



Den Haag

Aansluitvoorwaarden Generiek

Versie 1.0

Status <Concept/Definitief>

02-09-2022

Samengesteld door: Gerard van Lieshout

Colofon

Titel	<i>Aansluitvoorwaarden Generiek</i>
Versie, datum	1.0 , vrijdag 2 september 2022
Referentie	
Samengesteld door	<i>Gerard van Lieshout</i>
Projectcode	
Project	
Laatste versie bewerkt door	<i>André van den Nouweland</i>
Bestandsnaam	<i>Aansluitvoorwaarden generiek.docx</i>

© 2022 Gemeente Den Haag

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze ook, zonder voorafgaande toestemming van Gemeente Den Haag.

No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission by Gemeente Den Haag.

Documenteigenschappen

Revisie historie

Datum	Versie	Omschrijving	Auteur
04-05-2022	0.1	Initiele document	Gerard van Lieshout
02-09-2022	1.0	1 ^e versie	André van den Nouweland

Distributielijst

Datum	Versie	Verzonden aan	Opmerkingen

Relatie met andere documenten

Ref. nr.	Document	Opmerking	Locatie

Relatie met andere projecten

Dit is een overzicht van in de PSA benoemde en verder uitgewerkte relaties met andere projecten.

Project	Afhankelijkheid	Actie architectuur
Niet van toepassing	Niet van toepassing	Niet van toepassing

Inhoudsopgave

Documenteigenschappen	3
Revisie historie	3
Distributielijst	3
Relatie met andere documenten	3
Relatie met andere projecten	3
1. Inleiding	5
2. Gebruik aansluitvoorwaarden	7
3. Governance	9
4. Definities	13
5. Aansluitvoorwaarden	16
5.1. Platform	16
5.2. Platform Public Cloud	18
5.3. Platform Den Haag (Azure)	21
5.4. Software As A Service	22
5.5. Identity service	26
5.6. Security (generiek)	27
5.7. Mail Relay service	30
5.8. Integratie (Access Delivery)	32
5.9. Landelijke registraties	35
5.10. Urban Data Platform (Datawarehouse)	35
5.11. Werkplek (HDW) / Office365 / Applicaties werkplek	36

1. Inleiding

De opkomst van cloud heeft een mate van volwassenheid bereikt waardoor er een veelheid aan keuzes is ontstaan voor het benaderen van applicaties en data. Maar het hebben van keuzes leidt onherroepelijk ook tot het moeten kiezen. Daarbij spelen veel factoren een rol.

Om het overzicht niet te verliezen is het voor organisaties nuttig om vanuit een visie beleid vast te stellen dat sommige opties voorschrijft dan wel uitsluit. De realiteit is dat soms door wet- en regelgeving en soms door de markt een organisatie gedwongen wordt om van het beleid af te wijken. Architectuur wil helpen om de mogelijkheden te toetsen door kaders te stellen en te adviseren. Daarom hier een handreiking voor besluitvorming voor de te maken keuzes tussen de verschillende locaties waar een applicatie zich kan bevinden en hoe deze verbinding heeft met andere applicaties en systemen en met de gebruikers.

De referentie architectuur van de gemeente Den Haag verbeeld de visie en heeft volgende belangrijke kenmerken;

- We gaan uit van een Cloud landschap, Office365 en Azure Cloud voor intern Den Haag, Public Cloud als basis voor alle systemen.
- De verschillende omgevingen worden middels federatie gekoppeld zodat identiteitenbeheer altijd bij Den Haag ligt.
- Iedere applicatie heeft zijn eigen object storage, uitzondering hierop zijn de zakenregistratie en documentenopslag.
- Identity services van de overheid zoals DigiD en E-Herkenning lopen via het koppelvlak van Den Haag met deze voorzieningen.
- Koppelingen met overheidsregistraties (zoals BRP) verlopen via de Webservice Gateway Den Haag, tenzij logging aantoonbaar is geregeld.
- Mail voorzieningen verlopen altijd via een @....denhaag.nl mailadres.
- Koppelingen verlopen conform API strategie Nederlandse overheid.
- Applicaties zijn web-based en dusdanig geconstrueerd dat zij op alle devices gebruikersvriendelijk te gebruiken zijn.

Dit alles past ook in de visie van de VNG en aangesloten gemeenten verwoord in de informatiekundige visie “Common Ground”.

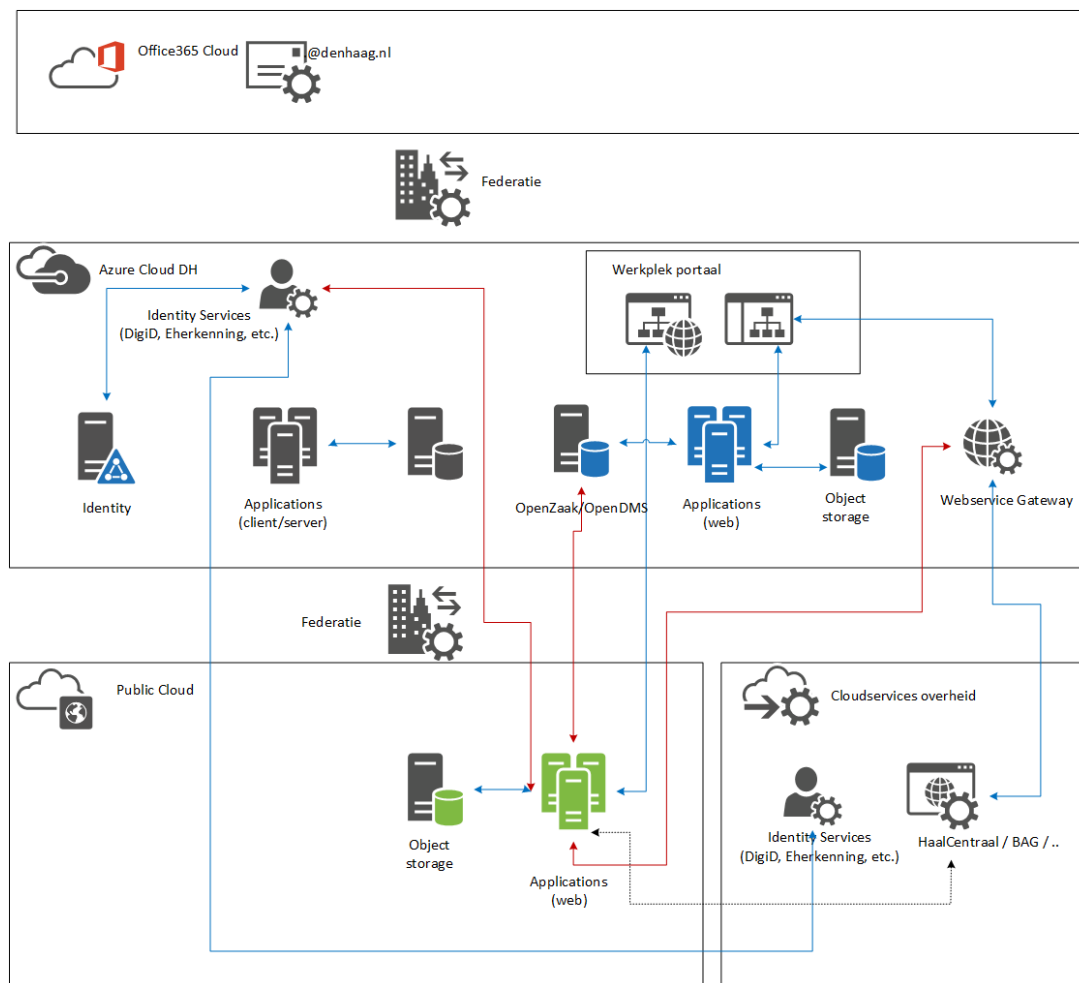
Common Ground draait in de kern om een structurele hervorming van de gemeentelijke informatievoorziening, door op een andere manier om te gaan met gegevens. De basisgedachte van Common Ground is:

- data worden losgekoppeld van werkprocessen en applicaties.
- data worden bevraagd bij de bron, in plaats van ze veelvuldig te kopiëren en op te slaan.

