Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

KANS

Kader Acceptatie Nieuwe Systemen

November 2020

Versie	1.4
Datum	30 november 2020
Status	Definitief

Colofon

DG Organisatie Bedrijfsvoering Rijk
SSC-ICT

Koningskade 4 Den Haag

Contactpersoon

S.H. Colenbrander
CTO Office | Afdeling IT-Office | Team architectuur
Domein architect connectiviteit
sjoevik.colenbrander@minbzk.nl

Introductie

KANS (Kader Acceptatie Nieuwe Systemen) beschrijft de voorwaarden waaraan nieuwe applicaties en technologische ontwikkelingen moeten voldoen om aangeboden te worden binnen de ICT omgeving en het verzorgingsgebied van SSC-ICT.

KANS volgt de structuur van de SSC-ICT Producten en Diensten Catalogus 2020 (PDC 2020) en volgende iteraties hiervan.

Deze voorwaarden zijn onderverdeeld in de volgende domeinen:

- Rijkswerkomgeving (RWO) Business Services
- Locatie Gebonden Services (LGS) Business Services
- Housing en & Hosting (H&H) Business
- Applicatie Business Services

Aan de hand van de indeling in domeinen wordt dienstverlening beschreven (in de PDC 2020). in dit KANS document staan de actuele technische standaarden en aansluitvoorwaarden. Let op: De PDC 2020 is leidend in de beschrijving van diensten en de serviceniveaus.

Dit document geeft huidige stand van zaken weer en staat niet op zichzelf, de technische standaarden zijn voortdurend in ontwikkeling. Het document bevat informatie voor een klant of leverancier over de technische standaarden van dienstverlening van SSC-ICT. Voor een goede inschatting van de mogelijkheden binnen de bestaande SSC-ICT dienstverlening wordt een intakegesprek met de klant sterk aanbevolen.

De SSC-ICT-organisatie ziet het als haar verantwoordelijkheid om het beheer van de technische infrastructuur zo goed mogelijk te doen, maar stelt zich ook ten doel om deze zo efficiënt mogelijk in te richten en daarover een inzichtelijke kostprijs af te geven.

Voor het bereiken van efficiency – en daarmee een zo laag mogelijke kostprijs - probeert SSC-ICT-schaalvoordelen te benutten. Dat kan onder meer door (het beheer van) de technische infrastructuur te centraliseren, te standaardiseren en te consolideren. De beschreven standaarden zijn van toepassing tenzij er zwaarwegende argumenten om hier van af te wijken.

SSC-ICT zet zich in om bouwstenen te realiseren waarbij een optimale afweging wordt gemaakt tussen kosten, kwaliteit, veiligheid en generieke toepasbaarheid. Standaardisatie en hergebruik van generieke componenten mag er niet toe leiden dat een concessie wordt gedaan aan het (per systeem) vereiste beveiligingsniveau.

1 Documentgegevens

1.1 Revisies

Op dit document zijn de volgende revisies toegepast:

Versie	Status	Datum	Wijzigingen
0.1	Concept	15-12-2016	Geheel nieuwe opzet
0.2	Concept	14-03-2017	Update Michel van Loon
0.9	Concept	12-02-2018	Versie voor AB
0.95	Concept	05-03-2018	Meerdere aanpassingen in H5 – Werkomgeving door TA/DA RWO
0.99	Concept	06-03-2018	Inleiding tekst toegevoegd
0.99a	Concept	07-03-2018	Disclaimer + typo's
1.0	Definitief	07-03-2018	Vastgesteld in Architectuurboard
1.01	Concept	20-09-2018	Aanscherping aansluitvoorwaarde 19 t.a.v. Office integratie onder par. 5.9
1.01 (**1.1**)	Definitief	26-09-2018	Vastgesteld in Architectuurboard
1.12	Concept	22-2-2019	Aanpassing WBP naar AVG (pagina 9) en verduidelijking ondersteunde browsers (paragraaf 5.6 en 5.9 – aansluitvoorwaarde 16)
1.12 (1.2)	Definitief	27-2-2019	Vastgesteld in Architectuurboard
1.21	Concept		Redigeren H1 Toevoegen Messaging Services
1.3	Definitief	27-11-2019	Update Hoofdstuk 5 goedgekeurd. Scan document door domeinarchitecten
1.3.1	Concept	13-11-2020	Nieuwe opzet conform beschrijving dienstverlening PDC 2020 + update technologie 2020
1.3.2	Concept	30-11-2020	Verwerken nagekomen commentaar vanuit de lijn en collegiaal commentaar vanuit de AB
1.4	Definitief	2-12-2020	Versie voor publicatie met goedkeuring van AB.

1.2 Goedkeuring

Dit document behoeft de volgende goedkeuringen:

Versie	Datum goedkeuring	Naam	Functie	Paraaf
1.0	07-03-2018	Helmer de Vries	Architectuurboard	
1.1	26-09-2018	Helmer de Vries	Architectuurboard	
1.2	27-2-2019	Helmer de Vries	Architectuurboard	
1.3	27-11-2019	Helmer de Vries	Architectuurboard	
1.4	02-12-2020	Helmer de Vries	Architectuurboard	

1.3 Distributie

Dit document is verstuurd aan:

Versie	Datum verzending	Naam	Functie
0.1	16-12-2016	Michel van Loon	
0.2	14-03-2017	14-03-2017	Platform Services
0.95	05-03-2018	Jan Pothof, Geert Vuijk, Rein Hennen	Architecten RWO
0.99	06-03-2018	Architectuurboard	Vaststelling
1.0	14-03-2018	Joost van Duinen	Publicatie
1.2	27-2-2019	Joost van Duinen	Publicatie
1.3	08-10-2019	Joost van Duinen	Publicatie
1.4	2-12-2020	Joost van Duinen	Publicatie

2 Inleiding

2.1 Doel van het document

Deze specificatie is opgesteld als kader beschrijft de technische- en aansluitvoorwaarden waar applicaties en technische componenten aan moeten voldoen om aangeboden of gebruikt te kunnen worden binnen de ICT omgeving en het verzorgingsgebied van SSC-ICT.

Afnemers van SSC-ICT diensten dienen dit als kader te hanteren.

Onder afnemers worden verstaan: Verzorgingsgebied (Klanten), Leveranciers van software en hardware, Projecten en Afdelingen van SSC-ICT die onderling diensten afnemen.

Het document heeft onderstaande doelen:

- Informatiebron voor (potentiële) afnemers over de inrichting van de dienstverlening en de gebruikte technische services en standaarden.
- Informatiebron voor ontwikkelaars van applicaties over de gebruikte technische services, technische standaarden en beveiligingsrichtlijnen.
- Kader voor kwaliteitscontrole tijdens en na oplevering aan de beheerorganisatie.
- Toelichten en scherpstellen van relevante begrippen.

