenticatie en autorisatie binnen de digitale werkplekomgeving.

Zoals weergegeven in de systeem configuratie onder technische architectuur zullen de identiteiten vanuit de on premise AD worden gesynchroniseerd naar AAD via het component AD Connect.

2.8.1.5 ADFS of pass through authentication

Voor gebruikers authenticatie is bepaald dat pass through authentication (PTA) in de cloud toegepast gaat worden. Voor bestaande federatiekoppelingen zal het ADFS koppelvlak opgeld blijven doen. Op termijn zal gekeken worden of deze federatiekoppelingen aansluitbaar zijn op PTA waarmee vereenvoudigd kan worden naar een koppelvlak.

2.8.1.6 OTAP

Vanuit ontwikkel en beheer perspectief werkt KB volgens een wijzigingsproces waarbij de verschillende fasen Ontwikkel, Test, Acceptatie en Productie worden doorlopen om zoveel mogelijk een voorspelbare dienstverlening te kunnen garanderen. Voor de digitale werkplek zal met name voor de koppelvlakken met de SaaS oplossing Office 365 deze behoefte kunnen ontstaan. Het uitgangspunt is dat voor de digitale werkomgeving altijd de productie-versie wordt gebruikt tenzij er structurele veranderingen opgeld doen waarbij tijdelijk een test of acceptatieomgeving kan worden bijgeschakeld.

2.8.2 Nog te nemen besluiten

2.8.2.1 Niet naar Cloud opslag migreerbare data

Het doel is om alle data binnen de huidige kantoorautomatisering te migreren naar Office 365. Dit zijn in ieder geval:

- de persoonlijke mappen van medewerkers (F:\) -> OneDrive
- de afdelingsdata (G:\) -> Teams/SharePoint
- de afdelingsoverstijgende data zoals projectdocumentatie (M:\) -> Teams/SharePoint

Wanneer data om wat voor reden dan ook niet migreerbaar is moet nog besloten worden wat hiermee gaat gebeuren.

2.8.2.2 Authenticatie - Cloud Access Security Broker

Toegang tot SAAS diensten als Office 365 wordt bij voorkeur verleend via een Cloud Access Security Broker om te voorkomen dat ons beveiligingsbeleid wordt omzeild door directe toegang tot de SAAS diensten. Vanuit Informatiebeveiliging zal hier nog een definitief standpunt in genomen moeten worden of dit een vereiste is voor dit project.

2.8.2.3 Web Apps

Voor het plaatsafhankelijk publiceren van web based applicaties dient nog een keuze te worden gemaakt welke technologie hiervoor wordt ingezet.

Op dit moment is een aantal applicaties ontsloten via een zogenaamde Local Traffic Manager module behorende bij het loadbalancer-platform. Deze lijn kan worden aangehouden. Een alternatief is het voeren van een Web Application Proxy welke op dit moment wordt gebruikt om Active Directory Federation Services te ontsluiten naar het Internet.

2.9 ARCHITECTUURISSUES

In dit hoofdstuk worden issues beschreven ten aanzien van de architectuur die nog open staan of die afwijken van de architectuur.

2.9.1 Openstaande issues

Geen openstaande issues.

2.9.2 Afwijkingen van de architectuur

Geen afwijkingen van de architectuur.