Om dit te realiseren, werken partijen samen op basis van vier uitgangspunten:

- gegevens worden uniform gemaakt;
- gegevens worden opgehaald met API's (software waarmee systemen gegevens kunnen uitwisselen);
- er wordt gewerkt met één gemeenschappelijke integratielaag;
- data blijven in de bron.

Op basis van de visie van de gemeente Den Haag en de daaruit voortvloeiende referentie architectuur en de vier uitgangspunten van Common Ground onstaat een nieuw gemeentelijk informatie landschap. Wat in onderstaande afbeelding summier is weergegeven.



Figuur 1 Referentiearchitectuur Den Haag

Deze referentiearchitectuur is de basis voor de aansluitvoorwaarden en de indeling van deze voorwaarden in de verschillende onderwerpen.

2. Gebruik aansluitvoorwaarden

Toetsing van de voorwaarden vindt plaats bij:

- Aanschaf
- Aanbesteding
- Migratie
- Vernieuwing

Bij aanschaf worden de architectuur voorwaarden, samen met de voorwaarden gesteld vanuit andere expertises en ITB, meegenomen bij de applicatie selectie criteria. Andere expertises zijn onder andere Security, Privacy en Inkoop. Bij een aanbesteding betekent dit dat deze voorwaarden worden opgenomen in het pakket van eisen en wensen.

De voorwaarden zijn ook op andere momenten relevant, zoals bij een migratie of bij vernieuwing van de applicatie of de infrastructuur.

De eerste stap bij de beoordeling en de weging van de voorwaarden ligt bij het advies- of het regieteam. Het samenstellen van de set van voorwaarden bij bijvoorbeeld een aanbesteding blijft voorbehouden aan het team betrokken bij deze aanbesteding. Dit document en de voorwaarden welke hierin zijn opgenomen dienen dus als gestandaardiseerde basis. Bij de weging geldt een volgorde van zwaarte zijn dat:

- Verplichtingen uit wet- en regelgeving
- Vastgesteld beleid door college en raad
- Functionele eisen
- Aansluitvoorwaarden

Deze **aansluitvoorwaarden zijn een verplichting** indien een of meerdere onderwerpen van toepassing zijn bij een aanbesteding, vernieuwing, etc.

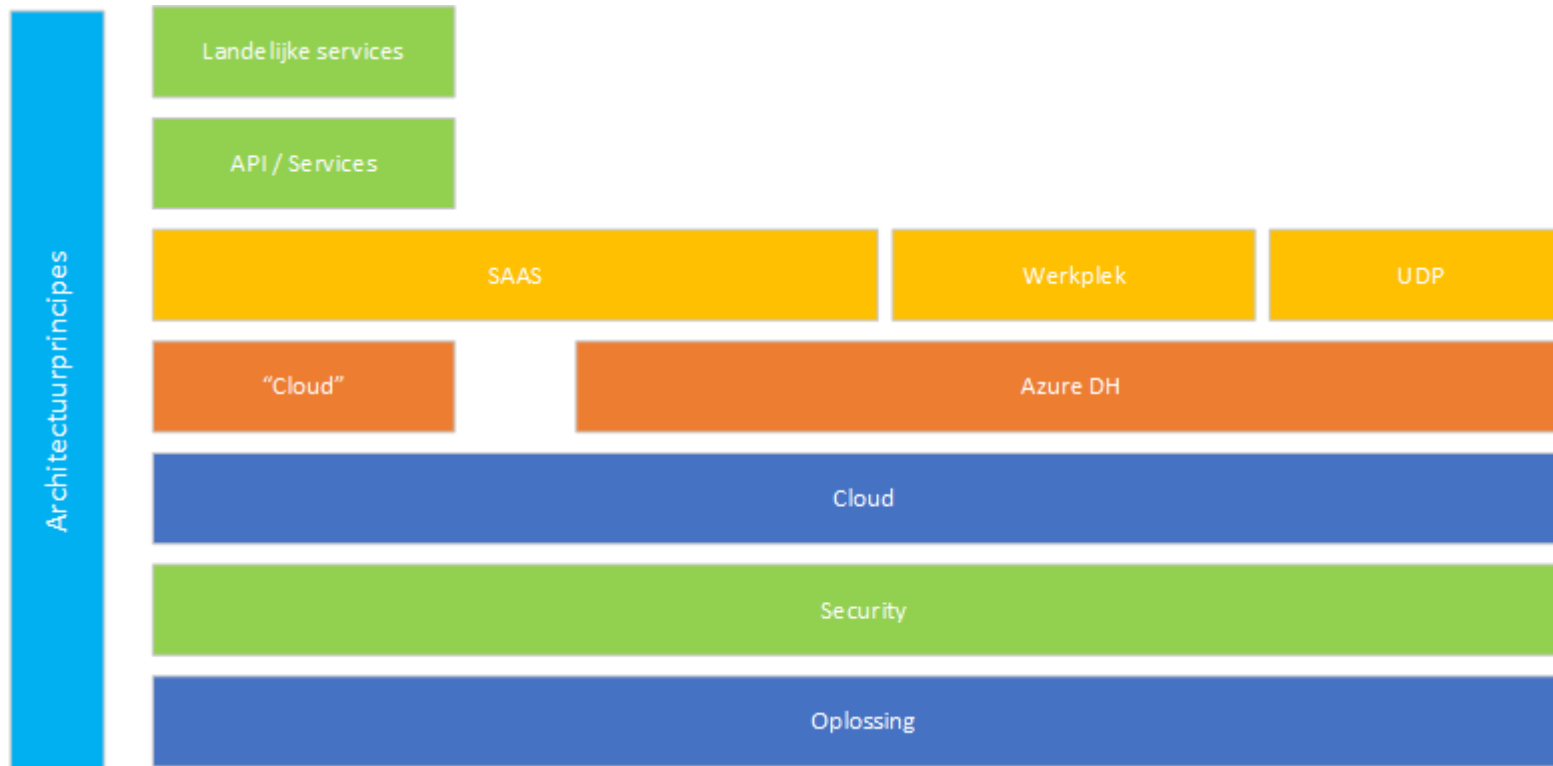
Wanneer de uitkomst van een selectie of aanbesteding leidt tot de keuze voor een product moet ervan kunnen worden uitgegaan dat de realisatie van de inspanning bij de gemeente kan worden uitgevoerd met reeds beschikbare bouwblokken, dit omdat aan de aansluitvoorwaarden kan worden voldaan. Indien de voorkeur van een selectie of aanbesteding uitkomt bij een product dat niet of alleen met aanpassingen van de voorwaarden kan worden geïmplementeerd zijn wellicht nieuwe bouwblokken noodzakelijk. Dit betekent meer inspanning en kosten en waarschijnlijk ook een verhoging van de exploitatiekosten. Een dergelijke afwijking kan alleen door het bevoegde gremium worden geaccepteerd (zie hoofdstuk 3 Governance).

Laatstelijk kan dit betekenen dat bestaande bouwblokken dienen te worden aangepast of nieuwe bouwblokken dienen te worden ontwikkeld. Dat kost tijd en de vragende partij zal deze extra tijd en de bijkomende kosten moeten accepteren.

In hoofdstuk 5 zijn de voorwaarden per onderwerp opgenomen. Per paragraaf wordt een specifiek deel uitgewerkt. Een voorwaarde bestaat uit een volgnummer een omschrijving en een nadere uitwerking ter verduidelijking of een beschrijving van het risico wat gemitigeerd wordt met de voorwaarde.

Vervolgens kan per classificatie worden aangegeven of deze voorwaarde verplicht (eis) of wenselijk (wens) is.

Bij een aanbesteding of uitwerking voor een systeem/applicatie kunnen de verschillende losse paragrafen gecombineerd worden, een voorbeeld is hieronder weergegeven.