2.2 Opbouw van dit document

SSC-ICT was de afgelopen jaren ingericht in vier domeinen. De structuur van dit document volgt die indeling per domein. De organisatie die de genoemde diensten levert bestaat uit de huidige Business Units, die indeling kan als gevolg van de transitie nog wijzigen.

De business services van SSC-ICT zijn onderverdeeld in de huidige vier domeinen:

Onder *Rijkswerkomgeving* (Hoofdstuk 3) valt onder andere de digitale werkomgeving, Steeds meer ambtenaren krijgen persoonlijke devices, zoals een smartphone of een laptop, waarmee zij tijd-, plaats- en apparaat onafhankelijk kunnen werken. Deze diensten maken deel uit van het domein Rijkswerkomgeving en zijn toe te wijzen aan individuele ambtenaren.

Locatie gebonden services (Hoofdstuk 4) maakt het binnen de Rijkskantoren mogelijk dat er steeds flexibeler wordt gewerkt en het aantal vaste werkplekken wordt verminderd. Er is dan ook steeds minder vaak een duidelijk aanwijsbare gebruiker van een aantal ICT-faciliteiten. Denk hierbij aan faciliteiten als wifi en printers. Alle services die verbonden zijn met een gebouw, zijn opgenomen in het domein Locatie gebonden services.

Binnen *Housing en Hosting* (Hoofdstuk 5) worden alle technische diensten zoals servercapaciteit, databases, opslag en de benodigde netwerkkoppelingen geleverd die ervoor zorgen dat alle applicaties die binnen het verzorgingsgebied gebruikt worden.

Het domein *Applicaties* (Hoofdstuk 6) heeft zich gespecialiseerd in het applicatiebeheer van de verschillende applicaties om de afnemers nog beter te kunnen helpen.
De vier servicedomeinen bevatten verschillende ondersteunende diensten die van belang zijn om de services uit de verschillenede domein veilig te kunnen leveren vanuit opgelegde kaders. De kosten voor deze ondersteunende processen zijn niet direct aan een service toe te rekenen en worden over alle diensten omgeslagen.

Hoofdstuk 7 van dit document is gewijd aan het definiëren en verklaren van de gebruikte begrippen. De begrippen zijn toepasbaar op verschillende domeinen. Voor de begrippen is aangegeven wanneer er een architectuur Ontwerprichtlijn is opgenomen. Waar dat zinvol wordt geacht zijn relaties gelegd met of interpretaties gegeven van de relevante rijksbrede of overheidsbrede kaders.

2.3 Relatie met andere documenten

Voor het opstellen van dit document zijn onderstaande bronnen gebruikt.

1. **SSC-ICT Producten en Diensten Catalogus 2020:** De Producten- & Diensten Catalogus (PDC) is een beschrijving van de dienstverlening waarmee SSC-ICT haar klanten vanaf 2020 van dienst zal333 zijn.
2. **Architectuur principes en bouwblokken:** De architectuur van SSC-ICT's dienstverlening is vastgelegd in de Architectuur Wiki. De Wiki is opgebouwd volgens de TOGAF methode waar stapsgewijs bouwblokken worden afgeleid uit basisprincipes die door het DMT zijn vastgesteld.
3. **High Level Designs van Bouwblokken:** Deze documenten geven aanvullende informatie over de gerealiseerde infrastructuur die van belang is voor het maken van de juiste keuzes. Deze zijn gekoppeld aan de architectuur bouwblokken in de Architectuur Wiki[1].
4. **Beveiliging - BIO**: Het technisch normenkader met betrekking tot de beveiliging is vastgelegd in de BIO wat staat voor Baseline Informatiebeveiliging Overheid en is gebaseerd op ISO270001/270002. De BIO is per 1 januari 2019 verplicht en vervangt voor de gemeenten, waterschappen, provincies en het Rijk respectievelijk de BIG, BIWA, IBI en de BIR (Baseline Informatiebeveiliging Rijksdienst).

[1] Deze wikipagina's zijn bereikbaar via de DWR werkplek

3 Rijkswerkomgeving (RWO) Business Services

SSC-ICT levert als dienstverlener aan gebruikers werkplekfunctionaliteit in zijn rol als ICT-dienstverlener voor gebruikers (IDV-G). De werkplek wordt verder aangeduid als werkomgeving omdat de werkomgeving ontkoppeld is van zijn fysieke component. De werkplek duidt de combinatie bureau, scherm en het toegangsdevice aan in een rijkskantoor, een persoonlijk device zoals een managed laptop of een privé device (BYOD). Als we spreken over de aangeboden functionaliteit, dan spreken we over de werkomgeving.

De details over de dienstverlening als leverancier van de werkomgeving staan omschreven in de Servicecatalogus SSC-ICT. De hieronder opgenomen specificaties dienen als referentie voor applicaties die een relatie hebben met de werkomgeving.

referentie voor applicaties die een relatie hebben met de werkomgeving.

3.1 Technische aansluitvoorwaarden Rijkswerkomgeving

Algemeen	
1	Een applicatie heeft minimale rechten nodig op de werkplek om te kunnen functioneren voor de eindgebruiker, verhoogde of systeemrechten (administrator) rechten zijn derhalve niet toegestaan.
2	Applicaties welke geïnstalleerd worden komen altijd in "C:\Program Files" of "C:\Program Files (x86)". Verhoogde systeemrechten zijn niet toegestaan op deze locatie.
3	Een applicatie heeft geen functionaliteit op het gebied van Telemetry, Customer Experience Improvement Programs, Diagnostics en dergelijke of deze kan aantoonbaar worden uitgeschakeld in de configuratie van de applicatie. Uitzonderingen hierop moeten worden goedgekeurd met uitgevoerde DPIA en zo nodig een IB risico-analyse.
4	Tijdelijke bestanden die nodig zijn voor het functioneren van een applicatie (logging, cache etc) worden in bekende standaard folders weggeschreven (%Variabele paden%). Applicaties moeten voldoen aan de Microsoft ontwikkelstandaarden. (Zie https://docs.microsoft.com/en-us/windows/win32/win_cert/certification-requirements-for-windows-desktop-apps).
5	Applicatiebestanden die nodig zijn voor het functioneren van de applicatie (.EXE, .DLL) moeten zijn ondertekend met een geldig Code Signing certificaat van de leverancier, bij voorkeur met Time Stamping. Hierbij is de klant/aanvrager zelf verantwoordelijk voor het aanleveren en het beheer over de geldigheid van het certificaat.
6	Licenties zijn niet gebonden aan specifieke machines, activatie van een applicatie wordt op basis van concurrent aantal gebruikers of specifiek toegekend aan de gebruiker. Er wordt geen gebruik gemaakt van voorzieningen zoals dongles om de applicatie te activeren of te laten functioneren.
7	Applicatie-instellingen zijn op gebruikersniveau in te regelen, applicatie-instellingen zijn niet actief wanneer de ingelogde gebruiker geen rechten heeft op de betreffende applicatie.
8	Wanneer een applicatie een verbinding nodig heeft naar het internet moet het internetverkeer via een proxy kunnen worden afgehandeld. Authenticatie gebeurt op basis van de huidige ingelogde gebruikers credentials op basis van federatieve identiteiten. Het leggen van een AD Trust is niet toegestaan.
9	Het benaderen van een applicatieserver en/of bronnen gebeurt altijd op basis DNS met een verwijzing naar een FQDN, gebruik van harde verwijzingen naar IP-adressen zijn niet toegestaan.