Figuur 2 Voorbeeld: Set van gecombineerde voorwaarden voor bijv. een aanbesteding

3. Governance

Er zijn twee processen te onderkennen in relatie tot de aansluitvoorwaarden;

1. Opstellen en onderhouden aansluitvoorwaarden
2. Gebruik van aansluitvoorwaarden

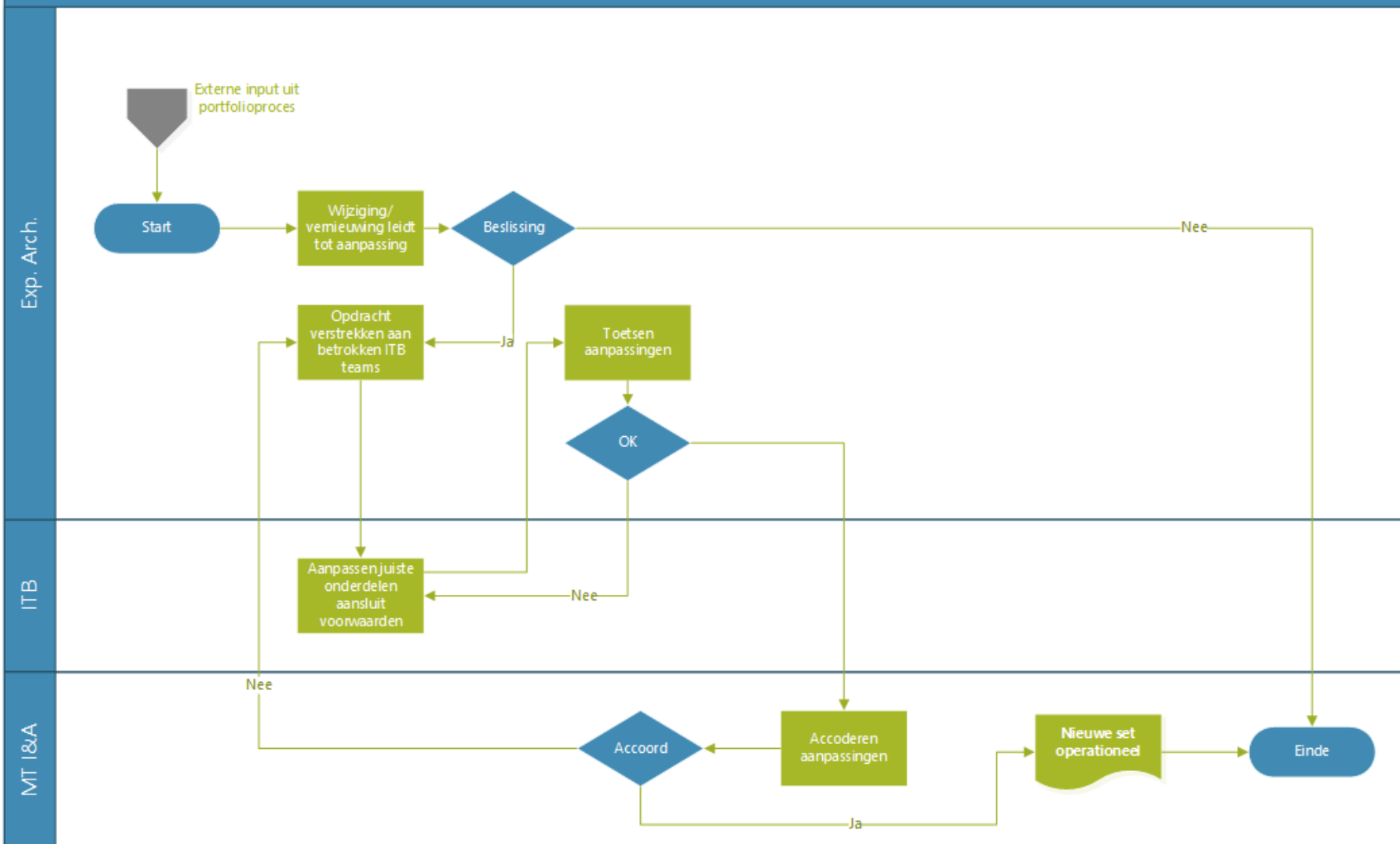
1. Opstellen en onderhouden aansluitvoorwaarden

Omdat wijzigingen in de infrastructuur welke invloed hebben op de aansluitvoorwaarden voortkomen uit het werken onder architectuur is primaire opzet, integraliteit en bewaking hiervan een verantwoording van het Expertiseteam Architectuur. De inhoudelijke kant van de aansluitvoorwaarden is belegd bij de verschillende disciplines van IT Basisdiensten. In onderstaande tabel zijn deze disciplines gekoppeld aan de verschillende onderwerpen.

Onderwerp	Team IT Basisdiensten / Expertiseteam
Platform	Team Windows Team Linux Team Netwerk Team Application Services - DC
Platform Public Cloud	Team Netwerk
Platform Den Haag (Azure)	Team Cloud Team Application Services - DC
Software As A Service	Team Application Services - DC
Identity service	IAM Identity & Access Management
Security (generiek)	Expertisecentrum Security
Mail Relay service	Team Windows
Integratie (Access Delivery)	ADM Access Delivery Management
Landelijke registraties	ADM Access Delivery Management (identity gerelateerd)
Urban Data Platform (Datawarehouse)	Expertisecentrum Data en Artificial Intelligence
Werkplek (HDW) / Office365	Office 365 / Team HDW AMS Application Management & Services End User Computing

Het proces voor aanpassen voorwaarden ziet er als volgt uit:

Onderhouden aansluitvoorwaarden



Figuur 3 Onderhoudsproces

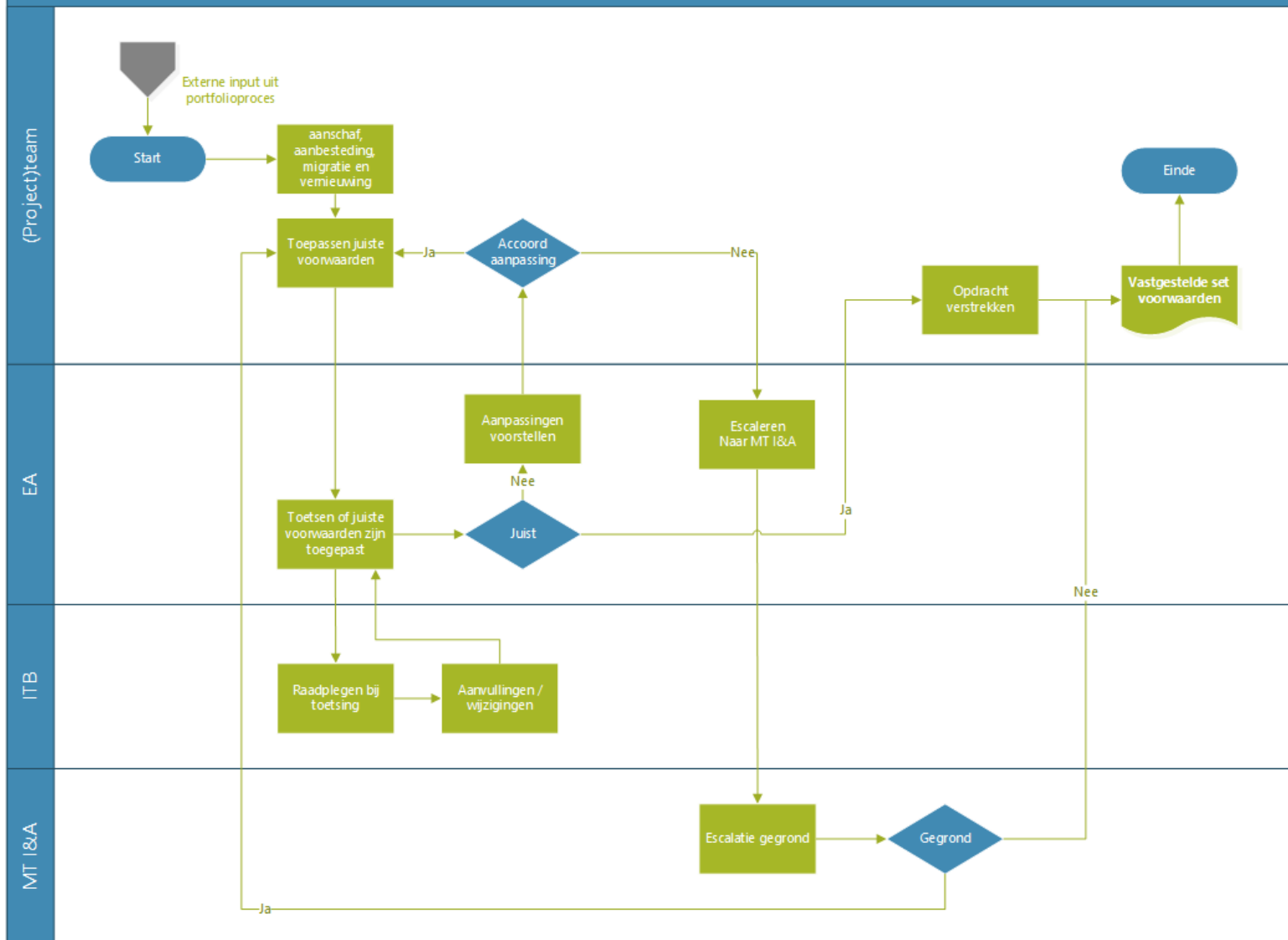
1. Als gevolg van uitvoering project of life cycle management welke onderdeel van het portfolio vormen wordt door Expertisecentrum Architectuur (EA) vastgesteld dat een of meerdere aanpassingen in de aansluitvoorwaarden noodzakelijk zijn.
2. Het EA bepaalt op welke onderwerpen aanpassing behoeven en verstrekt de juiste IT Basisdiensten (ITB) de opdracht deze uit te voeren.
3. Het EA coördineert de aanpassingen tussen de verschillende onderwerpen.
4. Na oplevering door ITB en goedkeuring door EA worden de aanpassingen aangeboden ter vaststelling aan het MT I&A.
5. Bij afkeuring door MT I&A herhaalt het proces zich, bij goedkeuring worden de nieuwe voorwaarden gepubliceerd.