10	Koppeling met of gebruik van een persoonlijk Microsoft account is niet toegestaan.
11	Universal Windows Platform (UWP) Apps worden aangeboden via RES of SCCM en kunnen niet rechtstreek vanaf de Publieke Microsoft Store geïnstalleerd worden.
12	Functionele cloud services zoals bv. opslag in de cloud kunnen worden uitgezet of dienen de eindgebruiker dusdanig duidelijk te zijn dat er buiten het vertrouwde domein data wordt gedeeld dat van een bewuste actie van de eindgebruiker kan worden gesproken.
13	Wachtwoorden mogen niet onversleuteld in de configuratie van applicaties voorkomen.
14	Single Sign-On op applicaties gebeurt op basis van federatieve authenticatie ofwel Kerberos, SAML of OAuth authenticatie. Trusts tussen domeinen zijn federatief ofwel Realm Trusts. AD Forest Trusts worden niet meer toegestaan.
Life Cycle Management en Ondersteuning	
1	Life Cycle Management van Basis en Basis+ applicaties is de verantwoordelijkheid van SSC-ICT. Life Cycle Management van klant-specifieke applicaties is de verantwoordelijkheid van de applicatie eigenaar. Applicaties zijn ten allen tijde ondersteund door een leverancier. Patch management (security fixes) wordt uitgevoerd onder goedkeuring van SSC-ICT.
2	Applicatie ondersteuning voor een volgende release in het Semi Annual Channel voor Windows 10 Enterprise moet binnen maximaal 90 dagen na RTM worden geleverd door leverancier / ontwikkelaar van de applicatie. Zie paragraaf 3.3.1 voor ondersteunde Windows versies.
Distributie van applicatie	
1	Voor de distributie van applicaties wordt het principe 'Virtueel tenzij' gehanteerd. Standaard worden Applicaties door middel van virtualisatie technieken op de werkplek aangeboden (Microsoft Application Virtualization, App-V).
2	Applicaties die geïnstalleerd worden op de werkplek kunnen niet automatisch bijgewerkt worden. Het gebruik van Auto-update is niet toegestaan.
3	Mobiele applicaties die binnen de beveiligde container moeten functioneren moeten worden ontwikkeld en onderhouden met de door BlackBerry beschikbaar gestelde SDK's.
4	Mobiele apps mogen alleen gedistribueerd worden als deze ondertekend zijn met een vertrouwd certificaat.
Webbrowser	
1	Op de werkplek worden Edge Chromium als primaire browser en Mozilla Firefox ESR als extra browsers aangeboden. Hierbij is Edge Chromium de standaard browser. Google Chrome kan alleen op speciaal verzoek via een NSK aangevraagd worden; Edge Chromium is de standaard.
2	IE11 wordt vanaf 1 januari 2021 niet meer ondersteund in de basis. Als applicaties nog niet zonder IE11 kunnen kan voor een beperkte periode IE11 beschikbaar worden gesteld als maatwerk.
3	Op de standaardbrowser worden plug-ins restrictief toegestaan: alleen als ze absoluut noodzakelijk zijn voor de werking van ondersteunde klantapplicaties, er geen acceptabel te achten workaround voor handen is en ze van gerenommeerde bedrijven komen. Op de extra browser kan SSC-ICT, na een security-toets, plug-ins als kleine applicatie installeren, maar wordt de werking ervan niet gegarandeerd. Daarop levert SSC-ICT slechts best effort support.
4	Het gebruik van de Mozilla Firefox extensions en plugins moet worden beperkt op basis van WebExtensions-API's en "Ask to Activate".

5	Gebruik van Adobe Flash en Microsoft Silverlight wordt niet meer ondersteund. Java Runtime wordt alleen nog aangeboden als klant-specifieke applicatie en is geen onderdeel van de standaard werkplek inrichting.
Office integratie	
1	Het gebruik van Office add-ons, plugins, extensions, VBA, macro's en dergelijke is in beginsel niet toegestaan. Uitzondering alleen als ze absoluut noodzakelijk zijn voor de werking van ondersteunde klantapplicaties, er geen acceptabel te achten workaround voor handen is en ze van gerenommeerde bedrijven komen. Indien noodzakelijkerwijs een applicatie toch een integratie met Office componenten moet hebben moet deze zijn ondertekend door een geldig certificaat (Code Signing) van een vertrouwde certificeringsinstantie. Hierbij is de klant/aanvrager zelf verantwoordelijk voor het aanleveren en het beheer over de geldigheid van het certificaat.
2	Microsoft Office 2016 wordt gaande 2021 vervangen door Office 365 ProPlus en wordt tot die tijd uitsluitend aangeboden in een 32-bits mode, in verband met applicaties die integreren met de Office Applicaties.
3	Office 365 ProPlus wordt uitsluitend aangeboden in een 64-bits mode. Dit betekent dat (toegestane) integraties in Office zoals Add-ins ook beschikbaar moeten zijn in een 64-bits versie aangezien 32-bits versies niet werken.
4	Gebruikte certificaten zijn ondertekend door een vertrouwde certificeringsinstantie bij voorkeur een PKI-O certificaat. Voor het Windows platform moet de Root CA zijn opgenomen in de 'Microsoft Trusted Root Certificate Program'. Zie voor een actuele lijst van root CA's: https://aka.ms/trustcertpartners.
5	Het berichten platform is toegankelijk ten behoeve van Office of het applicatielandschap. Hiervoor zijn drie interfaces in gebruik: - EWS (secure Exchange Web Services), poort 443 - SMTP (Simple Mail Transfer Protocol), poort 25 - IMAP (Internet Message Access Protocol), poort 993
Overig	
1	Aparte drivers voor bijvoorbeeld het aansluiten van additionele randapparatuur moeten voldoen aan de WHQL-eisen van Microsoft. (Windows Hardware Quality Labs)
2	Wanneer gebruik wordt gemaakt van frameworks (bijvoorbeeld .Net en C++) dient de applicatie actief onderhouden te worden om te blijven werken met (security-)updates en upgrades van het onderliggende framework die op de werkomgeving worden doorgevoerd.
Printing	
1	Follow-me printing van Xerox icm. Equitrack is de standaard.
2	Gebruik van Rijkspas of Pin is verplicht voor het ophalen van printopdrachten. Printen kan alleen vanuit de gebruiker worden geïnitieerd. Direct printing is niet toegestaan.
3	Anoniem printen (direct vanuit een applicatie) is niet toegestaan.