2. Gebruik van aansluitvoorwaarden

Bij aanschaf, aanbesteding, migratie en vernieuwing zijn de aansluitvoorwaarden van toepassing. Welke voorwaarden wordt bepaalt door het betrokken team wat de opdracht (project of anders) uitvoert. Controle hierop vindt plaats door het Expertiseteam Architectuur als lid of consultant van het team.

1. Er vindt een significante wijziging, aanschaf, aanbesteding of migratie plaats vanuit het portfolio. Er is/wordt een team geformeerd waarin een architect deel neemt. Dit is de trigger voor volgen Gebruik Aansluitvoorwaarden.
2. Het team bepaalt welke sets van voorwaarden van toepassing zijn en kiest hierbinnen de juiste voorwaarden. Een architect kan betrokken zijn bij dit proces.
3. De set van voorwaarden en oorspronkelijke opdracht worden aan Expertisecentrum Architectuur geleverd ter beoordeling.
4. EA beoordeelt of de juiste voorwaarden zijn toegepast. Eventuele aanpassingen worden teruggekoppeld.
5. Na verwerking en akkoord EA kan team verder met een set van vastgestelde voorwaarden.
6. In geval aanpassingen van EA niet worden gehonoreerd zal EA escaleren naar MT I&A, de voorwaarden zijn immers vastgesteld.
7. MT I&A kan aanpassingen EA negeren en team groen licht geven of alsnog verzoeken de aanpassingen door te voeren.
8. Team start opdracht en bij oplevering als onderdeel van de Definition of Done controleert EA vanuit haar reguliere rol of de set van voorwaarden ook daadwerkelijk is toegepast.

Gebruik aansluitvoorwaarden

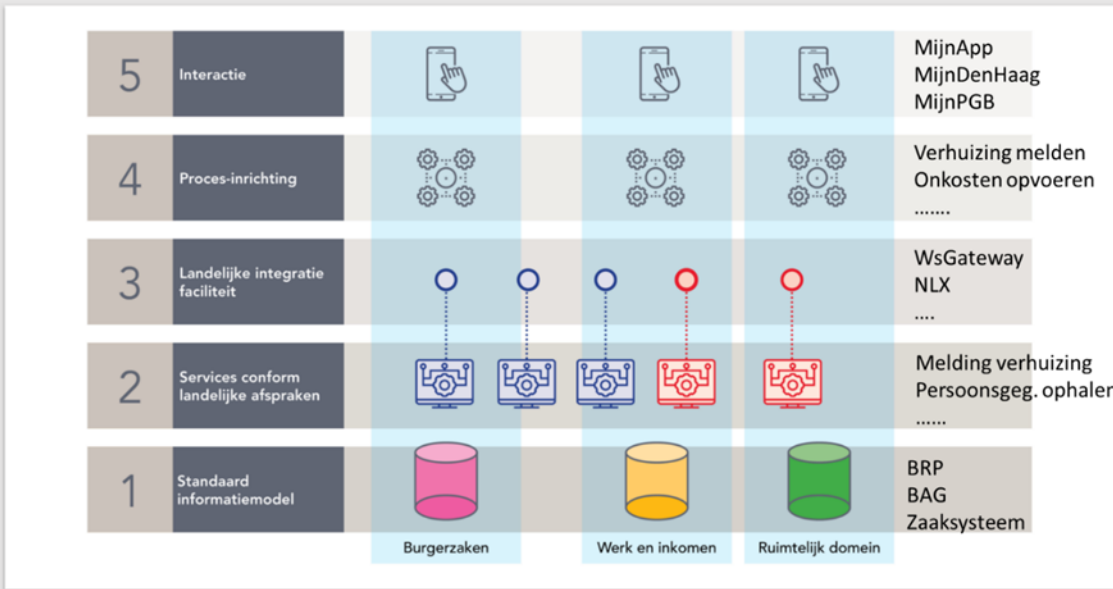


4. Definities

Om verwarring te voorkomen volgen hieronder enkele definities en de Haagse implementatie daarvan.

Term	Uitleg	Haagse implementatie
Cloud	Eenvoudig gezegd is “cloud” (computing) het leveren van computingservices, inclusief servers, opslag, databases, netwerkfuncties, software, analysefuncties en intelligentie) via internet ('de cloud') waarmee we snellere innovatie, flexibele resources en schaalvoordelen krijgen.	Voor Haagse begrippen bestaat de cloud uit de Office 365 omgeving (KA), een implementatie van Azure in het eigen datacenter, een implementatie van Azure via internet en alle implementatie van hard- en software op internet mits deze schaalbaar is.
SAAS	Software as a service, vaak afgekort als SaaS, ook weleens software on demand genoemd, is software die als een online dienst wordt aangeboden. De klant hoeft de software niet aan te schaffen, maar sluit bijvoorbeeld een contract per maand per gebruiker af, eventueel in combinatie met andere parameters. De SaaS-aanbieder zorgt voor installatie, onderhoud en beheer, de gebruiker benadert de software over het internet bij de SaaS-aanbieder. SaaS wordt gezien als de applicatie laag van Cloud computing, waarbij het platform (PaaS) en de infrastructuur (IaaS) als onderliggende lagen worden toegepast. Zonder deze onderliggende lagen is er geen sprake van flexibel verhogen of verlagen van het verbruik / de gebruikers.	Office365 en Sharepoint kun je een voorbeeld van SAAS noemen. Oracle EBS daarentegen is geen SAAS maar we maken gebruik van een Application Service Provider om de applicatie elders te hosten. Er is geen schaalvoordeel, geen flexibiliteit, etc.
PAAS	Platform as a Service (PaaS) of Application Platform as a Service (aPaaS) is een vorm van Cloud computing die als dienst wordt aangeboden, en biedt een platform aan waarmee klanten applicaties kunnen ontwikkelen, uitvoeren en beheren zonder de complexiteit van het bouwen en onderhouden van de infrastructuur die hier doorgaans mee samengaat.	In situatie Den Haag fungeert het Azure platform als een PAAS omgeving.
IAAS	Infrastructure as a service (IaaS) is een vorm van cloud computing. De infrastructuur wordt virtueel aangeboden. De hardware waaronder servers, netwerkkapparatuur en de werkstations zijn eigendom van de serviceprovider. De afnemer betaalt alleen voor hetgeen daadwerkelijk gebruikt wordt.	In situatie Den Haag fungeert het Azure platform als een IAAS omgeving.

Term	Uitleg				Haagse implementatie
Eigen datacenter	IAAS	CAAS	PAAS	SAAS (FAAS)	
Funcities	Funcities	Funcities	Funcities	Funcities	Den Haag managed
Applicaties	Applicaties	Applicaties	Applicaties	Applicaties	Den Haag managed beperkt
Runtime	Runtime	Runtime	Runtime	Runtime	Leverancier managed
Containers (optioneel)	Containers (optioneel)	Containers	Containers	Containers	
Operating System	Operating System	Operating System	Operating System	Operating System	
Virtualisatie	Virtualisatie	Virtualisatie	Virtualisatie	Virtualisatie	
Hardware	Hardware	Hardware	Hardware	Hardware	
API	Een application programming interface (API) is een verzameling definities op basis waarvan een computerprogramma kan communiceren met een ander programma of onderdeel (meestal in de vorm van bibliotheken). Vaak vormen API's de scheiding tussen verschillende lagen van abstractie, zodat applicaties op een hoog niveau van abstractie kunnen werken en het minder abstracte werk uitbesteden aan andere programma's.				Binnen Den Haag wordt het abstractieniveau van Common Ground nagestreefd.
Common Ground	Common Ground draait in de kern om een structurele hervorming van de gemeentelijke informatievoorziening, door op een andere manier om te gaan met gegevens. De basisgedachte van Common Ground is: • data worden losgekoppeld van werkprocessen en applicaties. • data worden bevraagd bij de bron, in plaats van ze veelvuldig te kopiëren en op te slaan.				Binnen Den Haag zien we vooral implementatie van generieke voorzieningen zoals HaalCentraal voor de Basis Registratie Personen en Zaakgericht werken. Onderstaand de implementatie Common Ground binnen Den Haag.

Term	Uitleg				Haagse implementatie																		
	 The diagram illustrates the implementation of the 'Standaard informatiemodel' across five domains, each represented by a row in a grid. The domains are numbered 1 to 5 from bottom to top. The implementation examples are listed on the right side of each row. <table><tr><th>Domain</th><th>Icon</th><th>Implementation Examples</th></tr><tr><td>5 Interactie</td><td>Hand icon</td><td>MijnApp MijnDenHaag MijnPGB</td></tr><tr><td>4 Proces-inrichting</td><td>Gears icon</td><td>Verhuizing melden Onkosten opvoeren</td></tr><tr><td>3 Landelijke integratie faciliteit</td><td>Circle icon</td><td>WsGateway NLX</td></tr><tr><td>2 Services conform landelijke afspraken</td><td>Chip icon</td><td>Melding verhuizing Persoonsgeg. ophalen</td></tr><tr><td>1 Standaard informatiemodel</td><td>Cylinder icon</td><td>BRP BAG Zaaksysteem</td></tr></table> Below the grid, three domains are highlighted: Burgerzaken, Werk en inkomen, and Ruimtelijk domein.				Domain	Icon	Implementation Examples	5 Interactie	Hand icon	MijnApp MijnDenHaag MijnPGB	4 Proces-inrichting	Gears icon	Verhuizing melden Onkosten opvoeren	3 Landelijke integratie faciliteit	Circle icon	WsGateway NLX	2 Services conform landelijke afspraken	Chip icon	Melding verhuizing Persoonsgeg. ophalen	1 Standaard informatiemodel	Cylinder icon	BRP BAG Zaaksysteem	
Domain	Icon	Implementation Examples																					
5 Interactie	Hand icon	MijnApp MijnDenHaag MijnPGB																					
4 Proces-inrichting	Gears icon	Verhuizing melden Onkosten opvoeren																					
3 Landelijke integratie faciliteit	Circle icon	WsGateway NLX																					
2 Services conform landelijke afspraken	Chip icon	Melding verhuizing Persoonsgeg. ophalen																					
1 Standaard informatiemodel	Cylinder icon	BRP BAG Zaaksysteem																					

5. Aansluitvoorwaarden

5.1. Platform

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
PF1	De systemen en informatie moeten gehost worden binnen de Europese Economische Ruimte (EER). Alle data (inclusief de back-ups) moeten binnen de EER blijven.		Eis			
PF2	Voorzieningen voor de Gemeente Den Haag worden gehost in een aparte <i>tenant</i> /omgeving.		Eis			
PF3	Bij een multi-tenant omgeving heeft de gemeente geen last van het opschalen van andere tenants.		Eis			
PF4	Dynamisch opschalen van de omgeving moet mogelijk zijn.		Eis			
PF5	TLS moet geconfigureerd zijn en blijven conform de adviezen, richtlijnen en verdere overwegingen van het NCSC, waarbij er gebruik gemaakt dient te worden van "GOEDE" -instellingen, met uitzondering van daar waar er geen "GOEDE" -instelling beschikbaar is, dient een "VOLDOENDE" -instelling toegepast te worden. ¹		Eis			
PF6	Voor versies van gebruikte protocollen geldt dat een gangbare versie wordt gebruikt. Hievoor geldt de huidige hoogst beschikbare versie of de hoogste versie -1.		Eis			

¹ Op moment van schrijven zijn TLS 1.2 en 1.3 als goede instelling beschreven door het NCSC

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
PF7	Er is een beschrijving van verantwoordelijkheden voor de beveiliging van de omgeving. De autoriteit om wijzigingen en beveiligingsrisico's te beheersen is duidelijk belegd.	Aanbieder is verantwoordelijk voor de beveiliging van de technische omgeving.	Nvt	Wens	Eis	Eis
PF8	Alle koppelingen met andere omgevingen en systemen moet plaatsvinden via versleutelde verbindingen.		Eis			
PF9	Gegevensopslag vindt encrypted plaats.		Eis			
PF10	Versleuteling vindt plaats conform best practices (de stand der techniek), waarbij geldt: de vereiste encryptie is sterker naarmate gegevens gevoeliger zijn.		Eis			
PF11	Self signed certificaten zijn in geen enkele omgeving toegestaan.					

5.2. Platform Public Cloud

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
PC1	De leverancier heeft een expliciete beschrijving van zijn/haar informatiebeveiligingsbeleid. In geval van onderaannemers geldt dit ook voor deze.	We streven ernaar dat de contractpartij een beveiligingsniveau heeft dat tenminste gelijkwaardig is aan dat van de gemeente Den Haag zelf.	Wens	Voorkeur	Eis	Eis
PC2	Er is een duidelijke beschrijving van rollen en verantwoordelijkheden binnen dat deel van de organisatie van de leverancier die betrekking heeft op de werkzaamheden voor de gemeente Den Haag.	Er moet voldoende functiescheiding aanwezig zijn tussen de verschillende rollen en verantwoordelijkheden.	Wens	Wens	Voorkeur	Eis
PC3	De leverancier heeft een Non-Disclosure Agreements, Acceptable Use en een passende Code of Conduct?	Leverancier gaat akkoord met een NDA [geheimhoudingsverklaring]	Nvt	Wens	Eis	Eis
PC4	Het intellectueel eigendom van alles wat de gemeente exploiteert op het platform mag niet geschonden worden op alles berust een onvervreemdbaar copyright.	Alles wat door Den Haag geëxploiteerd op de omgeving van de leverancier blijft eigendom van de gemeente.	Nvt	Wens	Eis	Eis
PC5	De gemeente heeft het recht op de uitvoering van een audit door een derde onafhankelijke partij.	De aanbieder staat de klant toe om in overleg een audit uit te laten voeren door een derde onafhankelijke partij. Dit kan vervangen worden door het overleggen van en van toepassing zijnde verklaring gelijkwaardig aan ISAE 3402.	Wens	Wens	Eis	Eis
PC6	Indien gebruik gemaakt wordt van onderaannemers / subcontractors is de leverancier verplicht de Gemeente Den Haag in te lichten.	De aanbieder is gedurende de looptijd van de dienstverlening verplicht om de klant te informeren wanneer er met onderaannemers wordt gewerkt of wanneer de geboden dienstverlening op andere wijze wordt uitbesteed.	Wens	Wens	Eis	Eis