3.2 Relevante Technische standaarden voor de Werkomgeving

3.2.1 Algemene ondersteunde standaarden

Onderstaande lijst is deels gebaseerd op de lijst van open standaarden welke wordt gepubliceerd door het Forum Standaardisatie, zie voor overige standaarden: https://www.forumstandaardisatie.nl/open-standaarden.

Type	Versie	Status	Omschrijving

Certificaten	Minimaal SHA-2	Productie	De ondersteuning voor SHA-1 in o.a. Microsoft producten is niet meer aanwezig.
Protocol (TLS)	Minimaal TLS 1.2	Productie	https://www.forumstandaardisatie.nl/standaard/tls
Protocol (SMB)	Minimaal SMB v3	Productie	Oudere SMB versies (met name SMB v1) worden niet ondersteund enzijn uitgeschakeld op het Windows besturingsysteem.
Frameworks	DotNet	Productie	Elke Windows 10 Build biedt ondersteuning voor een nieuwe DotNet versie. Voor een compleet overzicht zie: https://docs.microsoft.com/en-us/dotnet/framework/migration-guide/versions-and-dependencies
Frameworks	Visual C++	Productie	Ondersteunde C++ frameworks: 2005, 2008, 2010, 2012, 2013, 2015, 2017, 2019.

Standaard dienstverlening conform PDC 2020 voor Paragraaf 3.3 t/m 3.6

3.3 Digitale Werkomgeving (DWO)

3.3.1 Werkomgeving besturingssysteem

OS	Type	Versie	Status	Toelichting
Windows 10 SAC	64 bits - Enterprise	1909	Productie	1 x per jaar OS Update (H2-versie met 30 maanden ondersteuning)
Windows 10 SAC2	64 bits - Enterprise	1803	Verouderd	1 x per jaar OS Update (H2-versie met 30 maanden ondersteuning)
Windows 10 SAC	64 bits - Enterprise	20H2	Gepland	Geplande Start uitrol: 2021
Apple	iOS iPadOS	N-1, nu v14	Productie	Installatie van updates door eindgebruikers. Lite managed Werkomgeving.
Apple	iOS iPadOS	15	Gepland	Geplande release door Apple september 2020, ondersteuning SSC-ICT voor Q1 2020.
Android	BYOD COPE	8 (voorzien van actuele security patch)	Productie	Installatie van updates door eindgebruikers. Lite managed Werkomgeving.
Android	BYOD COPE	9 (voorzien van actuele security patch)	Productie	Installatie van updates door eindgebruikers.

[2] SAC, staat voor Semi Annual Channel, dit houdt in dat tweemaal per jaar een major OS Update plaatsvindt. SSC-ICT volgt de H2 release van Windows 10 welke 30 maanden ondersteund wordt.

				Lite managed Werkomgeving.
Android	COPE	10 (voorzien van actuele security patch)	Productie	Installatie van updates door eindgebruikers. Lite managed Werkomgeving.
Android	COPE	11	Gepland	Gepland release Q1/Q2 2020.
ChromeOS	-	N-1 (Rolling Update -1)	Productie	Managed OS, Managed public profile, unmanaged personal profile. Applicatie distributie via publieke store.

3.4 Digitale Werkomgeving Basis

Standaard dienstverlening conform PDC 2020

3.5 Digitale Werkomgeving Online

Platform	TS	Versie	Status	Toelichting
Windows	Persistente Desktop	Windows 10 SAC	Productie	Werkomgeving waar veranderingen aan het applicatie landschap bewaard blijven. (Managed Laptop, Special & Persistent VDI)
Windows	Niet-Persistente Desktop	Windows 10 SAC	Productie	Werkomgeving die bij iedere herstart weer gereset wordt naar de default waarden. (Non persistent VDI)

3.6 Digitale Werkomgeving Light

Voor ontwikkeling van interne beveiligde apps voor de mobiele werkomgeving moet gebruik worden gemaakt van BlackBerry Dynamics.

Service	TS	Versie	Status	Toelichting
Mobile Device Management	BlackBerry Unified Endpoint Management (UEM)	N-1, nu 12.x	Productie	Endpoint Management (MDM en MAM) van smartphones en tablets (Android en iOS)

Standaard dienstverlening conform PDC 2020 voor paragraaf 3.7 t/m 3.9 en paragraaf 3.11 t/m 3.20

3.7 Toegang Digitale Werkomgeving Online

3.8 Opslag Netwerkschijven (shares)

3.9 Gedeelde mailbox / Dienst postbus

3.10 Applicatie Distributie DWO

Voor de distributie van applicaties wordt het principe 'Virtueel tenzij' gehanteerd. Standaard worden Applicaties door middel van virtualisatie technieken op de werkplek aangeboden (Microsoft Application Virtualization, App-V).

Platform	TS	Versie	Status	Toelichting
Windows	Microsoft AppV Via Ivanti Workspace Control	5.x	Productie	Gevirtualiseerde software die on demand gestreamd wordt naar de werkomgeving
Windows	MSI/Unattended – Win32 Via Microsoft SCCM		Productie	Software die in het image van Windows 10 of Windows server 2016 opgenomen wordt of gedistribueerd wordt naar de persistent desktop.
Windows	Universal Windows Platform (UWP) App's		Nog geen Productie	Beperkte ondersteuning
Windows 10 SAC Enterprise	Citrix Published App's		Productie	In specifieke gevallen kan een applicatie worden aangeboden als een Published app.
iOS & Android	SSC-ICT Appstore (Public en custom apps)		Productie	Specifieke bedrijfsapplicaties worden aangeboden middels BlackBerry UEM. Voor publieke apps wordt een verwijzing aangeboden naar publieke store.
ChromeOS	Google Chrome Management Console	nvt	Productie	ChromeOS en verplichte software in het publieke profiel.