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
PC7	Er is een beschrijving van het niveau en de aard van van de relevante medewerkers.	Beschrijf het niveau en de aard van informatiebeveiligingscertificatie aanwezig bij de relevante medewerkers.	Nvt	Wens	Eis	Eis
PC8	De leverancier heeft een continuïteitsplan.	Leverancier is verantwoordelijk voor het opstellen van de continuïteitsplannen van de technische omgeving	Eis	Eis	Eis	Eis
PC9	Hersteltijd en dataverlies Kpi's zijn beschreven.	in SLA opgenomen?	Eis	Eis	Eis	Eis
PC10	De systeem uptime requirements zijn beschreven. Bijvoorbeeld: Gegarandeerd 99.9 procent uptime per jaar of niet meer dan 8 uur en 45 minuten downtime per jaar (binnen de gestelde servicewindows).	in SLA opgenomen?	Eis	Eis	Eis	Eis
PC11	Er vindt continuous monitoring van security controls en risico's plaats.	De aanbieder heeft een proces voor het continu monitoren van beveiligingsmaatregelen.	Nvt	Wens	Eis	Eis
PC12	Logging & monitoring op kritieke systeem/applicatiefuncties vindt plaats.	Op de technische systemen vindt auditlogging en monitoring plaats	Nvt	Wens	Voorkeur	Eis
PC13	Er vindt rapportage van security events plaats.	De aanbieder rapporteert direct na het ontstaan van een beveiligingsincident de gemeentelijke functionaris.	Nvt	Wens	Eis	Eis
PC14	De leverancier voert periodiek kwetsbaarheidsanalyses, penetratietests en/of systeemreviews uit op de voor de Gemeente Den Haag relevante omgeving(en).	De aanbieder is verplicht om periodiek kwetsbaarheidsanalyses, penetratietests en/of systeemreviews uit te voeren op de technische systemen.	Nvt	Nvt	Wens	Voorkeur

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
PC15	Bekende zwakheden in de beveiliging worden procesmatig opgepakt.	De aanbieder is verplicht om bekende zwakheden in de beveiliging procesmatig op te pakken.	Nvt	Nvt	Voorkeur	Voorkeur
PC16	Bevindingen en getroffen maatregelen van zwakheden worden teruggekoppeld aan de Gemeente Den Haag.	De aanbieder is verplicht om bevindingen en getroffen maatregelen van de zwakhedenanalyses te delen met de klant	Nvt	Nvt	Voorkeur	Voorkeur
PC17	Er is een incident management procedure voor beveiligingsincidenten.	De aanbieder heeft een incidentbeheer procedure voor beveiligingsincidenten	Nvt	Wens	Voorkeur	Eis
PC18	Leverancier is verplicht beveiligingsincidenten te rapporteren.	De aanbieder is verplicht om beveiligingsincidenten te melden aan de CISO van Den Haag.	Wens	Wens	Voorkeur	Eis
PC19	Er is een procesbeschrijving hoe incidenten worden bijgehouden (registratie, opvolging).	De aanbieder is verplicht een beveiligingsincidentlogboek aan te leggen met daarin minimaal datum incident, tijdstip incident, gegevens melder incident waaronder naam, telefoonnummer, e-mail adres, locatie/kamernummer, meldendienst/afdeling, omschrijving van het incident inclusief omstandigheden, objecten die bij het incident zijn betrokken, reeds getroffen maatregelen en overige relevante zaken.	Wens	Wens	Voorkeur	Eis
PC20	Er vindt een registratie plaats van medewerkers welke toegang hebben tot de informatie van de gemeente Den Haag. De manier waarop de integriteit van deze medewerkers is vastgesteld staat beschreven.					

5.3. Platform Den Haag (Azure)

[illegible]

5.4. Software As A Service

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
SA1	De applicatie is een webapplicatie.		Eis	Eis	Eis	Eis
SA2	De SaaS applicatie voor de Gemeente Den Haag wordt gehost in een aparte <i>tenant</i> /omgeving. Dit wil zeggen dat er geen delen van de applicaties of databases worden gedeeld met andere klanten van de leverancier.					
SA3	De SaaS-applicatie dient benaderbaar te zijn via een "fully qualified domain name". Er zal een denhaag.nl naam worden toegekend aan deze applicatie. Voor de cliënt zal denhaag.nl ten alle tijden zichtbaar zijn in de url.		Eis			
SA4	Het benaderen van de SaaS-applicatie dient via het https protocol (de toepassingslaag volgens het TCP/IP model) te geschieden. Http als benaderingsprotocol (t.o.v. https) is niet toegestaan.		Eis			
SA5	Aangezien Indien er ook klantinteractie via de applicatie zal zijn is er een brede browserondersteuning nodig. Er kan gebruik gemaakt worden van moderne browsers. In ieder geval worden de recente versies van Chrome, Edge (Chromium), Safari en Firefox ondersteunt.		Eis			
SA6	Ondersteuning voor gangbare browsers op mobiele devices (Android en IOS). In iedere geval ondersteunde versies van Safari, Chrome en de Android Browser.		Eis			

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
SA7	De SaaS-applicatie is geschikt voor gebruik vanaf de Haagse KA-Werkplek ²		Eis			
SA8	Voor het functioneren van de SaaS applicatie op het cliënt device zijn geen verdere instellingen, dan wel installaties benodigd. Dit geldt zowel voor het cliënt device als ook in de browser.		Eis			
SA9	De SaaS-applicatie mag geen gebruik maken van plug-in componenten		Eis			
SA10	Voor het functioneren van de SaaS applicatie op het cliënt device zijn geen verdere instellingen, dan wel installaties benodigd. Dit geldt zowel voor het cliënt device als ook in de browser.					
SA11	Het gebruik van display protocollen denk hierbij aan b.v. RDP/ICA/PCOIP voor het benaderen van de SaaS applicatie is niet toegestaan (ook niet ingepakt in het http en/of https protocol).		Eis			
SA12	Koppelingen met andere applicaties (zowel binnen als buiten de Gemeente Den Haag) moeten verlopen via de API Gateway Service van de Gemeente Den Haag (conform de aansluitvoorwaarden)					
SA13	Koppelingen worden bij voorkeur gelegd conform open standaarden en op open koppelvlakken.					

² Op moment van schrijven (Windows 10, Office 365, Exchange 2016/Exchange Online) met de Edge (Chromium browser).

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
SA14	Voor API koppelingen tussen applicaties moet tenminste geauthentiseerd worden middels en client-certificaat. In het geval dat een gebruiker bekend is, moet ook de identiteit onweerlegbaar worden overgedragen via OpenID Connect/OAuth2 (voorkeur) of SAML2 protocol					
SA15	Alle koppelingen worden gemonitord worden. Deze monitoring gegevens moeten voor (bevoegde) beheerders kunnen worden ingezien zonder verdere handelingen vanuit de leverancier.					
SA16	Het moet mogelijk zijn om toegang te krijgen tot alle gegevens van het systeem via een database export en via een API.					
SA17	Er zal door de leverancier een federatieve koppeling worden gemaakt met de Azure AD van de Gemeente Den Haag.					
SA18	De applicatie maakt gebruik van Single Sign On (SSO) op basis van het OpenID Connect/OAuth2 of SAML2 protocol.					
SA19	Toegang tot applicaties en rechten voor Gemeente Den Haag medewerkers vindt altijd plaats d.m.v. AD groep lidmaatschap.					
SA20	Wijzigingen in de keten van componenten die gezamenlijk de koppeling vormen worden wederzijds vooraf expliciet gemeld, geaccepteerd en geaccordeerd door zowel de leverancier als de Gemeente Den Haag.					

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
SA21	De leverancier zorgt dat burgers toegang kunnen krijgen tot de applicatie conform de aansluitvoorwaarden zonder zich opnieuw te hoeven aanmelden. Burgers en bedrijven zullen zich eerst aanmelden via de identity service van de gemeente met Digid / E-Herkenning (en in de nabije toekomst ook via DigiD Machtigen, Idensys, mogelijk iDIN).					

5.5. Identity service

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
ID1	Provisioning en deprovisioning van gebruikers binnen de applicatie vindt plaats via een koppeling met de IAM omgeving van de Gemeente Den Haag.					
ID2	De leverancier is verantwoordelijk voor authenticatie van de gebruikers volgens de voor afnemer geldende richtlijnen en/of normenkaders.					
ID3	Er zal door de leverancier een federatieve koppeling worden gemaakt met de Azure AD van de Gemeente Den Haag.					
ID4	Voor versies van de gebruikte authenticatie protocollen geldt dat een gangbare versie wordt gebruikt. Hiervoor geldt de huidige hoogst beschikbare versie of de hoogste versie -1.					
ID5	Self signed certificaten zijn in geen enkele omgeving toegestaan.					
ID6	Toegang tot applicaties en rechten voor Gemeente Den Haag medewerkers vindt altijd plaats d.m.v. AD groep lidmaatschap.					
ID7	De leverancier zorgt voor een correcte tijdstelling (time service).					
ID8	Wijzigingen in de keten van componenten die gezamenlijk de koppeling vormen worden wederzijds vooraf expliciet gemeld, geaccepteerd en geaccordeerd door zowel de leverancier als de Gemeente Den Haag.					

5.6. Security (generiek)

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
SEC1	Beschrijft het contract certificering van/controls uit beveiligingsstandaarden zoals ISO 27001 / NIST SP 800-53?	Beschrijf met welke beveiligingsstandaarden voor beheersmaatregelen wordt gewerkt (bijvoorbeeld ISO27002, NIST SP800-53, CSA Cloud Control Matrix)	Nvt	Wens	Eis	Eis
SEC2	Beschrijft het contract de continuïteitsplannen van de organisatie?	Leverancier is verantwoordelijk voor het opstellen van de continuïteitsplannen van de technische omgeving	Eis	Eis	Eis	Eis
SEC3	Zijn hersteltijd en dataverlies Kpi's beschreven?	in SLA opgenomen?	Eis	Eis	Eis	Eis
SEC4	Zijn systeem uptime requirements beschreven? Bijvoorbeeld: Gegarandeerd 99.9 procent uptime per jaar of niet meer dan 8 uur en 45 minuten downtime per jaar (binnen de gestelde servicewindows).	in SLA opgenomen?	Eis	Eis	Eis	Eis
SEC5	Zijn relevante functies, contactpersonen en taken ten aanzien van contingency/continuïteitsbeheer voldoende vastgelegd?	voor aanbieder	Wens	Wens	Eis	Eis
SEC6	Beschrijft het contract het gezamenlijk testen van continuïteitsplannen met een frequentie van ten minste eens per jaar?	De aanbieder verzorgt minimaal 1x per jaar een test van de continuïteitsplannen. (gecombineerd met CP-01-E)	Nvt	Wens	Voorkeur	Voorkeur
SEC7	Beschrijft het contract de manier waarop continuous monitoring van security controls en risico's plaatsvindt?	De aanbieder heeft een proces voor het continu monitoren van beveiligingsmaatregelen.	Nvt	Wens	Eis	Eis
SEC8	Beschrijft het contract of logging & monitoring op kritieke systeem/applicatiefuncties plaatsvindt?	Op de technische systemen vindt auditlogging en monitoring plaats	Nvt	Wens	Voorkeur	Eis
SEC9	Beschrijft het contract hoe rapportage van security events plaatsvindt?	De aanbieder rapporteert direct na het ontstaan van een beveiligingsincident de gemeentelijke functionaris.	Nvt	Wens	Eis	Eis

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
SEC10	Beschrijft het contract de mogelijkheid om onsite inspecties/audits uit te voeren door de Gemeente Den Haag?	De klant heeft het recht om audits uit te voeren op locatie(s) van de aanbieder. (identiek aan OM-05). Een gelijkwaardige verklaring van een onafhankelijke audit partij conform zaken als SOC2. ISAE 3402	Nvt	Nvt	Wens	Voorkeur
SEC11	Vereist het contract de organisatie om periodiek kwetsbaarheidsanalyses, penetratietests en/of systeemreviews uit te voeren op de voor de Gemeente Den Haag relevante omgeving?	De aanbieder is verplicht om periodiek kwetsbaarheidsanalyses, penetratietests en/of systeemreviews uit te voeren op de technische systemen.	Nvt	Nvt	Wens	Voorkeur
SEC12	Vereist het contract de organisatie om bekende zwakheden in de beveiliging procesmatig op te pakken?	De aanbieder is verplicht om bekende zwakheden in de beveiliging procesmatig op te pakken.	Nvt	Nvt	Voorkeur	Voorkeur
SEC13	Beschrijft het contract op welke wijze bevindingen en getroffen maatregelen van deze analyses teruggekoppeld worden naar de Gemeente Den Haag?	De aanbieder is verplicht om bevindingen en getroffen maatregelen van de zwakhedenanalyses te delen met de klant	Nvt	Nvt	Voorkeur	Voorkeur
SEC14	Beschrijft het contract een incident management procedure voor beveiligingsincidenten?	De aanbieder heeft een incidentbeheer procedure voor beveiligingsincidenten	Nvt	Wens	Voorkeur	Eis
SEC15	Beschrijft het contract de contactpersonen en wijze van rapportage ten aanzien van beveiligingsincidenten?	De aanbieder is verplicht om beveiligingsincidenten te melden aan de CISO.	Wens	Wens	Voorkeur	Eis
SEC16	Beschrijft het contract de manier waarop incidenten worden bijgehouden (registratie, opvolging)?	De aanbieder is verplicht een beveiligingsincidentlogboek aan te leggen met daarin minimaal datum incident, tijdstip incident, gegevens melder incident waaronder naam, telefoonnummer, e-mail adres, locatie/kamernummer, meldendienst/afdeling, omschrijving van het incident inclusief omstandigheden, objecten die bij het incident zijn betrokken, reeds getroffen maatregelen en overige relevante zaken.	Wens	Wens	Voorkeur	Eis

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
SEC17	Is in het contract opgenomen dat zoveel mogelijk aansluiting gevonden dient te worden met relevante en aanwezige Technische Configuratie Voorschriften Beveiliging (TCVB) van de Gemeente Den Haag?	Aanbieder handhaaft een beveiligingsniveau dat gelijkwaardig is aan de gemeente Den Haag.	Nvt	wens	eis	eis
SEC18	Beschrijft het contract het gebruik van security baselines of andere technische voorschriften voor de beveiliging van de IT-omgeving?	Aanbieder handhaaft een beveiligingsniveau dat gelijkwaardig is aan de gemeente Den Haag.	Nvt	wens	eis	eis
SEC19	Beschrijft het contract op welke wijze compliancy met deze policies aangetoond zal worden?	Aanbieder bewijst via een auditrapport compliant te zijn met de gestelde beveiligingseisen. NVT: dubbel met certificering	Nvt	wens	eis	eis
SEC20	Beschrijft het contract de manier waarop de organisatie de externe medewerkers met toegang tot gemeentelijke informatie registreert?	Aanbieder ziet er op toe dat alleen eigen medewerkers [van de aanbieder] toegang hebben tot de gegevens van de klant.	Nvt	Wens	Voorkeur	Eis
SEC21	Beschrijft het contract de manier waarop en de frequentie waarmee (b.v. jaarlijks) security awareness en privacytraining aan de medewerkers wordt aangeboden?	Aanbieder ziet er op toe dat er periodiek security awareness en privacy-training aan de medewerkers wordt geboden.	Nvt	Nvt	Voorkeur	Voorkeur
SEC22	Beschrijft het contract de manier waarop de integriteit van medewerkers is vastgesteld (b.v. screening)?	Beschrijf hoe de integriteit van de medewerkers is vastgelegd.	Nvt	Nvt	Voorkeur	Voorkeur
SEC23	Risico: de aanbieder vereist stringente beveiligingsmaatregelen van de klant waardoor de dienstverlening wordt de gewenste verhinderd.	Beschrijf aan welke eisen de klant moet voldoen om te borgen dat de totale keten als "aantoonbaar veilig" kan worden bestempeld.	Nvt	Nvt	Voorkeur	Voorkeur

5.7. Mail Relay service

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
MS1	Email die namens @denhaag.nl wordt verzonden moet verlopen via de SMTP service die de Gemeente Den Haag conform de aansluitvoorwaarden hiervoor.					
MS2	Een onderscheid tussen het afzenderadres per Clouddiensten omgeving moet helder zijn. De gehanteerde naamgevingsconventie van de benaming voor een afzender adressen kan zijn het volgende: Applicatiennaam.omgeving.noreply@denhaag.nl					
MS3	Bij aanvraag door externe partij of Cloud gebaseerde dienst dient de lijst met toegestane afzender adressen opgeleverd te worden (afzender whitelisting). Deze worden ter goedkeuring aangeboden aan afdeling Security. Ná goedkeuring mogen alleen deze afzender adressen door aanvrager gebruikt worden					
MS4	Géén bulkmail (alle mail is het gevolg van een interactie met de gebruiker). De standaard instelling is 100 berichten per uur.					
MS5	De afnemer van de SMTP-service moet ervoor zorgen dat de mail afgeleverd wordt bij de ontvangers. Indien nodig moet het mogelijk zijn om via een queue email later af te leveren.					
MS6	Géén mail met persoon als afzender. Alleen no-reply, info, enz.					