3.11 Applicatie distributie iOS/Android

3.12 Belgroep Mobiel

3.13 Confidentiële Nummers

3.14 Premium Support

3.15 Fat Client DWO Special

Special dienstverlening conform PDC 2020

3.16 Persoonlijke devices

3.17 Randapparatuur

3.18 SIM only (BYOD)

3.19 Hoog Risico Devices

3.20 Basisplus Applicaties

Type	TS	Versie	Status	Toelichting
Applicatie	Basis	Zie PDC	Productie	Software die voor alle gebruikers beschikbaar zijn gesteld en door SSC-ICT actueel worden gehouden.
Applicatie	Basis Plus	Zie PDC	Productie	Software die door diverse ministeries te gebruiken zijn waarbij de kosten voor licenties, packaging, distributie en beheer per gebruiker doorberekend wordt en door SSC-ICT actueel worden gehouden.
Applicatie	Specifiek (Maatwerk)	Zie PDC	Productie	Software die alleen door een ministerie gebruikt wordt, of door een specifieke gebruikersgroep binnen dat ministerie.

3.21 Ondersteunende dienstverlening

Standaard dienstverlening conform PDC 2020

3.21.1 SSC-ICT Servicedesk

3.21.2 SSC-ICT Servicebalie

3.21.3 SSC-ICT Self-Service Portal

3.21.4 SSC-ICT website

4 Locatie Gebonden Services (LGS) Business Services

Voor de dienstverlening in Rijkskantoren geldt dat de PDC 2020 leidend is. Tevens kunnen er, behoudens de door LGS en Facilitaire dienstverlening geleverde diensten, geen applicaties landen in een kantooromgeving. Applicaties landen in het datacenter. Op de (Rijks)kantoorlocaties zijn geen technische ruimtes meer die applicatie-hosting (aan anderen dan de voor de het Pand verantwoordelijke IT dienstverlener (de IDV-P) kunnen bieden, noch personeel om die te onderhouden.

Standaard dienstverlening conform PDC 2020 voor paragraaf 4.1 t/m 4.9

4.1 Basisinrichting kantoorpand

Waaronder inbegrepen:

- Lokaal Netwerk
- Netwerk compartimenten (per gebruikersgroep)
- Wifi Netwerk
- Pandgebonden werkplek
- Koppelnetwerk pandgebonden (CDV/Toegang/Pandgebonden diensten)

4.2 Kiosk pc

4.3 Afdrukdiensten (MFP)

4.4 Telefonie

4.5 Call center Agent

4.6 Videoconferencing

4.7 Plekchecker

4.8 Fax naar E-Mail

4.9 Verhuizen pandgebonden werkplekdiensten

5 Housing en & Hosting (H&H) Business Services

5.1 Housing

Het ODC Rijswijk voldoet aan de eisen die aan een tier-3 datacenter worden gesteld, te weten:

- 99,982% beschikbaarheid
- Jaarlijks niet meer dan 1,6 uur downtime t.g.v. datacenter
- Redundante distributie paden, d.w.z. apparatuur heeft dubbele voedingen en alle aansluitingen zijn dubbel en onafhankelijk uitgevoerd.
- Fout tolerant, alle voorzieningen zoals stroom en koeling zijn N+1 keer aanwezig
- Bestand tegen een stroomonderbreking van 72 uur.

Elk datacenter heeft een redundante connectie met een eigen Internetprovider. Evenzo zijn er redundante connecties met de Haagse Ring en met Internet. Voor Internet wordt gebruik gemaakt van de providers Tele2 en KPN en voor specifieke kantoorlocaties wordt gebruik gemaakt van de provider BT.

De datacenters ODC Rijswijk en locatie Korte Voorhout zijn onderling gekoppeld op een breedbandig laag 3 netwerk. Laag 2 koppelingen worden niet ondersteund.

Standaard dienstverlening conform PDC 2020 voor subparagraaf 5.1.1 t/m 5.1.4

5.1.1 Netwerk aansluitvoorwaarden voor housing

Contractpartij	Neemt af	Behoefte	Koppeling	Kosten
Housing Klant	PoD / Kast / RackUnit	Laag / Medium volume verkeer naar aangesloten netwerken in ODC Rijswijk	Basiskoppelnetwerk	Per Mb
ODC Houder	PoD / Kast	Hoog Volume verkeer tussen ODC's	Directe koppeling buiten BKN om	Uren realisatie connectiviteit

5.1.2 Vertrouwelijkheid

PDC 2020: Het beveiligingsbeleid toegepast op de dienstverlening van SSC-ICT is, tenzij expliciet anders is overeengekomen, BIR2017, BBN2.

Housing biedt standaard dienstverlening tot en met Departementaal Vertrouwelijk (Dep-V). Niveau BBN2. Voor specifieke klanten kan met inzet van aanvullende EU en NATO maatregelen BBN3 niveau worden bereikt.

5.1.3 Standaard Kast

5.1.4 High Density Kast

Web en applicatie Hosting

Standaard dienstverlening conform PDC 2020 voor paragraaf 5.1.5 t/m 5.1.12

5.1.5 Omgevingen

De term "Omgeving" wordt gebruikt in de context van O-, T-, A-, P- E omgeving. Functioneel gezien is een omgeving een verzameling systemen met een bepaalde classificatie binnen een Tenant. Omgevingen kunnen alleen services van elkaar gebruiken als zij eenzelfde classificatie hebben. Voorbeeld: Productie-werkplekken kunnen alleen met Productiesystemen communiceren.

SSC-ICT biedt klanten een O-T-A-P-(E) omgeving aan. De applicaties van klanten wordt ondersteund door basis infrastructuur diensten uit het Nuts compartiment. Het Nuts compartiment is een voorziening die onderdeel is van de basis infrastructuur, waar diensten in staan die alle servers gebruiken, zoals Active Directory, NTP, DHCP, Log collectoren, etc.

Omgeving	Bevat	Functie	Beheer	Ondersteuning
Productie	Productie data	Release in beheer nemen Wijzingen doorvoeren	SSC-ICT	
Acceptatie	Voor productie representatieve data	Release vrijgeven voor productie Wijzigingen testen	SSC-ICT	
Test	Test Datasets	Release vrijgeven voor Acceptatie Wijzigingen testen	Tenant Testteam	
Ontwikkel	Ontwikkel Datasets	Bouw aan volgende functionele release	Tenant Ontwikkelteam	
Educatie	Voor productie representatieve data	Opleiden gebruikers	Functioneel beheerders / Opleiders	

Omgevingen bestaan uit compartimenten. Een compartiment is een door toegangsregels en filtering afgeschermd netwerk waarop systemen zijn aangesloten die een vergelijkbare rol vervullen of data van eenzelfde vertrouwelijks niveau bevatten. Veel voorkomende compartiment zijn bijvoorbeeld Presentatie-Applicatie-Data. Compartimenten geven invulling aan de BIO definities van "Koppelvlakken". Compartimenteren is dus een technische maatregel om aan beveiligingscriteria te kunnen voldoen.