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
MS7	Volgens de richtlijnen van het NIST en NSCS is het gebruikt van STARTTLS verplicht.					
MS8	Relaying voor derde partijen is niet toegestaan (een aangesloten server mag dus niet voor andere servers relaysen)					
MS9	Volgens de richtlijnen van het NIST en NSCS is het gebruikt van STARTTLS verplicht.					
MS10	De SaaS leverancier is zelf verantwoordelijk voor het versleutelen van de PayLoad. De functie van de relay service is het beveiligd transporteren van de data.					

5.8. Integratie (Access Delivery)

Loket voor integratievraagstukken

Functioneel en technisch beheer van WS Gateway (Broadcom CA API Gateway)

Beheer Citrix ADC (reverse proxy/loadbalancing/accessmanagement).

Citrix Gateway t.b.v. virtuele werkplek (VDI)

SIAM/HBO beheer.

Digikoppelingen (CLEO VLTrader). DigiD, eHerkenning, eIDAS

Functioneel en technisch beheer centrale queueing broker (Red Hat AMQ)

Certificatenbeheer

Centrale registratie van webservices

Access management op Citrix ADC, SIAM, HBO en WS Gateway

WSGateway positionering binnen de gemeente Den Haag



Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
GW1	Als een consument buiten Den Haag wil aansluiten op de WS Gateway OF dat vanwege hoge data classificatie de aanbieder partij een cliënt certificaat vereist, zal deze door de	Zie de URL van Logius voor meer informatie over certificaten: welke hiërarchie heeft PKIoverheid en aan welke eisen moet een	Eis	Eis	Eis	Eis

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
	consument moeten worden gemaakt. Het certificaat moet voldoen aan de volgende voorwaarden: - SHA256 hashing-algoritme - RSA 2048 sleutellengte	certificaat voldoen. Het wordt aangeraden om een PKI-overheid-certificaat te gebruiken.				
GW2	Elke aanbiedende webservice is op de WS Gateway begrensd met een maximale grootte. Bij berichten die deze grens overschrijden zal de WS Gateway een foutmelding geven. De standaard waarde bedraagt 10MB. Het kan zijn dat deze waarde op verzoek van de eigenaar van de betreffende service is verhoogd.					
	Bij berichten met bijlages moeten 'inline' bijlages worden vermeden en moet bij SOAP services de standaard MTOM worden gebruikt. Bij berichten van 10MB tot 1GB wordt de z.g. 'streamed' variant gevraagd.					

5.9. Landelijke registraties

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
	Digid etc.					
	HaalCentraal					
	Basis Registraties					

5.10. Urban Data Platform (Datawarehouse)

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim

5.11. **Werkplek (HDW) / Office365 / Applicaties werkplek**

Zorgen voor een veilige en stabiele werkplek, any time, any place, any device, aansluitend op de veranderende behoeften voor digitaal werken.

Zorgen voor een veilige en stabiele digitale werkplek waarop Office 365 voor de GDH medewerkers wordt aangeboden, aansluitend op de wensen en behoeften voor digitaal werken.

Het bieden van de mogelijkheid tot veilig digitaal samenwerken binnen de Gemeente Den Haag en met andere partijen buiten GDH door:

de inrichting en het beheer van O365, waarin de gebruikers hun werk kunnen doen.

het op juiste wijze sturing te geven aan de implementatie van nieuwe O365 onderdelen voor Gemeente Den Haag.

het onderbrengen van regievoering (detect & respond) op O365 incidenten & meldingen.

AMS is verantwoordelijk voor het zorgen dat softwarepakketten geschikt gemaakt worden voor gebruik binnen de Windows 10 werkplek. Hiervoor worden op verzoek van de business pakketten gemaakt, e wordt gewerkt aan het oplossen van incidenten die op dit gebied worden aangemeld.

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
WP1	Het besturingssysteem is een recente 64 bits versie van MS Windows.					

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
WP2	Applicaties en applicatiecomponenten moeten expliciet geschikt zijn voor VMwareESX Enterprise, Hyper-V, Virtual Desktop Infrastructure (VDI) gebaseerde virtuele omgeving, inclusief continuïteitsoplossingen zoals DRS en HA.					
WP3	De client applicatie moet geschikt zijn om middels App-V beschikbaar te stellen.					
WP4	Omgevingsinstellingen worden bij voorkeur opgeslagen in een aan het OS toegekende repository; gebruikersinstellingen moeten via Ivanti Workspace Control te beheren zijn.					
WP5	Authenticatie (voor zover nodig) verloopt middels de (Azure) Active Directory.					
WP6	De applicatie gaat efficiënt om met de systeembronnen. Er moet een duidelijke indicatie worden gegeven voor het te verwachten beslag dat de applicatie legt op systeemresources: schijfgebruik, geheugengebruik, CPU-belasting, netwerkbelasting.					
WP7	De applicatie mag geen eisen stellen aan de omgeving, die conflicteren met andere applicaties, bijv. DLL's, registry inhoud, enzovoorts.					
WP8	De applicatie moet worden opgeleverd met een installatie programma (MSI) en systeemdokumentatie (release documentatie, installatiedokumentatie, gebruikersdocumentatie), waaruit duidelijk blijkt					

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
	wat de randvoorwaarden, de systeemvereisten, de best practices en afhankelijkheden zijn.					
WP9	De applicatie moet flexibel configureerbaar zijn. De uit te voeren code dient geen harde verwijzingen zijn naar driveletters, paden (incl. UNC) en tempbestandslocaties te bevatten					
WP10	Het functionele beheer kan worden uitgevoerd door gebruikers met aanvullende specifieke rechten (zonder administrator rechten). In de documentatie worden de rechten en de objecten/componenten waarop de rechten betrekking hebben beschreven.					
WP11	De applicatie maakt geen gebruik van specifieke hardware (token) voor licentiebeheer.					
WP12	De applicatie maakt gebruik van netwerkprinters.					
WP13	De applicatie maakt gebruik van de standaard logging faciliteiten van het operating systeem.					
WP14	De applicatie voldoet aan de eisen die de Nederlandse wet stelt ten aanzien van bijvoorbeeld archivering en bescherming van persoonsgegevens.					
WP15	Er moet een overzicht zijn van de eisen die de applicatie aan de infrastructuur stelt.					
WP16	Er is een functioneel beheerder toegewezen en bekend.					
WP17	Er is een applicatie eigenaar toegewezen en bekend.					

Voorwaarde	Omschrijving	Nadere omschrijving / risico	Openbaar	Intern	Vertrouwelijk	Geheim
WP18	Er wordt voldaan aan (versie)beleid, onder verantwoordelijkheid van de proces- of systeemeigenaar.					
WP19	Onder regie van IT-basisdiensten wordt in samenwerking met functioneel beheer een PVA/IA gemaakt en bepaald of functioneel testen noodzakelijk is, eventueel ook buiten kantoor tijden.					
WP20	Het licentiemodel is niet gebaseerd op het aantal installaties, maar bijvoorbeeld op het aantal gelijktijdige gebruikers (concurrent users), een licentie per gebruiker (named user), opensource of een site licentie.					
WP21	Het moet altijd mogelijk zijn de hardware te upgraden naar hardware met meer capaciteit, zonder dat daar wijzigingen in de applicatie/ licensering voor nodig zijn.					
WP22	Indien de applicatie is gebaseerd op MS .Net of Java, dan dient de applicatie niet Java-versie afhankelijk zijn. In geval van .Net moet de applicatie gebruik maken van een door Microsoft ondersteunde versie van het .Net framework.					
WP23	Licentie is hardware onafhankelijk om bij verstoring nieuwe hardware te kunnen plaatsen.					
WP24	De applicatie is cluster aware.					