Compartiment	Bevat	Functie	Beheer	Voorbeeld
Presentatie	Presentatie systemen	Aanbieden van functionaliteit aan gebruikers	SSC-ICT	Web servers, load balancers, front-end servers
Applicatie	Applicatie systemen	Aanbieden van applicatie functionaliteit aan presentatiesystemen	SSC-ICT	Applicatie servers
Data	Data systemen	Dataopslag ten behoeve van de applicatie systemen	SSC-ICT	Databases, Storage en File systemen

Let wel: In voorkomende gevallen kunnen compartimenten gecombineerd worden als de applicatie de drielaags structuur niet ondersteund. Er is dan de mogelijkheid presentatie-applicatie te combineren: PA. Ook bestaat de mogelijkheid om applicatie en data compartimenten te combineren: AD. Tenslotte kan er voor er voor applicaties die monolithisch zijn een PAD compartiment ingericht worden.

5.1.6 Load-balancing

Het bouwblok Load Balancer vult de functie reverse proxy en verdeling van verkeer over de (applicatie- of web)servers. De load balancer wordt ingezet in server farms waarbij de werklast wordt verdeeld over meerdere servers. Door servers toe te voegen is schaalbaarheid volgens het "scale-out" principe mogelijk. Een ander voordeel is de mogelijkheid om serverbeheer uit te voeren zonder onderbreking van de dienstverlening. (wel met enig verlies van capaciteit).

Het ODC Rijswijk heeft een standaard technische service voor load-balancing. Er zijn aparte fysiek gescheiden load balancers voor het DCLAN en de DMZ.

Service	TS	Versie	Status	Toelichting
Load balancing	Big IP F5	-	Productie	Standaard bouwsteen in ODC
	Dynamic traffic control	-	In ontwikkeling	Onderdeel van Infoblox bouwsteen
	Cisco ACE	-	Verouderd	

5.1.7 Proxy, Reverse Proxy, SSL Off-loading

Het ODC Rijswijk heeft een centrale voorziening voor proxy-support en SSL-off-loading. Er een proxy voorziening voor het DCLAN, voor situaties waar vertrouwde connecties een proxy nodig hebben.

Proxy functionaliteit wordt ingezet waar volgens het BIR er sprake is van een koppelvlak tussen zones met een verschillend vertrouwelijkheidsniveau en waar dientengevolge sessie ontkoppeling een eis is.

Service	TS	Versie	Status	Toelichting
(Reverse) Proxy	Big IP F5	-	Productie	Standaard bouwsteen in ODC

5.1.8 Server besturingssysteem

Alle nieuwe servers worden virtueel gerealiseerd, tenzij specifieke omstandigheden dit verhinderen. Het virtuele server platform biedt ontkoppeling van fysieke hardware en software: Hierdoor hebben hardware storingen en wijzigingen (w.o. vervanging) veel minder impact op de bovenliggende software lagen en kan het datacenter als geheel kosteneffectief en flexibel worden ingezet.

Platform	TS	Versie	Status	Toelichting
Windows	Windows server	2016 (64 bits)	Productie	Core editie wordt niet aangeboden.
	Windows Server	2012 R2 (64 bits)	Verouderd	Wordt niet meer uitgeleverd
	Windows server	2019 (64 bits)	Bouw	In de loop van 2021 te leveren
Linux	Red Hat Enterprise Linux	7.x	Productie	
Linux	Oracle Enterprise Linux unbreakable	6.x (64 bits)	Productie	Voor toepassing i.c.m. Oracle database

Voor Redhat (Linux) Installaties is het type minimal (Image), SElinux en de firewall moeten aan staan. Aanvullende software moet via Yum uit de beschikbare RedHat repositories (via satellite) komen. (i.v.m. updates uit een vertrouwde bron)
De applicatie moet om kunnen gaan met de OS-en “Productie” status uit de tabel. De software mag geen verstoringen aan de applicatie geven. Java, Apache en Tomcat is beschikbaar vanuit de Redhat repository (Alle gebruikte software komt uit een repo, geen losse rpm’s)

5.1.9 Virtuele servers

Voor het server besturingsysteem geldt de ontwerpregel “OR-15 Servers Virtueel”

Het virtualisatieplatform zorgt voor een laag tussen tussen de fysieke hardware en het besturingssysteem. De hypervisor zorgt voor een bundeling van onderliggende hardwareresources waardoor een efficiënter gebruik van de hardware mogelijk is.

Rationale: Inzet van virtualisatie zorgt voor een efficiënter gebruik van hardware en biedt betere beschikbaarheid, onderhoudbaarheid en failover mogelijkheden.

Platform	TS	Versie	Status	Toelichting
Windows	VMware VSphere	6.7	Productie	Wordt niet als IaaS of PaaS geleverd aan afnemers
Linux (RHEL)	VMware VSphere	6.7	Productie	Wordt niet als IaaS of PaaS geleverd aan afnemers

5.1.10 Web Servers

Platform	Type	Versie	Status	Toelichting
Windows	Internet Information Services	10.0	Productie	Versie behorend bij Windows server 2016
Windows	Internet Information Services	8.5	Verouderd	
Windows	Internet Information Services	7.5	Verouderd	
Linux (RHEL)	Apache	Laatste versie uit de REPO	Productie	

Techniek; PHP, Apache (httpd) en Apache/Tomcat worden alleen op het SSC-ICT Red Hat Linux platform aangeboden.

5.1.11 Database platform

Platform	TS	Versie	Status	Toelichting
Oracle	Oracle DBMS	12c R1	Productie	
	Oracle DBMS	19C	Productie	
Windows	MSSQL	2016	Productie	
	MSSQL	2017	Productie	
	MSSQL	2019	Bouw	
Linux/..	MariaDB	5.5	Productie	Special meegeleverd als onderdeel van de applicatie
Oracle Linux	PostgreSQL	9.x	Productie	
	PostgreSQL	10.X	Bouw	
	PostgreSQL	11.X	Bouw	
	PostgreSQL	12.X	Bouw	

5.1.12 Storage en backup

Let op: De storage en back-up bouwsteen voorziet niet in een archieffunctie van gegevens om bijvoorbeeld aan bewaarplichten te voldoen. Een specifiek voor dit doel te bouwen archiefsysteem kan gebruik maken van de storage en back-up bouwstenen.

De technische standaarden NFS over ethernet IP, LUN over Fibre Channel (SAN) en CIFS over LAN bepalen hoe en op welke storage hosts aangesloten worden.

Storage wordt in de volgende vormen aangeboden:

- Block opslag aangesloten op een Fiber Channel (SAN) netwerk
- File opslag aangesloten op een IP netwerk met de protocollen NFS en CIFS
- Software defined opslag op het VMware VSAN platform

Op grond van de ontwerpregels Servers Virtueel en afgeleid principe Exit strategie wordt storage aangeboden via een virtualisatie laag.

Platform	TS	Versie	Status	Toelichting
File based Storage	NetApp	-	Productie	CIFS en NFS
Block based Storage	EMC & HDS	-	Productie	
Storage Virtualisatie	IBM SVC	-	Productie	Ten behoeve van virtualisatie block based storage
Storage Virtualisatie	VMware VSAN	-		Ten behoeve van virtualisatie van lokale of direct gekoppelde storage

Platform	TS	Versie	Status	Toelichting
Backup	Commvault	11.x	Productie	
	EMC DDboost	nvt	Productie	

5.2 OS Hardening

Server worden gehard conform het patroon van de BIO richtlijnen. Dit betekent dat bij oplevering systemen security updates en patches zijn geïnstalleerd binnen de periode die is overeengekomen conform het vigerende beveiligingsbeleid. Binnen het OS worden verschillende instellingen aangepast om te voldoen aan de security eisen van de BIR-TNK.

SSC-ICT hanteert de StiG benchmarks (https://public.cyber.mil/stigs/) als richtlijn voor hardening van het OS en de daarop gebaseerde (applicatie)servers. Verder wordt OS hardening uitgevoerd met het oog op de inzet van de (applicatie)server. Er wordt gewerkt met een risicoanalyse op basis van een kwetsbaarheden scan.

Lokale firewalls, zoals die deel uitmaken van de meeste OS distributies, mogen gebruikt worden om functies ontoegankelijk te maken, maar andere methodes zoals het uitschakelen van services en listeners op netwerkpoorten zijn ook acceptabel.

5.3 Beheer richtlijnen

SSC-ICT bouwt een nieuwe beheeromgeving (B-Next), dit platform komt in de loop van 2021 beschikbaar. Vanuit deze centrale beheeromgeving zullen alle klantapplicaties en de daartoe ondersteunende diensten beheerd moeten kunnen worden.

Bij deze omgeving horen de volgende aansluitvoorwaarden wat betreft het beheer. De voorwaarden zijn nog in ontwikkeling en zullen Q2 2021 definitief beschikbaar komen.

Algemeen	
1	Applicaties en de daarvoor beschikbare beheersoftware voldoen aan de normen van de NORA, BIO, AVG en verplichte rijks-standaarden
2	Autorisaties en expliciete toegang wordt verleend op basis van een door de beheersorganisatie vastgestelde autorisatiematrix.

3	Applicaties voldoen aan de door SSC-ICT gestelde richtlijnen voor logging en monitoring.
4	Vooraf is bekend welke poorten en protocollen gebruikt moeten worden om beheer uit te kunnen voeren op een applicatie.
5	Beheer op afstand wordt voor alle klanten centraal vanuit de B-Next omgeving in het ODC Rijswijk gedaan door gebruik van een beheer VDI. Er zijn geen andere beheermethodes toegestaan.
6	In de B-Next beheeromgeving wordt voor alle klantomgevingen een virtuele beheerwerplek gecreëerd. Andere methoden voor beheer zijn niet toegestaan.

6 Applicatie Business Services

6.1 Federatieve Identity Management Services

Directory services voorzien in zoeken, identificeren, authenticatie en autorisatie van verschillende informatieobjecten zoals servers, websites, identitieten (gebruikers) groepen en configuraties. Het gebruik van Directory Services is verplicht voor alle bouwblokken.

Service	TS	Versie	Status	Toelichting
Accounts	Microsoft Active Directory	2016	Productie	Standaard bouwsteen voor Kerberos en op SAML gebaseerde authenticatie
SAML-Bridge	Microsoft Active Directory Federation Services	2012 R2 / ADFS 3.0	Productie	Protocoltransformatie tussen WS* en SAML
Attribuut	Microsoft Active Directory LDS	2016	Productie	Standaard bouwsteen voor beheer van applicatie-gebonden attributen
Federatie	OpenConext	-	Bouw	Standaard bouwsteen voor federatieve authenticatie op basis van SAML, OAuth en OpenID
Rijksdirectory	DIRX Directory / DIRX Identity	8.3 /8.4	Productie	Rijksbrede directory voor identiteiten van rijskmedewerkers
Azure AD	Microsoft Azure Directory	?	?	Cloud based directory voor cloud Identiteiten (Office 356)

6.2 Batch Manager / Bestandsuitwisseling

SSC-ICT biedt een beveiligde dienst voor bestandsoverdracht. Het gaat in eerste instantie om het faciliteren van end-to-end bestandsoverdracht over de protocollen SFTP, FTPS en HTTPS.

Platform	TS	Versie	Status	Toelichting
Appliance	Axway Managed File Transfer	-	Productie	Dienst is extern (DMZ) en intern beschikbaar

6.3 Technische Standaarden

SSC-ICT conformeert zich aan de rijksbrede open standaarden past deze toe in zijn produkten. De lijst van rijksbrede open standaarden is te vinden op de website van het Bureau Forum Standaardisatie: https://www.forumstandaardisatie.nl/lijst-open-standaarden.

Ontwikkelde programmatuur mag alleen bij hoge uitzondering gebruik maken van gesloten standaarden. Gebruik van gesloten standaarden dient vooraf gemeld te worden met een motivatie voor het waarom en mag alleen na expliciete toestemming worden ingezet.

In de architectuurwiki zijn in de beschrijvingen de standaarden opgenomen voor de architectuur bouwblokken en technische services

Web	Standaard	Versie	Status	Toelichting
Opmaak	HTML	5.0	Aanbevolen	Opvolger van XHTML

Opmaak	XHTML	1.1	Aanbevolen	
Opmaak	CSS	2.1/3.0	Aanbevolen	http://www.w3.org/Style/CSS/
	XML	1.0	Aanbevolen	Opmaaktaal voor gestructureerde gegevens
Communicatie	HTTP	1.1/2.0	Verplicht	IETF
Beveiliging	HTTPS en HSTS		Aanbevolen	RFC2818, RFC6797
Publicatie	RDF	1.1	Aanbevolen	W3C publicatie gestructureerde gegevens
Publicatie	Digitale Toegankelijkheid	2.0	Verplicht	EN301549 én WCAG2.0

Beveiliging	Standaard	Versie	Status	Toelichting
Transport	TLS	1.1	Verouderd	Onveilig /kwetsbaar
	TLS	1.2	Verplicht	Standaard voor transportbeveiliging
	TLS	1.3	Aanbevolen	Standaard voor transportbeveiliging

Beveiliging	Standaard	Versie	Status	Toelichting
Authenticatie	SAML	2.0	Verplicht	Standaard raamwerk voor uitwisseling van authenticatie- en autorisatie-gegevens
	OAuth	2.0	Aanbevolen	autorisatiestandaard voor met web gebaseerde applicaties die gegevens uitwisselen met behulp van API's
	OIDC		Aanbevolen	OIDC bouwt voort op OAuth 2.0. Het maakt het mogelijk om andere authenticatievoorzieningen middels een routeringsvoorziening te ontsluiten.
	~~FIDO~~			

Applicatie	Standaard	Versie	Status	Toelichting
Ontwikkeling	Javascript			
Ontwikkeling	ASP.NET	3.0, 3.5, 4.0		
Ontwikkeling	C#	3.0, 3.5, 4.0		
	JSON			JavaScript Object Notation (JSON) uitwisselen van datastructuren
	SCIM	2.0		REST protocol API voor creatie en beheer van identiteit gegevens op het web.

7 Begrippen

7.1 DMZ

De DMZ of Demilitariseerde Zone is het "niemandsland" tussen on- of semi-vertrouwde verbindingen en het vertrouwde interne Datacenter netwerk. Er is zowel in ODC Rijswijk als in Korte Voorhout een DMZ.

Een DMZ heeft eenzelfde opbouw in omgevingen en compartimenten als het DCLAN, echter de systemen die er staan hebben andere (lagere) vertrouwelijkheidsniveaus. Met eenzelfde opbouw wordt bereikt dat applicaties op eenzelfde wijze kunnen worden gecompartimenteerd, ongeacht of een deel ervan in de DMZ staat.

7.2 Tenant

De architectuur wiki definieert het afgeleide principe "Multi-Tenant" en de ontwerpregel "Multi Tenant".

Een "Tenant" is een organisatorische eenheid met specifieke functionele eisen en waarmee dienovereenkomstig afspraken voor dienstverlening gemaakt worden. De implicatie van die afspraken is er logische afscheidingen gebouwd moeten worden. Die afscheiding wordt met technische maatregelen in het netwerk ingevuld.

Tenants kunnen afspraken maken over diensten die zij van elkaar of van SSC-ICT afnemen. Het is dus bijvoorbeeld mogelijk dat een Tenant een gedeelde service zoals e-mail aan andere Tenants aanbiedt. Essentieel is dat de Tenant organisatie de sleutel in handen heeft tot wat hij wil delen.

7.3 Tiering in compartimenten

Met "Tiering" wordt bedoeld de manier waarop een systeem over servers is verdeeld. Tiering is van belang voor de schaalbaarheid en beheerbaarheid van systemen. Tiering heeft ook een relatie met de mogelijkheden die er zijn om een systeem te verdelen over verschillende netwerk compartimenten. "Tiers" die van belang zijn voor de indeling in compartimenten zijn:

- Presentatie –de interface van een applicatie naar de afnemers,
- Applicatie – waar de logica van een systeem zich bevindt,
- Data – waar opslaan van informatie plaats vindt.

De functies "Presentatie", "Applicatie" en "Data" worden onderscheiden. Echter systemen zijn niet altijd zo gemakkelijk op te knippen. De gecombineerde rollen "Presentatie/Applicatie", "Applicatie/Data" en "Presentatie/Applicatie/Data" komen voor. Verkeerstromen tussen compartimenten is mogelijk onder de voorwaarde dat deze "eenrichtingsverkeer" zijn van een van de "P" compartimenten naar een van de "D" compartimenten.

Voor applicaties is de functie van een systeem of server maatgevend voor het compartiment waar het in landt. Dit in tegenstelling tot de software die gebruikt wordt. Als voorbeeld: Database software (MS SQL, Oracle, etc) die geen of alleen tijdelijk (bijv. data queues of caching gedurende dataverwerking) informatie bevat ter ondersteuning aan de applicatie logica hoort niet in een data compartiment thuis.

7.4 Segment

Een segment is een laag 2 netwerk binnen een compartiment. Binnen een segment wordt geen toegangscontrole toegepast en geen filter maatregelen. Het kan nodig zijn om meerdere segmenten in een compartiment te plaatsen.

We maken onderscheid tussen Laag 2 filtering en Laag 3 filtering van verkeer. Gegeven het hierboven gestelde wordt geen Laag 2 filtering (op segmenten) toegepast. Laag 3 filtering wordt uitsluitend op het niveau van het compartiment toegepast.

7.5 Zone

Zone is een begrip dat in BIR wordt gehanteerd voor een gebied met een bepaalde vertrouwelijkheid. Een zone is een abstract begrip dat net zo goed betrekking kan hebben op netwerken als op ruimtes of terreinen. In de NORA is een zoneringmodel beschreven dat door SSC-ICT wordt gebruikt voor het nemen van beveiligingsmaatregelen (Security by Design)

Zonering geeft invulling aan "scheiding van systeemfuncties" door de technische infrastructuur in te delen in zones met een gedefinieerd beveiligingsniveau. Informatiesystemen binnen een zone hebben een bepaald beveiligingsdoel en communiceren met informatiesystemen in andere zones via een koppelvlak met een gedefinieerd stelsel van samenhangende beveiligingsmaatregelen.

De netwerkarchitectuur in de ODC's is ingedeeld op basis van het volgende zoneringsmodel: Onvertrouwd, Semi-vertrouwd en Vertrouwd.

- Onvertrouwd: Het Internet en buiten de control van SSC-ICT gelegen netwerken vallen in onvertrouwde zone
- Semi-Vertrouwd: De DMZ is als geheel een Semi-Vertrouwde zone en bevat de beveiligde koppelvlakken naar de Onvertrouwd en Vertrouwd zones. De DMZ bevat in sommige gevallen ook webservers met publiek toegankelijke gegevens.
- Vertrouwd: Het Datacenter netwerk en de (fysiek gescheiden) klantnetwerken in het datacenter vormen de vertrouwde zone.